01 - 2017

Tec Scan Journal

IT-SICHERHEIT

Das Magazin vom Information Professional

1086

wti

Kostenlose Recherche in unserem Themenpaket Technik und Management TEMA®

Testen Sie eine Woche unverbindlich die Recherche in unserem Themenpaket Technik und Management. Finden Sie Antworten auf Fragen zu Betriebsführung und -organisation, Maschinen- und Anlagenbau, Fertigungstechnik, Medizinische Technik, Textil, Werkstoffe und Fahrzeugtechnik.

Weitere Infos zur Datenbank finden Sie hier: http://bit.ly/1m7j03q

Fordern Sie Ihren Zugang einfach per Mail an. Schicken Sie Ihre Kontaktdaten mit dem Betreff "1 Woche TEMA kostenlos" an kontakt@wti-frankfurt.de.

TecScan Journal > Editorial

Liebe Leserinnen und Leser,

Sie informieren sich mit dem TecScan-Journal regelmäßig über Neuzugänge zu Ihrem Thema aus unseren Datenbanken. So bleiben Sie stets auf dem Laufenden und erschließen sich nützliche und relevante Wissensquellen. Vielleicht interessieren Sie sich für weitere Themen: Neben klassischen Technikbereichen wie z.B. Maschinenbau, Medizintechnik, Werkstoffe und Textiltechnologie decken die TecScan-Journale auch brandaktuelle, gesellschaftspolitisch relevante Querschnittsthemen, wie Industrie 4.0, IT-Sicherheit, Elektromobilität oder Neue Mobilität – Auf dem Weg zum autonomen Fahren ab.

Literatur und Web-Angebote zum großen Digitalisierungsthema "Sicherheit"

Mit zunehmender Digitalisierung aller betrieblicher Prozesse ist nicht mehr nur die Sicherheit der klassischen IT-Anlagen eines Unternehmens ein sehr ernst zu nehmender Risikofaktor. Auch die Anforderungen an die Sicherheit von Maschinen und Funktionale Sicherheit in automatisierten Prozessen wachsen im Zeichen von Industrie 4.0 stetig. Die WTI legt bei der Literaturauswahl und -erschließung einen Fokus auf die zu diesem Themenbereich veröffentliche Literatur und angebotenen Veranstaltungen. Sie wird künftig ihr bisheriges Top-Thema IT-Sicherheit entsprechend breiter aufstellen, was sich auch im TecScan-Journal IT-Sicherheit niederschlagen wird.

Auch unser letzter WTI-Newsletter “Safety and Security first” war diesem Thema gewidmet: http://bit.ly/1Ne4RWg . Darin stellten wir eine Publikation des VDE mit dem Titel “Sicherheit von Maschinen und Funktionale Sicherheit” vor, die wir für Sie etwas ausführlicher rezensiert haben. Das Buch enthält im Kern eine anwendungsorientierte Erörterung relevanter DIN-Normen.

Der VDE beschäftigt sich im Rahmen eines 12 Forschungsprojekte umfassenden Förderschwerpunkts “IT-Sicherheit für Kritische Infrastrukturen” ITS|KRITIS des BMBF mit neuen Ansätzen zur Beurteilung und Erhöhung der IT-Sicherheit. Die Forschungsprojekte vernetzen sich über die Forschungsplattform VeSiKi: http://bit.ly/2kItrZX .

Die Rezension der oben erwähnten VDE-Veröffentlichung finden Sie auf unserer Homepage (http://bit.ly/2lfh20f) , ebenso wie eine Auswahl interessanter Abstracts (http://bit.ly/2kCMylu) zum Thema.

Gudrun Schmidt

WTI-Frankfurt eG - Vorstand

Inhaltsverzeichnis

Netzwerksicherheit

- 001 -

Physiological-signal-based key negotiation protocols for body sensor networks: A survey.
Zhao, Huawei; Xu, Ruzhi; Shu, Minglei; Hu, Jiankun
In: ISADS, International Symposium on Autonomous Decentralized Systems, 12, in: Simulation Modelling Practice and Theory * Band 65 (2016) Seite 32-44 (13 Seiten, 28 Quellen)
http://dx.doi.org/10.1016/j.simpat.2015.12.003

A body sensor network (BSN) is a type of network for Internet of Things. A BSN typically consists of tens (dozens) of biosensor nodes distributed on/in the human body, and these autonomous nodes can form a wireless network to measure physiological signals and execute intelligent treatment automatically. BSNs have wide application prospects in intelligent healthcare. Because physiological signals measured and processed by BSNs involve patient privacy, security mechanisms must be developed to secure BSNs, and therefore the adoption of available key negotiation protocols is fundamental. Due to stringently limited operation resources, BSNs require these protocols to be highly energy efficient. Recent development has discovered that certain physiological signals can be used for efficiently negotiating common keys among biosensor nodes. These signals and fuzzy technology are used to design light-weight key negotiation protocols, and many solutions have been proposed. In this paper, we explore and classify these solutions, and evaluate their performance by analyzing their merits and drawbacks. Finally, we present open research issues that should be solved in the future.

- 002 -

Mitigation of Adverse Effect of False Data Injection in Optimally Controlled Smart Grid.
Ghosal, Malini; Rao, Vittal
In: ASME Power Conference, 2015 * (2015) Seite V001T11A010
http://dx.doi.org/10.1115/POWER2015-49689

The 'smart grid' is one of the largest critical infrastructure systems of any nation. Preventing the grid from data integrity attacks is vital for reliable operation of the grid. Various Phasor Measurement Units (PMUs) and other intelligent electronic devices play crucial role in real-time operations of the grid. Control actions are taken based on information received from such devices. However, all these modern measurement systems communicate with the control center via wireless network making them vulnerable to several security threats, data integrity attack being one of them. This paper addresses the issues associated with the injection of malicious data into the measurements. A model based 'trustiness' technique has been proposed to mitigate the adverse effect of such attacks in the performance of the electrical power grid. The proposed method has been demonstrated using the IEEE 14-bus test system.

- 003 -

Wireless Sensor Network in Vehicles.
Potdar, Milind; Wani, Suyog
In: SAE World Congress & Exhibition, 2015, in: SAE Technical Papers * 2015 (Seiten, 14 Quellen), Paper-Nr. 2015-01-0241
http://dx.doi.org/10.4271/2015-01-0241

Modern vehicle design involves configuration of various sensors and actuators spread across the vehicle. These sensors and actuators placed at various locations in the vehicle need to be connected with Electronic Control Units (ECUs). As long as wires are used for these connections, cost and time required for installation and maintenance are major concerns for OEMs. A wireless sensor network (WSN) can reduce length of wiring harness and can save time as well as cost of its installation. It also provides flexibility in deciding location of ECU according to desired shape of the vehicle. This paper presents a way to build a strong, secured wireless network in vehicle. The proposed method of encryption and decryption ensures that, sensor and actuator data is available only to required ECUs and not to any other unintended receiver. A novel method is proposed in order to achieve this. Sensors and actuators in the vehicle are segregated according to their location. Hence, single wireless node can be used to get data from sensors as well as to control actuators located at a particular region. E.g. Rear ultrasonic parking sensors and rear light console can be connected to their respective ECUs via single wireless node in 'rear zone'. Further, use of directional antenna instead of traditional Omni-directional antenna reduces power consumption and interference of signals.

- 004 -

Secure Data Access in Hadoop Using Elliptic Curve Cryptography.
Diaz, Antonio F.; Blokhin, Ilia; Ortega, Julio; Palacios, Raul H.; Rodriguez-Quintana, Cristina; Diaz-Garcia, Juan
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 16, ICA3PP Collocated Workshops: SCDT, TAPEMS, BigTrust, UCER, DLMCS, 2016, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 10049 (2016) Seite 136-145 (10 Seiten), Paper-Nr. Chapter 11, BigTrust 2016: The 1st International Workshop on Trust, Security and Privacy for Big Data
http://dx.doi.org/10.1007/978-3-319-49956-7_11

Big data analytics allows to obtain valuable information from different data sources. It is important to maintain control of those data because unauthorised copies could be used by other entities or companies interested in them. Hadoop is widely used for processing large volumes of information and therefore is ideal for developing big data applications. Its security model focuses on the control within a cluster by preventing unauthorised users, or encrypting data distributed among nodes. Sometimes, data theft is carried out by personnel who have access to the system so they can skip most of the security features. In this paper, we present an extension to the Hadoop security model that lets control the information from the source, avoiding that data can be used by unauthorised users and improving corporative e-governance. We use an eToken with elliptic curve cryptography that performs a robust operation of the system and prevents from being falsified, duplicated or manipulated.

- 005 -

Wireless Sensing - Future's Password to Digital Avionics System.
Vadgaonkar, Prashant; Janardhan, Ullas; Sivaramasastry, Adishesha
In: ASTC, SAE Aerospace Systems and Technology Conference, 2014, in: SAE Technical Papers * 2014 (Seiten, 3 Quellen), Paper-Nr. 2014-01-2132
http://dx.doi.org/10.4271/2014-01-2132

Performance of Avionics systems is dictated by the timely availability and usage of critical health parameters. Various sensors are extensively used to acquire and communicate the desired parameters. In today's scenario, sensors are hardwired. The number of sensors is growing due to automation which increases the accuracy of intended Aircraft functions. Sensors are distributed all over the Aircraft and they are connected through wired network for signal processing and communication. LRUs (Line Replaceable Unit) which are integrating various sensors also use a wired approach for communication. The use of a wired network approach poses challenges in terms of cable routing, stray capacitances, noise, mechanical structure and added weight to the structure. The weight of cables contributes significantly to the overall weight of the aircraft. As the weight of Aircraft increases, the required fuel quantity also increases. The Key driver for Airline operational cost is fuel. Fuel quantity is a direct function of weight. Use of wireless sensors in aircraft brings in tremendous advantages in terms of design optimization, flexibility in sensor configuration and weight optimization. Even though the avionics industry is trying to adopt wireless sensors, there are some points of concern in deploying wireless sensors and networks across the aircraft. This paper describes the comparative performance of wired and wireless sensors, type of wireless sensors & interfaces, frequency performance, protocols, network topologies and qualification standards. This paper also discusses the constraints and challenges in deploying wireless sensor network across the aircraft.

- 006 -

An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks.
Zhu, Liehuang; Yang, Zhen; Xue, Jingfeng; Guo, Cong
In: International Journal of Distributed Sensor Networks * Band 10 (2014) Heft 2 (Seiten, 20 Quellen)
http://dx.doi.org/10.1155/2014/565480

Wireless sensor networks (WSNs) are composed of sensor nodes with limited energy which is difficult to replenish. In-network data aggregation is the main solution to minimize energy consumption and maximize network lifetime by reducing communication overhead. However, performing data aggregation while preserving data confidentiality and integrity is challenging, because adversaries can eavesdrop and modify the aggregation results easily by compromised aggregation nodes. In this paper, we propose an efficient confidentiality and integrity preserving aggregation protocol (ECIPAP) based on homomorphic encryption and result-checking mechanism. We also implement ECIPAP on SimpleWSN nodes running TinyOS. Security and performance analysis show that our protocol is quite efficient while persevering both aggregation confidentiality and integrity.

- 007 -

Hardware and Software Constraints for Automotive Firewall Systems?.
Schmidt, Karsten; Zweck, Harald; Dannebaum, Udo
In: SAE World Congress & Exhibition, 2016, in: SAE Technical Papers * 2016 (Seiten, 9 Quellen), Paper-Nr. 2016-01-0063
http://dx.doi.org/10.4271/2016-01-0063

The introduction of Ethernet and Gigabit Ethernet as the main invehicle network infrastructure is the technical foundation for different new functionalities such as piloted driving, minimizing the CO_2-footprint and others. The high data rate of such systems influences also the used microcontrollers due the fact that a big amount of data has to be transferred, encrypted, etc. The usage of Ethernet as the in-vehicle-network enables the possibility that future road vehicles are going to be connected with other vehicles and information systems to improve system functionality. These previously closed automotive systems will be opened up for external access. This can be Car2X connectivity or connection to personal devices. Allowing vehicle systems to communicate with other systems that are not within their physical boundaries impose a previously non-existing security problem. Any external communication with the vehicle system must be considered as a potential security threat, which may impact the system functionality or any of the safety properties. This may result in new vulnerabilities that could be exploited by malicious attackers. Any external access to the system must be authorized and firewalled, so that only trustworthy users and services can make use of the functionality. In order to achieve a high level of security a holistic security concept is highly essential. A holistic security concept is based on the following basic building block: (1) Physical Security (tamper proof); (2) Network Security; (3) Secure System Software (ECU Hardening); (4) Application Hardening. In order to archive a high level of confidence for the internal secure network communication a firewall concept is required. A holistic firewall approach includes firewalls in different ECU with different firewall functionalities. This paper addresses the hardware and software architecture patterns for building automotive firewall systems. In the first chapter state-of-the-art firewall concepts will be shortly presented and afterwards special automotive requirements will be introduced. In following chapters the basic requirements for a firewall system from the OEM point of view will be discussed. It is followed by having a closer look on the hardware aspects which come along with automotive requirements. The paper finishes with some software aspects about realizing firewalls.

- 008 -

A Secure Routing Scheme for Wireless Mesh Networks.
Nanda, Ashish; Nanda, Priyadarsi; He, Xiangjian; Jamdagni, Aruna
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 393-408 (16 Seiten), Paper-Nr. Chapter 21, Wireless, Mobile and IoT Security
http://dx.doi.org/10.1007/978-3-319-49806-5_21

Wireless Mesh Network is an emerging technology with great potential for evolving into a self-sustained network. The traditional networks, which dominate the present day communication systems, rely on large and expensive setups of wired/wireless access points for connection between users. Unlike the traditional networks, a Wireless Mesh Network is formed by the user devices which connect to each other to form a network. The security of such networks is however very low as each data packet passes through multiple devices making it susceptible to vulnerabilities. This paper discusses a new network model that implements a strong security framework over a new routing technique. The new network model, unlike any other, features a new addressing scheme that is no longer limited by the drawbacks of the legacy systems and can hence implement better security measures.

- 009 -

Fertigung im Handumdrehen sicher steuern.
Weczerek, Jürgen
In: MM - Maschinenmarkt. Das IndustrieMagazin * (2016) Heft 48, Seite 38-41 (4 Seiten, Bilder)

Beim Einsatz von Smart Devices in der Fertigung sind bei der Auswahl der erforderlichen WLAN Access Points einige wichtige Punkte zu beachten, um die Sicherheitsanforderungen zu erfüllen. Oft scheint die kommunikative Anbindung von Smart Devices an Maschinen relativ leicht realisierbar zu sein. Der Aufbau eines WLAN-Zugangs zum Maschinennetz erfolgt einfach durch einen im Schaltschrank montierten WLAN Access Point einschließlich einer am Schaltschrank montierten Antenne. Für das WLAN wird dann ein Passwort vergeben, und der Betrieb der Funklösung kann beginnen. Das Problem besteht darin, dass auch unbekannte Nutzer bei Kenntnis des WLAN-Kennworts auf das Netz zugreifen können, und dies sogar von außen. Die Folge sind erhebliche Risiken für die Sicherheit der Maschinen und der Maschinendaten. Die in Maschinen- und Anlagennetzen genutzten WLAN-Systeme werden oft über einen gemeinsamen Netzwerkschlüssel (Wi-Fi Protected Access Pre Shared Key, WLAN WPA-PSK) geschützt. Hier kommt es auf die geschickte Verwaltung und regelmäßige Pflege des Passworts an, um sicherzustellen, dass stets nur berechtigte Nutzer Zugriff auf das Datennetz und die zugehörigen Ressourcen haben. Eine Lösung kann ein automatisiertes Kennwortmanagement durch die Maschinensteuerung sein. Dazu ist ein WLAN Access Point nötig, der von der Maschinen-SPS über das Datennetz gesteuert werden kann. Eine Erweiterung des Sicherheitskonzepts stellt der Einsatz einer Firewall mit DMZ-Port (Demilitarized Zone) dar, z. B. des FL Mguard 4000 von Phoenix Contact. Werden die Aspekte eines passenden Sicherheitskonzepts, einer guten Funkleistung und der Zulassungen für alle relevanten Betriebsorte bei der Konzeption der WLAN-Schnittstelle beachtet, kann die WLAN-

Lösung mit hoher Sicherheit betrieben werden. Es müssen jedoch leistungsstarke industrielle Access Points gemäß IEEE 802.11n mit Mimo-Antennentechnik (Multiple Input Multiple Output) verwendet werden, die sich durch die Maschinensteuerung kontrollieren lassen. Diese Anforderungen erfüllt der WLAN Access Point 5100 von Phoenix Contact.

- 010 -

A Greedy Algorithm on Constructing the Minimum Connected Dominating Set in Wireless Network.
Fu, Deqian; Han, Lihua; Yang, Zifen; Jhang, Seong Tae
In: International Journal of Distributed Sensor Networks * Band 12 (2016) Heft 7 (Seiten, 24 Quellen)
http://dx.doi.org/10.1177/155014771703201

In the past 20 years, the connected dominating set (CDS) as a virtual backbone network has been widely used in the wireless networks. Many researchers have been devoted to designing approximate algorithms for CDS problem since constructing the minimum CDS (MCDS) is NP-hard problem. Different from the most existing algorithms with two phases, we employ greedy strategy to design a centralized algorithm GR_CDS in only one phase to get MCDS, with the time complexity of $O((D^2+\log n)n)$. Afterwards, another algorithm P_CDS is designed for pruning redundant nodes in the obtained MCDS with the time complexity of $O(n^2)$.

- 011 -

Stealthy Protocols: Metrics and Open Problems.
Chen, Olga; Meadows, Catherine; Trivedi, Gautam
In: Concurrency, Security, and Puzzles, Essays Dedicated to Andrew William Roscoe on the Occasion of His 60th Birthday, in: Lecture Notes in Computer Science, Programming and Software Engineering * Band 10160 (2017) Seite 1-17 (17 Seiten), Paper-Nr. Chapter 1
http://dx.doi.org/10.1007/978-3-319-51046-0_1

This paper is a survey of both methods that could be used to support stealthy communication over both wired and wireless networks and techniques for evaluating them. By stealthy communication we mean communication using channels that guarantee that the nature of the communication, or even the fact that communication is taking place at all, is hidden. Although stealthy communication and information hiding have been studied from a number of different points of view, e.g. image steganography, network covert channels, and covert wireless communication, not much has been done to tie these different threads together and attempt to see how the different branches of stealthy communication research can inform each other. In this paper we take the first steps to remedying this deficiency. We identify open problems, point out gaps, and indicate directions for further research.

- 012 -

Research and Analysis of Open Security Issues in Communication for Wireless Sensor Network.
Luhach, Ravindra; Jha, Chandra K.; Luhach, Ashish K.
In: SmartCom, International Conference on Smart Trends for Information Technology and Computer Communications, 1, in: Communications in Computer and Information Science * Band 628 (2016) Seite 135-142 (8 Seiten), Paper-Nr. Chapter 17
http://dx.doi.org/10.1007/978-981-10-3433-6_17

Sensors are resource constrained and computing devices used in wireless networks. These networks are comprised of large numbers sensors deployed randomly over an area. The wireless sensor network (WSN) has a direct impact on human welfare as their application can be extended to military surveillance, environmental monitoring and to healthcare also. Security breaches might lead to grave consequences, so it is important to protect wireless sensor networks against such threats. The specific characteristics of wireless sensor networks make them vulnerable to attacks on their communication channels and their hardware. This research work discusses the open security issues in WSN. Section 2 focuses on the problem statement and later, existing security mechanisms are discussed. This research paper also present an discussion on the Cryptographic mechanisms, which can be employed to protect against some of the possible attacks such as eavesdropping and the injection of messages by the attacker is prevented by authentication.

- 013 -

Cumulated Checksum and Dynamic Addresses for Secure Wireless Sensor Networks.
Zhang, Qiong
In: International Journal of Distributed Sensor Networks * Band 12 (2016) Heft 7 (Seiten, 24 Quellen)
http://dx.doi.org/10.1177/155014773984961

Due to the broadcast nature of wireless channel, attacks against wireless sensor networks are much easier to carry out as compared to wired networks. Passive attacks such as eavesdropping and traffic analysis cannot be eliminated

even if cryptographic technologies are used. Conventional frames are usually designed to include checksum, which facilitates to adversaries capturing correct frames for further attacks. In most wireless sensor networks, source address and destination address at data link layer are unprotected, which makes traffic analysis quite easy. In this paper, we argue that the long-hold design principles of data link layer protocols are unreasonable from the perspective of wireless security. A secure ARQ scheme for wireless sensor networks named Sec-ARQ is proposed. Without the help of preshared keys or complex authentication infrastructure, Sec-ARQ protects frame checksum and addresses by cumulated checksum. Cumulated checksum is unknown to adversaries because of unavoidable wireless transmission errors. As frame checksum is unavailable to adversaries, error frames caused by collision cannot be detected, rendering eavesdropping useless. Addresses protection provided by cumulated checksum disables traffic analysis attacks. Sec-ARQ can defend against passive attacks effectively. Simulation results prove that Sec-ARQ can improve wireless security with little performance sacrifice, which is more suitable for resource-constrained wireless sensor networks.

- 014 -

Vertical Handoff Decision Algorithm Based on PRSS and Dwell Time.
Kashyap, Indu - E-Mail:indu.fet@mriu.edu.in; Madaan, Jyoti - E-Mail:jyotiverma.fet@mriu.edu.in
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 7, p 31-42, 17 refs.
http://dx.doi.org/10.5815/ijcnis.2016.07.05
http://www.mecs-press.org/ijitcs/index.html
Next generation wireless network (NGWN) is a mixture of various heterogeneous technology. It allows the global information access to the user while moving from one network to another. The challenging issue in NGWNs to design an intelligent vertical handoff decision algorithm beyond traditional one. The traditional algorithms are based on signal strength only to determine the right time and right network. But, these algorithms have a large number of unnecessary handoff due to fluctuating RSS. Although, the number of unnecessary handoffs can be reduced by an RSS with hysteresis margin scheme. But these algorithms increases the risk of high dropping and low utilization. Therefore, the aim of our research is to develop a vertical handoff decision algorithm that can select an optimum target network based on bandwidth requirement, battery power, cost of service, network performance and network condition. By the implementation of our algorithm, we can provide a mechanism that can select the best network at the appropriate time and provides the uninterrupted services to mobile users, that allows connectivity between universal mobile telecommunication system (UMTS) and wireless local area network (WLAN). The inclusion of hysteresis margin and dwell time in predicted RSS helps in reducing the early handoff, ping pong effect, decision delay and utilization rate..

- 015 -

Vertical Handoff with Predictive Received Signal Strength in Next Generation Wireless Network.
Kashyap, Indu - E-Mail:indu.fet@mriu.edu.in
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 8, p 27-38, 28 refs.
http://dx.doi.org/10.5815/ijcnis.2016.08.04
http://www.mecs-press.org/ijitcs/index.html
Since the last few decades, tremendous innovations and inventions have been observed in every field, but especially in wireless network technology. The prevailing demand curves and trends in this particular area of communication show the importance of real-time multimedia applications over several networks with guaranteed quality of service (QoS). The Next Generation Wireless Network (NGWN) consists of heterogeneous wireless networks that will grant high data rate and bandwidth to mobile users. The primary aim of Next Generation Wireless Network (NGWN) is to conceal heterogeneities and to achieve convergence of diverse networks to provide seamless mobility. So that mobile user can move freely between networks without losing the connection or changing the setting at any moment. When the mobile user moves between different networks, there is a requirement to handover the channel, from one network to another by considering its services, features and user preferences. Channel handover between two different networks is done with the help of vertical handoff (VHO). In a heterogeneous environment, numerous technologies co-exist with their unique characteristics. Therefore, it is very difficult to design efficient handoff decision algorithm. The poorly designed handoff algorithm tends to increase the traffic load and, thereby tend to dramatic decrease in quality of service. A mobile node equipped with multiple network interfaces will be able to access heterogeneous wireless access network. But the availability of alternatives give rise to a problem of unnecessary handoff. To avoid this, we have proposed a decision algorithm based on predictive received signal strength, hysteresis margin and dwell time to select an optimum target network. The handoff policies are designed using received signal strength (RSS), available bandwidth, service cost, user preference, type of application and network condition to reduce the number of handoffs, decision delay, probability of handoff failure and probability of unnecessary handoff. We have also made a comparative analysis of various vertical handoff decision algorithms in this paper..

- 016 -

Modelling and Implementation of Network Coding for Video.
Eyupoglu, Can - E-Mail:ceyupoglu@ticaret.edu.tr; Yesilyurt, Ugur - E-Mail:uyesilyurt@takasbank.com.tr
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 8, p 1-10, 26 refs.
http://dx.doi.org/10.5815/ijcnis.2016.08.01
http://www.mecs-press.org/ijitcs/index.html
In this paper, we investigate Network Coding for Video (NCV) which we apply for video streaming over wireless networks. NCV provides a basis for network coding. We use NCV algorithm to increase throughput and video quality. When designing NCV algorithm, we take the deadline as well as the decodability of the video packet at the receiver. In network coding, different flows of video packets are packed into a single packet at intermediate nodes and forwarded to other nodes over wireless networks. There are many problems that occur during transmission on the wireless channel. Network coding plays an important role in dealing with these problems. We observe the benefits of network coding for throughput increase thanks to applying broadcast operations on wireless networks. The aim of this study is to implement NCV algorithm using C programming language which takes the output of the H.264 video codec generating the video packets. In our experiments, we investigated improvements in terms of video quality and throughput at different scenarios..

- 017 -

Cryptology and Network Security. 15th International Conference, CANS 2016. Proceedings: LNCS 10052, Milan, Italy, 14-16 Nov. 2016.
Foresti-Sara; Persiano-Giuseppe
In: 2016 (xvi+762 pp) Cham, Switzerland: Springer International Publishing
The following topics are dealt with: cryptology; network security; cryptanalysis; side-channel attacks; lattice-based cryptography; virtual private network; signatures; hash; multi-party computation; authentication; system security; functional encryption; homomorphic encryption; information theoretic security; and malware..

- 018 -

Decentralized Approach for Jamming Illegal Access and Secure Data Recovery in Military Networks.
Dhawas, V. N. - E-Mail:vnd.sit@sinhgad.edu
In: (2016) p 344-9 Piscataway, NJ, USA: IEEE
Wireless Sensor Network (WSN) is a high and new innovation comprises of spatially distributed autonomous sensors. These sensors are used to monitor physical or natural conditions over a far reaching territories. The Individual sensor is in charge of detecting the required sort of information and offers that information to the approved users. This WSN is also used by the military for several number of uses including monitoring violent activities, to detect and analyze the enemy movement, enemy force etc. Mobile nodes in the military applications, such as in front of the line district are prone to discontinuous network connectivity and frequent partitions. To overcome this issue, Disruption-tolerant network (DTN) is an innovative idea, which permits the node to communicate with one another in secure way to access classified data. This paper is motivated by need of secure information recovery in wireless network. So in proposed framework we are developing various key authorities, from where individual keys must be drawn. For efficient key generation and distribution we are utilizing ECC algorithm which can be more powerful and secure..

- 019 -

2016 International Conference on Communication and Signal Processing (ICCSP). Proceedings, Melmaruvathur, India, 6-8 April 2016.
anonym
In: 2016 (476 pp) Piscataway, NJ, USA: IEEE
The following topics are dealt with: CDMA; delay tolerant networks; dipole antenna; routing protocols; InSAR; WDM-DWDM-PON; 4G heterogeneous cellular networks; wireless mesh network; quad-band bandstop filter; digital image watermarking; Doherty power amplifier; LDPC decoder; wireless multimedia sensor networks; content based video retrieval; color image encryption; UWB radar; cognitive radio; VLSI CMOS circuits design; OFDMA; Rician fading channel; RFID; MIMO channel equalizer; X-ray image classification; and OFDM system..

- 020 -

Performance Analysis and Enhancement of TCP in Presence of Jitter in Wireless Networks.
Goudru, N. G. - E-Mail:nggoudru@gmail.com; Vijaya Kumar, B. P. - E-Mail:vijaykbp@yahoo.co.in
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 6, p 9-21, 21 refs.
http://dx.doi.org/10.5815/ijcnis.2016.06.02
http://www.mecs-press.org/ijitcs/index.html
In wireless networks two types of losses namely congestion loss and transmission loss are significant. One of the important transmission losses is jitter. Variation in inter-arrival time is called jitter. When jitter value is greater than half

of the average round trip time cause timeout loss and sender window size falls to one packet resulting reduction in throughput and degradation in the quality of service (QoS). In this paper, we are discussing a new model for transmission control protocol (TCP) which is capable of changing its window size based on the feedback. In the new model TCP is added with intelligence so that it can distinguish the type of losses. If the loss is due to congestion, congestion control algorithm is invoked and loss is due to jitter immediate-recovery algorithm is invoked to recover from the throughput loss. The technique also provides an endto-end congestion control. The performance of TCP is further enhanced by discussing stability. Time-delay control theory is applied for the analysis of asymptotic stability. The stability boundaries of random early detection (RED) control parameter Pmax and jitter control parameter beta are derived. Using the characteristic equation of Hermite matrix an approximate solution of q(t) (queue length) which converges to a given target value is derived. The results are analyzed based on graphs and statistical data using Matlab R2009b..

- 021 -

2016 8th IEEE International Conference on Communication Software and Networks (ICCSN). Proceedings, Beijing, China, 4-6 June 2016.
anonym
In: 2016 (499 pp) Piscataway, NJ, USA: IEEE

The following topics are dealt with: information theory; information security; signal processing; communication system; information system; navigation system; satellite communication; antenna technology; microwave engineering; electronic engineering; communication engineering; network resource management; wireless sensor networks; mobile communication; wireless technology; information network; multimedia technology; image processing and computer science..

- 022 -

A survey on routing techniques for transmission of packets in networks.
Mangathayaru, Nimmala; Kumar, T. Satish - E-Mail:satish.savvy@gmail.com
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ICEMIS.2016.7745349

Secured Packet transmission in wireless networks is the main research carried out. The packets those are transmitted in the network moves through the routing path which might reach the destination or might get loss in between the transmission. The paper discusses on how to transmit the packets securely in adhoc networks. The transmission of packets depends upon the size of the information for transmission. The delay is caused in encrypting huge amount of data. To avoid this delay, the paper discusses various approaches used on how to encrypt and provide security for small fragments of data, in order to reduce the transmission delay. Decryption and de-fragmentation of data is performed at destination end. The packets which are transmitted through the routing path, is made secured, so as to avoid the loss of packets in the network. By performing the secure routing, the efficiency in transmission of packets can be improved and the packets can be transmitted with reduced data loss in the network..

- 023 -

Developing and evaluating a hands-on lab for teaching local area network vulnerabilities.
Anna Yu - E-Mail:cshmyu@ncat.edu; Jinsheng Xu - E-Mail:jxu@ncat.edu; Jung Hee Kim - E-Mail:jungkim@ncat.edu; Xiaohong Yuan - E-Mail:xhyuan@ncat.edu; Taehee Kim - E-Mail:tkim@ncat.edu; Jinghua Zhang - E-Mail:zhangji@wssu.edu
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/FIE.2016.7757364

Verizon's Data Breach Investigations Report states that local area network (LAN) access is the top vector for insider threats and misuses. In Ethernet, the common vulnerabilities come from Address Resolution Protocol (ARP). It is critical for students to learn these vulnerabilities, understand the mechanisms of exploits, and know the countermeasures, which include static ARP cache entries, improved ARP module in operating systems, encryption, intrusion detection, and data backup. In this paper, we introduce a hands-on lab to help students learn how ARP spoofing attack works. The objective of this lab is to let students successfully become a Man-In-The-Middle by manually creating attack packets. Although tools exist that carry out ARP spoofing attack automatically, asking students to create raw ARP spoofing packets themselves can help them understand the mechanisms of this attack method much deeper than with the automatic tools. We have studied the effectiveness of this lab on the students' understanding of LAN vulnerabilities. Tests were conducted to measure the performance of students before and after using this tool. We gave students surveys after they completed the hands-on lab. A few students were selected for an interview by an independent evaluator. The result shows that this tool can help students understand the concept of ARP spoofing attacks and motivate them in learning more about cyber security..

- 024 -

Adaptive Weighted Clustering Algorithm for Mobile Ad-hoc Networks.
Yasin, Adwan - E-Mail:Adwan.yasin@aauj.edu; Jabareen, Salah - E-Mail:Salah.jabareen@aauj.edu
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 4, p 30-6, 22 refs.
http://dx.doi.org/10.5815/ijcnis.2016.04.04
http://www.mecs-press.org/ijitcs/index.html
In this paper we present a new algorithm for clustering MANET by considering several parameters. This is a new adaptive load balancing technique for clustering out Mobile Ad-hoc Networks (MANET). MANET is special kind of wireless networks where no central management exits and the nodes in the network cooperatively manage itself and maintains connectivity. The algorithm takes into account the local capabilities of each node, the remaining battery power, degree of connectivity and finally the power consumption based on the average distance between nodes and candidate cluster head. The proposed algorithm efficiently decreases the overhead in the network that enhances the overall MANET performance. Reducing the maintenance time of broken routes makes the network more stable, reliable. Saving the power of the nodes also guarantee consistent and reliable network..

- 025 -

Impact of wireless channel model on 802.15.6 standard performance for wireless body sensor networks.
El azhari, Maryam - E-Mail:maryam.elazhari@edu.uiz.ac.ma; El moussaid, Nadya - E-Mail:nadya.elmoussaid@edu.uiz.ac.ma; Latif, Rachid - E-Mail:latif_rachid@yahoo.fr; Toumanari, Ahmed - E-Mail:atoumanari@yahoo.fr
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 5, p 1-8, 17 refs.
http://dx.doi.org/10.5815/ijcnis.2016.05.01
http://www.mecs-press.org/ijitcs/index.html
Wireless Body Sensor Network (WBAN) is a set of wearable and implantable devices capable of measuring physiological parameters and monitoring patient with chronic disease where early diagnosis is highly demanded. Several models introduced the general characterization of WBAN devices path loss considering possible shadowing due to obstruction of the signal (by the human body or any other obstacles) as well as the different postures of the human body. This paper aims at reporting an overview of WBSNs technologies, particular applications, system architecture and channel modeling. Emphasis is given to the IEEE 802.15.6 standard which enables the development of WBAN for medical and nonmedical applications. The standard's performance within a time based variation and log-distance path loss is presented based on various simulations..

- 026 -

Improving the AODV Protocol to Satisfy the Required Level of Reliability for Home Area Networks.
Bateni, Mehdi - E-Mail:bateni@shbu.ac.ir; Mohammadinejad, Hossein - E-Mail:mohammadi.n@shbu.ac.ir; Pozveh, Hossein Jafari - E-Mail:hosein.jafari@gmail.com
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 6, p 22-8, 21 refs.
http://dx.doi.org/10.5815/ijcnis.2016.06.03
http://www.mecs-press.org/ijitcs/index.html
For decades, the structure of existing power grids has not changed. It is an old structure that depends heavily on fossil fuel as an energy source, and in the future, this is likely to be critical in the field of energy. To solve these problems and to make optimal use of energy resources, a new concept is proposed, called Smart Grid. Smart Grid is an electric power distribution automation system, which can provide a two-way flow of electricity and information between power plants and consumers. The Smart Grid communications infrastructure consists of different network components, such as Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN). Achieving the required level of reliability in the transmission of information to all sections, including the HAN, is one of the main objectives in the design and implementation of Smart Grid. This study offers a routing protocol by considering the parameters and constraints of HAN, which, by improving AODV routing protocol, achieves the level of required reliability for data transmission in this network. These improvements include: making table-driven AODV routing protocol, extending the routing protocol to compute multiple paths in a route discovery, simplification and providing the effect of HAN parameters. The results of the NS2 simulation indicate that applying this improved routing protocol in the HAN, satisfies the required level of reliability of the network, which is over 98%..

- 027 -

Intrusion detection system to overcome a novel form of replay attack (data replay) in wireless sensor networks.
[02] Sahraoui, Somia - E-Mail:somiasahraoui@ymail.com
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 7, p 50-60, 32 refs.
http://dx.doi.org/10.5815/ijcnis.2016.07.07
http://www.mecs-press.org/ijitcs/index.html
Wireless Sensor Networks (WSNs) are widely and successfully employed in various application domains. They are easily deployed to collect valuable information and monitor potential environmental phenomena. However, the special nature of WSNs as well as their severe constraints and resource limitations make them vulnerable to various types of

threats. Replay attack, is one example. According to this attack, the adversary intercepts and replays several times the same (old) message leading either to missed alerts or to false alerts. Many solutions have been proposed to mitigate message replay attack. However, all these solutions are of cryptographic natures and consider only external attacks exercising a trivial scenario of replay attack. In fact, the attacker could be a lot smarter, and in this case, it replays only the data field in the message while keeping the remaining fields updated. This novel form of replay attack is much more dangerous and difficult to be detected. We call this attack variant by data replay attack. As sensor nodes may be easily captured and compromised, the worst scenario occurs if data replay attack is performed by an internal intruder. In this paper we propose an efficient intrusion detection framework to overcome data replay attack in WSNs. The proposed intrusion detection system is named DR-IDS (Data Replay Intrusion Detection System). The performance evaluations performed under NS2 simulator show that the proposed solution is sufficiently robust..

- 028 -

Trust-based ad hoc on-demand multipath distance vector routing in MANETs.
Hui Cao
In: (2016) p 210-15 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ISCIT.2016.7751623

Mobile Ad-hoc networks (MANETs) are self-organizing multi-hop wireless networks composed of independent mobile nodes. Due to the characteristics of dynamic topology and limited resources, MANETs are vulnerable to attacks from malicious nodes. However, traditional security policies with encryption and authentication cannot be well suited for MANETs, because of absence of trusted third party. In order to decrease hazards from malicious nodes, the concept of trust has been introduced to MANETs. In this paper, we first propose a novel trust model, in which nodes calculate trust value according to multiple events including historical interactions, interactions context factors and recommendations from neighbor nodes. Then the model is introduced into AOMDV, forming a novel trusted multipath routing protocol, termed as Trust-based Ad Hoc On-demand Multipath Distance Vector protocol (TAOMDV). The TAOMDV provides a flexible way to select the shortest path or multiple shortest paths from all trust satisfied paths to balance load. Experiments show that TAOMDV improves significantly in network loss ratio and average end-to-end latency..

- 029 -

LEAP: A Next-Generation Client VPN and Encrypted Email Provider.
Kaneko, Kali - E-Mail:kali@leap.se; Pollan, Ruben - E-Mail:meskio@leap.se; Sparrow, Elijah - E-Mail:elijah@leap.se; Halpin, Harry - E-Mail:harry.halpin@inria.fr
In: (2016) p 176-91 Cham, Switzerland: Springer International Publishing
http://dx.doi.org/10.1007/978-3-319-48965-0_11

As demonstrated by the revelations of Edward Snowden on the extent of pervasive surveillance, one pressing danger is in the vast predominance of unencrypted messages, due to the influence of the centralizing silos such as Microsoft, Facebook, and Google. We present the threat model and architectural design of the LEAP platform and client applications, which currently provisions opportunistic email encryption combined with a VPN tunnel and cross-device synchronization..

- 030 -

Breaking PPTP VPNs via RADIUS encryption.
Grothe, Martin - E-Mail:martin.grothe@rub.de; Horst, Matthias - E-Mail:matthias.horst@rub.de; Jager, Tibor - E-Mail:tibor.jager@rub.de; Schwenk, Joerg - E-Mail:joerg.schwenk@rub.de
In: (2016) p 159-75 Cham, Switzerland: Springer International Publishing
http://dx.doi.org/10.1007/978-3-319-48965-0_10

We describe an efficient cross-protocol attack, which enables an attacker to learn the VPN session key shared between a victim client and a VPN endpoint. The attack recovers the key which is used to encrypt and authenticate VPN traffic. It leverages a weakness of the RADIUS protocol executed between a VPN endpoint and a RADIUS server, and allows an 'insider' attacker to read the VPN traffic of other users or to escalate its own privileges with significantly smaller effort than previously known attacks on MS-CHAPv2..

- 031 -

Network performance evaluation of VPN protocols (SSTP and IKEv2).
Lawas, Jay Bryan R. - E-Mail:jay.bryan@ntec.ac.nz; Sharma, Ankit; Vivero, Allan C.
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/WOCN.2016.7759880

A Virtual Private Network (VPN) is a technology that is used to securely connect private network passing through a public network such as the Internet. Using a VPN, a computer, tablet, or smartphone is able to securely connect with others in the Internet as if they were part of a private network. Using this technology may also bring security threats like spoofing, snipping, and hacking as the data travels using the Internet connection. In order to avoid any security attacks, a VPN uses encryption and authentication to secure the data that is travelling in the Internet. A tunnel con-

nection will be established among partners, connected by using a VPN that the attackers cannot infiltrate. This research focuses on the performance evaluation of VPN protocols, mainly the Secure Socket Tunneling Protocol (SSTP) and Internet Key Exchange Version 2 (IKEv2). Throughput, jitter, and delay were measured when the packets were sent from the VPN clients to other client in a test-bed environment. After the test-bed environment research, it was found that IKEv2 had significantly better performance than SSTP in relation to throughput, jitter, and delay..

Kryptographische Verfahren

- 032 -

Generic Construction of Certificateless Signcryption Scheme.
Kar, Jayaprakash; Naik, Kshirasagar
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 489-498 (10 Seiten), Paper-Nr. Chapter 28, Short Papers
http://dx.doi.org/10.1007/978-3-319-49806-5_28
Confidentiality and message authentication are the most important security goals that can be achieved simultaneously by Signcryption scheme. It is a cryptographic technique that performs both the functions of digital signature and public key encryption in a single logical step significantly at a lower cost than that of conventional method of signature-then-encryption. The paper proposes an efficient Certificateless Signcryption Scheme (CLSC) in random oracle model on bilinear mapping. It is provably secure under the assumptions of intractability of k-CAA, Inv-CDH, q-BDHI and CDH problems.

- 033 -

AES Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using FPGA Implementation.
Ahmad, Nabihah; Rifen, A.Aminurdin M.; Wahab, Mohd Helmy Abd
In: IRIS, International Engineering Research and Innovation Symposium, 2016, in: IOP Conference Series: Materials Science and Engineering (Online) * Band 160 (2016) Seite 012113/1-10 (10 Seiten, 32 Quellen)
http://dx.doi.org/10.1088/1757-899X/160/1/012113
Automated Teller Machine (ATM) is an electronic banking outlet that allows bank customers to complete a banking transactions without the aid of any bank official or teller. Several problems are associated with the use of ATM card such card cloning, card damaging, card expiring, cast skimming, cost of issuance and maintenance and accessing customer account by third parties. The aim of this project is to give a freedom to the user by changing the card to biometric security system to access the bank account using Advanced Encryption Standard (AES) algorithm. The project is implemented using Field Programmable Gate Array (FPGA) DE2-115 board with Cyclone IV device, fingerprint scanner, and Multi-Touch Liquid Crystal Display (LCD) Second Edition (MTL2) using Very High Speed Integrated Circuit Hardware (VHSIC) Description Language (VHDL). This project used 128-bits AES for recommend the device with the throughput around 19.016Gbps and utilized around 520 slices. This design offers a secure banking transaction with a low rea and high performance and very suited for restricted space environments for small amounts of RAM or ROM where either encryption or decryption is performed.

- 034 -

QOS Affluent Web Services Message Communication Using Secured Simple Object Access Protocol (SOAP) Technique.
Anithadevi, N.; Sundarambal, M.
In: Digital Connectivity - Social Impact, CSI, Annual Convention of the Computer Society of India, 51, in: Communications in Computer and Information Science * Band 679 (2016) Seite 191-207 (17 Seiten), Paper-Nr. Chapter 16, Network Computing
http://dx.doi.org/10.1007/978-981-10-3274-5_16
In IT services SOA is one of the most elastic and modular approaches and it is a prerequisite for arising technologies like cloud, these cloud services are exposed as web services based on industry standards, which follows WSDL for service illustration. These services depend on SOAP to handle service request and response. Hence Web services security is one of the important factors which are used to assess cloud system security. While creating a new web service or with an existing web service communication, it is prudent to have secure data transmission with end users identity such as card numbers, user names, passwords etc. Security standards like WS-Security only addresses message integrity, confidentiality, user authentication, and authorization. The proposed system offers confidentiality and integrity protection from the creation of the message to its consumption. This system will look at a color palette scheme which records the RGB color values of the chosen color during registration and these values are used during sign on, subsequently it performs the access control mechanism. To strengthen web services towards message level

by encrypting SOAP messages with AES and shared key is derived using new cryptosystem called Rbits (Random bits) cipher as a service and digital signature handler facilitates secure key exchange which is completed ahead with SOAP message generation. The essential aspect of this proposed system is from core key form multiple random keys which safeguards the messages with highest possible immunity to crack when the applications or services communicating with web services.

- 035 -

Updatable Hash Proof System and Its Applications.
Yang, Rupeng; Xu, Qiuliang; Zhou, Yongbin; Zhang, Rui; Hu, Chengyu; Yu, Zuoxia
In: Computer Security, ESORICS, European Symposium on Research in Computer Security, 20, in: Lecture Notes in Computer Science * Band 9326 (2015) Seite 266-285 (20 Seiten), Paper-Nr. Chapter 14, Cryptography
http://dx.doi.org/10.1007/978-3-319-24174-6_14
To tackle with physical attacks to real world cryptosystems, leakage resilient cryptography was developed. In this setting, the adversary is allowed to have access to the internal state of a cryptographic system, thus violates the black-box reduction used in cryptography. Especially when considering continual memory leakage (CML), i.e., there is no predetermined bound on the leakage of the internal information, the task is extremely tough. In this paper, we solve this problem by introducing a new primitive called updatable hash proof system (UHPS). A UHPS can be viewed as a special Hash proof system (HPS), which served as a fundamental tool in constructing public key encryption (PKE) schemes in both leakage-free and leaky settings. A remarkable property of UHPS is that by simply substituting the HPS component with a UHPS component in a PKE scheme, one obtains a new PKE scheme secure in the CML setting. Moreover, the resulting PKE scheme enjoys the same advantage of the original HPS-based PKE, for instance, still "compatible" with known transforms [8,20,24,32]. We then give instantiations of UHPS from widely-accepted assumptions, including the symmetric external Diffie-Hellman assumption and the d-linear assumption. Interestingly, we notice that when instantiated with concrete assumptions, the resulting chosen-ciphertext secure PKE scheme is by far the most efficient.

- 036 -

Secure data processing with massive-parallel SIMD matrix for embedded SoC in digital-convergence mobile devices.
Kumaki, Takeshi; Koide, Tetsushi; Fujino, Takeshi
In: IEEJ Transactions on Electrical and Electronic Engineering * Band 12 (2017) Heft 1, Seite 96-104 (9 Seiten, 12 Bilder, 7 Tabellen)
http://dx.doi.org/10.1002/tee.22349
This paper presents secure data processing with a massive-parallel single-instruction multiple-data (SIMD) matrix for embedded system-on-chip (SoC) in digital-convergence mobile devices. Recent mobile devices are required to use private-information-secure technology, such as cipher processing, to prevent the leakage of personal information. However, this adds to the device's required specifications, especially cipher implementation for fast processing, power consumption, low hardware cost, adaptability, and end-user's operation for maintaining the safety condition. To satisfy these security-related requirements, we propose the interleaved-bitslice processing method, which combines two processing concepts (bitslice processing and interleaved processing), for novel parallel block cipher processing with five confidentiality modes on mobile processors. Furthermore, we adopt a massive-parallel SIMD matrix processor (MX-1) for interleaved-bitslice processing to verify the effectiveness of parallel block cipher implementation. As the implementation target from the Federal Information Processing Standardization-approved block ciphers, a data encryption standard (DES), triple-DES, and Advanced Encryption Standard (AES) algorithms are selected. For the AES algorithm, which is mainly studied in this paper, the MX-1 implementation has up to 93% fewer clock cycles per byte than other conventional mobile processors. Additionally, the MX-1 results are almost constant for all confidentiality modes. The practical-use energy efficiency of parallel block cipher processing with the evaluation board for MX-1 was found to be about 4.8 times higher than that of a BeagleBoard-xM, which is a single-board computer and uses the ARM Cortex-A8 mobile processor. Furthermore, to improve the operation of a single-bit logical function, we propose the development of a multi-bit logical library for interleaved-bitslice cipher processing with MX-1. Thus, the number of clock cycles is the smallest among those reported in other related-studies. Consequently, interleaved-bitslice block cipher processing with five confidentiality modes on MX-1 is effective for the implementation of parallel block cipher processing for several digital-convergence mobile devices.

- 037 -

On Secrecy Amplification Protocols.
Ostadal, Radim; Svenda, Petr; Matyas, Vashek
In: Information Security Theory and Practice, WISTP, IFIP WG 11.2 International Workshop, Information Security Theory and Practice, 9, in: Lecture Notes in Computer Science * Band 9311 (2015) Seite 3-19 (17 Seiten), Paper-Nr. Chapter 1, Security and Privacy Services
http://dx.doi.org/10.1007/978-3-319-24018-3_1
We review most important secrecy amplification protocols that are suitable for ad-hoc networks of devices with limited resources, providing additional resistance against various attacks on used cryptographic keys without necessity for asymmetric cryptography. We discuss and evaluate different designs as well as approaches to create new protocols. A special focus is given to suitability of these protocols with respect to different underlying key distribution schemes and also to open issues.

- 038 -

Sicherheit relativ definieren. Das Real/Ideal-Paradigma in der Kryptographie.
Broadnax, Brandon; Mechler, Jeremias; Müller-Quade, Jörn; Nagel, Matthias; Rill, Jochen
In: DuD Datenschutz und Datensicherheit * Band 41 (2017) Heft 1, Seite 24-28 (5 Seiten), Kryptographie - Aktuelle Entwicklungen
http://dx.doi.org/10.1007/s11623-017-0720-4
In der modernen Kryptographie wird "Sicherheit" mathematisch definiert. Einer der etablierten Ansätze, Sicherheit zu definieren, ist die "Simulationsbasierte Sicherheit", bei der Sicherheit keine absolute Größe ist, sondern durch Vergleich mit fiktionalen, ideal sicheren kryptographischen Protokollen definiert wird. Dieser Artikel stellt neue Entwicklungen vor.

- 039 -

Serial Number Based Encryption and Its Application for Mobile Networks.
Ma, Rong; Cao, Zhenfu
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 396-406 (11 Seiten), Paper-Nr. Chapter 39
http://dx.doi.org/10.1007/978-3-319-21837-3_39
Security and privacy of many mobile applications rely on lightweight cryptographic protocol. In this paper, we develop a lightweight functional public key encryption scheme and demonstrate its applictions for mobile networks. We call such a scheme the Serial Number Based Encryption (SNBE). Our scheme is provable secure base on the DBDH assumption in the standard model, while the ciphertext consists of only three elements. We also discuss some applications of SNBE scheme in the mobile environment.

- 040 -

Authentication in Wireless Sensor Networks Using Dynamic Identity Based Signatures.
Suganthi, S.D.; Anitha, R.; Thanalakshmi, P.
In: Digital Connectivity - Social Impact, CSI, Annual Convention of the Computer Society of India, 51, in: Communications in Computer and Information Science * Band 679 (2016) Seite 155-168 (14 Seiten), Paper-Nr. Chapter 13, Network Computing
http://dx.doi.org/10.1007/978-981-10-3274-5_13
A Wireless sensor network (WSN) is composed of a large number of sensor nodes, which perform multiple tasks, namely sensing, data processing and forwarding of observed data. WSNs nodes may possess sensitive data that are prone to various attacks. For such a network to be viable, integrity and authenticity should be provided to the data generated by the sensor nodes. For example, in military surveillance and enemy tracking applications, the localization system of the nodes is the target for many attackers. In such applications, the base station would broadcast the command for localization to all the sensor nodes in the field. The sensor nodes would respond to this query with the required data. Any compromised node at this point would generate false data and may lead to miscalculation of the localization process and incorrect decision making. Hence, a resilient authentication is necessary to authenticate a node. As a first step towards this objective, a lightweight identity based signature for authentication of the sensor nodes is proposed in this paper. The scheme uses "fingerprint", i.e. a lifetime secure memory fraction in the sensor nodes as a parameter for signature generation. In addition, the parameters for fingerprints are generated dynamically and the computed fingerprint values are not stored permanently in the hardware. Because of these features, the sensor nodes can overcome identity based attack like Sybil attack. Also, it is impossible to read the contents of the sensor node even if the node is captured by the attacker. The security proof for this scheme is based on the Computational Diffie-Hellman assumption and proved in the random oracle model. On the computation point of view, the proposed scheme requires minimal operations in signing than the existing identity based signature approaches.

- 041 -

Constant-Size Ciphertext Attribute-Based Encryption from Multi-channel Broadcast Encryption.
Canard, Sebastien; Trinh, Viet Cuong
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 193-211 (19 Seiten), Paper-Nr. Chapter 10, Cryptosystem and Protocols
http://dx.doi.org/10.1007/978-3-319-49806-5_10

Attribute-based encryption (ABE) is an extension of traditional public key encryption in which the encryption and decryption phases are based on user's attributes. More precisely, we focus on ciphertext-policy ABE (CP- ABE) where the secret-key is associated to a set of attributes and the ciphertext is generated with an access policy. It then becomes feasible to decrypt a ciphertext only if one's attributes satisfy the used access policy. CP- ABE scheme with constant-size ciphertext supporting fine-grained access control has been investigated at AsiaCrypt'15 and then at TCC'16. The former makes use of the conversion technique between ABE and spatial encryption, and the later studies the pair encodings framework. In this paper, we give a new approach to construct such kind of CP- ABE scheme. More precisely, we propose private CP- ABE schemes with constant-size ciphertext, supporting CNF (Conjunctive Normal Form) access policy, with the simple restriction that each attribute can only appear k_{max} times in the access formula. Our two constructions are based on the BGW scheme at Crypto'05. The first scheme is basic selective secure (in the standard model) while our second one reaches the selective CCA security (in the random oracle model).

- 042 -

Genetic Algorithm in Stream Cipher Cryptanalysis.
Polak, Iwona; Boryczka, Mariusz
In: Computational Collective Intelligence, ICCCI, International Conference on Collective Intelligence, 7, in: Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence * Band 9330 (2015) Seite 149-158 (10 Seiten), Paper-Nr. Chapter 15, CSI: Special Session on Computational Swarm Intelligence
http://dx.doi.org/10.1007/978-3-319-24306-1_15

Cryptography nowadays is a very important field of protecting information from falling into wrong hands. One of modern cryptography branch is stream cipher cryptography. This paper focuses on cryptanalysis of such ciphers using genetic algorithm. Genetic algorithm as one of optimisation methods isn't quite obvious to use in the field of cryptography, nevertheless it can give interesting results. In this article authors look for the shortest equivalent linear system which approximate given keystream with linear shift feedback register.

- 043 -

Short Accountable Ring Signatures Based on DDH.
Bootle, Jonathan; Cerulli, Andrea; Chaidos, Pyrros; Ghadafi, Essam; Groth, Jens; Petit, Christophe
In: Computer Security, ESORICS, European Symposium on Research in Computer Security, 20, in: Lecture Notes in Computer Science * Band 9326 (2015) Seite 243-265 (23 Seiten), Paper-Nr. Chapter 13, Cryptography
http://dx.doi.org/10.1007/978-3-319-24174-6_13

Ring signatures and group signatures are prominent cryptographic primitives offering a combination of privacy and authentication. They enable individual users to anonymously sign messages on behalf of a group of users. In ring signatures, the group, i.e. the ring, is chosen in an ad hoc manner by the signer. In group signatures, group membership is controlled by a group manager. Group signatures additionally enforce accountability by providing the group manager with a secret tracing key that can be used to identify the otherwise anonymous signer when needed. Accountable ring signatures, introduced by Xu and Yung (CARDIS 2004), bridge the gap between the two notions. They provide maximal flexibility in choosing the ring, and at the same time maintain accountability by supporting a designated opener that can identify signers when needed. We revisit accountable ring signatures and offer a formal security model for the primitive. Our model offers strong security definitions incorporating protection against maliciously chosen keys and at the same time flexibility both in the choice of the ring and the opener. We give a generic construction using standard tools. We give a highly efficient instantiation of our generic construction in the random oracle model by meticulously combining Camenisch's group signature scheme (CRYPTO 1997) with a generalization of the one-out-of-many proofs of knowledge by Groth and Kohlweiss (EUROCRYPT 2015). Our instantiation yields signatures of logarithmic size (in the size of the ring) while relying solely on the well-studied decisional Diffie-Hellman assumption. In the process, we offer a number of optimizations for the recent Groth and Kohlweiss one-out-of-many proofs, which may be useful for other applications. Accountable ring signatures imply traditional ring and group signatures. We therefore also obtain highly efficient instantiations of those primitives with signatures shorter than all existing ring signatures as well as existing group signatures relying on standard assumptions.

- 044 -

Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections.
Kadir, Abdurahman; Aili, Mireguli; Sattar, Mutallip
In: Optik * Band 129 (2017) Seite 231-238 (8 Seiten, 19 Quellen)
http://dx.doi.org/10.1016/j.ijleo.2016.10.036

The paper proposes a color image encryption scheme based on coupled hyper chaotic Lorenz systems. The novelty is to randomly inject impulse signals into coupled Lorenz system during iterations to enhance the complexity of trajectory. Six state variables sequences are generated to encrypt the red, green and blue components by bitwise operations of exclusive or (XOR) and left or right cyclic shift. Six initial values and indeterminate multiple impulse signals can make the cryptosystem own larger variable key space to resist against exhaustive attack, even the attack from quantum computer. Simulation results show that the mean encryption speed is stable, which means the speed depends solely upon hardware equipment and algorithm. Statistical analysis demonstrates the high effectiveness of the proposed image encryption algorithm.

- 045 -

A Secure Multi-unit Sealed First-Price Auction Mechanism.
Larson, Maya; Li, Wei; Hu, Chunqiang; Li, Ruinian; Cheng, Xiuzhen; Bie, Rongfang
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 295-304 (10 Seiten), Paper-Nr. Chapter 29
http://dx.doi.org/10.1007/978-3-319-21837-3_29

Due to the popularity of auction mechanisms in real-world applications and the increase in the awareness of securing private information, auctions are in dire need of bid-privacy protection. In this paper, we deliberately design a secure multi-unit sealed-bid first-price auction scheme, in which the auction is processed on the bidders' encrypted bids by the server and the final output is only known by the auctioneer. As a result, neither the auctioneer nor the server can obtain the full information of the bidders. What's more, the auctioneer can verify whether a winner pays its full payment in the auction. Finally, a comprehensive analysis on the performance of our auction mechanism is conducted.

- 046 -

A Bidder-Oriented Privacy-Preserving VCG Auction Scheme.
Larson, Maya; Li, Ruinian; Hu, Chunqiang; Li, Wei; Cheng, Xiuzhen; Bie, Rongfang
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 284-294 (11 Seiten), Paper-Nr. Chapter 28
http://dx.doi.org/10.1007/978-3-319-21837-3_28

Vickrey-Clarke-Groves (VCG) is a type of sealed-bid auction of multiple items which has good economic properties. However, VCG has security vulnerabilities, e.g. it is vulnerable to auctioneer fraud. To make VCG more practical, bid prices must be well protected. To tackle this challenge, we propose a bidder-oriented, privacy-preserving auction scheme using homomorphic encryption, where the bidders can calculate the results by themselves, and the auctioneer is able to verify the results. Compared to previous research, our scheme is more trustworthy with stronger privacy.

- 047 -

Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme.
Challa, RatnaKumari; Gunta, VijayaKumari
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 499-508 (10 Seiten), Paper-Nr. Chapter 29, Short Papers
http://dx.doi.org/10.1007/978-3-319-49806-5_29

Several number theoretic and algebraic homomorphic encryption schemes were proposed in the literature, which have been remained theoretical due to their high computational complexities. Coding theory is believed to be a promising alternative for the construction of homomorphic encryption schemes. A few of such schemes exist, but, they support limited operations of additions and multiplications over the ciphertexts. Based on a special class of linear codes called Reed-Muller codes, in this paper, a new symmetric key Fully Homomrphic Encryption (FHE) scheme is proposed, which employs a novel method of ciphertext post processing to achieve unlimited homomorphic multiplications. The security of the proposition is analysed with respect to all the known attacks.

- 048 -

An Efficient Certificateless Signature Scheme in the Standard Model.
Canard, Sebastien; Trinh, Viet Cuong
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 175-192 (18 Seiten), Paper-Nr. Chapter 9, Cryptosystem and Protocols
http://dx.doi.org/10.1007/978-3-319-49806-5_9

Identity-based cryptography has been introduced by Shamir at Crypto'84 to avoid the use of expensive certificates in certified public key cryptography. In such system, the identity becomes the public key and each user needs to interact with a designated authority to obtain the related private key. It however suffers the key escrow problem since the authority knows the private keys of all users. To deal with this problem, Riyami and Paterson have introduced, at Asiacrypt'03, the notion of certificateless public key cryptography. In this case, there is no need to use the certificate to certify the public key, and neither the user nor the authority can derive the full private key by himself. There have been several efforts to propose a certificateless signature (CLS) scheme in the standard model, but all of them either make use of the Waters' technique or of the generic conversion technique (proposed by Yum and Lee at ACISP'04 and later modified by Hu et al. at ACISP'06) which both lead to inefficient schemes. In this paper, we introduce a new and direct approach to construct a CLS scheme, secure in the standard model, with constant-size of all parameters and having efficient computing time. Our scheme is therefore very efficient when comparing to existing CLS schemes in the standard model.

- 049 -

Verifying Protocol Implementations by Augmenting Existing Cryptographic Libraries with Specifications.
Vanspauwen, Gijs; Jacobs, Bart
In: Collocated Workshops: ATSE, HOFM, MoKMaSD, and VERY*SCART, SEFM, International Conference on Software Engineering and Formal Methods, 13, in: Lecture Notes in Computer Science, Programming and Software Engineering * Band 9276 (2015) Seite 53-68 (16 Seiten), Paper-Nr. Chapter 4, Program Verification
http://dx.doi.org/10.1007/978-3-319-22969-0_4

Specifying correct cryptographic protocols has proven to be a difficult task. The implementation of such a protocol in a lower-level programming language introduces additional room for errors. While a lot of work has been done for proving the correctness of high-level (often non-executable) protocol specifications, methodologies to prove properties of protocol implementations in a lower-level language are less well-studied. Such languages however, like the C programming language, are still frequently used to write cryptographic software. We propose a static verification approach for cryptographic protocol implementations written in the C programming language. This approach employs our own extended symbolic model of cryptography which we formalized in VeriFast, a separation logic-based verifier for C programs. By giving formal contracts to the primitives of an existing cryptographic library (i.e. PolarSSL), we were able to prove, besides memory safety, interesting security properties of a small protocol suite thatdemonstrates the usage of those primitives.

- 050 -

A Family P System of Realizing RSA Algorithm.
Guo, Ping; Xu, Wei
In: BIC-TA, International Conference ob Bio-Inspired Computing - Theories and Applications, 11, in: Communications in Computer and Information Science * Band 681 (2016) Seite 155-167 (13 Seiten), Paper-Nr. Chapter 16, Membrane Computing
http://dx.doi.org/10.1007/978-981-10-3611-8_16

P system is a new kind of distributed parallel computing model, and many variants of it are proposed to solve the problems such as NP problems, arithmetic operation, image processing. RSA is a classic asymmetric encryption algorithm which plays a very import role in the field of the information security and it is used widely in data transmission and digital signature. This paper is based on P system to realize the RSA algorithm in parallel which includes key generation and encryption & decryption, then a cell-like RSA P system P_{RSA} is designed from this. An instance is given to illustrate the feasibility and effectiveness of our designed P systems.

- 051 -

A simple yet efficient S-box method based on chaotic sine map.
Belazi, Akram; El-Latif, Ahmed A. Abd
In: Optik * Band 130 (2017) Seite 1438-1444 (7 Seiten, 16 Quellen)
http://dx.doi.org/10.1016/j.ijleo.2016.11.152

Substitution-boxes, or simply S-boxes, are used to increase confidentiality in the substitution stage of most cryptosystem approaches. In this paper, an efficient method for the construction of an S-box based on a sine map is proposed. The proposed S-box is able to generate random integer sequences with highly efficient nonlinearity in the generated

values. The cryptographic analyses show that the proposed S-box method is of high performance and can be used with great potential for prominent prevalence in designing symmetric cryptosystems and copy right protection.

- 052 -

A Multi-round Side Channel Attack on AES Using Belief Propagation.
Bouder, Helene Le; Lashermes, Ronan; Linge, Yanis; Thomas, Gael; Zie, Jean-Yves
In: Foundations and Practice of Security, FPS, International Symposium on Foundations and Practice of Security, 9, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10128 (2017) Seite 199-213 (15 Seiten), Paper-Nr. Chapter 13, Crypto and Communication Security
http://dx.doi.org/10.1007/978-3-319-51966-1_13
This paper presents a new side channel attack to recover a block cipher key. No plaintext and no ciphertext are required, no templates are built. Only the leakage measurements collected in many different rounds of the algorithm are exploited. The leakage is considered as a Hamming weight with a Gaussian noise. The chosen target is the Advanced Encryption Standard (AES). Bayesian inference is used to score all guesses on several consecutive round-key bytes. From these scores a Belief Propagation algorithm is used, based on the relations of the KeyExpansion, to discriminate the unique correct guess. Theoretical results according to various noise models are obtained with simulations.

- 053 -

Steganography on multiple MP3 files using spread spectrum and Shamir's secret sharing.
Yoeseph, N.M.; Purnomo, F.A.; Riasti, B.K.; Safiie, M.A.; Hidayat, T.N.
In: ICOPIA, International Conference on Physics and its Applications, 8, in: Journal of Physics: Conference Series (Online) * Band 776 (2016) Seite 012089/1-6 (6 Seiten, 9 Quellen)
http://dx.doi.org/10.1088/1742-6596/776/1/012089
The purpose of steganography is how to hide data into another media. In order to increase security of data, steganography technique is often combined with cryptography. The weakness of this combination technique is the data was centralized. Therefore, a steganography technique is develop by using combination of spread spectrum and secret sharing technique. In steganography with secret sharing, shares of data is created and hidden in several medium. Medium used to concealed shares were MP3 files. Hiding technique used was Spread Spectrum. Secret sharing scheme used was Shamir's Secret Sharing. The result showed that steganography with spread spectrum combined with Shamir's Secret Share using MP3 files as medium produce a technique that could hid data into several cover. To extract and reconstruct the data hidden in stego object, it is needed the amount of stego object which more or equal to its threshold. Furthermore, stego objects were imperceptible and robust.

- 054 -

Generation of grid multi-scroll chaotic attractors via hyperbolic tangent function series.
Chen, Zhong; Wen, Guilin; Zhou, Huaan; Chen, Junyao
In: Optik * Band 130 (2017) Seite 594-600 (7 Seiten, 24 Quellen)
http://dx.doi.org/10.1016/j.ijleo.2016.10.085
A chaotic model for generating multi-directional multi-scroll attractors via hyperbolic tangent function series is proposed in this paper. The dynamical mechanisms of this chaotic model are further investigated, including M-scroll, M×N-grid scroll, M×N×L-grid scroll chaotic attractors. Moreover, the dynamical behaviors of this system are theoretically analyzed and numerically simulated, such as equilibria and their stability, Lyapunov exponents and bifurcation diagrams. This system can be widely used in data encryption and secure communication.

- 055 -

Mean value based reversible data hiding in encrypted images.
Agrawal, Smita; Kumar, Manoj
In: Optik * Band 130 (2017) Seite 922-934 (13 Seiten, 46 Quellen)
http://dx.doi.org/10.1016/j.ijleo.2016.11.059
A novel reversible data hiding technique for encrypted images is proposed in this paper. Proposed technique utilizes additive modulo 256 for encryption purpose and a property of mean for embedding watermark in the encrypted image. Preserved mean values are used for watermark extraction and image recovery. In contrast to several state of art reversible data hiding techniques for encrypted images, proposed technique provides complete reversibility in terms of bit by bit recovery of original image after decryption and watermark extraction. Proposed technique is computationally very simple and executes in very less computational time. Experimental results, on various standard grayscale test images, and comparison with recently proposed existing techniques exhibit the superiority of the proposed tech-

nique in terms of security, reversibility, privacy protection and computational efficiency.

- 056 -

QR code based noise-free optical encryption and decryption of a gray scale image.
Jiao, Shuming; Zou, Wenbin; Li, Xia
In: Optics Communications * Band 387 (2017) Seite 235-240 (6 Seiten, 27 Quellen)
http://dx.doi.org/10.1016/j.optcom.2016.11.066
In optical encryption systems, speckle noise is one major challenge in obtaining high quality decrypted images. This problem can be addressed by employing a QR code based noise-free scheme. Previous works have been conducted for optically encrypting a few characters or a short expression employing QR codes. This paper proposes a practical scheme for optically encrypting and decrypting a gray-scale image based on QR codes for the first time. The proposed scheme is compatible with common QR code generators and readers. Numerical simulation results reveal the proposed method can encrypt and decrypt an input image correctly.

- 057 -

A Generic Simulation Framework for Non-Entangled based Experimental Quantum Cryptography and Communication: Quantum Cryptography and Communication Simulator (QuCCs).
Buhari, Abudhahir; Zukarnain, Zuriati Ahmad; Khalid, Roszelinda; Zakir Dato, Wira Jaafar Ahmad
In: IRIS, International Engineering Research and Innovation Symposium, 2016, in: IOP Conference Series: Materials Science and Engineering (Online) * Band 160 (2016) Seite 012095/1-12 (12 Seiten, 17 Quellen)
http://dx.doi.org/10.1088/1757-899X/160/1/012095
The applications of quantum information science move towards bigger and better heights for the next generation technology. Especially, in the field of quantum cryptography and quantum computation, the world already witnessed various ground-breaking tangible product and promising results. Quantum cryptography is one of the mature field from quantum mechanics and already available in the markets. The current state of quantum cryptography is still under various researches in order to reach the heights of digital cryptography. The complexity of quantum cryptography is higher due to combination of hardware and software. The lack of effective simulation tool to design and analyze the quantum cryptography experiments delays the reaching distance of the success. In this paper, we propose a framework to achieve an effective non-entanglement based quantum cryptography simulation tool. We applied hybrid simulation technique i.e. discrete event, continuous event and system dynamics. We also highlight the limitations of a commercial photonic simulation tool based experiments. Finally, we discuss ideas for achieving one-stop simulation package for quantum based secure key distribution experiments. All the modules of simulation framework are viewed from the computer science perspective.

- 058 -

Partial Encryption Based Secure Sharing of CAD Models for Cloud-Based Design.
Cai, Xiantao; Li, Weidong; He, Fazhi
In: MSEC, ASME International Manufacturing Science and Engineering Conference, 2014 * (2014) Seite V001T04A021
http://dx.doi.org/10.1115/MSEC2014-4079
Model security for collaborative product design in a networked environment (or called networked manufacture, grid manufacture, and cloud manufacture) is an important but also challenging research issue. In order to support collaborative product design in a secure and flexible means, a partial encryption based secure sharing method for Computer Aided Design (CAD) model is presented in this paper. Based on the above method, parts of a CAD model can be selected flexibly by users for encrypting according to different users' requirements. The secret keys for the different parts of the CAD model can be customized to meet the requirements of users. Case studies have been developed to demonstrate the effectiveness of the proposed method.

- 059 -

An interpolation-based lossless hiding scheme based on message recoding mechanism.
Lu, Tzu-Chuen
In: Optik * Band 130 (2017) Seite 1377-1396 (20 Seiten, 10 Quellen)
http://dx.doi.org/10.1016/j.ijleo.2016.11.176
The secret message can be an image that encoded using a binary string. In a pure symbol such as the Japanese flag, there are many smooth areas. Such images degrade the quality of the stego image considerably because they contain many white-colored pixels in the secret image, most of which are encoded as "11111111." Hiding schemes shift the cover pixel to conceal the secret bit 1. Hence, many pixels will be shifted for hiding a simple secret image such that the image quality of the stego image deteriorates. To solve this problem, we proposed a re-encoding

mechanism to rearrange the value of the secret message. The proposed scheme re-encodes the secret message according to its occurrence probability. The frequently appearing patterns are encoded with the smallest distortion code to minimize image distortion. According to the results, the image quality of the proposed scheme is approximately 3 dB higher than that of other methods. In particular, for very smooth secret messages such as logo images, the image quality of the proposed scheme is 12 dB higher than those of the existing methods. Furthermore, the embedding capacity of the proposed method is 1 bpp higher than those of the existing methods.

- 060 -

Minimize the Replication for Secure Cloud Data Storage Systems Using Error Correction Codes.
Sahaya Stalin, Jose G.; Seldev, Christopher C.
In: Applied Information and Digital Image Technologies, Control and Power Engineering, ICEETS, International Conference on Energy Efficient Technologies for Sustainability, 2014, in: Applied Mechanics and Materials * Band 626 (2014) Seite 26-31 (6 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.626.26
http://www.scientific.net/AMM.626.26
Cloud data centers should be flexible and available to the data forever. The replication method is used to achieve high availability and durability of cloud data center, if there is any failure to recover the messages from the cloud databases. The concern of this replication technology is that, the replica size is equal to the size of the original data object. When Error Detection Schemes were used, there is a reduction in the number of cloud distributed storage systems. The scope of this paper is to store the data efficiently in cloud data centers unlike the previous schemes which used erasure codes such as Reed Solomon codes only with a view to store data in datacenters. This paper proposes to encrypt the message using DES and to encode the message using Reed Solomon code before storing the message. Storing time is convincingly good in Reed Solomon code when compared with tornado code.

- 061 -

On Algebraic Immunity of Weight Symmetric H Boolean Functions.
Huang, Jing-Lian; Wang, Zhuo; Li, Juan
In: Engineering Providing of Industrial Development, APCMCE, Asian Pacific Conference on Mechatronics and Control Engineering, 2, in: Applied Mechanics and Materials * Band 643 (2014) Seite 124-129 (6 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.643.124
http://www.scientific.net/AMM.643.124
Using the derivative of Boolean functions and the e-derivative defined by ourselves as research tools, we discuss the relationship among a variety of cryptographic properties of the weight symmetric H Boolean functions in the range of the weight with the existence of H Boolean functions. We also study algebraic immunity and correlation immunity of the weight symmetric H Boolean functions and the balanced H Boolean functions. We obtain that the weight symmetric H Boolean function should have the same algebraic immunity, correlation immunity, propagation degree and nonlinearity. Besides, we determine that there exist several kinds of H Boolean functions with resilient, algebraic immunity and optimal algebraic immunity. The above results not only provide a theoretical basis for reducing nearly half of workload when studying the cryptographic properties of H Boolean function, but also provide a new research method for the study of secure cryptographic property of Boolean functions. Such researches are important in cryptographic primitive designs.

- 062 -

An Improved Search Algorithm About Spam Firewall.
Li, Kangshun; Xiong, Lu; Wen, Zhichao
In: BIC-TA, International Conference ob Bio-Inspired Computing - Theories and Applications, 11, in: Communications in Computer and Information Science * Band 682 (2016) Seite 95-100 (6 Seiten), Paper-Nr. Chapter 12, Evolutionary Computing
http://dx.doi.org/10.1007/978-981-10-3614-9_12
Although most of the existing encryption system takes the privacy issues of storing data into consider, the reveal of user access pattern is inevitable during the e-mail filtering. Therefore, how to protect the private data in the process of spam filtering becomes one of the urgent problems to be solved. Combined with two filtering techniques which are based on keyword and blacklist respectively, this paper achieves the goal of sorting and filtering spams. Meanwhile, given the privacy issues in sorting and filtering the spams, the paper is based on an experimental project, the Pairing Based Cryptography, which is performed by Stanford University to achieve the e-mail encryption program. It adopts a searchable public key encryption in the process of sorting and filtering, which needs no decryption and can realize searching and matching operations. By this method, it fully protects the privacy and access patterns of the mail receiver from disclosing.

- 063 -

A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion.
Lu, Xu; Xu, Gou; Zhi, Li; Jian, Li
In: Optics and Lasers in Engineering * Band 91 (2017) Seite 41-52 (12 Seiten, 48 Quellen)
http://dx.doi.org/10.1016/j.optlaseng.2016.10.012

In this paper, we propose a novel chaotic image encryption algorithm which involves a block image scrambling scheme and a new dynamic index based diffusion scheme. Firstly, the original image is divided into two equal blocks by vertical or horizontal directions. Then, we use the chaos matrix to construct X coordinate, Y coordinate and swapping control tables. By searching the X coordinate and Y coordinate tables, the swapping position of the processing pixel is located. The swapping control table is used to control the swapping of the pixel in the current block or the other block. Finally, the dynamic index scheme is applied to the diffusing of the scrambled image. The simulation results and performance analysis show that the proposed algorithm has an excellent safety performance with only one round.

- 064 -

Anonymizable Ring Signature Without Pairing.
Blazy, Olivier; Bultel, Xavier; Lafourcade, Pascal
In: Foundations and Practice of Security, FPS, International Symposium on Foundations and Practice of Security, 9, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10128 (2017) Seite 214-222 (9 Seiten), Paper-Nr. Chapter 14, Crypto and Communication Security
http://dx.doi.org/10.1007/978-3-319-51966-1_14

Ring signature is a well-known cryptographic primitive that allows any user who has a signing key to anonymously sign a message according to a group of users. Some years ago, Hoshino et al. propose a new kind of ring signature where anybody can transform a digital signature into an anonymous signature according to a chosen group of users; authors present a pairing-based construction that is secure under the gap Diffie-Hellman assumption in the random oracle model. However this scheme is quite inefficient for large group since the generation of the anonymous signature requires a number of pairing computations that is linear in the size of the group. In this paper, we give a more efficient anonymizable signature scheme without pairing. Our anonymization algorithm requires n exponentiations in a prime order group where n is the group size. Our proposal is secure under the discrete logarithm assumption in the random oracle model, which is a more standard assumption.

- 065 -

2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity). Proceedings, Chengdu, China, 19-21 Dec. 2015.
Xingang-Liu-Hsu-Robert-Peicheng-Wang-Feng-Xia-Yufeng-Wang-Mianxiong-Dong-Yuhui-Deng
In: 2015 (524 pp) Los Alamitos, CA, USA: IEEE Computer Society

The following topics are dealt with: smart cities; urban informatics; network infrastructure; embedded computing; embedded networks; urban monitoring; environment monitoring; Internet of Things; smart transportation; social behavior modelling; social network analysis; social network mining; social media infrastructure; social media analytics; social intelligence; cryptography; data security; data privacy; trustworthy computing; social system design; social system architectures; information retrieval; data mining; artificial intelligence; agent-based technology; group interaction; mobile social computing; handheld social computing; collaborative filtering; sustainable computing; sustainable MPI; sustainable communications; Big Data intelligence; Big Data computing; service computing; cloud computing systems; and cloud computing architectures..

- 066 -

Spam detection of Twitter traffic: A framework based on random forests and non-uniform feature sampling.
Gianoglio, Christian - E-Mail:christian.gianoglio@edu.unige.it; Meda, Claudia - E-Mail:claudia.meda@edu.unige.it; Ragusa, Edoardo - E-Mail:edoardo.ragusa@edu.unige.it; Zunino, Rodolfo - E-Mail:rodolfo.zunino@unige.it; Ottaviano, Augusto; Scillia, Eugenio; Surlinelli, Roberto - E-Mail:roberto.surlinelli@poliziadistato.it
In: (2016) p 811-17 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ASONAM.2016.7752331

Law Enforcement Agencies cover a crucial role in the analysis of open data and need effective techniques to filter troublesome information. In a real scenario, Law Enforcement Agencies analyze Social Networks, i.e. Twitter, monitoring events and profiling accounts. Unfortunately, between the huge amount of internet users, there are people that use microblogs for harassing other people or spreading malicious contents. Users' classification and spammers' identification is a useful technique for relieve Twitter traffic from uninformative content. This work proposes a framework that exploits a non-uniform feature sampling inside a gray box Machine Learning System, using a variant of the Random Forests Algorithm to identify spammers inside Twitter traffic. Experiments are made on a popular Twitter dataset

and on a new dataset of Twitter users. The new provided Twitter dataset is made up of users labeled as spammers or legitimate users, described by 54 features. Experimental results demonstrate the effectiveness of enriched feature sampling method..

- 067 -

Toward understanding the cliques of opinion spammers with social network analysis.
Chih-Chien Wang - E-Mail:wangson@mail.ntpu.edu.tw; Min-Yuh Day - E-Mail:myday@mail.tku.edu.tw
In: (2016) p 1163-9 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ASONAM.2016.7752386
Consumer generated product reviews are considered as more persuasive than commercial advertising, and are now an important message source to make purchase decision. Nevertheless, firms may purposely hire spammers to create fake reviews to promote their products and to demote products of their competitors. To create the opinion majority, firms may hire a group of spammers rather than just one or few individual spammers to write fake reviewers. These spammers may act as a group to support other spammers to create a social consensus or majority of opinions. In the study, we attempt to adopt a real case to analyze the social network of spammers by K-core and Clique analysis. Our research results show that the social connection among spammers is stronger than that among non-spammers. Moreover, K-cores and cliques can be used as cues to identify spammers..

- 068 -

2016 Second International Conference on Science, Technology, Engineering and Management (ICONSTEM), Chennai, India, 30-31 March 2016.
anonym
In: 2016 (437 pp) Piscataway, NJ, USA: IEEE
The following topics are dealt with: wireless sensor networks; wireless mesh networks; Twitter; data storage systems; facial image spoofing; cloud environment; online social network; palmprint recognition; semantic Web services; pattern mining; Luo converter; power system transient stability; distribution system; reactive power dispatch; middleware; smart grid; mobile robot; cognitive radio; and data theft attacks..

- 069 -

Investigating Link Inference in Partially Observable Networks: Friendship Ties and Interaction.
Brandes, Ulrik - E-Mail:christophe.prieur@telecom-paristech.fr; Nasim, Mehwish - E-Mail:mehwish.nasim@uni-konstanz.de; Charbey, Raphael - E-Mail:ulrik.brandes@uni-konstanz.de; Prieur, Christophe - E-Mail:raphael.charbey@telecom-paristech.fr
In: IEEE Transactions on Computational Social Systems, USA * vol 3 (2016) no 3, p 113-19, 39 refs.
http://dx.doi.org/10.1109/TCSS.2016.2618998
While privacy preserving mechanisms, such as hiding one's friends list, may be available to withhold personal information on online social networking sites, it is not obvious whether to which degree a user's social behavior renders such an attempt futile. In this paper, we study the impact of additional interaction information on the inference of links between nodes in partially covert networks. This investigation is based on the assumption that interaction might be a proxy for connectivity patterns in online social networks. For this purpose, we use data collected from 586 Facebook profiles consisting of friendship ties (conceptualized as the network) and comments on wall posts (serving as interaction information) by a total of 64 000 users. The link-inference problem is formulated as a binary classification problem using a comprehensive set of features and multiple supervised learning algorithms. Our results suggest that interactions reiterate the information contained in friendship ties sufficiently well to serve as a proxy when the majority of a network is unobserved..

- 070 -

An energy efficient privacy-preserving content sharing scheme in mobile social networks.
Yingshu Li; Zaobo He; Zhipeng Cai - E-Mail:zcai@gsu.edu; Qilong Han - E-Mail:hanqilong@hrbeu.edu.cn; Weitian Tong; Limin Sun
In: Personal and Ubiquitous Computing, Germany * vol 20 (2016) no 5, p 833-46, 43 refs.
http://dx.doi.org/10.1007/s00779-016-0952-6
The rising popularity of mobile social media enables personalization of various content sharing and subscribing services. These two types of services entail serious privacy concerns not only to the confidentiality of shared content, but also to the privacy of end users such as their identities, interests and social relationships. Previous works established on the attribute-based encryption (ABE) can provide fine-grained access control of content. However, practical privacy-preserving content sharing in mobile social networks either incurs great risk of information leaking to unauthorized third parties or suffers from high energy consumption for decrypting privacy-preserving content. Motivated by these issues, this paper proposes a publish-subscribe system with secure proxy decryption (PSSPD) in mobile social networks. First, an effective self-contained privacy-preserving access control method is introduced to protect the confidentiality of the content and the credentials of users. This method is based on ciphertext-policy ABE and public-key

encryption with keyword search. After that, a secure proxy decryption mechanism is proposed to reduce the heavy burdens of energy consumption on performing ciphertext decryption at end users. The experimental results demonstrate the efficiency and privacy preservation effectiveness of PSSPD..

- 071 -

Twitter turing test: Identifying social machines.
Alarifi, Abdulrahman - E-Mail:aarifi@kacst.edu.sa; Alsaleh, Mansour - E-Mail:maalsaleh@kacst.edu.sa; Al-Salman, AbdulMalik - E-Mail:salman@ksu.edu.sa
In: Information Sciences, Netherlands * vol 372 (2016) p 332-46, 53 refs.
http://dx.doi.org/10.1016/j.ins.2016.08.036
Many machine-controlled Twitter accounts (also called 'Sybils') are created each day to provide services, flood out messages for astroturf political campaigns, write fake product reviews, or produce an underground marketplace for purchasing Twitter followers, retweets, or URL advertisements. In addition, fake identities and user accounts in online communities are resources used by adversaries to spread malware, spam, and harmful links over social networks. In social networks, Sybil detectors rely on the assumption that Sybils will find it harder to befriend real users; thus, Sybils that are connected to each other form strongly connected subgraphs, which can be detected using the graph theory. However, a majority of Sybils have actually successfully integrated themselves into real social media user communities (such as Twitter and Facebook). In this study, we compared the current methods used for detecting Sybil accounts. We also explored the detection features of various types of Twitter Sybil accounts in order to build an effective and practical classifier. To evaluate our classifier, we collected and manually labeled a dataset of Twitter accounts, including human users, bots, and hybrids (i.e., tweets posted by both human and bots). We consider that this Twitter Sybils corpus will help researchers to conduct high-quality measurement studies. We also developed a browser plug-in, which utilizes our classifier and warns the user about possible Sybil accounts before accessing or following them after clicking on a Twitter account. [All rights reserved Elsevier]..

- 072 -

If it looks like a spammer and behaves like a spammer, it must be a spammer: Analysis and detection of microblogging spam accounts.
Alabdulkareem, Ahmad - E-Mail:kareem@mit.edu; Alfaris, Anas - E-Mail:anas@mit.edu; Almaatouq, Abdullah - E-Mail:amaatouq@mit.edu; Pentland, Alex - E-Mail:pentland@mit.edu; Shmueli, Erez - E-Mail:shmueli@mit.edu; Singh, Vivek K. - E-Mail:singhv@mit.edu; Nouh, Mariam - E-Mail:mariam.nouh@cs.ox.ac.uk; Alarifi, Abdulrahman - E-Mail:aarifi@kacst.edu.sa; Alsaleh, Mansour - E-Mail:maalsaleh@kacst.edu.sa
In: International Journal of Information Security, Germany * vol 15 (2016) no 5, p 475-91, 59 refs.
http://dx.doi.org/10.1007/s10207-016-0321-5
Spam in online social networks (OSNs) is a systemic problem that imposes a threat to these services in terms of undermining their value to advertisers and potential investors, as well as negatively affecting users' engagement. As spammers continuously keep creating newer accounts and evasive techniques upon being caught, a deeper understanding of their spamming strategies is vital to the design of future social media defense mechanisms. In this work, we present a unique analysis of spam accounts in OSNs viewed through the lens of their behavioral characteristics. Our analysis includes over 100 million messages collected from Twitter over the course of 1 month. We show that there exist two behaviorally distinct categories of spammers and that they employ different spamming strategies. Then, we illustrate how users in these two categories demonstrate different individual properties as well as social interaction patterns. Finally, we analyze the detectability of spam accounts with respect to three categories of features, namely content attributes, social interactions, and profile properties..

- 073 -

Emerging threats abusing phone numbers exploiting cross-platform features.
Gupta, Srishti - E-Mail:srishtig@iiitd.ac.in
In: (2016) p 1339-41 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ASONAM.2016.7752410
Phone number, a unique identifier has emerged as an important Personally Identifiable Information (PII) in the last few years. Other PII like e-mail and online identity have been exploited in the past to launch phishing and spam attacks against them. The reach and security of a phone number provide a genuine advantage over e-mail or online identity, making it the most vulnerable attack vector. In this work, we explore the emerging threats that abuse phone numbers by exploiting cross-platform features. Given that phone number space hasn't been extensively studied in the past, there is a dire need to understand the threat landscape and develop solutions to prevent its abuse..

- 074 -

ClearView: data cleaning for online review mining.
Abu-El-Rub, Noor; Minnich, Amanda; Mueen, Abdullah; Gokhale, Maya; Minnich, Ronald
In: (2016) p 555-8 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ASONAM.2016.7752290
How can we automatically clean and curate online reviews to better mine them for knowledge discovery? Typical online reviews are full of noise and abnormalities, hindering semantic analysis and leading to a poor customer experience. Abnormalities include non-standard characters, unstructured punctuation, different/multiple languages, and misspelled words. Worse still, people will leave 'junk' text, which is either completely nonsensical, spam, or fraudulent. In this paper, we describe three types of noisy and abnormal reviews, discuss methods to detect and filter them, and, finally, show the effectiveness of our cleaning process by improving the overall distributional characteristics of review datasets..

- 075 -

Security frameworks for mobile cloud computing: A survey.
Bindagi, Gururaj - E-Mail:gururajnb@yahoo.com; Khanai, Rajashri - E-Mail:rajashri.khanai@gmail.com
In: (2016) p 2507-11 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICEEOT.2016.7755144
Cloud Computing is the long envisaged vision of computing as a utility. Innovative advances in hardware, networking, middleware, and virtual machine technologies have led to an emergence of new, globally distributed computing platforms, namely cloud computing. Cloud Computing provides computation facilities and storage as services accessible from anywhere via the Internet without investing in new infrastructure, training, or software licensing. In other words, Cloud Computing is a way to increase the capacity or add capabilities dynamically. The main advantage of Cloud Computing is that users only utilize what they require and only pay for what they really use. With an exponential growth of the mobile applications and evolution of cloud computing concept, Mobile Cloud Computing (MCC) has been presented as a potential technology for mobile services. MCC incorporates the cloud computing into the mobile environment. Mobile Cloud Computing refers to an infrastructure where data processing and storage can happen away from mobile device. Mobile Cloud Computing (MCC) has transformed the way in which mobile users across the globe leverage services on the go. The obstacles related to performance (e.g. battery life, storage, and bandwidth), environment (e.g. heterogeneity, scalability, availability) and security (e.g. reliability and privacy) are overcome by integrating cloud computing into the mobile environment using MCC. Mobile cloud is a service model, where a mobile device can use the cloud for information storage, searching, data mining and multimedia processing. Cloud Computing technology also brings forth many new challenges for data security and access control when users store sensitive data on cloud servers. As the users no longer have physical possession of the outsourced data, makes the data integrity, privacy and authenticity protection in Cloud Computing a very challenging and potentially difficult task. Though the Cloud Computing benefits are clear, surrendering physical possession of user data, inevitably poses new security risks. In this paper, we discuss Mobile Cloud Computing Security frameworks found in the literature related to Cloud Computing and its environment..

- 076 -

Renaissance system model improving security and third party auditing in cloud computing.
[02] Premalatha, J.
In: Wireless Personal Communications, Germany * vol 90 (2016) no 2, p 1051-66, 22 refs.
http://dx.doi.org/10.1007/s11277-016-3296-7
Cloud computing is the developing design of IT enterprise. Applications and the services that are present over the Internet are referred by the cloud computing. Critical issues on security and trust based are often a major problem in cloud computing. Different levels of security enforcement are offered by both public and private clouds. Auditing plays a vital role in evaluating an individual, process, system, product or an enterprise. A renaissance system model has been proposed for secure data storage in cloud. The proposed model involves four entities: Data owners, the cloud, cloud service provider and third party auditor (TPA). The TPA has the ability to create the awareness in order to bring out the public audits in the cloud having the coded data. The outcome seems to be trusted and is impartial for both the cloud servers and the data owners. The proposed model is a semi trusted proxy agent that performances instead of the data owner in order to reinstate the data blocks that are obtained during the repair process. Renaissance system model is proposed and implemented into the test bed..

- 077 -

A secure data outsourcing scheme based on Asmuth-Bloom secret sharing.
Kaiiali, Mustafa; Muhammad, Yusuf Idris - E-Mail:idrisawaa@gmail.com; Sani Ilyasu, Auwal; Habbal, Adib; Wazan, A. S.
In: Enterprise Information Systems, UK * vol 10 (2016) no 9, p 1001-23, 56 refs.
http://dx.doi.org/10.1080/17517575.2015.1120347
Data outsourcing is an emerging paradigm for data management in which a database is provided as a service by third-party service providers. One of the major benefits of offering database as a service is to provide organisations,

which are unable to purchase expensive hardware and software to host their databases, with efficient data storage accessible online at a cheap rate. Despite that, several issues of data confidentiality, integrity, availability and efficient indexing of users' queries at the server side have to be addressed in the data outsourcing paradigm. Service providers have to guarantee that their clients' data are secured against internal (insider) and external attacks. This paper briefly analyses the existing indexing schemes in data outsourcing and highlights their advantages and disadvantages. Then, this paper proposes a secure data outsourcing scheme based on Asmuth-Bloom secret sharing which tries to address the issues in data outsourcing such as data confidentiality, availability and order preservation for efficient indexing..

- 078 -

Searchable Encrypted Data File Sharing Method Using Public Cloud Service for Secure Storage in Cloud Computing.
[02] Raja, J. - E-Mail:s.t.jayamani@gmail.com
In: Wireless Personal Communications, Germany * vol 90 (2016) no 2, p 947-60, 20 refs.
http://dx.doi.org/10.1007/s11277-016-3273-1
Data owners are used to transmit the data using cloud computing in a low cost. The cloud computing is a popular technology to transmit the data through internet and will also act as third party users. Data owners outsource the data through the cloud server, which have to encrypt the data before outsourcing due to the security and privacy issues. After encrypting the data, users have to find out the respective data using the private key. All information has to be stored in the cloud storage unit. To optimize the cloud storage unit, safety transmission, minimize the cost and searching time, here we have proposed a new scheme as searchable encrypted data file sharing technique. This technique will allocate a keyword for every data during the encryption based on which the keyword matching will accept the data of respective users. The multi keyword search is been proposed for keyword searching. Experimental results analyze the overall performance and the proposed scheme has not only increased the efficiency but also decreased the searching time..

- 079 -

Efficient identity authentication and encryption technique for high throughput RFID system.
Ching-Hsien Hsu - E-Mail:chh@chu.edu.tw; Shangguang Wang; Daqiang Zhang; Hai-Cheng Chu; Ning Lu
In: Security and Communication Networks, USA * vol 9 (2016) no 15, p 2581-91, 32 refs.
http://dx.doi.org/10.1002/sec.1488
Radio Frequency Identification (RFID) technology provides a seamless link between physical world and the information system in cyber space. However, the emerging Internet of Things and cloud systems are full of security holes, which introduce new challenging security problems in both tag identification and data privacy. In this paper, we present efficient methods for identity authentication and data encryption to enhance RFID privacy. The proposed techniques aim to ensure no adversary interacting with the tags and the reader, to infer any information on a tag's identity from the communication. The main idea, a symmetric cryptography technique, termed as Advanced Encryption Standard, was applied to implement both mutual authentication and data encryption between the front and back ends of RFID systems. The Advanced Encryption Standard cryptographic algorithm was adopted because of its low hardware complexity and high security strength. In addition, the proposed key management protocol is proved resistant to several known RFID attacks such as Man-in-the-Middle, Denial-of-Service, replay, clone attack, and backward/forward traceability. The computational time complexity of the proposed scheme through the entire identity authentication and data encryption phases is 3T(sub encrypt) + 1T(sub nonce) + 4T(sub xor), which is superior to most existing approaches. The proposed scheme was also proved to be able to provide higher data encryption performance than other symmetric cryptographic algorithms with regard to the same level of security strength. Copyright (C) 2016 John Wiley & Sons, Ltd..

- 080 -

CloudMon: Monitoring Virtual Machines in Clouds.
Chuliang Weng - E-Mail:clweng@sei.ecnu.edu.cn; Qian Liu - E-Mail:liuqian@cert.org.cn; Kenli Li - E-Mail:lkl@hnu.edu.cn; Deqing Zou - E-Mail:deqingzou@hust.edu.cn
In: IEEE Transactions on Computers, USA * vol 65 (2016) no 12, p 3787-93, 33 refs.
http://dx.doi.org/10.1109/TC.2016.2560809
In the cloud platform, the startup security of guest virtual machines (VMs) can be guaranteed by existing techniques such as TBoot, however, how to monitor and guarantee their runtime security seems to be a non-trivial challenge, when they are exposed to the Internet. For a practical cloud system, security and performance are two important issues. In this paper, we propose a dynamic framework called CloudMon to detect kernel rootkits and guarantee the runtime security of guest VMs. CloudMon is transparent to a guest VM, neither requires its specific system information, nor has to one-on-one run with it. Meanwhile, CloudMon detects kernel rootkits through self-adjusting monitoring on memory with an acceptable overhead. A working prototype of CloudMon is implemented based on Xen. The case studies on security show that CloudMon is effective to detect kernel rootkits in guest VMs, while the performance experiments demonstrate that it brings a low performance overhead..

- 081 -

Data Security in Cloud computing and Outsourced Databases.
Pabboju, Suresh - E-Mail:plpsuresh@gmail.com; Sharma, K. Venkatesh - E-Mail:venkateshsharma.cse@gmail.com
In: (2016) p 2458-62 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICEEOT.2016.7755135
We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely distributed storage systems. It is also superior in performance by minimizing the use of expensive public-key cryptography in metadata management. We present the architecture and implementation of various SHAROES components and our experiments demonstrate performance superior to other proposals by over 40% on a number of benchmarks..

- 082 -

Cloud computing security in multi-clouds using Shamir's secret sharing scheme.
Pundkar, Sumedh N. - E-Mail:sumedh.pundkar@umit.sndt.ac.in; Shekokar, Narendra - E-Mail:narendra.shekokar@gmail.com
In: (2016) p 392-5 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ICEEOT.2016.7755427
In order to leverage a remote cloud based infrastructure, a company essentially gives away private data and information that might be sensitive and confidential to the service provider. Data Integrity and Confidentiality can be protected by using secret sharing schemes. To prevent service availability failure, multi-cloud data storage system can be implemented. In this paper, multimedia is protected using the Shamir's Secret Sharing in Multi-cloud Databases..

- 083 -

2016 4th International Symposium on Digital Forensics and Security (ISDFS), Little Rock, AR, USA, 25-27 April 2016.
anonym
In: 2016 (183 pp) Piscataway, NJ, USA: IEEE
The following topics are dealt with: cyber security; educational cloud computing environment; Android malware analysis; voice over IP traffic; wireless sensor networks; real time face recognition system; secure behavioral biometric authentication; phishing detection; SQL injection attacks; and digital image forensic authentication..

Internetsicherheit

- 084 -

Classification of News by Topic Using Location Data.
Dashdorj, Zolzaya; Khan, Muhammad Tahir; Bozzato, Loris; Lee, Sangkeun
In: Semantic Technology, JIST, Joint International Semantic Technology Conference, 6, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 10055 (2016) Seite 305-314 (10 Seiten), Paper-Nr. Chapter 23, Applications of Semantic Technologies
http://dx.doi.org/10.1007/978-3-319-50112-3_23
In this work, we will consider news articles to determine geo-localization of their information and classify their topics on the basis of an available open data source: OpenStreetMap (OSM). We propose a knowledge-based conceptual and computational approach that disambiguates place names (i.e., geo-objects and regions) mentioned in news articles in terms of geographic coordinates. The geo-located news articles are analyzed to identify local topics: we found that the mentioned geo-objects are a good proxy to classify news topics.

- 085 -

Fine-Grained Searchable Encryption over Encrypted Data in Multi-clouds.
Miao, Yinbin; Liu, Jiajia; Ma, Jianfeng
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 407-416 (10 Seiten), Paper-Nr. Chapter 40
http://dx.doi.org/10.1007/978-3-319-21837-3_40
Cloud computing has increased rapidly due to its abundant benefits in terms of low cost and accessability of data. Privacy protection and data security are two issues in cloud computing, as users often outsource sensitive information to honest-but-curious cloud storage providers (CSP). While encryption seriously obsoletes the traditional information retrieval over plaintext. Therefore, searchable encryption (SE) technology which allows the users to securely search over ciphertext through keywords and selectively retrieve files of interest becomes important. Dealing with single CSP is predicted to become less popular with cloud customers for fear of risks of single-point failure threat and potential malicious insiders. To tackle above problems, two schemes based on Identity-Based Encryption (IBE) and Key-Policy Attribute-Based Encryption (KP-ABE) are proposed in multi-clouds environment, respectively. Through rigorous security and performance analysis, both schemes can ensure security and reliability, and greatly reduce computational burden.

- 086 -

Online Popularity and Topical Interests through the Lens of Instagram.
Ferrara, Emilio; Interdonato, Roberto; Tagarelli, Andrea
In: HT, ACM Conference on Hypertext and Social Media, 25 * (2014) Seite 24-34 (11 Seiten, 50 Quellen) New York: ACM - Association for Computing Machinery
Online socio-technical systems can be studied as proxy of the real world to investigate human behavior and social interactions at scale. Here we focus on Instagram, a media-sharing online platform whose popularity has been rising up to gathering hundred millions users. Instagram exhibits a mixture of features including social structure, social tagging and media sharing. The network of social interactions among users models various dynamics including follower/followee relations and users' communication by means of posts/comments. Users can upload and tag media such as photos and pictures, and they can "like" and comment each piece of information on the platform. In this work we investigate three major aspects on our Instagram dataset: (i) the structural characteristics of its network of heterogeneous interactions, to unveil the emergence of self organization and topically-induced community structure; (ii) the dynamics of content production and consumption, to understand how global trends and popular users emerge; (iii) the behavior of users labeling media with tags, to determine how they devote their attention and to explore the variety of their topical interests. Our analysis provides clues to understand human behavior dynamics on socio-technical systems, specifically users and content popularity, the mechanisms of users' interactions in online environments and how collective trends emerge from individuals' topical interests.

- 087 -

PPSSER: Privacy-Preserving Based Scheduling Scheme for Emergency Response in Medical Social Networks.
Yu, Wenbin; Chen, Cailian; Yang, Bo; Guan, Xinping
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 715-724 (10 Seiten), Paper-Nr. Chapter 70
http://dx.doi.org/10.1007/978-3-319-21837-3_70
Mobile health monitoring, which can monitor the medical users' real-time physiology parameters, has been expected as an effective way to improve medical service quality and make response to the emergency. Unfortunately, it also risks the information privacy of both the medical users and the healthcare service providers when they upload their information. This paper is to propose a privacy-preserving based scheduling scheme for emergency response (PPSSER) to protect the privacy of the involved users when an emergency occurs. Moreover, the multi-dimensional region query method is introduced to conseal the personal health information and homomorphic encryption is used to protect the location and attribute privacy of the users. Finally, the simulation demonstrates the effectiveness and feasibility of the proposed scheme.

- 088 -

Secure and Verifiable Multi-owner Ranked-Keyword Search in Cloud Computing.
Li, Jinguo; Lin, Yaping; Wen, Mi; Gu, Chunhua; Yin, Bo
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 325-334 (10 Seiten), Paper-Nr. Chapter 32
http://dx.doi.org/10.1007/978-3-319-21837-3_32

To preserve the privacy of cloud data, sensitive files are always encrypted by data owners, which let the keyword search be more difficult to the crucial applications. Thus, a secure and efficient keyword search protocol over encrypted files is required. Most of the prior keyword search works over encrypted cloud files focus on single-data-owner settings. However, there are a large number of data owners involved in real applications. To retrieve user required files, single-owner keyword search schemes need to be repeated several times to search over files encrypted by different unique private keys, which is a very costly way. To achieve high efficiency and privacy preserving in multi-data-owner scenario, we propose a Secure and Verifiable Multi-owner Ranked-keyword Search protocol, named SVMRS, in this paper. Specifically, to preserve privacy and to improve the keyword search precision, we combine a modified asymmetric scalar-product encryption function with the TFtimesIDF rule. Furthermore, to preserve the integrity of search results, we extend the SVMRS based on circular bidirection-linked list, which can make the query result verifiable. Detailed analysis and experiments show that the SVMRS can preserve the file privacy and integrity, and confirms the high efficacy and efficiency of SVMRS.

- 089 -

Efficient and Decentralized Polling Protocol for General Social Networks.
Hoang, Bao-Thien; Imine, Abdessamad
In: Stabilization, Safety, and Security of Distributed Systems, SSS, International Symposium on Stabilization, Safety, and Security of Distributed Systems, 17, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9212 (2015) Seite 171-186 (16 Seiten), Paper-Nr. Chapter 12, Regular Papers
http://dx.doi.org/10.1007/978-3-319-21741-3_12

We address the polling problem in social networks where users want to preserve the confidentiality of their votes, obtain the correct final result, and hide, if any, their misbehaviors. Guerraoui et al. [15, 16] recently proposed polling protocols that neither rely on any central authority nor cryptography system. However, these protocols can be deployed safely and efficiently provided that the social graph structure should be transformed into a ring structure-based overlay and the number of participating users is a perfect square. Consequently, designing secure and efficient polling protocols regardless these constraints remains a challenging issue. In this paper, we present EPol, a simple decentralized polling protocol that is deployed on more general social graphs. More explicitly, we define a family of social graphs that satisfy what we call the m-broadcasting property (where m is not greater than the minimum node degree) and show their structures enable low communication cost and constitute necessary and sufficient condition to ensure vote privacy and limit the impact of dishonest users on the accuracy of the polling output. In a social network of N users with diameter D_g and $D \leq (m-1)D_g/2$ dishonest users (and similarly to the work [15, 16] where they considered D<*square root*(N)), a privacy parameter k enables us to obtain the following results: (i) the maximum probability of vote disclosure with certainty is $(D/N)^{k+1}$ and without certainty is (D/N/(1-2D/N)[1-*n-ary summation*$_{i=0}^{k} g_i(2D/N)^{2i+1}$], where g_i is the proportion of nodes voting for 2i+1 shares and $0 \leq i \leq k$; (ii) up to 2D votes can be revealed with certainty; (iii) the maximum impact on the final result is (6k+4)D, and the average impact is [(*n-ary summation*$_{i=0}^{k} g_i(2i+1)$(1+2*n-ary summation*$_{i=0}^{k} g_i(i+a)/(2i+1)+1$]D, where a is the proportion of users correctly voting; (iv) unlike [15, 16], EPol is effective to compute more precisely the final result; and (v) the communication and spatial complexities of EPol are close to be linear.

- 090 -

Secure Outsourced Frequent Pattern Mining by Fully Homomorphic Encryption.
Liu, Junqiang; Li, Jiuyong; Xu, Shijian; Fung, Benjamin C.M.
In: Big Data Analytics and Knowledge Discovery, DaWaK, International Conference on Big Data Analytics and Knowledge Discovery, 17, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 9263 (2015) Seite 70-81 (12 Seiten), Paper-Nr. Chapter 6, Data Mining
http://dx.doi.org/10.1007/978-3-319-22729-0_6

With the advent of the big data era, outsourcing data storage together with data mining tasks to cloud service providers is becoming a trend, which however incurs security and privacy issues. To address the issues, this paper proposes two protocols for mining frequent patterns securely on the cloud by employing fully homomorphic encryption. One protocol requires little communication between the client and the cloud service provider, the other incurs less computation cost. Moreover, a new privacy notion, namely a-pattern uncertainty, is proposed to reinforce the second protocol. Our scenario has two advantages: one is stronger privacy protection, and the other is that the outsourced data can be used in different mining tasks. Experimental evaluation demonstrates that the proposed protocols provide a feasible solution to the issues.

- 091 -

An Efficient and Secure Delegated Multi-authentication Protocol for Mobile Data Owners in Cloud.
Wei, Lifei; Zhang, Lei; Zhang, Kai; Dong, Mianxiong
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 612-622 (11 Seiten), Paper-Nr. Chapter 60
http://dx.doi.org/10.1007/978-3-319-21837-3_60

Due to plenty of cloud-based applications emerging and booming recently, data owners always store their data in cloud and share them to data consumers through cloud servers. For security equirements, data owners are often asked to provide authentication tags to the corresponding data. Data consumers obtain the authenticated data from the cloud and expect the computation on the authenticated data. However, it is impractical for the mobile data owners to be online all the time and provide the authenticated computing results according to various data consumers' request. To tackle this issue, we propose an efficient and secure delegated multi-authentication protocol for mobile data owners in cloud, which enables the mobile data owners to conditionally delegate signing right to specified cloud servers without exposing the secret signing keys. The cloud servers provide the authentication services when data owners are not available. The security is built on an identity-based multi-proxy signature (IBMPS) scheme, which depends on the cubic residue assumption, equaling to the factorization assumption. Furthermore, our protocol is efficient compared to the pairing based schemes and the overhead is almost independent of the number of cloud servers.

- 092 -

Multi-proxy Multi-signature Binding Positioning Protocol.
Chen, Huafeng; Xue, Qingshui; Li, Fengying; Zhang, Huajun; Cao, Zhenfu; Hou, Jianwen
In: Wireless Algorithms, Systems, and Applications, WASA, International Conference on Wireless Algorithms, Systems, and Applications, 10, in: Lecture Notes in Computer Science, Theoretical Computer Science and General Issues * Band 9204 (2015) Seite 9-18 (10 Seiten), Paper-Nr. Chapter 2
http://dx.doi.org/10.1007/978-3-319-21837-3_2

Position-based cryptography has attracted lots of researchers' attentions. In mobile Internet, there are many position-based security applications. For the first time, one new conception, multi-proxy multi-signature (MPMS) binding positioning protocol is proposed. Based on one secure positioning protocol, one model of MPMS binding positioning protocol is proposed. In the model, positioning protocol is bound to MPMS tightly, not loosely. Further, we propose one scheme of MPMS binding positioning protocol. As far as we know, it is the first scheme of MPMS binding positioning protocol.

- 093 -

On the Security of "Verifiable Privacy-Preserving Monitoring for Cloud-Assisted mHealth Systems".
Gajera, Hardik; Naik, Shruti; Das, Manik Lal
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 324-335 (12 Seiten), Paper-Nr. Chapter 17, Privacy
http://dx.doi.org/10.1007/978-3-319-49806-5_17

Protecting user data in public server is one of the major concerns in cloud computing scenarios. In recent trends, data owner prefers storing data in a third party server in a controlled manner, sometimes in an encrypted form. In this paper, we discuss a recent scheme [1] appeared in INFOCOM 2015 that claims verifiable privacy-preserving service in healthcare systems. We show that the scheme [1] suffers from security weaknesses, in particular, it does not provide privacy-preserving services, which is the main claim of the scheme. We provide an improved solution by slightly modifying the scheme, which retains the security and privacy claim intact without increasing any overhead.

- 094 -

Secure Lightweight User Authentication and Key Agreement Scheme for Wireless Sensor Networks Tailored for the Internet of Things Environment.
Jangirala, Srinivas; Mishra, Dheerendra; Mukhopadhyay, Sourav
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 45-65 (21 Seiten), Paper-Nr. Chapter 3, Authentication
http://dx.doi.org/10.1007/978-3-319-49806-5_3

In a wireless sensor networks (WSNs), there is a need of constant information access from the nodes, as the real-time data might never again be accessed. Thus, users are allowed to access the nodes in the real-time as and when required. The user authentication plays an indispensable part in this communication. Recently, Farash et al. proposed an efficient user authentication scheme for WSNs. Though their scheme is very efficient, we identify that their

scheme is vulnerable to off-line password guessing attack, off-line identity guessing attack, stolen smart card attack and user impersonation attack. As a result, we feel that there is a great need to improve Farash et al.'s scheme to present a secure communication protocol. In this paper, we propose a secure and lightweight user authentication and key agreement scheme for distributed WSN, which will also be handy in taking care of the Internet of Things (IoT). The lightweight property of our proposed scheme can be useful in resource-constrained architecture of WSNs. In addition, our scheme has merit to change dynamically the user's password locally without the help of the base station or gateway node. Furthermore, our scheme supports dynamic nodes addition, after the initial deployment of nodes in the existing sensor network. We prove the authentication property of our scheme using Burrows-Abadi-Needham (BAN) logic. The simulation results using the automated validation of internet security protocols and applications (AVISPA) tool shows the security of the proposed scheme against replay and man-in-the middle attacks.

- 095 -

Learning Detector of Malicious Network Traffic from Weak Labels.
Franc, Vojtech; Sofka, Michal; Bartos, Karel
In: Machine Learning and Knowledge Discovery in Databases, ECML PKDD, European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, 2015, in: Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence * Band 9286 (2015) Seite 85-99 (15 Seiten), Paper-Nr. Chapter 6, Part I - Industrial Track
http://dx.doi.org/10.1007/978-3-319-23461-8_6
We address the problem of learning a detector of malicious behavior in network traffic. The malicious behavior is detected based on the analysis of network proxy logs that capture malware communication between client and server computers. The conceptual problem in using the standard supervised learning methods is the lack of sufficiently representative training set containing examples of malicious and legitimate communication. Annotation of individual proxy logs is an expensive process involving security experts and does not scale with constantly evolving malware. However, weak supervision can be achieved on the level of properly defined bags of proxy logs by leveraging internet domain black lists, security reports, and sandboxing analysis. We demonstrate that an accurate detector can be obtained from the collected security intelligence data by using a Multiple Instance Learning algorithm tailored to the Neyman-Pearson problem. We provide a thorough experimental evaluation on a large corpus of network communications collected from various company network environments.

- 096 -

An Interface Theory for the Internet of Things.
Lohstroh, Marten; Lee, Edward A.
In: Collocated Workshops: ATSE, HOFM, MoKMaSD, and VERY*SCART, SEFM, International Conference on Software Engineering and Formal Methods, 13, in: Lecture Notes in Computer Science, Programming and Software Engineering * Band 9276 (2015) Seite 20-34 (15 Seiten), Paper-Nr. Chapter 2, Invited Papers
http://dx.doi.org/10.1007/978-3-319-22969-0_2
This paper uses interface automata to develop an interface theory for a component architecture for Internet of Things (IoT) applications. Specifically, it examines an architecture for IoT applications where so-called "accessors" provide an actor-oriented proxy for devices ("things") and services. Following the principles of actor models, an accessor reacts to input stimuli and produces outputs that can stimulate reactions in other accessors or actors. The paper focuses on a specialized form of actor models where inputs and outputs to accessors and actors are time-stamped events, enabling timing-sensitive IoT applications. The interaction between accessors and actors via time-stamped events forms a "horizontal contract," formalized in this paper as an interface automaton. The interaction between an accessor and the thing or service for which it is a proxy is a "vertical contract," also formalized as an interface automaton. Following common practice in network programming, our vertical contract uses an asynchronous atomic callback (AAC) pattern. The formal composition of these interface automata allows us to reason about the combination of a timed actor model and the AAC pattern, enabling careful evaluation of design choices for IoT systems.

- 097 -

Malware Detection Using Higher Order Statistical Parameters.
Arul, Easwaramoorthy; Manikandan, Venugopal
In: Digital Connectivity - Social Impact, CSI, Annual Convention of the Computer Society of India, 51, in: Communications in Computer and Information Science * Band 679 (2016) Seite 42-56 (15 Seiten), Paper-Nr. Chapter 4, Information Science
http://dx.doi.org/10.1007/978-981-10-3274-5_4
Malware holds an important place in system performance degradation and information embezzling from the victim system. Most of the malware writers choose their path to reach the victim system through the internet, infected browsers, injected files, memory devices, etc., highly obscured malwares evade the automated tools installed in the victim. Once the victim system gets affected by the malware, executable processes are controlled by malware. In this

paper, an algorithm has been developed to identify the malware using image processing. The malware detection process has three phases. In first phase, the files (.exe) are converted into a gray scale image. The binary values of corresponding files are converted into 8 - bit gray scale intensity value. The band pass frequency of gray scale image is computed in second phase. In the final phase, third and fourth order statistical parameter such as skewness and kurtosis are calculated at the each sub region of band pass frequency image. The region which has the highest skewness and kurtosis value is marked as the malware file. The detection performance of the proposed method has been evaluated by using 1300 portable executable files. The detection method has a true positive ratio of 93.33% with 0.1 false positives. Preliminary results indicate that the proposed algorithm is better than other conventional malware detection methods.

- 098 -

IT-Sicherheit auf Rädern.
IT security on wheels.
Hammerschmidt, Christoph
In: VDI-Nachrichten * Band 70 (2016) Heft 43, Seite 18 (1 Seite, Bilder)

Informationsflüsse vom Fahrzeug und zum Fahrzeug werden in Zukunft zunehmend eine wesentliche Rolle spielen und die gesamte Fahrzeugelektronik beeinflussen. Vernetzte Autos müssen aber eine ausreichende Datensicherheit aufweisen, um sie gegen Hackerangriffe und Datenspionage zu schützen. Das Thema IT-Security nahm auf der Eliv 2016 (Treffen der Elektronik- und Softwareentwickler) einen zentralen Platz ein. Der Halbleiterhersteller NXP entwarf ein Szenario für eine sichere Elektronikarchitektur in Fahrzeugen. Über die Einbindung in die Cloud-Strukturen von Fahrzeugherstellern und Dienstleistern holen sich Autos in Zukunft von außen nicht nur Daten in ihre Navigations- und Unterhaltungssysteme, sondern auch Rechenleistung. Es wird eine Functional Security als Ergänzung der Functional Safety erforderlich. Das bedeutet auch Absicherung der Fahrzeugelektronik durch sichere Authentifizierung auf der Ebene der Schnittstellen und der Datenbusse.

- 099 -

Formal Verification of a Cross-Layer, Trustful Space-Time Protocol for Wireless Sensor Networks.
Silva, Douglas Simoes; Resner, Davi; Souza, Rick Lopes de; Martina, Jean Everson
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 426-443 (18 Seiten), Paper-Nr. Chapter 23, Wireless, Mobile and IoT Security
http://dx.doi.org/10.1007/978-3-319-49806-5_23

In this paper we verify the security aspects of a cross-layer, application-oriented communication protocol for Wireless Sensor Networks (WSN). The Trustful Space-Time Protocol (TSTP) encompasses a majority of features recurrently needed by WSN applications like medium access control, geographic routing, location estimation, precise time synchronization, secure communication channels and a key distribution scheme between sensors and the sink. Key distribution in TSTP happens after deployment via time-based session keys. The key distribution scheme relies on public cryptography primitives and synchronous clocks as shared data between the parties. We analyzed TSTP's key distribution protocol using ProVerif and we were able to find two security flaws: one related to the time synchronization component and another being a bad approach related to a mac-then-encrypt method employed. With our findings we propose an improved version of the key distribution protocol, where we change the message authentication scheme in the initial message exchange so that ProVerif's goals are fulfilled; we also introduce the encrypt-then-mac method so that secret information passing through the communication channel has integrity and does not fall to known attacks.

- 100 -

Device Synchronisation: A Practical Limitation on Reader Assisted Jamming Methods for RFID Confidentiality.
Hu, Qiao; Dinca, Lavinia Mihaela; Hancke, Gerhard
In: Information Security Theory and Practice, WISTP, IFIP WG 11.2 International Workshop, Information Security Theory and Practice, 9, in: Lecture Notes in Computer Science * Band 9311 (2015) Seite 219-234 (16 Seiten), Paper-Nr. Chapter 14, Challenges of Security and Reliability
http://dx.doi.org/10.1007/978-3-319-24018-3_14

Radio frequency identification (RFID) is a core component of the Internet-of-Things. In certain cases the communication between the tag and the reader needs to be confidential. Some passive RFID tags have very limited computational power and can therefore not implement standard cryptographic mechanisms. This has led to several proposals where data sent by the RFID tag is 'hidden' by noisy signals generated by the RFID reader. The RFID reader can remove the noise but third-party adversaries cannot, thereby ensuring a confidential backward-channel for tag data without the need for cryptography. Although this is a promising research direction there are also some practical limitations on the effectiveness of such schemes. This paper shows that at least one recent scheme is vulnerable to data recovery despite varying the reader's transmission power if there is a slight difference in the phase of the reader's

blocking signal and the tag's data. We experimentally verify our attack and conclude that our eavesdropping and data recovery approach is effective and realistic. Finally we test three possible mitigation methods and show that two of the three approaches can provide protection against our attack while having little impact on the bit error rate of the reader in decoding the tag data.

- 101 -

Leveraging Behavior Diversity to Detect Spammers in Online Social Networks.
Cao, Jian; Fu, Qiang; Li, Qiang; Guo, Dong
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9530 (2015) Seite 323-336 (14 Seiten), Paper-Nr. Chapter 25, Service Dependability and Security in Distributed and Parallel Systems
http://dx.doi.org/10.1007/978-3-319-27137-8_25
Online social networks have become very popular and convenient for communication. However, spammers often take control of accounts to create and propagate attacks using messages and URLs. Most existing studies to detect spammers are based on machine learning methods. Features are the key factors considered in these methods, and most documented features in existing studies can be evaded by spammers. In this study, we propose behavior features, which are based on behavior diversity when sending messages, combined with existing effective features, to build a detection system. We leverage entropy to present differences in behavior diversity between spammers and normal accounts. In the cases of evasion by periodically changing a behavior model in the sending of messages by spammers, we also introduce conditional entropy, which is calculated based on the Markov model. To achieve our goal, we have collected information from approximately 489,451 accounts including 108,168,675 corresponding messages from Sina Weibo. Through evaluation of our detection methods, the accuracy rate of this system is approximately 91.5%, and the false positive rate is approximately 3.4%.

- 102 -

A Scheme to Manage Encrypted Data Storage with Deduplication in Cloud.
Yan, Zheng; Ding, Wenxiu; Zhu, Haiqi
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9530 (2015) Seite 547-561 (15 Seiten), Paper-Nr. Chapter 40, Service Dependability and Security in Distributed and Parallel Systems
http://dx.doi.org/10.1007/978-3-319-27137-8_40
Cloud computing offers a new way of service provision by re-arranging various resources and IT structures over the Internet. Private user data are often stored in cloud in an encrypted form in order to preserve the privacy of data owners. Encrypted data sharing introduces new challenges for cloud data deduplication. We found that existing solutions of deduplication suffer from high computation complexity and cost and therefore few of them can be really deployed in practice. In this paper, we propose a scheme to deduplicate encrypted data stored in cloud based on proxy re-encryption. We evaluate its performance and advantages based on extensive analysis and implementation. The results show the efficiency and effectiveness of the scheme for potential practical deployment.

- 103 -

Efficient Private Matching Scheme for Friend Information Exchange.
Qi, Fang; Wang, Wenbo
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9530 (2015) Seite 492-503 (12 Seiten), Paper-Nr. Chapter 36, Service Dependability and Security in Distributed and Parallel Systems
http://dx.doi.org/10.1007/978-3-319-27137-8_36
In the recent years, with the rapid development of social networks and mobile devices, mobile users can exchange the information and find the potential friends in vicinity through comparing the similarity degree between their personal attributes and make a connection via Wi-Fi/Bluetooth. The personal attributes, however, usually contain some private information, and users are not willing to reveal these to others in the process of friend discovery. In this paper, we proposed a novel efficient private matching scheme, which adopts an asymmetric scalar-preserving encryption according to the idea of k-nearest neighbor (kNN) queries. The personal profile of users will be processed in different ways, which is not recoverable. Moreover, our scheme relies on no Trusted Third Party (TTP). Detailed security and performance analysis demonstrate that our scheme can protect users' private information and resist outside attack during the matching process.

- 104 -

Practical Experiences on NFC Relay Attacks with Android. Virtual Pickpocketing Revisited.
Vila, Jose; Rodriguez, Ricardo J.
In: Radio Frequency Identification. Security and Privacy Issues, RFIDSec, International Workshop on Radio Frequency Identification: Security and Privacy Issues, 11, in: Lecture Notes in Computer Science * Band 9440 (2015) Seite 87-103 (17 Seiten), Paper-Nr. Chapter 6, RFID System Attacks
http://dx.doi.org/10.1007/978-3-319-24837-0_6

Near Field Communication (NFC) is a short-range contactless communication standard recently emerging as cashless payment technology. However, NFC has been proved vulnerable to several threats, such as eavesdropping, data modification, and relay attacks. A relay attack forwards the entire wireless communication, thus communicating over larger distances. In this paper, we review and discuss feasibility limitations when performing these attacks in Google's Android OS. We also perform an in-depth review of the Android implementation of the NFC stack. We show an experiment proving its feasibility using off-the-shelf NFC-enabled Android devices (i.e., no custom firmware nor root required). Thus, Android NFC-capable malicious software might appear before long to virtually pickpocket contactless payment cards within its proximity.

- 105 -

HCBE: Achieving Fine-Grained Access Control in Cloud-Based PHR Systems.
Liu, Xuhui; Liu, Qin; Peng, Tao; Wu, Jie
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9530 (2015) Seite 562-576 (15 Seiten), Paper-Nr. Chapter 41, Service Dependability and Security in Distributed and Parallel Systems
http://dx.doi.org/10.1007/978-3-319-27137-8_41

With the development of cloud computing, more and more users employ cloud-based personal health record (PHR) systems. The PHR is correlated with patient privacy, and thus research suggested to encrypt PHRs before outsourcing. Comparison-based encryption (CBE) was the first to realize time comparison in attribute-based access policy by means of the forward/backward derivation functions. However, the cost for encryption is linearly with the number of attributes in the access policy. To efficiently realize a fine-grained access control for PHRs in clouds, we propose a hierarchical comparison-based encryption (HCBE) scheme by incorporating an attribute hierarchy into CBE. Specifically, we construct an attribute tree, where the ancestor node is the generalization of the descendant nodes. The HCBE scheme encrypts a ciphertext with a small amount of generalized attributes at a higher level, other than lots of specific attributes at a lower level, largely improving the encryption performance. Furthermore, we encode each attribute node with the positive-negative depth-first (PNDF) coding. By virtue of the backward derivation function of the CBE scheme, the users associated with the specific attributes can decrypt the ciphertext encrypted with the generalized attributes, within the specified time. The experiment results show that the HCBE scheme has better performance in terms of the encryption cost, compared with the CBE scheme.

- 106 -

CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud.
Wang, Qian; Hu, Shengshan; Ren, Kui; He, Meiqi; Du, Minxin; Wang, Zhibo
In: Computer Security, ESORICS, European Symposium on Research in Computer Security, 20, in: Lecture Notes in Computer Science * Band 9327 (2015) Seite 186-205 (20 Seiten), Paper-Nr. Chapter 10, Cloud Security
http://dx.doi.org/10.1007/978-3-319-24177-7_10

Biometric identification has been incredibly useful in the law enforcement to authenticate an individual's identity and/or to figure out who someone is, typically by scanning a database of records for a close enough match. In this work, we investigate the privacy-preserving biometric identification outsourcing problem, where the database owner outsources both the large-scale encrypted database and the computationally intensive identification job to the semi-honest cloud, relieving itself from data storage and computation burden. We present new privacy preserving biometric identification protocols, which substantially reduce the computation burden on the database owner. Our protocols build on new biometric data encryption, distance-computation and matching algorithms that novelly exploit inherent structures of biometric data and properties of identification operations. A thorough security analysis shows that our solutions are practically-secure, and the ultimate solution offers a higher level of privacy protection than the-state-of-the-art on biometric identification outsourcing.We evaluate our protocols by implementing an efficient privacy-preserving fingerprint-identification system, showing that our protocols meet both the security and efficiency needs well, and they are appropriate for use in various privacy-preserving biometric identification applications.

- 107 -

A Middleware to Allow Fine-Grained Access Control of Twitter Applications.
Buccafurri, Francesco; Lax, Gianluca; Nicolazzo, Serena; Nocera, Antonino
In: Mobile, Secure, and Programmable Networking, MSPN, International Conference on Mobile, Secure and Programmable Networking, 2, in: Lecture Notes in Computer Science, Computer Communication Networks and Telecommunications * Band 10026 (2016) Seite 168-182 (15 Seiten), Paper-Nr. Chapter 14
http://dx.doi.org/10.1007/978-3-319-50463-6_14

Mobile applications security is nowadays one of the most important topics in the field of information security, due to their pervasivity in the people's life. Among mobile applications, those that interact with social network profiles, have a great potential for development, as they intercept another powerful asset of the today cyberspace. However, one of the problems that can limit the diffusion of social network applications is the lack of fine-grained control when an application use the APIs of a social network to access a profile. For instance, in Twitter, the supported access control policy is basically on/off, so that if a (third party) application needs the right to write in a user profile, the user is enforced to grant this right with no restriction in the entire profile. This enables a large set of security threats and can make (even inexpert) users reluctant to run these applications. To overcome this problem, we propose an effective solution working for Android Twitter applications based on a middleware approach. The proposed solution enables other possible benefits, as anomaly-based malware detection leveraging API-call patterns, and it can be extended to a multiple social network scenario.

- 108 -

PNSICC: A Novel Parallel Network Security Inspection Mechanism Based on Cloud Computing.
He, Jin; Dong, Mianxiong; Ota, Kaoru; Fan, Minyu; Wang, Guangwei
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9531 (2015) Seite 402-415 (14 Seiten), Paper-Nr. Chapter 28, Performance Modeling and Evaluation
http://dx.doi.org/10.1007/978-3-319-27140-8_28

As we all know, application firewall provides in-depth inspection to ensure application-layer security services, but brings a serious decline for network performance of application service, even more serious impact on service usability, worse, in the face of increasingly complex and diverse network application services that require an integrated network security protection, different types of application firewall collaborate together to ensure security use of integrated services, but multiple application firewalls lead to more serious performance problems than a single one. Recent efforts have provided a large number of optimization measures and algorithms, what is more, have offered a lot of new security architecture for application firewalls, unfortunately, most of them did not achieve the desired results. We have proposed a novel architecture that combines the characteristics of cloud computing, namely, parallel network security inspection Mechanism based on cloud computing (PNSICC) that is able to addresses performance problems for multiple intertwined application firewalls that protect network security of integrated service. PNSICC not only provides effective network security protections for the protected objects, but also has greatly improved security inspection efficiency. We have proved by experiments that our scheme is an effective and efficient method.

- 109 -

Nichts geht mehr. Aktuelle Situation zu Distributed-Denial-of-Service-(DDoS)-Angriffen.
Manske, Markus
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 5, Seite 59-63 (5 Seiten, Bilder, Tabellen)

Während interne Netze und Server durch verschiedene Security-Layer mehr oder weniger gut vor Angreifern geschützt sind, eröffnen sich über DDoS-Attacken für jedermann Methoden, um Unternehmen mit geringem Mitteleinsatz maximal zu schaden. Durch Trends wie das "Internet der Dinge" (IoT) oder Industrie 4.0 erhöht sich noch die Abhängigkeit von der IT, sodass Organisationen und sogar Einzelne noch leichter erpressbar werden. Unser Autor informiert über aktuelle Entwicklungen globaler DDoS-Bedrohungen.

- 110 -

DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare.
Mansfield-Devine, Steve
In: Network Security * Band 2016 (2016) Heft 11, Seite 7-13 (7 Seiten, 9 Quellen)
http://dx.doi.org/10.1016/S1353-4858(16)30104-0

In mid-October, a distributed denial of service (DDoS) attack hit the headlines in a big way. Targeting DNS service provider Dyn, it rendered a significant portion of the Internet inoperable and left many high-profile web services unreachable for several hours. But while this was arguably the most visible DDoS attack in history, it's only one among many. In this interview, Paul Nicholson, responsible for global product marketing and strategy at A10 Networks, talks about how DDoS is becoming an ever-growing threat and what organisations can do about it. We've just witnessed the biggest distributed denial of service (DDoS) attacks in history, which turned seemingly harmless devices such as

video recorders into cyber-weapons. With both the scale and frequency of attacks increasing, many organisations are left wondering how they can protect themselves and how those defences should be deployed, whether on-premise or in the cloud. In this interview with Paul Nicholson of A10 Networks, we examine how DDoS is becoming an ever-growing threat and what organisations can do about it.

- 111 -

A Modular Secure Framework Based on SDMN for Mobile Core Cloud.
Zkik, Karim; Tachihante, Tarik; Orhanou, Ghizlane; Hajji, Said El
In: Mobile, Secure, and Programmable Networking, MSPN, International Conference on Mobile, Secure and Programmable Networking, 2, in: Lecture Notes in Computer Science, Computer Communication Networks and Telecommunications * Band 10026 (2016) Seite 137-152 (16 Seiten), Paper-Nr. Chapter 12
http://dx.doi.org/10.1007/978-3-319-50463-6_12
During these last few years, mobile data traffic has been strongly growing while the voice traffic decreases (fixed and mobile), This new reality pushes operators to invest in a new next generation of mobile network (Mobile Cloud Computing, 5G) to enhance their competitivity and provide more innovative marketing products and services to the end user. But they were facing a major obstacle: the computer networks management is too complex and difficult. The research community proposes Software Defined Mobile Networks (SDMNs) as a solution to provide more flexibility and to ease the management of the next-generation mobile networks especially Mobile Cloud Computing (MCC). This new solution offers a huge advantage to the mobile operators and enables innovation through network programmability. SDMN provides several benefits including, network and service customized, improved operations and better performance, but there are some security issues that need to be taken care of. This paper describes the emergence of SDMN as an important new networking technology, discusses the different problems related to security issue. We propose a framework to secure the different levels in SDMN architecture with an implementation of our framework. A simulation has been done of some main threats such as DDoS attack and malware infection.

- 112 -

Fault Injection Attacks: Attack Methodologies, Injection Techniques and Protection Mechanisms. A Tutorial.
Bhasin, Shivam; Mukhopadhyay, Debdeep
In: Security, Privacy, and Applied Cryptography Engineering, SPACE, International Conference on Security, Privacy, and Applied Cryptography Engineering, 6, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10076 (2016) Seite 415-418 (4 Seiten), Paper-Nr. Chapter 24, Leakage, Power and Fault Analysis
http://dx.doi.org/10.1007/978-3-319-49445-6_24
Fault Injection Attacks are a powerful form of active attack mechanism which can threaten even the strongest of cryptographic algorithms. This attack vector has become more pertinent with the growing popularity of the Internet of things (IoT), which is based on small omnipresent embedded systems interacting with sensitive data of personal or critical nature. This tutorial addresses this issue of fault attacks, covering a wide range of topics which has accumulated through years of research. The first part of the talk will cover fault attacks and its application to attack standard cryptosystems. Different popular forms of fault attacks, namely Differential Fault Attacks (DFA) and Differential Fault Intensity Attacks (DFIA) are presented. It is followed subsequently by a discussion on the underlying injection techniques. Finally, protection mechanism will be discussed highlighting on information redundancy based reactive countermeasures and sensor-based protection mechanisms as two alternative strategies for security against the menacing fault attacks.

- 113 -

A Novel Search Engine-Based Method for Discovering Command and Control Server.
Guo, Xiaojun; Cheng, Guang; Pan, Wubin; Dinhtu, Truong; Liang, Yixin
In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9530 (2015) Seite 311-322 (12 Seiten), Paper-Nr. Chapter 24, Service Dependability and Security in Distributed and Parallel Systems
http://dx.doi.org/10.1007/978-3-319-27137-8_24
To solve the problem of getting command and control (C&C) server address covertly for malware of Botnet or advanced persistent threats, we propose a novel C&C-server address discovery scheme via search engine. This scheme is com-posed of five modules. The botmaster uses publish module to issue C&C-server IPs in diaries of several free blogs on Internet firstly. Then these diaries could be indexed by search engine (SE). When the infected terminal becomes a bot, it uses keyword production module to produce search keyword and submits some or all these keywords to SEs to obtain the search engine result pages (SERPs). For items in SERPs, the bot uses filtering algorithm to remove noise items and leave valid items whose abstract contain C&C-server IPs. Lastly the bot utilizes extraction and conversion module to extract these C&C-server IPs and translates them into binary format. The experimental results show that our proposed scheme is fully able to discover and obtain C&C-server IPs via various search engines. Furthermore, if we set proper threshold value for SE, it can extract C&C-server IPs accurately and efficiently.

- 114 -

Exploiting Group Signature to Implement User Authentication in Cloud Computing.
Ji, Sai; Liu, Dengzhi; Shen, Jian
In: Advances in Computer Science and Ubiquitous Computing, CSA & CUTE, CSA, International Conference on Computer Science and its Applications, 8, CUTE, International Conference on Ubiquitous Information Technologies and Applications, 11, in: Lecture Notes in Electrical Engineering * Band 421 (2017) Seite 323-331 (9 Seiten), Paper-Nr. Chapter 51, Part I - Advances in Information Technologies and Applications
http://dx.doi.org/10.1007/978-981-10-3023-9_51
Cloud computing is a technology which is developed from the distributed computing. The cloud server provider gathers the redundant storage and computing resource to realize the goal of providing scalable computing resources to consumers. The infrastructures of the cloud computing are virtualized and they can be considered infinite. Therefore, the user side does not need to consider the local storage and computing resource. However, the cloud services are provided by the third party. As a general rule, the user who stores the data in the cloud is not safe. The security of the data is really concerned by the user. In other words, the cloud is interested in the data. We proposed a scheme that can support cloud user's identity authentication, which is based on the group signature. From the security analysis, our scheme can resist some possible attacks.

- 115 -

A Security Model for Protecting Virtualization in Cloud Computing.
Park, Jong-Hyuk; Sharma, Pradip Kumar
In: Advances in Computer Science and Ubiquitous Computing, CSA & CUTE, CSA, International Conference on Computer Science and its Applications, 8, CUTE, International Conference on Ubiquitous Information Technologies and Applications, 11, in: Lecture Notes in Electrical Engineering * Band 421 (2017) Seite 385-388 (4 Seiten), Paper-Nr. Chapter 60, Part I - Advances in Information Technologies and Applications
http://dx.doi.org/10.1007/978-981-10-3023-9_60
Virtualization is the key component of cloud computing that refers to the abstraction of sharing resources. The basic idea is to implement the virtualization in cloud computing environment because of its flexibility, scalability, its cost-reducing and resource utilization. Instead of many good attributes virtualization still facing with security flaws like availability, mutual authentication, potential attack in the virtual network, DoS attack on virtual servers and storage also. In the paper, we propose a general security model to protect the virtual environment and also discuss the flow of data which is monitored by hypervisors.

- 116 -

Behavior-Based Detection for Malicious Script-Based Attack.
Yoon, Soojin; Choo, Hyun-lock; Bae, Hanchul; Kim, Hwankuk
In: Advances in Computer Science and Ubiquitous Computing, CSA & CUTE, CSA, International Conference on Computer Science and its Applications, 8, CUTE, International Conference on Ubiquitous Information Technologies and Applications, 11, in: Lecture Notes in Electrical Engineering * Band 421 (2017) Seite 97-103 (7 Seiten), Paper-Nr. Chapter 15, Part I - Advances in Information Technologies and Applications
http://dx.doi.org/10.1007/978-981-10-3023-9_15
Several DoS attacks have occurred through web browsers, not from malicious executable files. Most tools used in web attacks are downloaded malware. As the dynamic functions of HTML5 can be performed on a web browser, however, the latter can be abused as an attack tool. The features of web browser-based attacks are different from those of previous attacks, so a different detection method is needed for malicious behavior on web browsers. This paper introduces script-based attacks made through web browsers, and proposes a detection method based on a web browser's behavior.

- 117 -

Network Anomaly Detection Based on Probabilistic Analysis.
Park, Jinsoo; Choi, Dong-Hag; Jeon, You-Boo; Min, Se-Dong; Park, Doo-Soon
In: Advances in Computer Science and Ubiquitous Computing, CSA & CUTE, CSA, International Conference on Computer Science and its Applications, 8, CUTE, International Conference on Ubiquitous Information Technologies and Applications, 11, in: Lecture Notes in Electrical Engineering * Band 421 (2017) Seite 699-704 (6 Seiten), Paper-Nr. Chapter 107, Part II - Advances in Computer Science and Ubiquitous Computing
http://dx.doi.org/10.1007/978-981-10-3023-9_107
In this paper, we provide a detection technology for a common type of network intrusion (traffic flood attack) using an anomaly data detection method based on probabilistic model analysis. Victim's computers under attack show various symptoms such as degradation of TCP throughput, increase of CPU usage, increase of RTT (Round Trip Time), frequent disconnection to the web sites, and etc. These symptoms can be used as components to comprise k-dimensional feature space of multivariate normal distribution where an anomaly detection method can be applied for

the detection of the attack. These features are in general correlated one another. In other words, most of these symptoms are caused by the attack, so they are highly correlated. Thus we choose only a few of these features for the anomaly detection in multivariate normal distribution. We study this technology for those IoT networks prepared to provide u-health services in the future, where stable and consistent network connectivity is extremely important because the connectivity is highly related to the loss of human lives eventually.

- 118 -

"Not Some Trumped Up Beef": Assessing Credibility of Online Restaurant Reviews.
Kobayashi, Marina; Sosik, Victoria Schwanda; Huffaker, David
In: Human-Computer Interaction, INTERACT, IFIP TC 13 International Conference on Human-Computer Interaction, 15, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 9298 (2015) Seite 116-131 (16 Seiten), Paper-Nr. Chapter 9
http://dx.doi.org/10.1007/978-3-319-22698-9_9
Online reviews, or electronic word of mouth (eWOM), are an essential source of information for people making decisions about products and services, however they are also susceptible to abuses such as spamming and defamation. Therefore when making decisions, readers must determine if reviews are credible. Yet relatively little research has investigated how people make credibility judgments of online reviews. This paper presents quantitative and qualitative results from a survey of 1,979 respondents, showing that attributes of the reviewer and review content influence credibility ratings. Especially important for judging credibility is the level of detail in the review, whether or not it is balanced in sentiment, and whether the reviewer demonstrates expertise. Our findings contribute to the understanding of how people judge eWOM credibility, and we suggest how eWOM platforms can be designed to coach reviewers to write better reviews and present reviews in a manner that facilitates credibility judgments.

- 119 -

A Design of Key Agreement Scheme Between Lightweight Devices in IoT Environment.
Hague-Chung; Choi, Keun-Chang; Jun, Moon-Seog
In: Advances in Computer Science and Ubiquitous Computing, CSA & CUTE, CSA, International Conference on Computer Science and its Applications, 8, CUTE, International Conference on Ubiquitous Information Technologies and Applications, 11, in: Lecture Notes in Electrical Engineering * Band 421 (2017) Seite 224-229 (6 Seiten), Paper-Nr. Chapter 37, Part I - Advances in Information Technologies and Applications
http://dx.doi.org/10.1007/978-981-10-3023-9_37
The IoT (Internet of Things) environment develops in which all the necessary information among things is exchanged due to the development of information and communications. The home IoT continuously develops, because of a merit that a user can control the home IoT remotely in the IoT environment. As the home IoT environment is built, communications using low specification devices, as well as high specifications devices, also increase. For safety communications in the home IoT environment, encryption algorithms, such as RSA providing message encryption and authorization, are required. However, they are difficult to be used for the low specification devices, where calculation function is limited in the home IoT environment. This study actually proposes the protocol by which low power and low specification devices communicate with user's smart devices through safe authorization procedure in the home IoT environment. The protocol proposed in this paper has a merit that it is safe, and it protects the re-use attack and middle attack.

- 120 -

Identity in the Internet-of-Things (IoT): New Challenges and Opportunities.
Lam, Kwok-Yan; Chi, Chi-Hung
In: Information and Communications Security, ICICS, International Conference on Information and Communications Security, 18, in: Lecture Notes in Computer Science, Security and Cryptology * Band 9977 (2016) Seite 18-26 (9 Seiten), Paper-Nr. Chapter 2, IoT Security
http://dx.doi.org/10.1007/978-3-319-50011-9_2
From digitization to datafication, Internet-of-Things (IoT) plays an important role as enabler in the value creation process from big data. As is expected, security has naturally become one main concern in the IoT deployment. Due to the unique features and requirements of IoT, including limited compute resources, power, bandwidth and massive number of deployed IoT objects, and its loosely coupled networked architecture, new strategies and techniques are needed to provide feasible and practical solutions to IoT security. While substantial research efforts have been focusing on the lightweight communication protocols and cryptography/compression engines, one fundamental science question being asked is on the notion of "Identity in the Internet-of-Things" (or IDoT). In this paper, we would like to first explore the concept of IDoT and analyze why it is so unique as compared to the concept of "Identity of Users" (IDoU) in traditional networks and systems. Then we will survey on attribute-based, multi-factor authentication as an important approach to put this IDoT concept into practice. We will conclude this paper with open research issues in this direction.

- 121 -

A Study of Simple Classification of Malware Based on the Dynamic API Call Counts.
Kim, Jihun; Lee, SeungWon; Youn, Jonghee M.; Choi, Haechul
In: Advances in Computer Science and Ubiquitous Computing, CSA & CUTE, CSA, International Conference on Computer Science and its Applications, 8, CUTE, International Conference on Ubiquitous Information Technologies and Applications, 11, in: Lecture Notes in Electrical Engineering * Band 421 (2017) Seite 944-949 (6 Seiten), Paper-Nr. Chapter 147, Part II - Advances in Computer Science and Ubiquitous Computing
http://dx.doi.org/10.1007/978-981-10-3023-9_147

Recently, as the rapid development of the Internet enabled easy downloading of diverse files, the number of cases of file download from unreliable paths has been increasing. This situation is advantageous in that accessibility to information is improved while being disadvantageous in that there is no defense against exposure to malware. The present paper proposes a method of judging whether programs are malicious based on Cuckoo Sandbox, which is a dynamic malware analysis system and classify the programs by comparing malware programs collected and classified in advance based on the dynamic API call counts of the programs.

- 122 -

Image encryption using a synchronous permutation-diffusion technique.
Enayatifar, Rasul; Abdullah, Abdul Hanan; Isnin, Ismail Fauzi; Altameem, Ayman; Lee, Malrey
In: Optics and Lasers in Engineering * Band 90 (2017) Seite 146-154 (9 Seiten, 37 Quellen)
http://dx.doi.org/10.1016/j.optlaseng.2016.10.006

In the past decade, the interest on digital images security has been increased among scientists. A synchronous permutation and diffusion technique is designed in order to protect gray-level image content while sending it through internet. To implement the proposed method, two-dimensional plain-image is converted to one dimension. Afterward, in order to reduce the sending process time, permutation and diffusion steps for any pixel are performed in the same time. The permutation step uses chaotic map and deoxyribonucleic acid (DNA) to permute a pixel, while diffusion employs DNA sequence and DNA operator to encrypt the pixel. Experimental results and extensive security analyses have been conducted to demonstrate the feasibility and validity of this proposed image encryption method.

- 123 -

A Full-Text Retrieval Algorithm for Encrypted Data in Cloud Storage Applications.
Song, Wei; Cui, Yihui; Peng, Zhiyong
In: Natural Language Processing and Chinese Computing, NLPCC, CCF Conference on Natural Language Processing and Chinese Computing, 4, in: Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence * Band 9362 (2015) Seite 229-241 (13 Seiten), Paper-Nr. Chapter 20, NLP for Search Technology and Ads
http://dx.doi.org/10.1007/978-3-319-25207-0_20

Nowadays, more and more Internet users use the cloud storage services to store their personal data, especially when the mobile devices which have limited storage capacity popularize. With the cloud storage services, the users can access their personal data at any time and anywhere without storing the data at local. However, the cloud storage service provider is not completely trusted. Therefore, the first concern of using cloud storage services is the data security. A straightforward method to address the security problem is to encrypt the data before uploading to the cloud server. The encryption method is able to keep the data secret from the cloud server, but cloud server also can not manipulate the data after encryption. It will greatly undermine the advantage of the cloud storage. For example, a user encrypts his personal data before uploading them to the cloud. When he wants to access some data at the cloud, he has to download all the data and decrypt them. Obviously, this service mode will incur the huge overheads of communication and computation. Several related works have been proposed to enable the search over the encrypted data, but all of them only support the encrypted keyword search. In this paper, we propose a new full-text retrieval algorithm over the encrypted data for the scenario of cloud storage, in which all the words in a document have been extracted and built a privacy-preserved full-text retrieval index. Based on the privacy-preserved full-text retrieval index, cloud server can execute full-text retrieval over the large scale encrypted documents. The numerical analysis and experimental results further validate the high efficiency and scalability of the proposed algorithm.

- 124 -

A Novel Proxy Re-Encryption with Keyword Search.
Meng, Xian-Yong; Chen, Zhong; Meng, Xiang-Yu
In: Information Technology Applications in Industry III, ICITMI, International Conference on Information Technology and Management Innovation, 3, in: Applied Mechanics and Materials * Band 631-632 (2014) Seite 897-901 (5 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.631-632.897
http://www.scientific.net/AMM.631-632.897

In this paper, a novel proxy re-encryption (PRE) scheme with keyword search is proposed, where only the ciphertext containing the keyword set by the delegator can be transformed by the semi-trusted proxy and then decrypted by delegatee. In the proposed scheme, the semi-trusted proxy can convert the ciphertext encrypted under the delegator's public key into the ciphertext encrypted under the delegatee's public key. In addition, only the delegatee's email gateway with a trapdoor can test whether or not a given cipheretext containing some keyword, but can learn nothing else about the sensitive data of email. We proposed an identity-based proxy re-encryption with keyword search scheme, where the delegator and the delegatee extract keys from a trusted party called the key generator center (KGC), who generates public-private key pair for delegator and delegatee based on their identities. Meanwhile, the identity-based proxy re-encryption with keyword search scheme satisfies the properties of PRE including unidirectionality, multi-use and transparency. Additionally, the proposed scheme is efficient in terms of both computation and communication, and can realize security privacy preserving in cloud computing environments.

- 125 -

A phish detector using lightweight search features.
Varshney, Gaurav; Misra, Manoj; Atrey, Pradeep K.
In: Computers & Security * Band 62 (2016) Seite 213-228 (16 Seiten, 41 Quellen)
http://dx.doi.org/10.1016/j.cose.2016.08.003

Web phishing is a well-known cyber-attack which is used by attackers to obtain vital information such as username, password, credit card number, social security number, and/or other credentials from Internet users via deception. A number of web phishing detection solutions have been proposed and implemented in the recent years. These solutions include the use of phishing black list, search engine, heuristics and machine learning, visual similarity techniques, DNS, access list and proactive phishing URLs detection based techniques. However, the current solutions are quite heavy in terms of their computational and communication requirements. Most of these solutions are dependent on third parties and require dedicated servers for their operation. It has been observed that search engine based solutions are the most lightweight and viable. This paper advances search engine based antiphishing research and presents the lightest possible phishing detection system, named the Lightweight Phish Detector (LPD). The LPD can run on client browsers for phishing detection. The development of LPD was done using the Google Chrome browser. Exhaustive testing has been performed to evaluate its accuracy and effectiveness. Comparisons are performed with currently available search engine based antiphishing approaches and other approaches that are currently used by popular browsers such as Chrome, Firefox, Internet Explorer, Netcraft toolbar and Cascaded Phish Detector. For testing, phishing sites reported from the Phishtank and normal sites available from Alexa ranking are used in the experiments. A true negative rate varying from 92.4% to 100% was obtained from the Alexa dataset of normal URLs while a true positive rate of 99.5% was recorded from the Phishtank URLs. Results show that the proposed scheme is very accurate. A competitive response time and intelligent action-response mechanism makes LPD a fast and intelligent antiphishing solution.

- 126 -

COBIT Evaluation as a Framework for Cloud Computing Governance.
Hafiddi, Hatim; Bounagui, Yassine; Mezrioui, Abdellatif
In: International Journal of Cloud Applications and Computing (IJCAC) * Band 6 (2016) Heft 4, Seite 65-82 (18 Seiten, 29 Quellen)
http://dx.doi.org/10.4018/IJCAC.2016100104

The present paper aims at providing an approach for evaluating COBIT as a base framework for cloud computing governance. For that purpose, the authors firstly conducted a systematic research reviews to identify, analyze, and structure the main cloud computing governance requirements. Secondly, with respect to the systematic research review, a mapping of COBIT control objectives to the corresponding cloud computing governance requirements is proposed. Thirdly, the evaluation of the mapped control objectives against the cloud computing governance requirements is performed to identify and analyze the framework gaps. The paper results are relevant outcomes for the extension of COBIT processes and capabilities and thus can provide a base framework for building a holistic cloud computing governance approach.

- 127 -

An Identity-Based Conditional Proxy Re-Encryption in Cloud Computing Environments.
Meng, Xian-Yong; Chen, Zhong; Meng, Xiang-Yu; Sun, Bing
In: Computers and Information Processing Technologies I, ICCIPT, International Conference on Computers and Information Processing Technologies, 2014, in: Applied Mechanics and Materials * Band 571-572 (2014) Seite 74-78 (5 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.571-572.74
http://www.scientific.net/AMM.571-572.74

In this paper, an identity-based conditional proxy re-encryption (PRE) scheme is proposed, where a delegator provides a re-encryption key satisfying one condition to a semi-trusted proxy who can convert a ciphertext encrypted under the delegator's public key into one that can be decrypted using the delegatee's private key. We address the identity-based proxy re-encryption scheme, where the delegator and the delegatee request keys from a trusted party known as a key generator center (KGC), who generates private keys for delegator and delegatee based on their identities. Meanwhile, the identity-based conditional proxy re-encryption scheme satisfies the properties of PRE including unidirectionality, non-interactivity and multi-hop. Additionally, the identity-based conditional proxy re-encryption scheme is efficient in terms of both the communication cost and the computing cost, and can realize security secret sharing in cloud computing environments.

- 128 -

Smarte Sensoren - aber bitte ohne Kabel! Wie sich klassische 4...20 mA-Architektur für Regelkreise und drahtlose Netzwerke für smarte Sensoren ergänzen.
Merlin, Tilo; Xu, Chaojun
In: atp edition. Automatisierungstechnische Praxis * Band 58 (2016) Heft atp+ plus: Smart Sensors, Seite 72-76 (5 Seiten, Bilder, 3 Quellen)
http://dx.doi.org/10.17560/atp.v58i01-02.554

Zur Erweiterung der festverdrahteten 4...20 mA-Infrastruktur in der Prozessindustrie durch neue intelligente (smarte) Sensoren wird die drahtlose Anbindung durch WirelessHART vorgeschlagen. Der WirelessHART-Standard zeichnet sich durch folgende sechs Vorteile aus: (1) Weltweite Standardisierung in lizenzfreien Frequenzbändern, (2) Interoperabilität zwischen Geräten und Gateways verschiedener Hersteller, (3) einheitliche Schnittstellen, (4) etablierte Gerätetreiber (EDD, DTM, FDI) für systemweite Konfiguration und Diagnose, (5) vermaschte, hochverfügbare Netzwerkstruktur mit leistungsfähiger Verschlüsselung und (6) Zertifizierbarkeit für die Anwendung im explosionsgefährdeten Bereich bis in die Zone 0. Zur integrierten Energieversorgung steht, als Alternative zur Batterie, das Energy Harvesting zur Verfügung, beispielsweise durch die Nutzung der Temperaturunterschiede zwischen Medium und Umgebung. Wenn ein WirelessHART-Gateway auch etablierte Protokolle wie Modbus unterstützt, steht eine leistungsfähige 'sekundäre' Infrastruktur zur Verfügung zur Anlagenüberwachung, Prozessbeobachtung und Prozessoptimierung sowie der zustandsorientierten Instandhaltung. Die Einbindung von internetbasierten Lösungen wie Industrie 4.0 oder Cloud ist möglich. Für Anwendungen stellt ABB eine Reihe von drahtlosen Druck- und Temperaturfühlern mit optionalem Energy Harvesting vor. Der Temperaturfühler TSP300-W ist der erste Temperaturfühler mit integrierter Energieversorgung für die Zone 0. Vibrations- und Temperatursensoren mit WirelessHART vernetzt, liefern die Daten für die zustandsorientierte Instandhaltung bei rotierenden Maschinen. Bei Pumpen, beispielsweise deuten sich Ausfälle frühzeitig durch zunehmende Vibrationen und Temperaturerhöhung an. Leicht lassen sich WirelessHART-Netzwerke durch andere smarte-Temperatur-, Druck- oder Füllstandssenoren erweitern. Diese passen sich automatisch ab und stellen ihre Daten im Firmennetz oder einem Industrie-4.0-Netz zur Verfügung.

- 129 -

The Design and Implementation of a Hot Switch Isolation Circuit Card.
Wen, Quan-Gang
In: Advanced Manufacturing and Information Engineering, Intelligent Instrumentation and Industry Development, ICPMIMT, International Conference on Precision Mechanical Instruments and Measurement Technology, 2, in: Applied Mechanics and Materials * Band 602-605 (2014) Seite 2807-2810 (4 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.602-605.2807
http://www.scientific.net/AMM.602-605.2807

To protect the security of critical data and application system, generally, many companies or departments use a parallel way of intranet and internet. Because every kind of security technology has its limitations, traditional security products such as firewall, VPN, data encryption, intrusion detection and network vulnerability scanning can not completely solve various security problems in information exchange between different networks. It is not able to meet all the security needs of critical networks and security data with the general products only. The way of data exchange of most of the existing products of "GAP" is mainly logic isolation. This paper describes a design and implementation of a hot switch circuit card in way of physical isolation. The data exchange mode of this circuit card is a half-duplex which can physically completely isolate intranet and internet. Through functional test and performance test, we can draw a conclusion that the circuit card can effectively achieve our demand of data exchange between different networks.

- 130 -

Smarte Überwachung. Mobilfunkgestützte Videoanlagen im Praxiseinsatz.
Pannarale, Simon
In: Protector & WIK, München * Band 44 (2016) Heft 11, Seite 26-27 (2 Seiten, Bilder)

Sollen kleinere Filialien, abseits gelegene Lagerhallen oder Agrarbetriebe vollständig aus der Ferne videoüberwacht werden, scheitert dies oft an einem zu geringen Upstream des dortigen Internetanschlusses. IP-Kameras benötigen in 720p-Auflösung und einer Bildfrequenz von 12 Bildern pro Sekunde eine Bandbreite von etwa 7,3 Megabit. Selbst bei VDSL mit zehn Megabit Upstream würde fast die gesamte Bandbreite von einer einzigen Kamera belegt. Mit steigenden Bandbreiten wird das LTE-Netz auch für die Videoüberwachung zunehmend interessant. Benötigt wird dazu ein geeigneter Mobilfunktarif. Auch ist für die Anlage ein Outdoor-LTE-Router erforderlich. Im Headquarter wird darüber hinaus eine VPN-Firewall benötigt. Die Konfiguration ist so auszulegen, daß VPN-Tunnel zu den Filialien aufrechterhalten beziehungsweise bei einer Unterbrechung von der Filialie aus automatisch neu initiiert wird. Die Auswahl der Kamera ist immer von der jeweiligen Überwachungsaufgabe abhängig. Bei einer Mobilfunklösung sind jedoch weitere Kriterien zu berücksichtigen: Auflösung kostet Bandbreite und Datenkontingent. Ferner sollen die Kameras mehrere Videostreans parallel ausliefern können, einen für die Aufzeichnung in bester Qualität, weitere datenreduzierte Streams für die Remote-Aufzeichnung oder Liveansichten. Wilkon liefert die benötigte Hardware, übernimmt die Integration in bestehende IT-Infrastrukturen und bietet auf Wunsch auch Video-Hosting-Lösungen.

- 131 -

Security für Produktionsanlagen. Industrial Security im Spannungsfeld zwischen Anlagenbauer und Betreiber.
Müller, Siegfried
In: PC & Industrie - Fachzeitschrift für Mess-, Steuer- und Regeltechnik * Band 21 (2017) Heft 1/2, Seite 84-86 (3 Seiten, Bilder) Marburg: beam-Verlag

Security war lange Zeit nur ein Problem der klassischen IT. Spätestens seit Stuxnet ist klar, dass auch Produktionsanlagen und Automatisierungssysteme gefährdet sind. Allerdings sind die klassischen Security- Konzepte nicht mit der Automatisierungswelt kompatibel. Die zunehmende Digitalisierung, auch im Hinblick auf Industrie 4.0, sorgt dafür, dass die Informations- und die Automatisierungstechnik immer mehr verschmelzen. Regelmäßige Meldungen über versuchte Denial-of-Service-Angriffe (DoS), gestohlene Kreditkartendaten oder manipulierte Finanztransaktionen treiben daher berechtigte Sorgenfalten auf die Stirn der Verantwortlichen. Soll nun jedoch eine Vernetzung und Fernwartung stattfinden, ist eine Lösung gefordert, welche sowohl den Anforderungen der IT als auch der Automatisierungstechnik entspricht. Als nicht akzeptabel gelten Konzepte, bei denen über das Internet von außen auf Maschinen oder Anlagen zugegriffen werden soll. Dieser Ansatz würde zu einem erheblichen technisch- administrativen Aufwand führen. Für jedes zusätzlich installierte Gerät müsste die Konfiguration der Firewall manuell angepasst werden. Neben dem Arbeitsaufwand muss auch das Sicherheitsrisiko betrachtet werden. Bei der manuellen Konfiguration der Firewall ist schnell ein Fehler passiert, der die Schutzfunktion beeinträchtigen kann. Industrielle Sicherheit umfasst nicht nur den sicheren Betrieb von Maschinen und Anlagen im Sinne von gefährdungs- und unfallfrei, sondern auch den Schutz von Know-how und die Sicherstellung der Systemintegrität. Das beginnt mit einer Segmentierung der Netzwerke in einzelne Automatisierungszellen und setzt sich darin fort, die Datenzugriffe nur einem begrenzten Teilnehmerkreis zugänglich zu machen. Was in diesem Zusammenhang oft unterschätzt wird, ist die Bedrohung von innen. Etwa dadurch, dass Mitarbeiter Downloads von kompromittierten Internetseiten oder E-Mails machen - oder Schadsoftware von USB-Sticks mit unklarer Herkunft einschleusen. Industrial Security ist keine rein technische Angelegenheit. Auch organisatorische Umstände und der Faktor Mensch spielen eine wichtige Rolle. Allgemein bekannte Abteilungspasswörter müssen ebenso der Vergangenheit angehören wie die kleinen gelben Haftnotizen, welche die Passwörter für jedermann zugänglich machen. Die Anforderungen an Qualifikationen und Ausbildung der Mitarbeiter werden steigen. Während im Produktionsumfeld und in der Automatisierungsrungstechnik grundlegende Kenntnisse in Sachen Security erforderlich sind, werden sich Verantwortliche der IT-Sicherheit, wie der Chief Information Security Officer (CISO), mit den Anforderungen der Produktionstechnik befassen müssen. Und nicht zuletzt muss dem Management klar sein, dass es Industrial Security nicht zum Nulltarif geben kann.

- 132 -

A DDoS Detection and Mitigation System Framework Based on Spark and SDN.
Yan, Qiao; Huang, Wenyao
In: Smart Computing and Communication, SmartCom, International Conference on Smart Computing and Communication, 1, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 10135 (2017) Seite 350-358 (9 Seiten), Paper-Nr. Chapter 35
http://dx.doi.org/10.1007/978-3-319-52015-5_35

Distributed Denial of Service (DDoS) attack is a serious threat to commercial service network. DDoS attack has been studied for years. However, detecting and relieving DDoS attacks are still a problem. Especially, nowadays more and more DDoS attacks produce heavy network traffic, it is hard to response rapidly because that needs high processing performance to process massive traffic data. With big data technology, volumes of network traffic data can be processed much faster. Apache Spark can process a great amount of data in a reasonable time so that DDoS attack can be detected in time. Besides, it is difficult to modify the network configuration in traditional network. With Software-Defined Networking (SDN), a new paradigm in networking, networking can be controlled by programs, which makes modifying the network configuration easier. In this paper, a DDoS detection and mitigation system framework in SDN

is introduced, a framework that can control network based on analyzing the network traffic data. Comparing to the traditional defense methods of DDoS attack, the framework can response to DDoS attack by rules automatically.

- 133 -

Akademisch und vernetzt.
Böhme, Uwe; Tesch, Silke
In: Nachrichten aus der Chemie * Band 64 (2016) Heft 12, Seite 1180-1184 (5 Seiten, 2 Bilder)
http://dx.doi.org/10.1002/nadc.20164053034
In den letzten Jahren entstanden neue Portale, Communities und Online-Tools, welche die Kommunikation in allen Phasen der wissenschaftlichen Arbeit erleichtern. Was sind Nutzen und Risiken dieser wissenschaftlichen Netzwerke? Die Einstiegshürden akademischer sozialer Netzwerke sind niedrig: Anmeldung und Nutzung sind gratis, die Nutzer benötigen kaum technische Kenntnisse. Vorteile sind Kontakte, aktuelle Informationen und die Möglichkeit, Kooperationspartner oder Arbeitsstellen zu finden. Ein Nachteil: Persönliche Daten werden zu Ware, eine Folge sind mehr Spam-E-Mails. Solange es mehr als ein akademisches soziales Netzwerk gibt, ist es schwierig, bestimmte Wissenschaftler zu finden. Denn diese legen häufig nur bei einem Anbieter ein Profil an.

- 134 -

A Secure Device and Service Discovery Protocol for Proximity Based Social Networks (PBSNs).
Mocktoolah, Asslinah; Askoolum, Krishiv; Khedo, Kavi Kumar
In: Emerging Trends in Electrical, Electronic and Communications Engineering, ELECOM, International Conference on Electrical, Electronic and Communications Engineering, 1, in: Lecture Notes in Electrical Engineering * Band 416 (2017) Seite 272-282 (11 Seiten), Paper-Nr. Chapter 24, Communication Engineering and Computing
http://dx.doi.org/10.1007/978-3-319-52171-8_24
Technical advances of Online Social Networking (OSN) have promoted new types of social interactions such as Proximity Based Social Networking (PBSN) where proximate users interact with each other using their mobile devices. However, personal details users share on these networks are not secured and messages exchanged are prone to different attacks and eavesdropping. Qualcomm introduces AllJoyn, which eases the development of such applications discovering with nearby devices and establishing a secure communication. In this paper, a secure device and service discovery protocol is introduced leveraging the AllJoyn framework. It allows mobile users to perform secure device advertising and discovery, authentication, encryption and decryption of exchanged messages. The security and performance of the proposed architecture are thoroughly analyzed and evaluated by using penetration tools and scenarios. Results showed that exchanged messages could not be captured and the system is not prone to attacks such as man-in-the-middle attacks.

- 135 -

FMPC: A Fast Multi-Dimensional Packet Classification Algorithm.
Guo, Zhen-Hong; Li, Lin; Wang, Qing; Lin, Meng; Pan, Rui
In: Machine Tool Technology, Mechatronics and Information Engineering, ICMTTME, International Conference on Machine Tool Technology and Mechatronics Engineering, 2014, in: Applied Mechanics and Materials * Band 644-650 (2014) Seite 3365-3370 (6 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.644-650.3365
http://www.scientific.net/AMM.644-650.3365
With the rapid development of the Internet, the number of firewall rules is increasing. The enormous quantity of rules challenges the performance of the packet classification that has already become a bottleneck in firewalls. This dissertation proposes a rapid and multi-dimensional algorithm for packet classification based on BSOL(Binary Search On Leaves), which is named FMPC(FastMulti-dimensional Packet Classification). Different from BSOL, FMPC cuts all dimensions at the same time to decompose rule spaces and stores leaf spaces into hash tables; FMPC constructs a Bloom Filter for every hash table and stores them into embedded SRAM. When classifying a packet, FMPC performs parallel queries on Bloom Filters and determines how to visit hash tables according to the results. Algorithm analysis and the result of simulations show: the average number of hash-table lookups of FMPC is 1 when classifying a packet, which is much smaller than that of BSOL; inthe worst case, the number of hash-table lookups of FMPCisO($\log(w_{max})$+1), which is also smaller than that of BSOL in multi-dimensional environment, where w_{max} is the length, in bits, of the dimension whose length is the longest..

- 136 -

An Improved Ciphertext-Policy Attribute-Based Encryption Scheme.
Zheng, Hua; Zhang, Xi; Yang, Qi
In: Smart Computing and Communication, SmartCom, International Conference on Smart Computing and Communication, 1, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 10135 (2017) Seite 400-411 (12 Seiten), Paper-Nr. Chapter 41
http://dx.doi.org/10.1007/978-3-319-52015-5_41
According to characteristics of mass encryption service in cloud storage, this paper proposed an improved SCP-OOABE scheme which uses the access control tree as a control structure and decomposes key generation and encryption into online and offline phase respectively that could be finished in a short time in online phase. In addition, it also avoids the problem that CP-OOABE scheme can't generate keys when constructing access control structures. What's more, it meets the demand of the complex access control structure in cloud storage and was proved that the scheme is against chosen-plaintext attack secure. In a word, our scheme was security, efficient and universal, which suits for the demands of cloud storage.

- 137 -

uKeMa: An Ultra-Lightweight Key Management and Authentication Scheme for Wearable Ad Hoc Networks Based on Body Language.
Xie, Yin-Hui
In: Mechatronics and Industrial Informatics II, ICMII, International Conference on Mechatronics and Industrial Informatics, 2, in: Applied Mechanics and Materials * Band 596 (2014) Seite 986-989 (4 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.596.986
http://www.scientific.net/AMM.596.986
Wearable consumer electronics such as Google glasses, Apple iWatch, Nike Shoes have been envisioned as next consuming hot spot. It invokes a large amount of applications in the personal healthy, personal safety, and digital entertainment. To save power consumption, those wearable devices usually connect to Internet via a smart phone that performs as a gateway. To avoid unauthorized access from unfriendly devices, it is desirable to encrypt the personal data in the communications of wearable devices. Therefore, the keys for encryption and integrity are required. In this paper, we make the first attempt to solve both key management and authentication together for wearable devices in an ultra-lightweight manner. We propose a scheme called uKeMa that can provide key generation, key updating and authentication for wearable devices with ultra-lightweight power consumption.

- 138 -

The Study of a Fingerprint Encryption Code Model.
Jia, Yo-Bo; Liu, Dan-Li; Ding, Qian-Qian; Zhang, Jian-Feng; Zhang, Yun-Long
In: Frontiers of Manufacturing Science and Measuring Technology IV, ICFMM, International Conference on Frontiers of Manufacturing Science and Measuring Technology, 4, in: Applied Mechanics and Materials * Band 599-601 (2014) Seite 1781-1784 (4 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.599-601.1781
http://www.scientific.net/AMM.599-601.1781
This paper introduces the present situation of the two-dimensional code and problems in two-dimensional code in the process of development, and discusses the security problem of two-dimensional code decoding information, then proposes a human fingerprint encryption algorithm based on two-dimensional code model. The realization of the model results not only improve the safety of two-dimensional code information, but also develop a broader space for the development of two-dimensional code in the future. In recent years, the intelligent mobile phone of popularization provides a solid foundation for the development of two-dimensional code software function. The application of two-dimensional code has changed the traditional mode of the Internet users by using URL to browse and download. This way combine with the traditional value-added service, and bring convenience for people's life. However, due to usually adopt open mode, people did not centralized management and control of it, therefore the personal information in two dimensional code was decoded easily, and the safety of two-dimensional code information becomes an important aspect of new value-added service application of two-dimensional code.

- 139 -

Attribute-Based and Keywords Vector Searchable Public Key Encryption.
Wang, Huiwen; Li, Jianqiang; Yang, Yanli; Ming, Zhong
In: Smart Computing and Communication, SmartCom, International Conference on Smart Computing and Communication, 1, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 10135 (2017) Seite 317-326 (10 Seiten), Paper-Nr. Chapter 32
http://dx.doi.org/10.1007/978-3-319-52015-5_32

Nowadays, for third-party cloud platforms are not fully trustable, in order to ensure data security and user privacy when storing data on cloud servers, many enterprises and users choose to store their data in the ciphertext form. So it is essential to search the needed cryptographic information in the cloud servers. In this paper, we proposed public key encryption module based on the attributes-multi keyword vector. Firstly, we adopt the prime order bilinear pairings method to improve time efficiency. Secondly, we introduced the attribute and keywords vector to optimize the vector encryption algorithm. Finally, considering conditions of the limited resources, we proposed the storage domain differentiation policy to save the computing resources and improve efficiency. In order to verify the result of this module, we built up a system based on jPBC, a Java class library. The result shows that the system can achieve the strict access control and multi-user shared fast search mechanism. In the future, it will be applied to the new medical cloud scenes.

- 140 -

A Secure Homomorphic Encryption Algorithm over Integers for Data Privacy Protection in Clouds.
Yeh, Jyh-Haw
In: Smart Computing and Communication, SmartCom, International Conference on Smart Computing and Communication, 1, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 10135 (2017) Seite 111-121 (11 Seiten), Paper-Nr. Chapter 12
http://dx.doi.org/10.1007/978-3-319-52015-5_12

If a secure and efficient fully homomorphic encryption algorithm exists, it should be the ultimate solution for securing data privacy in clouds, where cloud servers can apply any operation directly over the homomorphically encrypted ciphertexts without having to decrypt them. With such encryption algorithms, clients' data privacy can be preserved since cloud service providers can operate on these encrypted data without knowing the content of these data. Currently only one fully homomorphic encryption algorithm proposed by Gentry in 2009 and some of its variants are available in literature. However, because of the prohibitively expensive computing cost, these Gentry-like algorithms are not practical to be used to securing data in clouds. Due to the difficulty in developing practical fully homomorphic algorithms, partially homomorphic algorithms have also been studied in literature, especially for those algorithms homomorphic on arithmetic operations over integers. This paper presents a secure variant algorithm to an existing homomorphic algorithm over integers. The original algorithm allows unlimited number of arithmetic additions and multiplications but suffers on a security weakness. The variant algorithm patches the weakness by adding a random padding before encryption. This paper first describes the original algorithm briefly and then points out it's security problem before we present the variant algorithm. An efficiency analysis for both the original and the variant algorithms will be presented at the end of the paper.

- 141 -

An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing.
Hu, Jin-Xin; Chen, Chin-Ling; Fan, Chun-Long; Wang, Kun-hao; Ji, Hai-Feng
In: Journal of Sensors * Band 2017 (2017) Seite 1-11 (11 Seiten, 20 Quellen)
http://dx.doi.org/10.1155/2017/3734764

Internet of Things (IoT) is the network of physical objects where information and communication technology connect multiple embedded devices to the Internet for collecting and exchanging data. An important advancement is the ability to connect such devices to large resource pools such as cloud. The integration of embedded devices and cloud servers offers wide applicability of IoT to many areas of our life. With the aging population increasing every day, embedded devices with cloud server can provide the elderly with more flexible service without the need to visit hospitals. Despite the advantages of the sensor-cloud model, it still has various security threats. Therefore, the design and integration of security issues, like authentication and data confidentiality for ensuring the elderly's privacy, need to be taken into consideration. In this paper, an intelligent and secure health monitoring scheme using IoT sensor based on cloud computing and cryptography is proposed. The proposed scheme achieves authentication and provides essential security requirements.

- 142 -

PHR in Cloud Environment Using Enhanced Attribute Based Encryption and Advanced Encryption Standard.
Sivakumar, T.B.; Geetha, S.
In: Advancements in Automation and Control Technologies, ICAAC, International Conference on Advancements in Automation and Control, 2014, in: Applied Mechanics and Materials * Band 573 (2014) Seite 588-592 (5 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.573.588
http://www.scientific.net/AMM.573.588
Personal Health Record is internet based application that enables individuals to access and coordinates their womb-to-tomb health data. The patients have management over access to their own PHR. To attain security of non-public health records, we have a tendency to use the attribute based secret writing to write in code to inform before out-sourcing it. Here we have a tendency to specialize in multiple forms of PHR owner situation and division of non-public health records users into multiple security domains that cut back key management complex for house owners and users. A high degree of patient's privacy is secured. Our theme offer a personal health record owner full management of his/her information. In depth security and performance analysis shows that the projected theme is very economical.

- 143 -

A mobile sensing method to counteract social media website impersonation.
ELMassry, Mohamed Y.; Almogren, Ahmad S.
In: International Journal of Distributed Sensor Networks * Band 12 (2016) Heft 10 (Seiten, 19 Quellen)
http://dx.doi.org/10.1177/1550147716671265
Phishing is a serious threat to online users, especially since attackers have tremendously improved their techniques in impersonating important websites. With websites looking visually the same, users are fooled more easily. Visual similarity algorithms may help to detect and counteract some phished websites. Through similarity algorithms, the phishers play with the colors and visual properties of the website in a way that cannot be noticed by the users. However, the phishers make the unnoticed changes to fool the similarity algorithms as well. In this article, we propose an efficient phishing website detection algorithm using three-step checking. The performance results are compared to the state-of-the-art approaches that show new kinds of phishing warnings with better outcomes and less false positives. Our approach provides similar accuracy to the blacklisting methods with the advantage that it can easily classify the phishing websites with less overhead and without being victimized.

- 144 -

Preeminent System for Detecting Venomous Banking Sites in Online Business.
Sudharsan, N.S.; Latha, K.
In: Advancements in Automation and Control Technologies, ICAAC, International Conference on Advancements in Automation and Control, 2014, in: Applied Mechanics and Materials * Band 573 (2014) Seite 519-522 (4 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.573.519
http://www.scientific.net/AMM.573.519
. Phishing has become most notorious security issues in online real time web pages. Many studies and ideas have been proposed related to phishing attack in order to overcome the security issues. Phishing attack can be easily done by Uniform resource locator (URL) obfuscation. It is the trick where the user will be forwarded to fake web page which has look and feel effect as the original web page when they click through the fake link. Organizations which use online business and transaction like ebay, paypal use many preventive approaches like blacklist, whitelist of URL in order to prevent any online theft using phishing attack. This paper propose a novel idea for detecting Phishing attack by checking the URL patterns of the suspected page with generated legitimate common URL pattern by inspecting different international URL patterns of that particular banking site.

- 145 -

Are you The One to Share? Secret Transfer with Access Structure.
Zhao, Yongjun; Chow, Sherman S.M.
In: Proceedings on Privacy Enhancing Technologies * Band 2017 (2017) Heft 1, Seite 149-169 (21 Seiten, 48 Quellen) Warsaw: De Gruyter Open
http://dx.doi.org/10.1515/popets-2017-0010
Sharing information to others is common nowadays, but the question is with whom to share. To address this problem, we propose the notion of secret transfer with access structure (STAS). STAS is a twoparty computation protocol that enables the server to transfer a secret to a client who satisfies the prescribed access structure. In this paper, we focus on threshold secret transfer (TST), which is STAS for threshold policy and can be made more expressive by using linear secret sharing. TST enables a number of applications including a simple construction of oblivious transfer (OT) with threshold access control, and (a variant of) threshold private set intersection (t-PSI), which are the first of

their kinds in the literature to the best of our knowledge. The underlying primitive of STAS is a variant of OT, which we call OT for a sparse array. We provide two constructions which are inspired by state-of-the-art PSI techniques including oblivious polynomial evaluation (OPE) and garbled Bloom filter (GBF). The OPEbased construction is secure in the malicious model, while the GBF-based one is more efficient. We implemented the latter one and showed its performance in applications such as privacy-preserving matchmaking.

- 146 -

Research and Implementation of Relational Database Encryption Technology Based on Main Memory Database.
Xu, Yong-Kang; Wan, Zheng-Jing; Zhang, Ji-Lan; Wu, Jia-ju
In: Computers and Information Processing Technologies I, ICCIPT, International Conference on Computers and Information Processing Technologies, 2014, in: Applied Mechanics and Materials * Band 571-572 (2014) Seite 591-599 (9 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.571-572.591
http://www.scientific.net/AMM.571-572.591
As the relational database is applied widely, how to protect the sensitive data and state secrets has become a problem which needs to be solved urgently. The conventional relational database encryption technology not only reduces the system's performance, but also results that we can not quickly inquire the encryption data through the original index mechanism due to the loss of the original partial order relation among data. This paper proposes a kind of relational database encryption technology based on the main memory database. It has not only realized the transparent encryption, decryption and ciphertext storage of the relational database, but also still retained the original response and retrieval performance. This technical proposal has very strong adaptability as well as strong practice guidance meaning for protecting the internet business data and the war-industry informative state secrets.

- 147 -

A Survey of Discriminating Distributed DoS Attacks from Flash Crowds.
Rao, N. Srihari; Sekharaiah, K.Chandra; Rao, A. Ananda
In: SmartCom, International Conference on Smart Trends for Information Technology and Computer Communications, 1, in: Communications in Computer and Information Science * Band 628 (2016) Seite 733-742 (10 Seiten), Paper-Nr. Chapter 88
http://dx.doi.org/10.1007/978-981-10-3433-6_88
The Internet is becoming part and parcel of everyone in everyday life. Almost all people are depending heavily on the Internet for all types of online activities. Hence, many Information Technology (IT) companies and organizations do business with people or enable businesses for people by running and/or supporting online web services continuously and try to attain or guarantee continuous service availability. From the old and recent bitter experiences of web servers with Distributed DoS (DDoS) attacks, one can realize that they become a serious threat to web site's availability. Along similar lines, flash crowds also prove to be damaging to web servers by losing business, if not properly discriminated from DDoS attacks and handled well. In this context, the task of differentiating the DDoS attacks from the flash crowds gets more significance and hence, we carried out an extensive survey over this. We analysed numerous existing approaches and compared important features used for discrimination.

- 148 -

SG-PASS: A Safe Graphical Password Scheme to Resist Shoulder Surfing and Spyware Attack.
Panda, Suryakanta; Mondal, Samrat
In: Intelligent Human Computer Interaction, IHCI, International Conference on Intelligent Human Computer Interaction, 8, in: Lecture Notes in Computer Science, Information Systems and Applications, incl. Internet/Web, and HCI * Band 10127 (2017) Seite 27-38 (12 Seiten), Paper-Nr. Chapter 3, Intelligent Interfaces
http://dx.doi.org/10.1007/978-3-319-52503-7_3
In general, it is difficult to remember a strong password i.e. a long and random password. So, the common tendency of a user is to select a weak alphanumeric password that is easy to remember. But the password which is easy to remember is also easy to predict. In contrast, the password that is very difficult to predict or requires more computation to break is also difficult to remember. To overcome this limitation of creating secure and memorable passwords, researchers have developed graphical password scheme which takes images as passwords rather than alphanumeric characters. But graphical password schemes are vulnerable to shoulder-surfing attack where an attacker can capture a password by direct observation. In this paper a graphical password scheme, namely SG-PASS is proposed which can prevent the shoulder-surfing attack by a human observer and also spyware attack, using a challenge response method.

- 149 -

Daten- und Anlagenintegrität: IT-Forensik schützt vor Cyberangriffen.
Kroll, Lars
In: P&A : Prozesstechnik & Automation * Band 13 (2016) Heft 9, Seite 24-26 (3 Seiten)

Bisher wurde in der fertigenden Industrie unter dem Begriff Sicherheit vor allem Betriebssicherheit verstanden. Im Industrie-4.0-Zeitalter liegt ein mindestens genauso hohes Gewicht auf der Integrität der Daten und Anlagen. Um sie zu schützen, sollten Unternehmen auf ein umfassendes IT-Sicherheitssystem setzen. Ein wichtiger Baustein ist hier die IT-Forensik. Industrielle Anlagen und Produktionsstätten geraten verstärkt ins Visier von Cyberkriminellen. Mehr als zwei Drittel der Industrieunternehmen in Deutschland sind in den vergangenen zwei Jahren Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden. Das ergab eine aktuelle Umfrage des Bitkom. Dabei ereigneten sich die kriminellen Vorfälle am häufigsten in der Produktion. In der Vergangenheit waren Produktionsstätten autarke Maschinenkomplexe, die abgekoppelt vom Unternehmensnetzwerk agierten. Mit der zunehmenden Digitalisierung der Produktion und der Vernetzung von Maschinen über das Internet entstehen neue Einfallstore, die nicht nur Datendiebstahl, sondern auch den Zugriff auf Maschinen und Produktionsketten ermöglichen. Für produzierende Unternehmen bedeutet das, der Aspekt der Informationssicherheit muss in jeder Phase des Lebenszyklus einer Produktionsstätte berücksichtigt werden. Sinnvoll ist eine Art Komplettpaket, das sowohl den Schutz der Anlage vor äußeren und inneren Angriffen, als auch ausdefinierte Handlungspläne für den Fall eines Datenverlustes oder anderen Zwischenfalls einschließt. Mithilfe streng methodischer, forensischer Verfahren können - ähnlich wie in der Kriminalistik - verdächtige Vorfälle im Zusammenhang mit IT-Systemen untersucht und digitale Spuren ausgewertet werden. Die Ergebnisse liefern wichtige Hinweise für notwendige Prozesse und Handlungsspielräume, um zukünftige Attacken einzudämmen. Wichtig hierbei ist es zu verstehen, wie der identifizierte Cyberangriff funktionierte, welches Ziel er verfolgte und welche Kollateralschäden die Attacke verursacht hat. Produzierende Unternehmen können aus dem Ablauf eines Angriffs zahlreiche Rückschlüsse ziehen. Anhand der bei einer Cyber-Attacke genutzten Malware lässt sich zum Beispiel das Angriffsmuster der Schadsoftware analysieren und daraus eine mögliche Abwehr konstruieren. Dazu empfiehlt sich der Einsatz unternehmenseigener SIEM-Systeme (Security Information and Event Management). Diese sammeln Informationen aus den einzelnen IT-Komponenten, etwa Log-Daten, und stellen mögliche Zusammenhänge her. Sollten sie verdächtige Aktivitäten bemerken, schlagen sie umgehend Alarm.

- 150 -

Digital Music Copyright Protection Engineering Based on Encryption and Digital Watermarking.
Xu, Changkai; Du, Jiagang; Xiao, Jinlin; Sun Wei
In: GCN, International Conference on Green Communications and Networks, 3, in: WIT Transactions on Information and Communication Technologies * Band 54 (2014) Seite 355-361 (7 Seiten, 7 Quellen) Southampton: WIT Press

This paper presents two fast and robust schemes for compressed music format and MIDI format based on encryption and digital watermark, which are suitable for online distribution through Internet. For compressed music, then presents a method for controlling usage and protecting against copying of digital music contents and their associated players, at the end of this paper summarizes the effects of the two technologies for digital music copyright protection.

- 151 -

Using proxies to calculate the carbon impact of investment into electricity network assets.
Daniels, Laura; Coker, Phil; Gunn, Alice; Potter, Ben
In: Applied Energy * Band 162 (2016) Seite 551-560 (10 Seiten, 49 Quellen)
http://dx.doi.org/10.1016/j.apenergy.2015.10.111

Replacement and upgrading of assets in the electricity network requires financial investment for the distribution and transmission utilities. The replacement and upgrading of network assets also represents an emissions impact due to the carbon embodied in the materials used to manufacture network assets. This paper uses investment and asset data for the GB system for 2015-2023 to assess the suitability of using a proxy with peak demand data and network investment data to calculate the carbon impacts of network investments. The proxies are calculated on a regional basis and applied to calculate the embodied carbon associated with current network assets by DNO region. The proxies are also applied to peak demand data across the 2015-2023 period to estimate the expected levels of embodied carbon that will be associated with network investment during this period. The suitability of these proxies in different contexts are then discussed, along with initial scenario analysis to calculate the impact of avoiding or deferring network investments through distributed generation projects. The proxies were found to be effective in estimating the total embodied carbon of electricity system investment in order to compare investment strategies in different regions of the GB network.

- 152 -

Sicherheitsrisiko Schokolade.
Vollmuth, Jan
In: Die Früchte von Vernetzung und Digitalisierung * (2016) Heft Jubiläumsschrift, Seite 22-24 (3 Seiten, Bilder) Würzburg: Vogel

Intelligente und vernetzte Produktionsanlagen sollen der deutschen Industrie die Zukunft sichern. Doch damit steigt auch die Verletzlichkeit von Unternehmen und kritischen Infrastrukturen durch Cyberattacken - die sich zunehmend menschliche Schwächen zunutze machen. Die Top-5-Bedrohungen: (1) Social Engineering und Phishing: Betrügerische E-Mails sollen Mitarbeiter verleiten, Anhänge mit Schadsoftware zu öffnen. (2) Einschleusen von Schadsoftware über externe Hardware wie etwa USB-Sticks. (3) Infektion mit Schadsoftware über Intra- und Internet - die heute in Unternehmen verbreitete Verbindung zwischen Office-Netz und Anlagensteuerung erleichtert Angriffe. (4) Einbruch über Fernwartungszugänge - diese werden häufig nicht ausreichend geschützt. (5) Menschliches Fehlverhalten und Sabotage, etwa falsch konfigurierte Software oder Manipulation der Firewall. Wer sind die potenziellen Angreifer? Laut Bitkom-Studie in den meisten Fällen aktuelle oder ehemals Beschäftigte der betroffenen Unternehmen (65 Prozent), gefolgt von Kunden, Lieferanten oder Dienstleistern - oft mit Insiderkenntnissen - (rund 30 Prozent) sowie von Wettbewerbern (16 Prozent). "Unternehmen sollten ihren Mitarbeitern nicht misstrauen, sondern eine Sicherheitskultur etablieren, die das Bewusstsein für den Schutz des Betriebs schärft." Ebenso wichtig sei es, die technische IT-Sicherheit zu steigern, etwa durch spezielle Systeme für die Erkennung und Abwehr von Angriffen, und die organisatorische Sicherheit zu erhöhen: Dazu gehören unter anderem Regelungen, wer im internen Netzwerk auf welche Daten zugreifen darf und wer Zutritt zu sensiblen Bereichen eines Unternehmens bekommt.

- 153 -

Efficient Remote User Authentication Technique for Internet Based Applications Using Keystroke Dynamics.
Neha; Chatterjee, Kakali
In: SmartCom, International Conference on Smart Trends for Information Technology and Computer Communications, 1, in: Communications in Computer and Information Science * Band 628 (2016) Seite 881-888 (8 Seiten), Paper-Nr. Chapter 105
http://dx.doi.org/10.1007/978-981-10-3433-6_105

Now-a day's remote users can get the benefit of different services from different servers using the internet. In such multi-server environment, one major security drawback is to identify the legitimate remote user of a web service on the internet. Traditional two factor authentication technique is vulnerable to, password guessing attack, stolen verifier attack, man-in-the-middle attack, etc. To eliminate this security problem, biometric authentication is essential. Keystroke dynamics, one of the behavioural biometric features can be used for remote user authentication. In this paper, a three factor based remote user authentication protocol has been proposed which uses keystroke dynamics as a third factor with two other previous factors. This authentication protocol will use machine learning techniques which results low false acceptance rate (FAR), false rejection rate (FRR) and low equal error rate (ERR).

- 154 -

eDAAAS: Efficient distributed anonymous authentication and access in smart homes.
Braeken, An; Porambage, Pawani; Stojmenovic, Milos; Lambrinos, Lambros
In: International Journal of Distributed Sensor Networks * Band 12 (2016) Heft 12 (Seiten, 30 Quellen)
http://dx.doi.org/10.1177/1550147716682037

The smart home field has witnessed rapid developments in recent years. Internet of Things applications for the smart home are very heterogeneous and continuously increasing in number, making user management from a security perspective very challenging. Moreover, the resource-constrained nature of most of the devices implies that any security mechanisms deployed should be lightweight and highly efficient. In this article, we propose an authentication scheme based on symmetric key cryptography, combined with a capability-based access control system, to provide the different stakeholders (residents, recurring guests, or temporary guests) end-to-end secure access to the Internet of Things devices in a smart home, managed by the home owner in an anonymous way. The operations in our scheme only include a small number of communication phases and protect the identities of the entities involved (i.e. stakeholders and end-nodes) from any outside entity. The proposed scheme ensures that even if the stakeholder's device or the Internet of Things device is attacked, the system remains secure.

- 155 -

Securing Internet of Things in 5G Using Audio Steganography.
Singh, Tanya; Verma, Seema; Parashar, Vidushi
In: SmartCom, International Conference on Smart Trends for Information Technology and Computer Communications, 1, in: Communications in Computer and Information Science * Band 628 (2016) Seite 365-372 (8 Seiten), Paper-Nr. Chapter 44
http://dx.doi.org/10.1007/978-981-10-3433-6_44

The data usage pattern is changing rapidly in many real life applications and these applications have converged in Smart Phones. 5th generation wireless networks will envision a widespread use of Internet of Things (IoT). With the growing demands for communication between Internet of Things using 5G networks, securing devices will emerge as a big challenge. There will be hidden exchange of data between the devices for which security can be achieved with audio steganography. The aim of the paper is to formulate the model supports the methodology and infrastructure desired to implement the security for IoT in 5G networks. Audio steganography is an invisible communication used for hidden exchange of the data. Internet of things applications varies from ubiquitous computing to machine to machine communications with most applications will be on Voice over IP and will require securing of data from eavesdroppers and attackers. So, the focus of this research paper is on how can we secure internet of things using audio steganography in 5G Platform.

- 156 -

Combining residue arithmetic to design efficient cryptographic circuits and systems.
Martins, Paulo; Sousa, Leonel; Antao, Samuel
In: IEEE Circuits and Systems Magazine, USA * vol 16 (2016) no 4, p 6-32, 73 refs.
http://dx.doi.org/10.1109/MCAS.2016.2614714

Cryptography plays a major role assuring security in computation and communication. In particular, public-key cryptography enables the asymmetrical ciphering of data along with the authentication of the parties that are attempting to share data. The computation of asymmetrical encryption is costly, thus it has motivated extensive research to efficiently accelerate the execution of the most relevant algorithms and improve resistance against Side-Channel Attacks (SCAs), which leverage exposed features by the cryptographic systems, such as power consumption and execution timings, to gain access to private information. Herein, we present a state-of-the-art overview of the use of the Residue Number System (RNS) to exploit parallelism in the computation of the most important public-key algorithms. We also address how it can be exploited to prevent side-channel attacks. The experimental results presented in the literature show that not only the currently used RSA and Elliptic Curve Cryptographic (ECC) algorithms but also emerging postquantum algorithms, namely the ones supporting Lattice-based Cryptosystems (LBCs), can take advantage of the RNS. It enables the design of more efficient cryptographic systems and also reinforces the prevention of side-channel attacks, improving their security. Finally, we also present the characteristics of the Computing with the Residue Number System Framework (CRNS), which aims to automatize the design of fully functional cryptographic accelerators based on RNS..

- 157 -

Proposal new s-box depending on DNA computing and mathematical operations.
Ali, Rasha Subhi - E-Mail:danafush@gmail.com; Kadhim, F. Alaa - E-Mail:dralaa_cs@yahoo.com; Abdul Majeed, Ghassan H. - E-Mail:ghassan@uob.edu.iq
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/AIC-MITCSA.2016.7759926

Today, information has become an important resource and so is its security. Many scientists attempted to use new methods inspired from DNA bio-techniques in the field of cryptography and steganography. The idea of using DNA cryptography has been specified as possible technology that gets a new hope for unbreakable algorithms as traditional cryptographic systems are now vulnerable to certain attacks. S-boxes (Substitution boxes) are keystones of modern symmetric cryptosystems (block ciphers and stream ciphers). In this research a new s-box creation scheme was proposed based on encoding into DNA codon, XOR operation and some mathematical operations. The results of the tests showed that the proposed method was effectively passed the S-Box tests criteria of such as balanced, completeness, avalanche criterion and strict avalanche criterion. The results showed that the proposed method provides secure S-box, which is 255 differences was found when changing only 1 bit of key, thus approximately %99 the S-Box was changed. In this method the secret key and the server name are used as example for generating new values of S-box two keys was used to strengthen the security of the created S-Box. Also, one key can be used to generate the S-Box values because of another key was generated by using the proposed method and it is equal to 0. The s-box inverse was also generated depending on the same strings that are used in generating the s-box. The generation time measured in milliseconds. The proposed method does not include several stages such as genetic algorithms. So the proposed method faster than genetic algorithms to the fact that genetic algorithm passed through several stages to find the best solution..

- 158 -

Elliptic-Curves Cryptography on High-Dimensional Surfaces [arXiv].
[02] Sonnino, Giorgio - E-Mail:gsonnino@ulb.ac.be
In: arXiv, USA * 2016

We discuss the use of elliptic curves in cryptography on high-dimensional surfaces. In particular, instead of a Diffie-Hellman key exchange protocol written in the form of a bi-dimensional row, where the elements are made up with 256 bits, we propose a key exchange protocol given in a matrix form, with four independent entries each of them constructed with 64 bits. Apart from the great advantage of significantly reducing the number of used bits, this methodology appears to be immune to attacks of the style of Western, Miller, and Adleman, and at the same time it is also able to reach the same level of security as the cryptographic system presently obtained by the Microsoft Digital Rights Management. A nonlinear differential equation (NDE) admitting the elliptic curves as a special case is also proposed. The study of the class of solutions of this NDE is in progress..

- 159 -

VLSI implementation of text to image encryption algorithm based on private key encryption.
Remya Ajai, A. S. - E-Mail:remya.amrita@gmail.com; Suresh, Anjali - E-Mail:anjali.srsh@gmail.com
In: (2016) p 4879-81 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICEEOT.2016.7755647

In cryptographic applications, the data sent to a remote host are encrypted at the source machine using an encryption key and then the encrypted data are sent to the destination machine, where it is decrypted to get the original data. Thus the attacker will not have the encryption key which is required to get the original data and so a hacker can do nothing with any cryptographic system. Reprogrammable devices such as Field Programmable Gate Arrays (FPGAs) are used for hardware implementations of cryptographic algorithms. As FPGA devices progressed both in terms of resources and performance, the latest FPGAs provide solutions that are easily customizable for system connectivity, DSP, and data processing applications. In this paper, implementation of an efficient cryptographic algorithm is done in Xilinx SPARTEN 3E FPGA. Also the algorithm is analyzed by calculating the number of all possible key permutations..

- 160 -

Efficient random number generator using novel modulo 2(sup n)-2(sup k)-1 adder for RNS.
Jacob, Vinodkumar - E-Mail:vinodkumar_jacob@rediffmail.com
In: (2016) p 1659-63 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICEEOT.2016.7754967

Modulo adder is the key component in the residue number system. In this paper a novel modulo 2(sup n) - 2(sup k) - 1 adder is designed and implemented to generate random numbers for use in cryptographic applications. The modulus used in this paper is of the form 2(sup n) - 2(sup k) - 1 (1 less than or equal to k less than or equal to n-2), which is best suitable for multichannel RNS processing. The modulo 2(sup n) - 2(sup k) - 1 adder is divided into four modules the pre processing, the carry generation, the carry modification and the sum calculation module. In the proposed modulo 2(sup n) - 2(sup k) - 1 adder, twice carry correction technique is used which reduces area and delay compared with same type of modulo adder with traditional structure..

- 161 -

Design of chaotic neural network based method for cryptographic substitution box.
Ahmad, Musheer - E-Mail:musheer.cse@gmail.com; Malik, Manish - E-Mail:manishmalikkvs@gmail.com
In: (2016) p 864-8 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ICEEOT.2016.7754809

The cryptographic substitution boxes are the substantive constituent of most modern day block cryptosystems. Here, we proposed a novel method to generate cryptographically potent S-boxes by exploring the blended strength of chaos and neural network in its design. The designed chaos-based neural network, engaged to yield S-boxes, consists of four layers each of which have eight, four, two and one neuron(s), respectively. The excogitation and cognitive operation of chaotic neural network is couched to sample the random elements which eventually render infrangible configuration of S-box. By utilizing the features of chaos and neural network efficiently, we explicate cryptographically strong S-boxes that have the desired potentiality and practicability. The statistical scrutiny of proposed method against widely accepted performance measures suggest that the method is amicable to contrive dynamical S-boxes for strong block cryptosystem with respectable cryptographic features..

- 162 -

Application-level security for ROS-based applications.
Dieber, Bernhard - E-Mail:bernhard.dieber@joanneum.at; Kacianka, Severin - E-Mail:kacianka@in.tum.de; Rass, Stefan - E-Mail:stefan.rass@aau.at; Schartner, Peter - E-Mail:peter.schartner@aau.at
In: (2016) p 4477-82 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/IROS.2016.7759659
While the topic of security in industrial applications has gained some momentum in recent years, there are still severe security vulnerabilities which are actively exploited for attacks. The robot operating system (ROS) is expected to further grow in usage and to be used in many industrial applications. Analysis, however, shows that it lacks several security enhancements in order to make it suitable for industrial use. In its current state, false data and commands can be injected posing a possible safety risk for the resulting product and humans in the production. In addition, data may be eavesdropped and used by outsiders to gain insight into the production process. In this paper we propose a security architecture intended for use on top of ROS on the application level. We use a dedicated authorization server to ensure that only valid nodes are part of the application. Cryptographic methods ensure data confidentiality and integrity. We show in a demonstration with a collaborative robot how our architecture can be used to secure a ROS-based application..

- 163 -

Privacy-preserving authentication systems using smart devices.
Hajny, Jan - E-Mail:hajny@feec.vutbr.cz; Malina, Lukas - E-Mail:malina@feec.vutbr.cz; Martinasek, Zdenek - E-Mail:martinasek@feec.vutbr.cz
In: (2016) p 11-14 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/TSP.2016.7760820
The paper deals with using modern smart handheld and wearable devices such as smartphones, smartwatches and microcomputers in privacy-preserving authentication and access control systems. Authentication and access control systems usually employ chip cards and smart cards as users' authentication devices. Nevertheless, current privacy-preserving authentication schemes often require more powerful devices such as smartphones and smartwatches. This paper provides the performance assessment of cryptographic and math methods on the smart devices. Further, a privacy-preserving authentication scheme is implemented in order to investigate its performance on these smart devices. Finally, the benefits and limits of deploying the smart devices in privacy preserving authentication systems are discussed..

- 164 -

Alternative Equations for Guillou-Quisquater Signature Scheme.
Ettanfouhi, J. - E-Mail:ettanfouhi@gmail.com; Khadir, O. - E-Mail:khadir@hotmail.com
In: International Journal of Computer Network and Information Security, China * vol 8 (2016) no 9, p 27-33, 14 refs.
http://dx.doi.org/10.5815/ijcnis.2016.09.04
http://www.mecs-press.org/ijitcs/index.html
In 1990, Guillou and Quisquater published an article where they described a new digital signature system. Their technique was based on the RSA algorithm. In this paper, we present several modified Guillou-Quisquater digital signature protocols. We discuss their security and complexity. These schemes can be seen as alternative signature methods if existing systems are completely broken..

- 165 -

Exploration of Benes network in cryptographic processors: a random infection countermeasure for block ciphers against fault attacks.
Bo Wang; Chenchen Deng; Leibo Liu - E-Mail:liulb@tsinghua.edu.cn; Min Zhu; Shaojun Wei; Shouyi Yin; Zhuoquan Zhou
In: IEEE Transactions on Information Forensics and Security, USA * vol 12 (2017) no 2, p 309-22, 43 refs.
http://dx.doi.org/10.1109/TIFS.2016.2612638
Traditional detection countermeasures against fault attacks have been criticized as insecure because of the fragile comparison operation that can be maliciously bypassed. In order to avoid the comparison, infection countermeasures have been designed to confuse the faulty ciphertexts so that the output cannot be further explored. This paper presents an infection method that resists fault attacks using the existing Benes network module in high-performance crypto processors. The Benes network is originally used to accelerate permutation operations in block ciphers. The hamming weight of the differential results is balanced by modifying specific network switches, without changing the network topology. A further confusion is performed to destroy the determinacy by configuring part of the network with a random bit-stream. Furthermore, a statistical evaluation method is presented to quantitatively verify the proposed countermeasure in addition to a formal proof of security. This also provides a new concept for the evaluation of future random-enhanced infection methods. Experiments are carried out using Advanced Encryption Standard (AES), triple Data Encryption Standard (DES), and Camellia as examples. Under statistical evaluation, the results show that the

proposed countermeasure improves the fault resistance by over four orders of magnitude compared with the unprotected case. Also, the performance and the area overhead are within 10% compared with the original Benes network..

- 166 -

Towards a timing attack aware high-level synthesis of integrated circuits.
Givargis, Tony; Peter, Steffen - E-Mail:st.peter@uci.edu
In: (2016) p 452-5 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ICCD.2016.7753326
Variabilities in the execution time of integrated circuits are frequently exploited as a side channel attack to expose secret information of deployed systems. Standard countermeasures analyze and change the explicit timing behavior in lower level hardware description languages, but their application is time consuming and error-prone. In this paper we investigate the integration of timing attack resilience into the high-level synthesis (HLS). HLS translates programs expressed in higher level programming languages, such as C, seamlessly to synthesizable hardware. We use timing annotations of basic blocks in C to add scheduling constraints that in the synthesis process balance the execution time of security-related execution branches. We integrate our approach to the scheduling of the open source LegUp HLS tool and apply the proposed method for the asymmetric cryptography algorithms RSA and ECC. The results proof the resistance against timing attacks, with a negligible overhead in synthesis efforts, area, and run-time..

- 167 -

Physicians Medicament using Linear Public Key Crypto System.
Senthilkumar, M. - E-Mail:mosenkum@gmail.com
In: (2016) p 1936-9 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICEEOT.2016.7755025
Now-a-days, in the medical field, prescribing a medicine for a patient without mentioning its brand name is a tedious job. But it can be made possible, when both the parties (physician and pharmacist) are adapting well and standardized methodology. Our aim is to suggest an idea to make this process easy to understand and light to use. Based on the types of common diseases, the medicinal prescription lists can be categorized with relevant medicinal blocks. If a physician prescribes the medicine through this standardized predefined scheme, then the system will generate a unique number using Grace Code Cryptography and Linear RSA algorithms. The unique number will be given to the patient in the prescription sheet. Through this unique number, the pharmacist can get back the medical unit which is intended for a particular patient with the help of the same algorithms and using the standardized predefined scheme as it is a general template, and he delivers the medicine. So the patient will be given the prescribed medicine without specifying the brand name at any stage..

- 168 -

An Implementation of Modified Lightweight Advanced Encryption Standard in FPGA.
[02] Kumar, Deepa S.
In: Procedia Technology, Netherlands * vol 25 (2016) p 582-9, 10 refs.
http://dx.doi.org/10.1016/j.protcy.2016.08.148
Advanced Encryption Standard (AES) is the standardized block cipher, which is used in various applications. AES is well suited for software and hardware implementation with versions of 128,192,256 key sizes. In hardware implementation AES is advantageous as it is more secure, low cost, and has minimized hardware utilization. Lightweight block ciphers are developed for the efficient implementation in hardware. An approach to design a technique to implement AES as lightweight block cipher is an immediate requirement of the time. An approach, to make AES a lightweight block cipher, is being discussed such that designing the steps of AES such as mix columns, substitute byte in AES is to be implemented in a parallel manner. The latency in this implementation is considered to be less comparing the conventional implementation of AES. The conventional and the new approach are to be simulated in XILINX 14.2 and is being compared in the aspects of area and latency. The design is to be implemented in FPGA. [All rights reserved Elsevier]..

- 169 -

Software implementation of a module for encryption and decryption using the RSA algorithm.
Borodzhieva, Adriana Naydenova - E-Mail:aborodzhieva@uni-ruse.bg
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ET.2016.7753464
The paper describes MS EXCEL-based application implementing the processes of encryption and decryption of texts in English and/or Bulgarian using the RSA algorithm. The processes of encryption and decryption are illustrated. The material is used in the educational process in the course 'Telecommunication Security' but it can be applied in other disciplines involving issues of cryptographic information protection..

- 170 -

Area optimized and high throughput AES algorithm based on permutation data scramble approach.
Babu, C. - E-Mail:c_babu@blr.amrita.edu; Dilna, V. - E-Mail:dilnavnambiar@gmail.com
In: (2016) p 3056-60 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICEEOT.2016.7755263
In today's scenario most of the things in human life is E-banking where everything is faster and smoother. With the various exchange of electronics signals between any two servers or systems, the money transactions can be done and this process is E-banking. Third party software is used for this E-banking feature where end to end users are secured. The proposed AES algorithm enhances the performance by resolving the security related issues for E-banking features and provides better throughput operations. The permutation step involved in the proposed AES algorithm resembles to Data Encryption Standard (DES) algorithm. The mode of data transmission in the modified AES is 128 bit plaintext and keys which converted into four 32bit blocks and exclusion of shift row. Using this feature not only area is optimized but also higher throughput is achieved. The high potential usage of same cryptographic algorithms risks the secure data processing so advanced changes should be incorporated. Design has been done using Verilog and simulated using Modelsim. The design has been synthesized using Xilinx for target device Vertex6..

- 171 -

2016 XXV International Scientific Conference Electronics (ET). Proceedings, Sozopol, Bulgaria, 12-14 Sept. 2016.
anonym
In: 2016 (299 pp) Piscataway, NJ, USA: IEEE
The following topics are dealt with: ECG signal acquisition; brain-computer interface; electronic nose; analog-to-digital convertors; RSA algorithm; digital phase locked loop; image recognition; cloud computing; smart energy metering; TSV; CNTFET model; power MOSFET; regenerative braking; electric vehicles; and induction heating..

- 172 -

A novel approach to enhance the security dimension of RSA algorithm using bijective function.
Bhattacharya, Ishan; Chakraborty, Ajoy Kumar; Hazra, Tapan Kumar - E-Mail:tapankumar.hazra@iemcal.com; Mazumder, Maniratna; Sheikh, Nazimuddin - E-Mail:sheikh.cs@gmail.com
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/IEMCON.2016.7746304
The essence of data security has exponentially increased in last few decades in order to protect the privacy and secrecy of confidential information of different organizations, intelligence agencies and defense departments. The intruders are continuously trying to breach security systems to reveal the transmitted data over the network. The RSA algorithm has applications in many confidential fields such as credit card information. So the security level of RSA must be high and must be difficult to breach. In order to enhance the security dimension of RSA algorithm we have proposed a novel and unique approach to modify this algorithm using two-variable bijective function. This bijective function maps the ASCII derived from the plaintext or any integer values into another set of definite integer values which can be recovered by applying its inverse formula during decryption. Our proposed methodology of modification of RSA scheme shall eliminate possible security threats against this algorithm and advance a step further towards secure communication system..

- 173 -

Montgomery Multiplier for Faster Cryptosystems.
Thampi, Nitha; Jose, Meenu Elizabath
In: Procedia Technology, Netherlands * vol 25 (2016) p 392-8, 8 refs.
http://dx.doi.org/10.1016/j.protcy.2016.08.123
With the advancement in communication systems, security is a prime concern which is offered by cryptosystems Modular arithmetic is core operation in most of the cryptosystems. Many cryptosystems including RSA, DSA and ECC systems requires modular multiplication for private key generation. It uses modular exponentiation of large numbers to encrypt data, which is a slow process due to repeated modular multiplications. The efficiency of cryptography systems practically depend on how fast the modular multiplication is done, since these are at the base of computation. Many hardware and software implementations for faster modular multiplication have been proposed, Montgomery Multiplication Algorithm is recognized as the most efficient among these. This paper presents a 32-bit implementation of a Faster Montgomery algorithm for performing modular multiplication. The algorithm is based on the method proposed by Montgomery for modular multiplication and is complementary to the available techniques. Simulation shows that our design performs faster in terms of clock frequency while it requires lower area. [All rights reserved Elsevier]..

- 174 -

Where AES is for Internet, SIMON could be for IoT.
Nithya, R.
In: Procedia Technology, Netherlands * vol 25 (2016) p 302-9, 9 refs.
http://dx.doi.org/10.1016/j.protcy.2016.08.111
With the upcoming era of Internet of Things and the Pervasive Computing, there is a need to develop block ciphers with tight constraints such as area, power, memory, performance, throughput and others. These are so called the lightweight block ciphers which are specifically intended for resource constrained platforms. Lined up in the line is SIMON, a light weight block cipher proposed by NSA after the prompting from the U.S. Government in the year 2013 along with SPECK lightweight block cipher. SIMON implementation on hardware has excellent results in terms of area and has been found to be a very strong alternative to the existing AES. This paper involves the basic design considerations, round functions, key schedule and parameters of SIMON and also we can look forward into the implementations of SIMON in hardware comparing with the existing AES standard. This paper also focuses on the analysis in terms of area, power and delay of the SIMON 64/128 configuration in Cadence Synthesis RTL Compiler using the CMOS 180 nm and 90 nm technology libraries. [All rights reserved Elsevier]..

- 175 -

A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm.
anonym
In: International Journal of Image, Graphics and Signal Processing, China * vol 8 (2016) no 6, p 64-71, 14 refs.
http://dx.doi.org/10.5815/ijigsp.2016.06.08
http://www.mecs-press.org/ijigsp/index.html
A non-format compliant JPEG encryption algorithm is proposed which is based on a modification of the RSA encryption system. Firstly, an alternate form of entropy coding is described, which is more suited to the proposed algorithm, instead of the zigzag coding scheme used in JPEG. The algorithm for the encryption and decryption process is then elaborated. A variant of the algorithm, also based on the RSA algorithm is also described, which is faster than the original algorithm, but expands the bit stream slightly. Both the algorithms are shown to be scalable and resistant to 'sketch' attacks. Finally, the encrypted file sizes for both the algorithms are compared with the unencrypted JPEG compressed image file size. The encrypted image is found to be moderately expanded, but which is justified by the high security and most importantly, the scalability of the algorithm..

IS-Management

- 176 -

Haie fischt man nicht im Trüben. Grüße von der langen Bank - Dauerbaustellen der Security (2).
Weßelmann, Bettina; Wiele, Johannes
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 4, Seite 26-31 (6 Seiten, Bilder), (Fortsetzung aus 32(2016)3, S. 50-54)
(Fortsetzung aus 32(2016)3, S. 50-54) Der vorliegende Beitrag betrachtet Aspekte der Informationssicherheit, vor allem die Threat-Sicherheit zur Bedrohungsabwehr. Hierbei wird immer mehr kontextbezogen gearbeitet, d.h. man sammelt Informationen und will die auch auswerten in Bezug darauf welche Einflüsse im Netz welchen Zugriffen, Richtlinien, Risiko-Leveln oder anderen physischen oder gedanklichen Konstrukten zugeordnet sind. Dabei geht es um das Verständnis der Anwender- und der Angreifersicht. Da in vielen Unternehmen entsprechende Informationen fehlen, informiert der vorliegende Beitrag umfassend über das Thema. Anhand eines Szenarios werden Schwachstellen in der Informationssicherheit eines unternehmens gezeigt. Beschrieben werden die Situation und die wahrscheinlichen Folgen. Es wird gezeigt, wie sich die Mängel am besten und schnellsten beheben lassen und gezeigt, dass das nicht einfach ist. Die Ursachen für nicht vorhandene Sicherheitsszenarien werden untersucht und die Bedeutung von Kontextinformationen herausgestellt. Fragen der Bedeutung einer interdisziplinären Zusammenhang werden untersucht, um Verständigungsbarrieren auszuräumen. Es werden die Konsequenzen fehlender Kontext- und Risikolevelinformationen beschrieben.

- 177 -

Neue Verpflichtungen im Detail: Sicherheitskonzept und Wirksamkeitsprüfungen.
Lepperhoff, Niels; Müthlein, Thomas
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 5, Seite 64-66, 68 (4 Seiten)
Die neue europäische DS-GVO (Datenschutz-Grundverordnung) wird ab dem 25.05.2018 das Bundesdatenschutzgesetz ablösen und damit gesetzliche Mindeststandards wie ein Sicherheitskonzept und regelmäßige Wirksamkeitstests der Sicherheitsmaßnahmen vorschreiben. Der vorliegende Beitrag erläutert das Sicherheitskonzept und den Anpassungsbedarf am Beispiel des BSI-Standards 100-2 "IT-Grundschutz-Vorgehensweise" (Bundesamt für Sicherheit in der Informationstechnik). Als erster Schritt zu einem Sicherheitskonzept gehört eine Strukturanalyse, die regelmäßig erfolgt. Eine Risikoanalyse wird erwartet und neue Maßnahmen und Schutzziele. Der Beitrag betrachtet

den Stand der Technik aus europäischer Sicht unter Einbeziehung der Norm EN 45020 und ISO/IEC Guide 2:2004. Aufgelistet werden Prozesse, die das DS-GVO mit Blick auf die IT-Sicherheit im Unternehmen verlangt und die z.B. in Wirksamkeitstests zu kontrollieren sind. Es wird empfohlen bereits jetzt mit der Erstellung eines Sicherheitskonzeptes zu beginnen, das die Vorgaben des neuen Gesetzes berücksichtigt.

- 178 -

Managementsysteme im Vergleich.
Wegner, Dirk; Troschke, Marie-Luise
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 5, Seite 76-80 (5 Seiten, Tabellen)
Eine umfassende Gewährleistung von Informationssicherheit in Unternehmen kann am besten mit einem ISMS (Informationsmanagementsystem) erreichen. Der vorliegende Beitrag stellt einige neue Informationsmanagementsysteme vor und vergleicht sie miteinander. Das sind ISO 2700x der Internationalen Organisation für Standardisierung, BSI IT-Grundgesetz des Bundesamtes für die Sicherheit in der Informationstechnik, ISIS 12, das sich an der Methodik des BSI-Grundmodells orientiert und an kleine und mittlere Unternehmen und an Kommunen richtet und VdS Cyber-Security der VdS Schadenverhütung GmbH (Verband der Sachversicherer), eine der weltweit renommiertesten Institutionen für die Unternehmenssicherheit. Merkmale, Zielgruppe, Detaillierung, Aufbau, Maßnahmekatalog, Risikoanalyse, Umsetzung und Tertifizierung werden erfasst.

- 179 -

IT-Landschaften 2016: Lagebericht zur Sicherheit (2).
anonym
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 5, Seite 50-56, 58 (8 Seiten, Bilder, Tabellen), (Fortsetzung aus 32(2016)4, S. 45-55)
(Fortsetzung aus 32(2016)4, S. 45-55) Dieser Teil der Auswertung der kes-Microfoft Sicherheitsstudie beschäftigt sich mit der Frage der Vertraulichkeit und vor allem mit Strategie und Management sowie mit Kenntnissen und Weiterbildung zur Informationssicherheit. Es werden neben Vertraulichkeitsbrüchen auch Konsequenzen, die sich daraus ergeben, untersucht. Dabei haben wieder 79 % der Befragten Unternehmen festgestellt, dass eigene Mitarbeiterfür für die meisten Datenlecks zumindest mit verantwortlich sind. Sie sind sich einfach der Konsequenzen nicht bewusst, sie verstehen Datenschutz- und Sicherheitslösungen nicht und sie haben keine Kenntnis der Firmenpolitik. 11 % der Mitarbeiter wollen dem Unternehmen schaden. Wieder wurde nach der beruflichen Nutzung von Filesharing Diensten von Unternehmensnetzen aus gefragt. 47 % der Unternehmen gaben an, dass das mutmaßlich nie passiert, bei 13 % der Unternehmen häufig. Es wurde untersucht, ob und welche Strategien, Richtlinien und Konzepte zur Informationssicherheit es in den befragten Unternehmen gibt und in einer Tabelle gegenübergestellt. Es zeigt sich aber auch, dass ein Sechstel der Unternehmen ihre Sicherheitspolitik nie auf den Prüfstand stellen (kleine und mittlere Unternehmen 22 %, große 11 %). Es werden noch einmal die Kriterien zur Risikobewertung gezeigt und auf Regelungen, Gesetze und Standards hingewiesen. Hindernisse für eine Verbesserung der Informationssicherheit werden aufgezeigt. Die Einschätzung des Kenntnisstands der Manager und Mitarbeiter und die Häufigkeit von Schulungen werden dargestellt. (wird fortgesetzt)

- 180 -

Zwei Methoden - ein Ansatz. Schutzbedarfsfeststellung und Business-Impact-Analyse.
Plaul, Thomas; Vahldieck, Julia; Gündel, Markus
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 4, Seite 64-69 (6 Seiten, Bilder)
Von Unternehmen wird gefordert, das IT-Sicherheitsgesetz zu beachten und die EU-Datenschutz-Grundverordnung, wenn sie auf dem Europäischen Markt agieren wollen. Dabei werden die Einrichtung eines Informationssicherheitsmanagementsystems und eines Business-Contiuity-Managementsystems gefordert. Der Grund ist der, dass es immer mehr Angriffe auf Informationssysteme und dadurch Ausfälle der Informationstechnik gibt. Dazu kommt die immer größere Vernetzung und die daraus resultierenden Dienstleistungen, die angeboten werden müssen. Es geht darum Ausfallrisiken zu vermindern und zu vermeiden. Notwendig sind erstens eine Schutzbedarfsfeststellung und zweitens Business Impact Analysen. Beides sind Methoden zur Erhebung geschäftskritischer Daten für unterschiedliche Zielgruppen. Beide Methoden werdn im vorliegenden Beitrag beschrieben als einzelne Komponenten und im Zusammenspiel miteinander.

- 181 -

Informationssicherheits-Managementsystem (ISMS) bei Energieversorgern.
Hänel, Andreas; Wohlfart, Fabian
In: Energie-, Wasser-Praxis * Band 67 (2016) Heft 12, Seite 76-81 (6 Seiten)
Das Thema Informationssicherheit nimmt für Energieversorger einen immer größeren Stellenwert ein. Um im Netzbereich mit der Entwicklung des Energiemarktes Schritt zu halten, wurden und werden in den nächsten Jahren die IT-Systeme der LeitstelSen schrittweise modernisiert. Die damit einhergehende stärkere Vernetzung der Netzseite mit dem übrigen Unternehmen ist jedoch mit Risiken verbunden. Mit der Verabschiedung des BSI-Gesetzes und der

Veröffentlichung des "IT-Sicherheitskataloges" 2015 wurden im Kontext der Informationssicherheit für den Betrieb von Energienetzen die Anforderungen gesetzlich festgelegt. Um den aktuellen Wissens- und Umsetzungsstand zu evaluieren, haben die Energieforen Leipzig in Zusammenarbeit mit der SEVEN PRINCIPLES AG und der Universität Bayreuth die Studie "Informationssicherheits- Managementsysteme bei Energieversorgern" durchgeführt. Die Ergebnisse der Studie zeigen die Wirksamkeit eines ISMS. Diese Wirksamkeit wird maßgeblich durch den systematischen Prozess zur Analyse einzelner Unternehmensbereiche beeinflusst. Ein ISMS wäre damit tatsächlich in der Lage, organisatorische und technische Schwachstellen aufzudecken. Allerdings fühlen sich viele Energieversorger trotz des vorgegebenen IT-Sicherheitskatalogs bei der Einführung eines ISMS nicht ausreichend informiert, da viele notwendige Definitionen und Fallkonstellationen nicht konsistent ausgeführt sind. Andererseits sehen Experten die Regelungen des IT-Sicherheitskatalogs als eine gute Grundlage bzw. Mindestanforderung zur notwendigen Sensibilisierung im Bereich Informationssicherheit. Beide Punkte führen dazu, dass der Großteil der befragten Energieversorger plant, bei der Einführung eines ISMS die Beratungsleistung von Dienstleistungsunternehmen in Anspruch zu nehmen. Damit ein ISMS seine Wirksamkeit entfalten kann, sind gerade die Abteilungen miteinzubeziehen, die keine direkte Verbindung zur Erzeugung von Energie haben. Wie das Ergebnis der Befragung zeigt, sind relevante Türen zur Untergrabung der IT-Sicherheitsmechanismen auch abseits des industriellen Steuerungsnetzes, der Leitstelle und der Netzführung, zu finden. Demnach schätzen Probanden, die bereits ein ISMS eingeführt haben, insbesondere den Mehrwert eines ISMS in den betriebswirtschaftlichen Abteilungen. Bei globaler Betrachtung innerhalb der Befragung erkennen jedoch nur 4 Prozent die direkte Relevanz zur expliziten Einführung in diesen Bereichen. Die Ergebnisse der Studie deuten darauf hin, dass z. B. das Marketing und die Öffentlichkeitsarbeit wie auch die Buchhaltung und das Personalwesen im Unternehmen insbesondere zur Sensibilisierung aufgefordert sind. Sensibilisierung kann z. B. auf den Ebenen des technischen Grundverständnisses und der Medienkompetenz ansetzen. Insbesondere keine Digital Natives können von einer stärkeren Sensibilisierung profitieren, da u. a. viele Sicherheitslücken im Unternehmen heute durch sogenannte Social Attacks oder Social Engineering offenbart werden. Diese erfolgen sowohl offline als auch online. Neben dem Bewusstsein dienen konkrete technische Lösungen der Umsetzung des ISMS. Aufgrund historisch gewachsener, komplexer Infrastrukturen dienen die aktuellen IT-Sicherheitskomponenten im Energieversorgungsnetz dezidierten Aufgaben, besitzen eine eingeschränkte Sichtweise auf das Unternehmensnetzwerk und bedürfen im Resultat einer qualifizierten Administration, die in ständiger Wechselwirkung mit dem Unternehmensalltag stehen muss. Konkrete Lösungen müssten daher auf einen Anwendungsfall - die IP-Topologie im Unternehmen - zugeschnitten sein. Doch auch hier finden sich in der Praxis unterschiedliche Ansätze und ein breit gefächertes Verständnis. Eine allumfassende Lösung wird daher von Unternehmen gewünscht, oft seitens der Anbieter versprochen und dennoch gibt es sie nicht.

- 182 -

Cryptanalysis of SDES Using Modified Version of Binary Particle Swarm Optimization.
Dworak, Kamil; Boryczkainst, Urszula
In: Computational Collective Intelligence, ICCCI, International Conference on Collective Intelligence, 7, in: Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence * Band 9330 (2015) Seite 159-168 (10 Seiten), Paper-Nr. Chapter 16, CSI: Special Session on Computational Swarm Intelligence
http://dx.doi.org/10.1007/978-3-319-24306-1_16
Nowadays, information security is based on ciphers and cryptographic systems. What evaluates the quality of such security measures is cryptanalysis. This paper presents a new cryptanalysis attack aimed at a ciphertext generated with the use of the SDES (Simplified Data Encryption Standard). The attack was carried out with a modified version of the BPSO (Binary Particle Swarm Optimization) algorithm. A well-adjusted version of this method can have a positive effect on the quality of the results obtained in a given period of time.

- 183 -

DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption.
Morales-Sandoval, Miguel; Diaz-Perez, Arturo
In: Information Security Theory and Practice, WISTP, IFIP WG 11.2 International Workshop, Information Security Theory and Practice, 9, in: Lecture Notes in Computer Science * Band 9311 (2015) Seite 104-119 (16 Seiten), Paper-Nr. Chapter 7, Secure Resource Sharing and Access Control
http://dx.doi.org/10.1007/978-3-319-24018-3_7
Many works in the literature have proposed information security mechanisms relying on Paring Based Cryptography (PBC), for example, Ciphertext Policy Attribute Based Encryption (CP-ABE). However, a public set of software modules that allow integrating that kind of encryption for data security of information systems in an easy and transparent way is still missing. Available APIs like PBC (C-based) or jPBC (Java-based) are focused on low level arithmetic operations and several non trivial issues must still be addressed to integrate a functional PBC/ABE scheme into end-user applications for implementing end-toend encryption. We present a novel and portable Java library (API) to ensure confidentiality and access control of sensitive data accessed only by authorized entities having as credentials a set of attributes. Novel encryption and decryption processes are defined, using the digital envelope technique (DET) under a client-server computing model. The new DET-ABE scheme supports standard security levels (AES encryption) and provides the user with an easy interface for transparent use of next generation cryptography, hiding the complexity associated to PBC (field and group arithmetic, curve selection) and ABE (setup, key management, en-

cryption/decryption details). Running times of main API's modules at server (ABE setup and key generation) and client (DET-ABE encryption/decryption) side are presented and discussed. From these results, it is concluded that the proposed API is easy to use and viable for providing confidentiality and access control mechanisms over data in end-user applications.

- 184 -

Neue Signatur-Gesetzgebung: Sind aller guten Dinge drei?. eIDAS-Verordnung der EU regelt digitale Signaturen neu.
Schmeh, Klaus
In: DuD Datenschutz und Datensicherheit * Band 41 (2017) Heft 1, Seite 29-33 (5 Seiten), Kryptographie - Aktuelle Entwicklungen
http://dx.doi.org/10.1007/s11623-017-0721-3
Die europäischen Signaturgesetze haben bisher wenig bewegt. Mit der eIDAS-Verordnung der EU könnte nun einiges besser werden - dank einfacherer Technik, neuen Signatur-Varianten und einer besseren internationalen Abstimmung. Aus diesen Neuerungen ergeben sich interessante Anforderungen an die Krypto-Technik.

- 185 -

Zertifizierungsdienste in der Post-Quantum-Ära.
Nguyen, Kim
In: DuD Datenschutz und Datensicherheit * Band 41 (2017) Heft 1, Seite 17-20 (4 Seiten), Kryptographie - Aktuelle Entwicklungen
http://dx.doi.org/10.1007/s11623-017-0718-y
Die Sicherheit von Zertifizierungsdiensten in der bisher etablierten Form beruht wesentlich auf der Sicherheit der zugrunde liegenden asymmetrischen kryptographischen Mechanismen. Mit der Frage nach der Verfügbarkeit von Quantencomputern und der damit verbundenen Auswirkung auf kryptographische Algorithmen verbindet sich somit sofort die Frage nach der Auswirkung auf die Sicherheit von Zertifizierungsdiensten. Der vorliegende Aufsatz stellt mögliche Ablöseszenarien vor und diskutiert Anforderungen an Post-Quantum-Algorithmen und -Systeme aus Sicht von Zertifizierungsdiensten.

- 186 -

Blockchain-Ökosysteme. Identitäts- und Zugangsmanagement zur Blockchain und angedockten Ökosystemen.
Stommel, Sebastian
In: DuD Datenschutz und Datensicherheit * Band 41 (2017) Heft 1, Seite 7-12 (6 Seiten), Kryptographie - Aktuelle Entwicklungen
http://dx.doi.org/10.1007/s11623-017-0716-0
Seit 2008 fordert Bitcoin die etablierten Finanzinstitutionen heraus. In den letzten Monaten rückte die zugrundeliegende Blockchain-Technologie in den Fokus von Banken und Investoren, weil sie dem Internet über der Kommunikationsschicht eine weitere Schicht für wirtschaftliche Transaktionen bereitstellt. Digitale Wertschöpfungsprozesse werden so radikal verändert und eigene Ökosysteme geschaffen, zum Beispiel "on- und off-chain" PKI.

- 187 -

Exploiting Block-Chain Data Structure for Auditorless Auditing on Cloud Data.
Ghoshal, Sanat; Paul, Goutam
In: Information Systems Security, ICISS, International Conference on Information Systems Security, 12, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10063 (2016) Seite 359-371 (13 Seiten), Paper-Nr. Chapter 19, Software Security
http://dx.doi.org/10.1007/978-3-319-49806-5_19
Low cost, high performance and on-demand access of cloud infrastructure facilitates individuals and organizations to outsource their high volume of data to cloud storage system. With continuously increasing demand of cloud storage, security of users' data in cloud is becoming a great challenge. One of the security concerns is ensuring integrity of the data stored in the cloud, and trusted third-party based public auditing is a standard technique for cloud data authentication. In this paper, for the first time, we propose an auditing scheme for cloud data without requiring a third party. We exploit the block-chain data structure of Bitcoins to propose an auditing mechanism whereby any user can perform the validation of selected files efficiently. In case a user does not possess the required computational resource for verification, or a user is reluctant to do the verification, our scheme provides the option for third party verification as well, without any additional overhead of data structure, computation or storage.

- 188 -

Design, Demonstration, and Evaluation of an Information Security Contract and Trading Mechanism to Hedge Information Security Risks.

Pandey, Pankaj; Haes, Steven De

In: Security and Trust Management, STM, International Workshop on Security and Trust Management, 11, in: Lecture Notes in Computer Science * Band 9331 (2015) Seite 283-292 (10 Seiten), Paper-Nr. Chapter 19, Security Analysis, Risk Management, and Usability

http://dx.doi.org/10.1007/978-3-319-24858-5_19

Cyber-insurance products are the only financial instrument available as a risk-transfer mechanism in the information security domain. Furthermore, cyber-insurance markets are unable or unwilling to facilitate the transfer of risks, particularly those with a high probability and high intensity of loss. Thus, there is a need for a new mechanism to address the variety of information security risks. This article addresses the shortcomings in the existing information security risk hedging market. The article presents a financial instrument and a corresponding trading mechanism to be used for risk hedging in an information security prediction market. Also, the article uses an imaginary case to demonstrate the application of the contract. Furthermore, an evaluation of the contract and trading mechanism in its usefulness in hedging the underlying risks is presented. In our analysis, we found that information security contracts can be a solution (at least to some extent) to the problems in the existing risk hedging mechanisms in the information security domain.

- 189 -

Novel MITM Attacks on Security Protocols in SDN: A Feasibility Study.

Wang, Xin; Gao, Neng; Zhang, Lingchen; Liu, Zongbin; Wang, Lei

In: Information and Communications Security, ICICS, International Conference on Information and Communications Security, 18, in: Lecture Notes in Computer Science, Security and Cryptology * Band 9977 (2016) Seite 455-465 (11 Seiten), Paper-Nr. Chapter 35, Network Security

http://dx.doi.org/10.1007/978-3-319-50011-9_35

Software-Defined Networking (SDN) is a new paradigm that offers services and applications great power to manage network. Based on the consideration that the entire network visibility is the foundation of SDN, many attacks emerge in poisoning the network visibility, which lead to severe damage. Meanwhile, many defense approaches are proposed to patch the controller. It is noticed that powerful adversaries can bypass existing approaches to poison topology information and attack security protocols. In this paper, we present a method that the adversary can attack security protocols under existing approaches (e.g. TopoGuard, SPHINX). We also investigate a number of security protocols that may be compromised by our MITM attacks and propose an approach to detect the existence of the adversary. Our evaluation shows that the defense solution can effectively detect the fake link in normal environment. We hope our research can attract more attention on SDN security.

- 190 -

Scalable Access Policy for Attribute Based Encryption in Cloud Storage.

Wang, Jing; Huang, Chuanhe; Wang, Jinhai

In: Algorithms and Architectures for Parallel Processing, ICA3PP, International Conference on Algorithms and Architectures for Parallel Processing, 15, in: Lecture Notes in Computer Science * Band 9530 (2015) Seite 383-402 (20 Seiten), Paper-Nr. Chapter 29, Service Dependability and Security in Distributed and Parallel Systems

http://dx.doi.org/10.1007/978-3-319-27137-8_29

Cloud storage provides outsourced storage services in a cost-effective manner. A key challenge in cloud storage is the security and integrity of outsourced data. A security mechanism known as Attribute- Based Encryption (ABE) represents the state-of-the-art in providing finegrained access control for cloud storage. A critical issue in ABE is the managing of access policy. Policy managing may incur substantial computation and communication overhead in the ABE scheme with unscalable access policy. In this work, we propose a form of access policy named block Linear Secret Sharing Scheme (LSSS) matrix. The scalability of block LSSS matrix provides an efficient policy managing interface for ABE schemes. Thus, the ABE schemes use block LSSS matrix as access policy are light weight in computation and communication, as compared with other schemes during access policy managing. Furthermore, the block LSSS matrix enjoys advantages of efficiency, flexibility and security, bringing a number of improvements in various aspects of ABE.

- 191 -

Extending the UML Standards to Model Tree-Structured Data and Their Access Control Requirements.
Rosa Algarin, Alberto De la; Demurjian, Steven A.
In: Security Standardisation Research, SSR, International Conference on Security Standardisation Research, 3, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10074 (2016) Seite 187-204 (18 Seiten), Paper-Nr. Chapter 8
http://dx.doi.org/10.1007/978-3-319-49100-4_8

Secure data sharing between computational systems is a necessity to many workflows across domains such as healthcare informatics, law enforcement and national security. While there exist many approaches towards securing data for the purpose of dissemination, the vast majority follows the traditional thought of security engineering that occurs as the last step of the overall software engineering process. In this paper we extend the Unified Modeling Language (UML) standard to: (1) modeling tree-structured data and associated schemas and (2) information security via role-based, lattice-based, and discretionary access control; both push it towards the forefront of the software development life-cycle. Tree structured data and associated schemas are dominant in information modeling and exchange formats including: the eXtensible Markup Language (XML), JavaScript Object Notation (JSON), etc. New UML artifacts for tree-structured data and schemas would allow the modeling of generalized information solutions from which XML, JSON, RDF, etc., could be generated; this is akin to generating different object-oriented programming language code from UML class diagrams. This UML extension also allows security experts to model and define information security requirements at the schema level as well, before code is written. The end-result is the assurance of information security for the purpose of sharing across computational systems.

- 192 -

Industrieautomation per Funk: Drahtlos geht's besser.
Fecht, Nikolaus
In: VDMA Nachrichten * Band 95 (2016) Heft 9, Seite 68-75 (8 Seiten, Bilder)

Durchgängige Kommunikation ist ein wesentliches Element von Industrie 4.0. Automatisierungskomponenten enthalten deshalb zunehmend integrierte Technologien zur Vernetzung. Die Voraussetzung dafür sind gemeinsame Kommunikationsstandards. Damit befasst sich auch eine Arbeitsgruppe der Plattform Industrie 4.0. Die beteiligten Unternehmen sehen den neuen Industriestandard "IO-Link wireless" als ersten Industriestandard zur schnellen, drahtlosen Kommunikation innerhalb von Fertigungsanlagen an, vor allem für den Einsatz im Maschinen- und Anlagenbau. Zum Einsatz kommt IO-Link wireless beispielsweise bei Roboteranwendungen. Die sogenannte Wireless-Hart-Technologie beruht auf dem Hart-Protokoll (Highway Addressable Remote Transducer), einem standardisierten und weit verbreiteten Kommunikationssystem zum Aufbau industrieller Feldbusse. Auf das Hart-Übertragungsprotokoll setzen die Pepperl+Fuchs GmbH (Mannheim) bei ihrer Lösung für drahtlose Datenübertragung ebenso wie auch die ABB Automation Products GmbH (Frankfurt am Main) in Antrieben und Motoren von Schiffen. Die Fachpresse spricht bereits vom Hypethema Wireless. Doch in Wirklichkeit halten sich die Anwender noch zurück. Die Geschwindigkeit der Marktdurchdringung hängt davon ab, wie schnell die Hersteller die Bedenken der Anwender wie "Mangelnde Datensicherheit", "Störung durch andere Funksysteme" und "mangelnde Stabilität" ausräumen können. Ein vom Bundesministerium für Bildung und Forschung (BMBF) geförderter Forschungsverbund zur zuverlässigen, drahtlosen Kommunikation in der Industrie (ZDKI) soll die Probleme lösen, die den Einsatz von drahtloser Kommunikationstechnik in den Fabriken bisher be- und verhindern. Das Thema "Drahtlose Kommunikation" bleibt für den Maschinen- und Anlagenbau wichtig, vor allem bei der schrittweisen Umsetzung von Industrie 4.0 und der dazugehörigen Digitalisierung. Der Fachverband Elektrische Automation im VDMA und seine Mitglieder leisten mit ihrem Know-how zu diesem Thema fachliche Unterstützung.

- 193 -

Windows 10 - Anniversary Update. Sicherheitsfunktionen im Überblick.
Kranawetter, Michael
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 4, Seite 6-8, 10-11 (5 Seiten, Bilder, 7 Quellen)

Der vorliegende Beitrag beschäftigt sich mit Windows 10 und den Updates für Windows 10, die das System immer auf den aktuellsten Stand der Sicherheit bringen sollen. Das ist notwendig, da es immer mehr Cyberattacken gibt. Diese sind besonders bei Netzwerken, die mit veralteter Technik arbeiten oder nur rudimentäre Schutzmechanismen einsetzen und nicht gepatched oder nicht professionell verwaltet oder konfiguriert sind. Windows wird jetzt in kurzen und regelmäßigen Abständen mit neuen Funktionen verbessert und die immer neuen und verbesserten Sicherheitsmaßnahmen können einen Großteil der Angriffe verhindern. Das jetzt verfügbare Windows 10 Jahresupdate bringt wieder einige Neuerungen im Sicherheitsbereich.

- 194 -

Was schützen wir hier eigentlich? Grüße von der langen Bank - Dauerbaustellen der Security (3).
Busam, Michael; Wiele, Johannes
In: KES - Die Zeitschrift für Informations-Sicherheit * Band 32 (2016) Heft 5, Seite 70-74 (5 Seiten, Bilder), (Fortsetzung aus 32(2016)4, S. 26-31)
(Fortsetzung aus 32(2016)4, S. 26-31) Spätestens wenn IT-Arbeiten an andere Unternehmen abgegeben werden sollen, stellt sich die Frage, welche Unternehmensdaten aufgrund interner Richtlinien oder gesetzlicher Vorgaben neben den technischen Strukturen an andere Unternehmen abgegeben werden dürfen. Dazu ist eine gründliche Klassifizierung der betroffenen Informationen nötig und die ist nicht einfach und oft erst gar nicht oder nicht vollständig vorhanden. Der vorliegende Beitrag zeigt die Notwendigkeit einer vollständigen Informationsklassifizierung in den Unternehmen. Er zeigt Schwierigkeiten und Risiken dabei auf. Er zeigt erste Schritte mit denen ein Unternehmen zu einer Informationsklassifikation kommen kann. (wird fortgesetzt)

- 195 -

Schutz gegen Cyberkriminalität. Normenreihe ISO/IEC 2700x.
Heinzelmann, Regula
In: Management und Qualität * Band 51 (2016) Heft 10, Seite 22-23 (2 Seiten, Bilder)
Die Normen der ISO/IEC 2700x-Reihe haben mit dem Release 2013 die Struktur der ISO-Managementsysteme übernommen. Unternehmen, die sich nach 27001 zertifizieren lassen, verfügen über ein Sicherheits- und IT-Management, durch das ein ganzheitlicher Ansatz in Unternehmen - von Klein-, über KMU bis zu Großunternehmen - entwickelt werden kann, der eine hohe IT-Sicherheit unterstützt. Auf Basis der ISO 27001 werden nach einer Risiko- und Schwachstellenanalyse sowohl Ziele wie Prozesse und Verfahren definiert, wobei die Dokumentation der Maßnahmen und Prozesse selbstverständlich ist. Außerdem fordert die ISO 27003 eine laufende Kontrolle durch eine Security Policy. Ziel der Kontrolle ist die Klärung der Erreichung gesetzlicher Sicherheitsziele und der bestehenden Schwachstellen sowie die Analyse möglicher Verbesserungen. Auch in der Schweiz hat die SNV sich mit der ISO 27001 sowie 27002 befasst und bietet ausführliche Informationen.

- 196 -

A Security Framework for Cloud Manufacturing.
Wang, Yazhe; Ma, Shunan; Ren, Lei
In: MSEC, ASME International Manufacturing Science and Engineering Conference, 2014 * (2014) Seite V001T04A022
http://dx.doi.org/10.1115/MSEC2014-4082
Cloud manufacturing has been considered as a promising new service-oriented manufacturing paradigm that can transform traditional industry. However security is one of the major issues which hamper the growth of cloud manufacturing industry. In this paper, we analyze the cloud manufacturing security issues and challenges, and propose a security framework for cloud manufacturing, which includes four levels: infrastructure security, identity and access management, data protection and security, and cloud security as a service. The Infrastructure security level can ensure an organization's core IT infrastructure security at the network, host, and application levels; Identity and access management level can improve operational efficiency and to comply with privacy and data protection requirements; Data protection and security level can help users evaluate their data security scenarios and make informed judgments regarding risk for their organizations; security as a service level, which includes web security service, storage security service and IAM (Identity and Access Management) service, would extract security functions and capacities to assemble software as a service. The cloud manufacturing security framework we proposed can resolve the security issues and improve the security performance of cloud manufacturing industry.

- 197 -

Application of Linear and Non Linear Modified 3D Cellular Automata Rules in Cryptography for Improved Security of Transmitted Data.
Latha, K.; Amirthalingam, S.
In: Advancements in Automation and Control Technologies, ICAAC, International Conference on Advancements in Automation and Control, 2014, in: Applied Mechanics and Materials * Band 573 (2014) Seite 600-604 (5 Seiten)
Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.573.600
http://www.scientific.net/AMM.573.600
Internet is the prime vehicle to disseminate information from one place to another. Providing security to data is a major issue in transmitting data. One way of providing security to the data is encryption and decryption. Normal encryption is the way of changing the plaintext into cipher text using encryption and decryption algorithm and key. Literature reported different methods for encryption. An attempt is made in this paper to propose a modified encryption and decryption process performed with modified cellular automata rules. Cellular automata is idealized parallel processing machine which depends upon the cell value which is updated based on updating rule, which involves the cell and other cell values in a particular neighbourhood. Discrete references were made in the literature on the application of cellular automata rules. However lot more work remains to be done in this area. An attempt is made in this paper to

provide encryption and decryption with cellular automata rules, using Data Encryption Standard (DES) and Advance Encryption Standard (AES) algorithms. They are operated at various stages, with the number of stages involved in sequential and cellular automata operating parallel. The major contribution of present work is, to develop methodology for identifying and application of 1D and 2D cellular automata rules and to fix the issues and challenges there in. A modified cellular automata set of rules are considered to develop 3D cellular automata rules for improved safety. Further a comparison is provided between existing 1, 2D automata rules versus the modified 3D cellular automata rules with respect to certain parameters.

- 198 -

Action Design of Information Systems Security Governance for Bank Using COBIT 4.1 and Control Standard of ISO 27001.
So, Idris-Gautama; Setiadi, N.J.; Papak, B.; Aryanto, Rudy
In: Advances in Applied Materials and Electronics Engineering III, AMEE, International Conference on Applied Materials and Electronics Engineering, 3, in: Advanced Materials Research * Band 905 (2014) Seite 663-668 (6 Seiten)
Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMR.905.663
http://www.scientific.net/AMR.905.663
The aim of the study is to design remediation information systems security governance at Bank. This study provided proposed solutions to solve the existing gaps between the current condition and the expected information systems of the bank's security governance. A case study of a commercial bank is used in this study. There are 7 process frameworks of COBIT 4.1 used to measure the maturity level of information systems security governance. Of these processes, appropriate controls within the framework of COBIT 4.1 and ISO27001 are undertaken. As a result, the security of governance information systems is increasing. In conclusion, there is a need of reliable information systems security governance to achieve the intended business goals.

- 199 -

Secure Communication-Based Train Control: Performance Evaluation of a Design Framework.
Aziminejad, Arash; Seckin, Mustafa
In: JRC, ASME/IEEE Joint Rail Conference, 2014 * (2014) Seite V001T03A011
http://dx.doi.org/10.1115/JRC2014-3816
Railroads are increasingly using Communication-Based Train Control (CBTC) technology to improve service capacity and operating efficiency. CBTC is a mission-critical system under which train monitoring and train control are integrated into a single unified system through data links between vehicles, central processors, and wayside equipment. Radio over fiber technology provides a flexible and efficient solution for the Data Communication System (DCS) which needs to ensure integrity and reliability of message delivery in a transparent manner for the train control functions. A Security Device (SD) is defined as a network entity located between the railroad administration's (the customer) trusted wired network and the non-trusted portion of the DCS network including the radio-based segment, which runs on a customized piece of hardware with a secure operating system and provides secure gateway functionality. This paper puts forward a network architecture and SD software platform design which meets the requirements of a typical CBTC system. The IPSEC protocol used by the SD for data protection renders authentication service through X.509 certificates. A network setup is put together as the proof-of-concept for the presented design proposal and performance assessment is conducted through experimental studies.

- 200 -

Scalable Frameworks for Application Security and Data Protection.
Kabanov, Ilya
In: Global Security, Safety and Sustainability - The Security Challenges of the Connected World, ICGS3, Global Security, Safety, and Sustainability, International Conference, 11, in: Communications in Computer and Information Science * Band 630 (2016) Seite 82-95 (14 Seiten), Paper-Nr. Chapter 7, Cyber Intelligence and Operation
http://dx.doi.org/10.1007/978-3-319-51064-4_7
Nationwide organizations face the challenge of managing the cyber risk profile while delivering software solutions to meet growing and changing requirements of customers, regulators, and internal stakeholders. Companies operate in competing priorities having limited resources available. It is crucial to design and deploy scalable frameworks that help prioritizing actions in the "Identify. Protect. Detect. Respond. Recover." paradigm. Unsecure practices at developing, and deploying applications and dependency on improperly managed web and cloud-based services may lead to data compromise. In the article, the author introduces an approach to identify high-yield opportunities for building cybersecurity capabilities and proposes a framework for delivering application security and compliance on scale. Effective frameworks allow the transformation of costs into value for businesses and their customers through achieving compliance, measuring security risks, and keeping them under control.

- 201 -

Probleme bei Aufgrabungen.
Wesselborg, Hans-Hermann; Hülsbömer, Manuel
In: Straßen- und Tiefbau * Band 70 (2016) Heft 4, Seite 16-18 (3 Seiten, 6 Quellen)

Durch die Tätigkeit von Versorgungs- und Entsorgungsunternehmen entstehen im kommunalen Straßennetz Baumaßnahmen und damit Eingriffe in bestehende Straßenkonstruktionen. Die damit einhergehenden Störungen im Gefüge stellen Schwachstellen im Straßenoberbau dar, die das Qualitätsniveau der betroffenen Straßen senken. Das Risiko von Folgeschäden nach dem Verschließen von Aufgrabungen ist auf Grund der besonderen Rahmenbedingungen des kommunalen Straßenbaus als hoch einzuschätzen. Um dieses Risiko zu minimieren und einen Ansatz zur systematischen Qualitätssicherung zu entwickeln, führte die Senatsverwaltung für Stadtentwicklung der Stadt Berlin im Frühjahr 2010 überarbeitete Vorschriften für die Ausführung von Aufgrabungen ein. Das im Zuge der Überarbeitung der Ausführungsvorschriften eingeführte Kontrollsystem erfüllt die Zielsetzung eines vereinfachten Verwaltungsverfahrens im Sinne eines optimierten Qualitätsmanagements. Mit der Integration eines normierten Punktesystems wird ein repräsentativer Bewertungsmaßstab geschaffen, der eine unabhängige und vergleichbare Bewertung von wiederverschlossenen Aufgrabungsflächen ermöglicht. Die wissenschaftliche Begleitung und Auswertung der Kontrollprüfungen hat ergeben, dass bereits kurz nach der Einführung des Kontrollsystems positive Ergebnisse im Sinne einer Reduktion an mangelhaften Ausführungen und Qualitäten von Aufgrabungen aufgezeigt werden konnten. Dieser Trend konnte durch die Auswertung von drei Prüfzyklen und einer zeitlichen Disposition von rund drei Jahren verifiziert werden.

- 202 -

Cyberangriffe abwehren: Gefahr aus dem Verborgenen.
Pesch, Peter
In: P&A : Prozesstechnik & Automation * Band 13 (2016) Heft 9, Seite 20-22 (3 Seiten)

Je stärker Maschinen und Anlagen vernetzt sind, desto anfälliger sind sie auch für Datendiebstähle und Sabotage. Ist ein Gerät im Unternehmen infiziert, greifen Schadprogramme schnell auf das ganze Netzwerk über. Schutz bietet eine Reihe von bewährten Verfahren und Verhaltensweisen. Es ist ein häufiges Szenario bei Cybertattacken: Ein Mitarbeiter erhält eine offiziell aussehende E-Mail vom Verantwortlichen für IT-Sicherheit des Unternehmens. Diese fordert die Mitarbeiter dazu auf, sofort einen wichtigen Sicherheitspatch zu installieren. Dafür müsse lediglich auf den angegebenen Link geklickt werden. Führt ein wohlmeinender Mitarbeiter den scheinbar berechtigten Link aus, ermöglicht er Schadprogrammen den Zugriff auf das Gerät. Der übliche Ablauf bei Cyberattacken sieht folgendermaßen aus: Der Angreifer nutzt eine Schwäche im Netzwerk des Opfers, um die Malware einzuschleusen. Solche gezielten Übergriffe auf Schwachstellen in Soft- und Hardware nennt man Zero-Day-Attacken. Sie nützen Lucken aus, die unbekannt sind oder von den Herstellern der Komponenten noch nicht behoben wurden. Oft setzen die Angreifer auf das fehlende Verständnis der Anwender, gefälschte E-Mails oder Dateien zu erkennen. Die Bedrohung durch Cyber-Angriffe für produzierende Unternehmen lässt sich an der Vielzahl von Fälschungen und Kopien, von Fahrzeugen bis hin zu komplexer Militärausrüstung, erahnen, die den Markt überschwemmen. Hersteller müssen sich darauf einstellen, dass es Cyber-Kriminelle auf alle Arten von Produkten und geistigem Eigentum abgesehen haben. Eine genaue Betrachtung der einzelnen Bereiche von Produktionsanlagen kann Aufschluss über das Bedrohungspotential für einen Hersteller geben. Daraus lassen sich Maßnahmen ableiten für den Schutz seiner Investitionen und seines geistigen Eigentums. Das Herz der Netzwerksicherheit ist die Segmentierung. Sie sollte in jedem Werk eingesetzt werden. Das gewährleistet mehr Sicherheit und Effizienz bei der Verwaltung durch die Einrichtung einer industriellen demilitarisierten Zone (IDMZ), die das Netzwerk in kleinere Segmente oder Subnetze unterteilt. Bei diesem Verfahren wird die Sicherheit auf verschiedene Switch-Ebenen verteilt und der Zugang von Benutzern auf bestimmte vorgegebene Bereiche beschränkt. Auch wenn normaler, unauffälliger Netzwerkbetrieb herrscht, müssen die IT-Sicherheitsexperten wachsam sein. Normaler Netzwerkbetrieb bedeutet nicht unbedingt, dass keine Gefahren bestehen. Cyber-Angriffe lauern im Verborgenen und sind speziell darauf ausgelegt, elektronische Sicherheitssysteme zu überwinden. Kriminelle Aktivitäten lassen sich früher erkennen, wenn Protokolle, Anmeldedaten und Zeitstempel regelmäßig auf unerwartete Änderungen hin überprüft werden. Beim Fachpersonal sollten Unternehmen außerdem nicht sparen. Für die IT-Sicherheit bedarf es gut ausgebildeter Mitarbeiter. Um mit der Entwicklung der Schadprogrammen mithalten zu können, muss das dafür zuständige technische Personal regelmäßig in den Bereichen Mathematik, Informatik, Naturwissenschaften und Technologie (MINT-Fächer) weitergebildet werden. Investitionen in Aus- und Weiterbildung sind erheblich günstiger als Produktionsausfälle oder der Verlust kritischer Unternehmensdaten.

- 203 -

Deploying Mobile Construction Inspection Forms as a Case Study for Technology Adoption.
Vogt, Brett D.; Belcher, Raymond E.
In: IPC, International Pipeline Conference, 11 * (2016) Seite V002T02A017
http://dx.doi.org/10.1115/IPC2016-64637

Within pipeline construction field inspection data collection relies mostly on archaic systems and processes. For almost all projects, paper-based or at best word processor and spreadsheet reports are manually collected, reviewed, aggregated and archived. The effort and error in this typical process is reduced using a mobile inspection form system that simplifies the field data collection workflow, increases data accuracy and quality, and can be used to generate dynamic project management dashboards. An evaluation of two case study projects provides insight to overcom-

ing technology adoption for pipeline construction as well as performance, quality and forecasting benefits witnessed during these projects. The use of a mobile inspection form system creates the ability for improved analytics such as detailed construction tracking, dynamic forecasting and spatial overlays of construction progress. Improved data standardization and data integrity from the use of tablet forms produces detailed and functional key performance indicators (KPIs) delivered on-demand through a project dashboard. When both field data quality is improved and project managers are provided timely KPIs, projects have the opportunity to be delivered safer, faster and with higher quality, which is a win for the entire pipeline industry.

- 204 -

The hard truth about hardware in cyber-security: it's more important.
Wagner, Mathias
In: Network Security * Band 2016 (2016) Heft 12, Seite 16-19 (4 Seiten, 5 Quellen)
http://dx.doi.org/10.1016/S1353-4858(16)30117-9
When it comes to cyber-security, there is currently an emphasis on the need for software to be secured, while hardware appears to have taken a back seat. However, a recent Kaspersky report showed that 92% of hosts connected to Industrial Control Sstems (ICS) contained vulnerabilities that can be exploited to attack, take over or even harm devices and their normal mode of operation.

- 205 -

Vulnerability Analysis of Software Defined Networking.
Zerkane, Salaheddine; Espes, David; Parc, Philippe Le; Cuppens, Frederic
In: Foundations and Practice of Security, FPS, International Symposium on Foundations and Practice of Security, 9, in: Lecture Notes in Computer Science, Security and Cryptology * Band 10128 (2017) Seite 97-116 (20 Seiten), Paper-Nr. Chapter 7, Vulnerability Analysis and Security Metrics
http://dx.doi.org/10.1007/978-3-319-51966-1_7
Security of Software Defined Networking (SDN) is an open issue because of many reasons. Security requirements were not considered in the primary definition of SDN. Consequently, SDN enlarges the network vulnerability surface by introducing new vulnerabilities that do not exist in the conventional networking architecture. In addition, there are neither security risk management processes nor mathematical models that specifically address SDN security and the influence of its specific features. We provide a vulnerability analysis for SDN to study these weaknesses and to measure their impacts. Our analysis specifies a model of SDN assets that needs to be protected. Then, it derives 114 SDN generic vulnerabilities using standardized security objectives. It relies on an open standardized semi qualitative semi quantitative scoring system to calculate the severities of theses vulnerabilities. Then, it adapts them to SDN specific features using Analytical Hierarchical Process (AHP).

- 206 -

Zentralisierte Security-Orchestrierung. Datensicherheit für das IIoT: Industrieanlagen schützen.
O'Connell, Larry; Hill, Roger
In: Elektronik Industrie * Band 47 (2016) Heft 11, Seite 134-136 (3 Seiten, Bilder)
http://www.all-electronics.de/ei/
Über das industrielle Internet der Dinge (IIoT) sind Industrieanlagen sowie Maschinen und Geräte von Produktionsprozessen miteinander verbunden - Tendenz steigend. Während Automatisierer der mit dem IIoT erreichbaren Produktivitätssteigerung applaudieren, erleben Sicherheitsexperten schlaflose Nächte. Sicherheit in Industrienetzwerken lässt sich entweder durch Isolation oder durch Implementierung einer Firewall zwischen Unternehmens- und Industrienetzwerk erreichen. Maßnahmen zur Sicherung dieser Netzwerke in größerem Umfang erfordern normalerweise kostspielige Änderungen der Netzwerktopologie oder verursachen Netzwerkausfallzeiten, was sich negativ auf den Umsatz, die Produktivität und in manchen Fällen sogar auf die Funktionssicherheit auswirkt. Doch was wäre, wenn Administratoren von Industrienetzwerken bestehende Netzwerke schnell und problemlos um Security-Applikationen und Policies erweitern könnten? Was wäre, wenn es möglich wäre, dies mit minimaler Netzwerkausfallzeit und ohne die Netzwerkkomplexität zu erhöhen getan werden könnte? Dies verspricht ein Top-Down-Konzept für die Sicherheit von Industrienetzwerken - ein Konzept auf Basis zentraler Security-Orchestrierung mit programmierbaren und aufgeteilten Sicherheitszonen.

- 207 -

Richtungsweisend. Mehr Datensicherheit für die Industrie 4.0.
Haydt, Mary Sue
In: Elektronik Industrie * Band 47 (2016) Heft 11, Seite 32-35 (4 Seiten, Bilder)
http://www.all-electronics.de/ei/

Das Grundprinzip von Industrie 4.0 - die konsequente Vernetzung aller industriellen Komponenten - steigert zwar die Leistungsfähigkeit einer Fabrik, macht sie allerdings auch anfälliger für Hacker-Angriffe. Fünf wichtige Regeln helfen dabei, dennoch die erforderliche Datensicherheit zu gewährleisten. Der Aufbau eines industriellen Geräts, das in der neuen, anspruchsvollen Umgebung von Industrie 4.0 sicher arbeitet, verlangt ein durchgehendes Sicherheitsdesign, das die Datensicherheit und Zuverlässigkeit des vernetzten Geräts über den gesamten Lebenszyklus adressiert. Dies erfordert eine Sicherheitsarchitektur, die einen sicheren Betrieb garantiert und gewährleistet, dass Schlüssel, Zertifikate und sensible Daten während des gesamten Betriebs und bereits in der Fertigung durch eine Enterprise-Security-Infrastruktur geschützt sind. Die optimale Auswahl der Geräte- und Enterprise-Security-Lösungen hängt von den Betriebs- und Fertigungsumgebungen genauso ab wie von geschäftlichen Abwägungen. Hier bieten sich Experten in diesen Bereichen für eine eingehende Beratung an.

- 208 -

Research on Data Mining Optimization and Security Based on MapReduce.
Xia, Hui
In: Information Technology Applications in Industry III, ICITMI, International Conference on Information Technology and Management Innovation, 3, in: Applied Mechanics and Materials * Band 631-632 (2014) Seite 1053-1056 (4 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMM.631-632.1053
http://www.scientific.net/AMM.631-632.1053

The paper addressed the issues of limited resource for data optimization for efficiency, reliability, scalability and security of data in distributed, cluster systems with huge datasets. The study's experimental results predicted that the MapReduce tool developed improved data optimization. The system exhibits undesired speedup with smaller datasets, but reasonable speedup is achieved with a larger enough datasets that complements the number of computing nodes reducing the execution time by 30% as compared to normal data mining and processing. The MapReduce tool is able to handle data growth trendily, especially with larger number of computing nodes. Scaleup gracefully grows as data and number of computing nodes increases. Security of data is guaranteed at all computing nodes since data is replicated at various nodes on the cluster system hence reliable. Our implementation of the MapReduce runs on distributed cluster computing environment of a national education web portal and is highly scalable.

- 209 -

Research on Method of Information System Information Security Risk Management.
Cao, Xiao-Li
In: Progress in Applied Sciences, Engineering and Technology, ICMSCE, International Conference on Materials Science and Computational Engineering, 2014, in: Advanced Materials Research * Band 926-930 (2014) Seite 4105-4109 (5 Seiten) Zürich: Trans Tech Publications
http://dx.doi.org/10.4028/www.scientific.net/AMR.926-930.4105
http://www.scientific.net/AMR.926-930.4105

With the popularity of the Internet and global information continues to advance organizational information systems have become an important strategic resource for the survival of the importance of information security to protect its widespread concern. Once the information security organization information system is destroyed, the Organization for Security attribute information would cause tremendous impact the organization's business operation, the losses include not only economic, but also likely to organize image, reputation is a strategic competitive advantage even fatal injuries. However, the existing information systems of information security risk management approach to information system risk analysis and assessment with specific organizational environment and business background with fragmentation, lack of risk analysis and description of the formation process, carried only consider "technical" factors security decisions, lack of full expression to achieve the desired goal of a number of decisions on organizational decision-making. Therefore, the information system to carry information security risk management is essential.

- 210 -

Invisible watermarking optical camera communication and compatibility issues of IEEE 802.15.7r1 specification.
Le, Nam-Tuan
In: Optics Communications * Band 390 (2017) Seite 144-155 (12 Seiten, 27 Quellen)
http://dx.doi.org/10.1016/j.optcom.2016.12.073

Copyright protection and information security are two most considered issues of digital data following the development of internet and computer network. As an important solution for protection, watermarking technology has become

one of the challenged roles in industry and academic research. The watermarking technology can be classified by two categories: visible watermarking and invisible watermarking. With invisible technique, there is an advantage on user interaction because of the visibility. By applying watermarking for communication, it will be a challenge and a new direction for communication technology. In this paper we will propose one new research on communication technology using optical camera communications (OCC) based invisible watermarking. Beside the analysis on performance of proposed system, we also suggest the frame structure of PHY and MAC layer for IEEE 802.15.7r1 specification which is a revision of visible light communication (VLC) standardization.

- 211 -

Gathering Information from Transport Systems for Processing in Supply Chains.
Kodym, Oldrich; Unucka, Jakub
In: Open Engineering * Band 6 (2016) Heft 1, Seite 1-5 (5 Seiten, 16 Quellen) Warsaw: De Gruyter Open
http://dx.doi.org/10.1515/eng-2016-0096
Paper deals with complex system for processing information from means of transport acting as parts of train (rail or road). It focuses on automated information gathering using AutoID technology, information transmission via Internet of Things networks and information usage in information systems of logistic firms for support of selected processes on MES and ERP levels. Different kinds of gathered information from whole transport chain are discussed. Compliance with existing standards is mentioned. Security of information in full life cycle is integral part of presented system. Design of fully equipped system based on synthesized functional nodes is presented.

- 212 -

Review on the IT security: attack and defense.
Krit, Salah-Ddine - E-Mail:salahddine.krit@gmail.com; Haimoud, Elbachir - E-Mail:elbachirhaimoud@gmail.com
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ICEMIS.2016.7745386
Information technology security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. This paper gives an overview of information security management systems. By the end of this paper you should have developed an understanding of: some tactics used by hackers to hack into systems, computers, web servers, android phone, email, infrastructure systems and more. And conversely some precautions used to raise up the systems security level. This paper is dedicated for institutions, individuals, and every person interested in IT security..

- 213 -

Implementation of information security and data processing center protection standards.
Karaseva, Viktoria A. - E-Mail:golbery@yandex.ru; Kunakov, Egor P. - E-Mail:egor-kunakov@mail.ru; Lontsikh, Pavel A. - E-Mail:palon@list.ru; Livshitz, Ilia I. - E-Mail:livshitz.il@yandex.ru; Nikiforova, Ksenia A. - E-Mail:nikiforova.k.a@yandex.ru
In: (2016) p 138-43 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ITMQIS.2016.7751923
The article deals with the issue of information security. The purpose of the research is to analyze information security procedures, development information security systems and implementation of international information security standards. Information security involves both storing and accessing sensitive information and data warehousing. It can be carried out with Data Processing Centers. A number of standards were developed to improve efficiency of information security departments. One of them is ISO/IEC 27001. It involves requirements to information security management systems which are obligatory for certification. Along with management elements for computers and networks, ISO/IEC 27001 specifies the issues of security policy development, staff relations. Processed information security is one of the crucial issues when creating new data processing centers. Accordingly, reliability and fault-tolerance of data centers in the Uptime Institute's Tier Classification System are paid special attention to. Operational Sustainability is an additional characteristics to asses DPC's performance. Advantage of the standard is due to the flexibility of its requirements which enable objective evaluation of DPC's performance at the design stage and comparison of the current performance. Data centers can be awarded with Tier 1 to 4 depending upon the degree of reliability. Tiers is progressive: each Tier incorporates the requirements of all the lower Tiers. The Uptime Institute also developed Tier Standard: Topology and Tier Standard: Operational Sustainability which specify the methods of DPC performance evaluation. The article analyzes the key points of these standards, their advantages and implementation experience in Russian organizations..

- 214 -

2016 International Conference on Information Technology for Organizations' Development (IT4OD), Fez, Morocco, 30 March-1 April 2016.
anonym
In: 2016 (462 pp) Piscataway, NJ, USA: IEEE
The following topics are dealt with: software engineering and business intelligence; information security management; telecommunication and transmission systems; information management and service integration; multimedia information processing; wireless and network computing; natural language processing, machine learning and semantic analysis; and smart systems and green technology..

- 215 -

Mapping information security standard ISO 27002 to an ontological structure.
Fenz, Stefan - E-Mail:stefan.fenz@tuwien.ac.at; Plieschnegger, Stefanie; Hobel, Heidi
In: Information and Computer Security, UK * vol 24 (2016) no 5, p 452-73, 25 refs.
http://dx.doi.org/10.1108/ICS-07-2015-0030
http://www.emeraldinsight.com/loi/ics
Purpose: The purpose of this paper is to increase the degree of automation within information security compliance projects by introducing a formal representation of the ISO 27002 standard. As information is becoming more valuable and the current businesses face frequent attacks on their infrastructure, enterprises need support at protecting their information-based assets. Design/methodology/approach: Information security standards and guidelines provide baseline knowledge for protecting corporate assets. However, the efforts to check whether the implemented measures of an organization adhere to the proposed standards and guidelines are still significantly high. Findings: This paper shows how the process of compliance checking can be supported by using machine-readable ISO 27002 control descriptions in combination with a formal representation of the organization's assets. Originality/value: The authors created a formal representation of the ISO 27002 standard and showed how a security ontology can be used to increase the efficiency of the compliance checking process..

- 216 -

Information Security Standards in Healthcare Activities.
Gaiveo, Jose
In: International Journal of Reliable and Quality E-Healthcare, USA * vol 5 (2016) no 4, p 15-33, 20 refs.
http://dx.doi.org/10.4018/IJRQEH.2016100102
Information is mandatory in healthcare activities and in all that are related to it. In this same sense, people that deal with those information requires attention because patients information could be exposed. The use of directions stated by information security standards might allow a proactive attitude in the face of the diversity of threats that as the potential to explore the vulnerabilities of organizational assets. This article intends to recognize information threats and vulnerabilities that could be explored, using information security international standards to support the activities needed to assume information safeguard. Another intention is the establishment of a basis of references in information security to define a level of risk classification to build a referential to the potential that a given threat has to exploit the vulnerabilities of informational assets, preventing damages to personal and organizational property, and also activity continuity, assuming information as the main resource..

- 217 -

Security evaluation of cryptosystems used in cloud networks.
Sadkhan, Sattar B. - E-Mail:drengsattar@ieee.org; Abdulraheem, Farqad H. - E-Mail:frqhm@yahoo.com
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/AIC-MITCSA.2016.7759955
Cloud networking is the next generation architecture of IT. Clouds are very complex architectures. They have a replicated thousands of times, and common functional units and can be reduced to simple primitives. many issues related to security were created by complexity of cloud networking as well as all aspects of Cloud networking. Data security is one of the most important issues. The Cloud usually has a one security architecture but has many customers with variety requests. There are new risks introduced by clouds, like multi-tenancy, virtualization and data outsourcing in additional to existing security risks related to Cloud service providers (CSPs) and cloud customers (CCs). information security and their conformity with cloud networking security challenges targeted by Several international and industrial standards. Since there is a continuous increase in the field of communication regarding advanced data, there is an increase in need for time and statistical overhead that is associated with the application of cryptographic. Parallelizing the computation of cryptographic algorithms on many-core computing platforms can be a promising approach to reduce the execution time and eventually the energy consumption of such algorithms. In this paper we will analyze and compare a some of cryptosystems security evaluation approaches worked in cloud networking environment and depended on variety parameters to explain these approaches and show how it work in the few last years with the great modifying in cloud and great data growing..

- 218 -

Theorising on risk homeostasis in the context of information security behaviour.
Kearney, Wayne D.; Kruger, Hennie A. - E-Mail:hennie.kruger@nwu.ac.za
In: Information and Computer Security, UK * vol 24 (2016) no 5, p 496-513, 67 refs.
http://dx.doi.org/10.1108/ICS-04-2016-0029
http://www.emeraldinsight.com/loi/ics
Purpose: The purpose of this paper is to discuss and theorise on the appropriateness and potential impact of risk homeostasis in the context of information security. Design/methodology/approach: The discussion is mainly based on a literature survey backed up by illustrative empirical examples. Findings: Risk homeostasis in the context of information security is an under-explored topic. The principles, assumptions and methodology of a risk homeostasis framework offer new insights and knowledge to explain and predict contradictory human behaviour in information security. Practical implications: The paper shows that explanations for contradictory human behaviour (e.g. the privacy paradox) would gain from considering risk homeostasis as an information security risk management model. The ideas discussed open up the prospect to theorise on risk homeostasis as a framework in information security and should form a basis for further research and practical implementations. On a more practical level, it offers decision makers useful information and new insights that could be advantageous in a strategic security planning process. Originality/value: This is the first systematic comprehensive review of risk homeostasis in the context of information security behaviour and readers of the paper will find new theories, guidelines and insights on risk homeostasis..

- 219 -

A methodological proposal concerning to the management of information security in industrial control systems.
Diaz, Paul - E-Mail:mpdiaz@espe.edu.ec; Fuertes, Walter - E-Mail:wmfuertes@espe.edu.ec; Toulkeridis, Theofilos - E-Mail:ttoulkeridis@espe.edu.ec
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ETCM.2016.7750821
The most recent international reports of security issues documented a growing number of cybernetic attacks to Industrial Control Systems. Therefore, an increase of information technology implementations in manufacturing processes arose offering solutions in Information Security of the involved manufacturers and professionals. In this respect, a notable tendency emerges in which information security has been particularly intended to be used in businesses' administrative areas, where ISO-27000 is the most favored standard. Nonetheless, it has been determined that ISO is not yet an ideal standard for an industrial approach, due to the fact that it has not been created for these systems. We designed and implemented a methodology for the management of information security of the Industrial Control Systems of industrial businesses, based on standards issued by NIST. Such methodology presents the development of a series of phases, which provide two main contributions: firstly a group of strategies to reduce risks and secondly a Guide for standards-based instructions as well as security policies for the effective management of information security..

- 220 -

Method for information system risk management based on Markov logic networks.
Chen Yu; Wang Jindong; Wang Kun; Wang Yadi
In: Computer Engineering and Applications, China * vol 52 (2016) no 18, p 104-10, 17 refs.
http://cea.ceaj.org/EN/article/showOldVolumn.do
http://dx.doi.org/10.3778/j.issn.1002-8331.1512-0029
Recent years, in practices of the information security risk management of enterprises, there is no quantitative method to develop risk management scheme and select risk management tools, and manual risk analysis always takes too much time. In this paper, it proposes an information security risk management approach based on Markov logic network. First, it uses Markov logic network to describe dependencies between the components and services of the evaluated systems. Next, it uses marginal reasoning model of Markov logic network to estimate the system availability in case of different risk management measures, so as to provide a quantitative basis for the selection of management measures. Case studies show that, this method can provide reliable quantitative basis for selecting information system security risk management measures for enterprise, and the method is simple to implement..

- 221 -

Time-related vulnerability lookahead extension to the CVE.
Bhuddtham, Thanapon - E-Mail:Thanapon.B@ku.th; Watanapongse, Pirawat - E-Mail:Pirawat.W@ku.th
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/JCSSE.2016.7748927
Software scanning against the vulnerability database is one of the regular activities required by all information security management standards. However, the nature of the scanning system itself is reactive; a vulnerability has to be found, then the announcement made, with (and sometimes without) fixes. However, there exist classes of knowledge that are significant, reliable, and can be easily obtained, but are not represented in the vulnerability database. One such knowledge is the time-related vulnerabilities that signify the increasing risk of the system through time. We

therefore explore the design and implementation in representing and appending this information, and thus propose an extension to the original Common Vulnerabilities and Exposures (CVE) database, called Time-Related Vulnerability Lookahead Extension to the CVE (T-CVE). This extension would complement the classical CVE in providing a publicly early-warning system so that the information security managers will be able to proactively assess their resources' C-I-A risks through trend analysis and will be able to mitigate them in a timely fashion. This work will initially focus on four proactive time-related information categories, namely the obsolete (software) platform, out-of-date (malware) signature, (hardware) degradation due to wear-and-tear, and (software) expiry. Obviously, other categories can later be similarly appended based on this framework..

- 222 -

Storage and search tool for cloud provider security information in CSA STAR.
Phattanateeradej, Chosita - E-Mail:chosita.ph@student.chula.ac.th; Senivongse, Twittie - E-Mail:twittie.s@chula.ac.th
In: 2016 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/JCSSE.2016.7748935

At present, cloud computing is becoming a major IT service model. As the number of cloud providers is growing, prospective cloud consumers face difficulties in choosing the right provider for their use. As security is among the most important factors for the consumers to decide whether or not to adopt cloud services, cloud providers have to assure prospective consumers that the provided service is secure and can be trusted. One way is to publish security information of the service on Cloud Security Alliance's Security, Trust, & Assurance Registry (or CSA STAR) website. STAR offers three levels of providers' security information, i.e. self-assessment, 3rd-party-assessment-based certification, and continuous-monitoring-based certification. However, the STAR website does not provide a convenient and useful way for cloud consumers to find security information of the providers when they are selecting a cloud service. The consumers, for example, have to know provider names and cannot search for providers by certain security criteria. To address such limitations, this paper presents a development of a storage and search tool based on the security information published on the STAR website. The tool stores and synchronizes providers' security information with the CSA STAR website, and allows consumers to search by different security criteria based on CSA's Cloud Controls Matrix (CCM) security guideline and its accompanying CAIQ security questionnaire. The tool can also compare and visualize providers' security information. Hence it makes the CSA STAR information more accessible and more useful to prospective consumers when selecting cloud services..

- 223 -

Ranking criteria of enterprise information security architecture using fuzzy topsis.
Jalayer, Farzaneh Sadat; Nabiollahi, Akbar
In: International Journal of Computer Science & Information Technology, India * vol 8 (2016) no 5, p 44-58, 23 refs.
http://airccse.org/journal/ijcsit2012_curr.html
http://dx.doi.org/10.5121/ijcsit.2016.8504

Information security against hacking, altering, corrupting, and divulging data is vital and inevitable and it requires an effective management in every organization. Some of the upcoming challenges can be the study of available frameworks in Enterprise Information Security Architecture (EISA) as well as criteria extraction in this field. In this study a method has been adopted in order to extract and categorize important and effective criteria in the field of information security by studying the major dimensions of EISA including standards, policies and procedures, organization infrastructure, user awareness and training, security base lines, risk assessment and compliance. Gartner's framework has been applied as a fundamental model to categorize the criteria. To assess the proposed model, a questionnaire was prepared and a group of EISA professionals completed it. The Fuzzy TOPSIS was used to quantify the data and prioritize criteria. It could be concluded that the database and database security criteria, inner software security, electronic exchange security and supervising malicious software can be high priorities..

- 224 -

2015 International Conference on Computational Intelligence and Communication Networks (CICN). Proceedings, Jabalpur, India, 12-14 Dec. 2015.
anonym
In: 2015 (487 pp) Los Alamitos, CA, USA: IEEE Computer Society

The following topics are dealt with: microwave theory; integrated circuits; MW components; wireless networks; MANET; VANET; sensor networks; image processing; medical imaging; biomedical applications; signal processing; communication standards; computational intelligence; machine learning; data mining; cloud computing; big data; social networks; cryptography; steganography; network security; information security; neural networks; digital design; VLSI; Web services; ontology; power systems; control systems; smart homes; and intelligent systems..

- 225 -

Implementation of security model in cognitive networks.
Pandey, Nitin - E-Mail:npandeyg@gmail.com; Saini, Natasha - E-Mail:natashamaniktahla@gmail.com
In: (2016) p 2055-8 Piscataway, NJ, USA: IEEE, 2016
http://dx.doi.org/10.1109/ICCSP.2016.7754538
The paper will describe various types of security issues which include confidentiality, integrity and availability of data. There exists various threats to security issues traffic analysis, snooping, spoofing, denial of service attack etc. This paper focuses on symmetric and asymmetric cryptography. A new model is proposed RES(Requirement Encryption Standard) which combines various security parameters. There exists various security models in modern cryptography. However there still exists various security threats. RES is a new proposed model which overcomes various security active and passive attacks..

- 226 -

The architecture for data, security and application in Digital Earth platform.
Fang Miao - E-Mail:miaofang@.com; Huayue Chen; Wenhui Yang; Ye Ansheng
In: IOP Conference Series: Earth and Environmental Science, UK * vol 46 (2016)
http://dx.doi.org/10.1088/1755-1315/46/1/012050
Digital Earth platform is an application, service and decision support system, which integrates geo-spatial data acquisition, transmission, storage, processing, analysis, statistics and visualization. It realizes comprehensive management and widely application of different kinds of huge earth data under the geo-spatial framework and in a open environment. It should consider the continues growing of data and applications, as well as data security. According to the issues of how to safely use spatial data in Digital Earth platform, an architecture for data,security and application in Digital Earth platform was proposed in this paper. We call this architecture DOA(DOSA). In the digital earth platform on its goal is the Trusted Data. DOA(DOSA) and Trusted Data can provide data management, security grantee, application supporting for Digital Earth platform..

- 227 -

The new aspects for the instantaneous information security audit.
Livshitz, Ilya I. - E-Mail:livshitz.il@yandex.ru; Nikiforova, Kseniya A. - E-Mail:nikiforova.k.a@yandex.ru; Karasev, Sergey N. - E-Mail:sergei-karasev@yandex.ru; Lontsikh, Pavel A. - E-Mail:palon@list.ru
In: (2016) p 125-7 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ITMQIS.2016.7751920
This publication discusses the problem concerning the concept of the instantaneous information security (IT-Security) audits directed, including providing protection against 'zero-day' threats. It is noted that effective 'zero-day' counteraction based on implementation a set of preventive IT-Security controls, but not limited new technical facilities installation only. A key feature of this concept of instantaneous IT-Security audits is to assess how the left limit of the protection level in the process of IT-Security audits performing. Methodological basis of the concept of instantaneous IT-Security audits are ISO 27001 and 19011 standards series, supplemented by many (expandable) IT-Security metrics to quantify the object protection level. The obtained results can find application in create of models and methods of IT-Security audits performing and continuous improvement of an object protection under the influence of IT-Security violation threats..

- 228 -

CODA footprint continuous security management platform.
Grigorescu, Octavian - E-Mail:octavian.grigorescu@codaintelligence.com; Rughinis, Razvan - E-Mail:razvan.rughinis@cs.pub.ro; Sandescu, Cristian - E-Mail:cristian.sandescu@codaintelligence.com
In: 2016 Piscataway, NJ, USA: Networking in Education and Research, Bucharest, Romania, 7-9 Sept. 2016 * Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/RoEduNet.2016.7753223
World wide data infrastructure has increased in dimension and complexity due to consolidation, centralization and virtualization trends during the last 10 years. The enlargement of cloud services from data centers, the possibility of connecting different types of devices (Internet of Things) and the policy of authorizing employees to bring personally owned mobile devices to their work sites to access sensitive company information ('bring you own device') significantly increase daily challenges for cyber-security professionals. We propose a continuous security management platform, CODA Footprint, that audits an entire organization's critical services in real-time, analyzes whether the organization's critical services are adequately protected, and makes sure the information security defenses are effective 24/7..

- 229 -

A kind of Cyberspace security framework design and risk assessment method.
Zhou Wei; Xie Wenbin; Li Lei
In: Computer Engineering and Applications, China * vol 52 (2016) no 18, p 122-6, 15 refs.
http://cea.ceaj.org/EN/article/showOldVolumn.do
http://dx.doi.org/10.3778/j.issn.1002-8331.1603-0103
This paper, after researching the security requirements of Cyberspace, through security engine and mobile security middleware technology, to solve the problem of the heterogeneity and security of the mobile terminal, puts forward a security architecture in abstract level of Cyberspace and gives out the technical description. The system combines the technique of risk management, and integrates variety of security technology and security levels, realizes the effective protection of Cyberspace environment. At the same time, it puts forward an information security risk assessment method based on hidden markov models. Computer simulation experiment results show that to realize the quantitative evaluation of Cyberspace security risk, the method has certain feasibility..

- 230 -

A roadmap to the realization of wireless body area networks: a review.
Saarika, U. - E-Mail:saarika.niharika@gmail.com; Sharma, Purnima K. - E-Mail:purnima.kadali@gmail.com
In: (2016) p 439-43 Piscataway, NJ, USA: IEEE
http://dx.doi.org/10.1109/ICEEOT.2016.7755538
Wireless Body Area Network (WBAN) is extremely useful emerging technology having enormous utilities and benefits in everyday life not only for health care but also for athletic guidance, public protection, and end user electronics. With the arrival of less power and inexpensive wireless connectivity innovations, Body area Networks could be implemented using available complementary technology. Nonintrusive, miniature wearable sensors allow compilation of large amount of information mechanically, decreasing the cost and decreasing of regular visits to the doctor. In this paper, a comprehensive survey on the various aspects of the WBAN consisting of stand-alone sections on the standards for WBAN, Challenging issues of WBANs, key security necessities for information security and privacy furthermore different applications of WBANs are discussed..

Herausgeber
WTI-Frankfurt eG, Ferdinand-Happ-Straße 32, D-60314 Frankfurt am Main,

Redaktionsleitung
Holger Grebe
Telefon: +49 69 4308-222, Telefax: +49 69 4308-200, E-Mail: tecscan@wti-frankfurt.de

Abonnementverwaltung
Claudia Buchhold
Telefon: +49 69 4308-238, Telefax: +49 69 4308-200, E-Mail: tecscan@wti-frankfurt.de

Themen, Preise und Bezugsbedingungen
Bitte entnehmen Sie die gewünschten Informationen für ein Jahresabonnement (Laufzeit 12 Monate) einer ***Einzelplatznutzung*** bzw. für eine ***Netzwerknutzung*** unserer Homepage www.wti-frankfurt.de. Das Abonnement gilt für das Kalenderjahr, es verlängert sich jeweils um ein Jahr, wenn es nicht spätestens sechs Wochen vor Jahresende schriftlich gekündigt wird.
Volltexte können über https://www.tib.eu/de/ausleihen-bestellen/tib-dokumentlieferung/ bezogen werden.
Die Preislisten dazu finden Sie hier: https://www.tib.eu/de/ausleihen-bestellen/tib-dokumentlieferung/preise/