Security knowledge representation artifacts for creating secure IT systems.

Abstract
The creation of secure applications is more than ever a complex task because it requires from system engineers increasing levels of knowledge in security requirements, design and implementation. In fact, the fast increasing size and volatility of this knowledge has reached a point in which it is unrealistic to expect that system engineers can keep up to date with it. The most prominent paradigm for addressing this problem is the use of security patterns to communicate security knowledge from experts to system designers. This, and other security artifacts, have proved their utility and benefits in the past years, improving the way security is taken into account by system engineers and developers. On the other hand, these artifacts have some limitations that have prevented them from becoming more widespread. In particular, security patterns are human-oriented and as such heavily based on natural language, which implies intrinsic high degrees of imprecision and ambiguity. In our opinion, we need to make the move from purely human-oriented artifacts to hybrid artifacts that convey information for both humans (engineers and designers) and computer tools (engineering and development environments). Therefore, we have created a new security knowledge representation artifact that aims to cover the needs of system engineers and help them not only in applying a solution, but also in understanding the security aspects of a given domain as a highly-related set of security concepts (e.g. properties, requirements, solutions, etc.). This artifact, called Domain Security Metamodel (DSM), is, as its name suggests, domain-specific and contains information about all security aspects that are relevant in a specific domain.

Autor
Ruiz, Jose F.; Arjona, Marcos; Mana, Antonio; Rudolph, Carsten

Institution
Atos, Madrid, ES; Universidad de Malaga, ES; Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt, DE

Quelle

Dokumentart
J Zeitschrift

Erscheinungsjahr
2017