Universidad Carlos III de Madrid

OO/UC3M/22 - EVALUATION AND INTEROPERATIBILITY OF SECURITY PROTOCOLS and ARQUITECTURES

During the last years, use of security protocols has increased significantly. Protection of the communications had been provided by security protocols and architectures, however some problems have appeared, revealing that the potential expansion of ICT can be limited if some interoperability problems are not solved. Our group have created and implemented a new methodology in order to reduce the interoperability problems of the implementations of security protocols and architectures. This methodology develops a completed conformance evaluation with the particular security standard and furthermore realizes a performance analysis of the more important parameters for the development of security protocols.

Description of the technology
Communication networks have become a key component of information technologies, being the means through which computer systems all around the world, independently of their nature (from personal computers to ATMs, and on-board computers in high-end cars) share the information they need in order to accomplish the tasks they are charged with. These information exchanges are carried out following the guidelines of communications protocols, which guide and direct the way in which several entities exchange information in the most efficient and convenient way. As it happens more often than not, these information exchanges require some security services to be present (such as confidentiality, authentication or non-repudiation) which are not included in protocols designed in the early years of communication networks (those same protocols that are now widely spread and used nowadays). In order to provide with a solution for this need for security, security protocols and architectures which provide security services to other network protocols have been standardized. Security architectures are widely spread thanks to its seamless integration with applications and users, and also due to its integration with next-generation communication protocols provides a means for migrating to those new protocols in a safe and more convenient way. However, with the use of these security protocols and architectures new problems have emerged, some of which are the interoperability issues among different implementations of those protocols and architectures, or an increased chance to suffer attacks that consume the available computational capabilities. In order to gather information about those implementations that helps to prevent these kind of problems, we propose a new methodology that allows the evaluation of the conformance with the standard, as well as the performance of such implementation of security protocols and architectures. As practical application of our methodology we have already applied it to different implementations of the IPsec security architecture and to the TLS protocol.

Innovative aspects
The interoperability of security protocols is really complex because many and very different aspects are involved (cryptographic algorithms, communications protocols, key management, Remote authentication mechanism, performance, bandwidth, etc.). At present time, the evaluation of interoperability (conformance and performance evaluation) is based on common communication protocols that do not cover the particularities of security protocols and for these reason their results are not useful.

Universidad
Carlos III de Madrid

Competitive advantages
The implantation of security protocols and architectures generally provokes an important impact on Information systems and their communications. The evaluation of conformance and performance of security protocols is needed to reduce this impact. Lack of conformance with a security protocol standard may cause poor interoperability but also a false security sensation. The conformance evaluation can assure that the security measures applied are correct and complete according with the particular standard.

Current state of intellectual propert: ☒ Patent applied

Keywords
Security protocols and architectures; Interoperability;

Contact Person: María Dolores García-Plaza
Phone: + 34 91 624 9016 / 9030
E-mail: comercializacion@pcf.uc3m.es