

Designing Secure Protocol Implementations

Philipp A. Baer*

*University of Kassel, FB 16, FG Distributed Systems, Germany

Security network protocols specified in only a formal language normally cannot be translated into software right away, mostly due to missing implementation details. Furthermore, a naïve implementation is often error-prone because of the variety of environmental configurations. We propose the *interactive assisted modeling* (IAM) architecture for security protocol specification. Its objective is to improve the quality of protocol implementations and portability.

The IAM architecture offers detail level-filtered modeling, support for group communication, and optimized code generation. An abstract and platform-independent *representation language* is introduced to guarantee portability of protocol specifications.

The AIM modeling interface provides an abstract view on the communication scenario and the environment. It furthermore supports specification of environmental properties such as characteristics of the communication media. Third-party tools for protocol and security analysis will also be supported. Projects like [1] follow a similar approach.

Cryptographic or communication primitives and common networking parameters are directly mapped into our representation language. It is similar to MuCAPSL [2] which is primarily targeted towards specification of multicast authentication protocols. The objective of MuCAPSL is protocol analysis whereas our language was explicitly designed for automatic code generation.

In another transformation process a protocol specification is translated into intermediate or native code. The intermediate code target is similar to Microsoft's *Intermediate Language* (MSIL). An optimized interpreter executes this code (*communication sandboxing*).

Literatur

- [1] E. Saul, A.C.M. Hutchison. SPEAR II: The Security Protocol Engineering and Analysis Resource. 2nd Annual South African Telecommunications, Networks and Applications Conference, 1999.
- [2] J. Millen, G. Denker. CAPSL and MuCAPSL. Journal of Telecommunications and Information Technology 4, 2002.