Technische Berichte

Dokumenttyp: Technical Report
Autor(en): Maria Spichkova; Jan Juerjens
Titel des Berichts: Stream Based Specification of Cryptographic Protocols and Their Composition Properties
Abstract: The correct development of security-critical systems is very difficult, as demonstrated by many insecure systems that have been developed in research and practice. A particular challenge is the establishment of security properties for separate components in an open, distributed system, in a way that the interaction of these components will still satisfy the security properties established for each component in isolation. We present a methodology to represent crypto-based, distributed systems and software and their composition properties in a formal way using Focus, a framework for formal specification and development of interactive systems. Using this formal representation, one can argue about properties of protocol components and their composition in a methodological way. We use the Focus approach, because it was developed specifically to support the compositional development of distributed systems and offers a number of specification techniques including several practical notions of refinement. It also supports formal arguments about property combination using well-founded theories of component- and service-composition.

Stichworte: Formal Specification; Verification; Cryptographic Protocols; Protocols Properties
Jahr: 2008
Jahr / Monat: 2008-07-01 00:00:00
Seiten:
Occurences:

- Einrichtungen > Fakultäten > Fakultät für Informatik > Technische Berichte > 2008

entries: