A Verifiable Language for Cryptographic Protocols

We develop a formal language for specifying cryptographic protocols in a structured and clear manner, which allows verification of many interesting properties; in particular confidentiality and integrity. The study sheds new light on the problem of creating intuitive and human readable languages, that are analysable with respect to interesting properties. Furthermore it motivates and is an example of, a novel, more general methodology of language design by first verbosely describing the semantics in a mathematical language, e.g. a logic, then restricting the properties of interest to be computable, and finally systematically transforming it into a more intuitive specification language, maintaining this tractability.

Iterative Specialisation of Horn Clauses

We present a generic algorithm for solving Horn clauses through iterative specialisation. The algorithm is generic in the sense that it can be instantiated with any decidable fragment of Horn clauses, resulting in a solution scheme for general Horn clauses that guarantees soundness and termination, and furthermore, it presents sufficient criteria for completeness. We then demonstrate the use of the framework, by creating an instance of it, based on the decidable class $\mathcal{H}_1$, capable of solving a non-trivial protocol analysis problem based on the Yahalom protocol.
Relational Analysis for Delivery of Services
Many techniques exist for statically computing properties of the evolution of processes expressed in process algebras. Static analysis has shown how to obtain useful results that can both be checked and computed in polynomial time. In this paper we develop a static analysis in relational form which substantially improves the precision of the results obtained while being able to deal with the full generality of the syntax of processes. The analysis reveals a feasible complexity for practical examples and gives rise to a fast prototype. We use this prototype to automatically prove the correct delivery of messages for the implementation of an accident service, which is based on multiplexed communication, a crucial feature of global computing applications.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Bauer, J. (Intern), Nielsen, C. R. (Intern), Pilegaard, H. (Intern)
Pages: 73-89
Publication date: 2008
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 4912
ISSN (Print): 0302-9743
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
ISI indexed (2013): ISI indexed no
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49
ISI indexed (2012): ISI indexed no
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.721 CiteScore 0.49
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.314 SNIP 0.634
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.305 SNIP 0.548
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.281 SNIP 0.447
A Secure Simplification of the PKMv2 Protocol in IEEE 802.16e-2005

Static analysis is successfully used for automatically validating security properties of classical cryptographic protocols. In this paper, we shall employ the same technique to a modern security protocol for wireless networks, namely the latest version of the Privacy and Key Management protocol for IEEE 802.16e, PKMv2. This protocol seems to have an exaggerated mixture of security features. Thus, we iteratively investigate which components are necessary for upholding the security properties and which can be omitted safely. This approach is based on the LySa process calculus and employs the corresponding automated analysis tool, the LySaTool.

Cryptographic Pattern Matching

General information

State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielsen, C. R. (Intern), Nielsen, F. (Intern), Nielson, H. R. (Intern)
Pages: 91-107
Publication date: 2007
Main Research Area: Technical/natural sciences

Publication information
Static analysis for blinding
The classical key distribution protocols are based on symmetric and asymmetric encryption as well as digital signatures. Protocols with different purposes often require different cryptographic primitives, an example is electronic voting protocols which are often based on the cryptographic operation blinding. In this paper we study the theoretical foundations for one of the successful approaches to validating cryptographic protocols and we extend it to handle the blinding primitive. Our static analysis approach is based on Flow Logic; this gives us a clean separation between the specification of the analysis and its realisation in an automatic tool. We concentrate on the former in the present paper and provide the semantic foundation for our analysis of protocols using blinding - also in the presence of malicious attackers.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielsen, C. R. (Intern), Nielsen, H. R. (Intern)
Pages: 98 - 116
Projects:

Validation of Security Properties in Network Systems

Department of Informatics and Mathematical Modeling
Period: 15/09/2005 → 05/05/2009
Number of participants: 6
Phd Student:
Nielsen, Christoffer Rosenkilde (Intern)
Supervisor:
Nielsen, Flemming (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)
Examiner:
Fischer, Paul (Intern)
Mycroft, Alan (Ekstern)
Viganò, Luca (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: DTU-lønnet stipendie
Project: PhD