AIF-ω: Set-Based Protocol Abstraction with Countable Families

Abstraction based approaches like ProVerif are very efficient in protocol verification, but have a limitation in dealing with stateful protocols. A number of extensions have been proposed to allow for a limited amount of state information while not destroying the advantages of the abstraction method. However, the extensions proposed so far can only deal with a finite amount of state information. This can in many cases make it impossible to formulate a verification problem for an unbounded number of agents (and one has to rather specify a fixed set of agents). Our work shows how to overcome this limitation by abstracting state into countable families of sets. We can then formalize a problem with unbounded agents, where each agent maintains its own set of keys. Still, our method does not lose the benefits of the abstraction approach, in particular, it translates a verification problem to a set of first-order Horn clauses that can then be efficiently verified with tools like ProVerif.
Analysis of Security Protocols in Embedded Systems

Embedded real-time systems have been adopted in a wide range of safety-critical applications—including automotive, avionics, and train control systems—where the focus has long been on safety (i.e., protecting the external world from the potential damage caused by the system) rather than security (i.e., protecting the system from the external world). With increased connectivity of these systems to external networks the attack surface has grown, and consequently there is a need for securing the system from external attacks. Introducing security protocols in safety critical systems requires careful considerations on the available resources, especially in meeting real-time and resource constraints, as well as cost and reliability requirements. For this reason many proposed security protocols in this domain have peculiar features, not present in traditional security literature.

In this thesis we tackle the problem of analysing security protocols in safety critical embedded systems from multiple perspectives, extending current state-of-the-art analysis techniques where the combination of safety and security hinders our efforts. Examples of protocols in automotive control systems will follow throughout the thesis. We initially take a combined perspective of the safety and security features, by giving a security analysis and a schedulability analysis of the embedded protocols, with intertwined considerations. Then we approach the problem of the expressiveness of the tools used in the analysis, extending saturation-based techniques for formal protocol verification in the symbolic model. Such techniques gain much of their efficiency by coalescing all reachable states into a single set of facts. However, distinguishing different states is a requirement for modelling the protocols that we consider. Our effort in this direction is to extend saturation-based techniques so that enough state information can be modelled and analysed. Finally, we present a methodology for proving the same security properties in the computational model, by means of typing protocol implementations.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bruni, A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Number of pages: 155
Publication date: 2016

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2016
Number: 389
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd389_Bruni_A.pdf

Relations
Projects:
Analysis of Security Protocols in Embedded Systems
Publication: Research › Ph.D. thesis – Annual report year: 2016

Set-Pi: Set Membership pi-Calculus
Communication protocols often rely on stateful mechanisms to ensure certain security properties. For example, counters and timestamps can be used to ensure authentication, or the security of communication can depend on whether a particular key is registered to a server or it has been revoked. ProVerif, like other state of the art tools for protocol analysis, achieves good performance by converting a formal protocol specification into a set of Horn clauses, that represent a monotonically growing set of facts that a Dolev-Yao attacker can derive from the system. Since this set of facts is not state-dependent, the category of protocols of our interest cannot be precisely analysed by such tools, as they would report false attacks due to the over-approximation.

In this paper we present Set-τ, an extension of the Applied π-calculus that includes primitives for handling databases of objects, and propose a translation from Set-τ into Horn clauses that employs the set-membership abstraction to capture the non-monotonicity of the state. Furthermore, we give a characterisation of authentication properties in terms of the set properties in the language, and prove the correctness of our approach. Finally we showcase our method with three examples, a simple authentication protocol based on counters, a key registration protocol, and a model of the Yubikey security device.
Formal Security Analysis of the MaCAN Protocol.
Embedded real-time network protocols such as the CAN bus cannot rely on off-the-shelf schemes for authentication, because of the bandwidth limitations imposed by the network. As a result, both academia and industry have proposed custom protocols that meet such constraints, with solutions that may be deemed insecure if considered out of context. MaCAN is one such compatible authentication protocol, proposed by Volkswagen Research and a strong candidate for being adopted by the automotive industry.

In this work we formally analyse MaCAN with ProVerif, an automated protocol verifier. Our formal analysis identifies two flaws in the original protocol: one creates unavailability concerns during key establishment, and the other allows re-using authenticated signals for different purposes. We propose and analyse a modification that improves its behaviour while fitting the constraints of CAN bus. Although the revised scheme improves the situation, it is still not completely secure. We argue that the modified protocol makes a good compromise between the desire to secure automotive systems and the limitations of CAN networks.
Verification of Stateful Protocols - Set-Based Abstractions in the Applied Pi-Calculus

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bruni, A. (Intern), Mödersheim, S. A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 281-282
Publication date: 2014

Host publication information
Title of host publication: Proceedings of the 19th Nordic Conference on Secure IT Systems, NordSec 2014
Publisher: Springer
ISBN (Print): 978-3-319-11598-6
ISBN (Electronic): 978-3-319-11599-3
Series: Lecture Notes in Computer Science
Number: 8788
ISSN: 0302-9743
BFI conference series: Nordic Workshop on Secure IT-systems (5010160)
Main Research Area: Technical/natural sciences
DOIs:
10.1007/978-3-319-11599-3
Source: PublicationPreSubmission
Source-ID: 101466807
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Security Games for Cyber-Physical Systems
The development of quantitative security analyses that consider both active attackers and reactive defenders is a main challenge in the design of trustworthy Cyber-Physical Systems. We propose a game-theoretic approach where it is natural to model attacker’s and defender’s actions explicitly, associating costs to attacks and countermeasures. Cost considerations enable to contrast different strategies on the basis of their effectiveness and efficiency, paving the way to a multi-objective notion of optimality. Moreover, the framework allows expressing the probabilistic nature of the environment and of the attack detection process. Finally, a solver is presented to compute strategies and their costs, resorting to a recent combination of strategy iteration with linear programming.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Vigo, R. (Intern), Bruni, A. (Intern), Yuksel, E. (Intern)
Pages: 17-32
Publication date: 2013

Host publication information
Title of host publication: Secure IT Systems : 18th Nordic Conference, NordSec 2013, Ilulissat, Greenland, October 18-21, 2013, Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-41487-9
ISBN (Electronic): 978-3-642-41488-6
Series: Lecture Notes in Computer Science
Volume: 8208
ISSN: 0302-9743
BFI conference series: Nordic Workshop on Secure IT-systems (5010160)
Main Research Area: Technical/natural sciences
DOIs:
10.1007/978-3-642-41488-6_2
Source: dtu
Source-ID: n::oai:DTIC-ART:bl/425277192::34821
Projects:

**SESAMO: Security and Safety Modelling**

Technical University of Denmark  
Period: 01/10/2012 → 31/03/2016  
Number of participants: 6  
Phd Student: Bruni, Alessandro (Intern)  
Supervisor: Nielson, Hanne Riis (Intern)  
Main Supervisor: Nielson, Flemming (Intern)  
Examiner: Probst, Christian W. (Intern)  
Kremer, Steve (Ekstern)  
Maffeis, Sergio (Ekstern)

**Financing sources**
Source: Internal funding (public)  
Name of research programme: Institut, samfinansiering

**Relations**
Publications:
Analysis of Security Protocols in Embedded Systems  
Project: PhD