Analysing Protocol Stacks for Services
We show an approach, CaPiTo, to model service-oriented applications using process algebras such that, on the one hand, we can achieve a certain level of abstraction without being overwhelmed by the underlying implementation details and, on the other hand, we respect the concrete industrial standards used for implementing the service-oriented applications. By doing so, we will be able to not only reason about applications at different levels of abstractions, but also to build a bridge between the views of researchers on formal methods and developers in industry. We apply our approach to the financial case study taken from Chapter 0-3. Finally, we develop a static analysis to analyse the security properties as they emerge at the level of concrete industrial protocols.

CaPiTo: protocol stacks for services
CaPiTo allows the modelling of service-oriented applications using process algebras at three levels of abstraction. The abstract level focuses on the key functionality of the services; the plug-in level shows how to obtain security using standardised protocol stacks; finally, the concrete level allows to consider how security is obtained using asymmetric and symmetric cryptographic primitives. The CaPiTo approach therefore caters for a variety of developers that need to cooperate on designing and implementing service-oriented applications. We show how to formally analyse CaPiTo specifications for ensuring the absence of security flaws. The method used is based on static analysis of the corresponding LySa specifications. We illustrate the development on two industrial case studies; one taken from the banking sector and the other a single sign-on protocol.
Detecting and Preventing Type flaws at Static Time

A type flaw attack on a security protocol is an attack where an honest principal is cheated on interpreting a field in a message as the one with a type other than the intended one. In this paper, we shall present an extension of the LYSA calculus to cope with types, by using tags to represent the intended types of terms. We develop a Control Flow Analysis for this calculus which soundly over-approximates all the possible behaviour of a protocol and, in particular, is able to capture any type confusion that may occur during the protocol execution. The analysis acts in a descriptive way: it describes which violations may occur. In the same setting, our approach also offers a prescriptive usage: we can impose a type discipline, by forcing some data to be of the expected types. At this point, the analysis may statically check that type violations are not possible any longer. In other words, we instrument the code with the only checks necessary to enforce type security. Finally, we apply our framework to a multi-protocol setting, where the risk of having type flaw attacks is higher. Our analysis has been implemented and successfully applied to a number of security protocols, showing it is able to capture type flaw attacks. The implementation complexity of the analysis is low polynomial.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Bodei, C. (Ekstern), Brodo, L. (Ekstern), Degano, P. (Ekstern), Gao, H. (Intern)
Pages: 229-264
Publication date: 2010
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Computer Security
Volume: 18
Issue number: 2
ISSN (Print): 0926-227X
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.373 SNIP 0.999 CiteScore 1.17
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.508 SNIP 1.174 CiteScore 1.12
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.625 SNIP 1.78 CiteScore 1.62
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.784 SNIP 1.955 CiteScore 1.91
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.863 SNIP 2.352 CiteScore 2.03
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.71 SNIP 1.713 CiteScore 1.65
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.811 SNIP 2.413
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.866 SNIP 2.184
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.93 SNIP 2.105
Scopus rating (2007): SJR 1.057 SNIP 1.857
Scopus rating (2006): SJR 1.677 SNIP 2.356
Scopus rating (2005): SJR 1.362 SNIP 3.439
Scopus rating (2004): SJR 1.361 SNIP 3.135
Scopus rating (2003): SJR 1.717 SNIP 4.999
Analysis of Security Protocols by Annotations

The trend in Information Technology is that distributed systems and networks are becoming increasingly important, as most of the services and opportunities that characterise the modern society are based on these technologies. Communication among agents over networks has therefore acquired a great deal of research interest. In order to provide effective and reliable means of communication, more and more communication protocols are invented, and for most of them, security is a significant goal. It has long been a challenge to determine conclusively whether a given protocol is secure or not. The development of formal techniques, e.g. control flow analyses, that can check various security properties, is an important tool to meet this challenge. This dissertation contributes to the development of such techniques.

In this dissertation, security protocols are modelled in the process calculus LYSA. A variety of interesting security properties that protocols are often expected to have are formalised: authentication, confidentiality, freshness, absence of simple and complex type flaws. Those security properties are explicitly specified as annotations embedded in the LYSA syntax. Finally, a number of automatic techniques for the analysis of system behaviour are developed. These techniques are specified as control flow analyses and are, therefore, guaranteed to terminate. The perspectives for the analysis techniques are discussed. Thus the dissertation marks a step forward both for scientists, who gain a general framework for the study of several interesting security properties, and developers, who get a collection of tools that can validate protocols with respect to various aspects of security.

General information

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Gao, H. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: May 2008

Publication information

Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2008-190
Main Research Area: Technical/natural sciences
Electronic versions:
phd190_hg.pdf
Source: orbit
Source-ID: 210837
Publication: Research › Ph.D. thesis – Annual report year: 2008
A Formal Analysis of Complex Type Flaw Attacks on Security Protocols

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of Pisa
Authors: Gao, H. (Intern), Bodei, C. (Ekstern), Degano, P. (Ekstern)
Pages: 167-183
Publication date: 2008

Host publication information
Title of host publication: Lecture Notes in Computer Science
Volume: 5140
Publisher: Springer
Main Research Area: Technical/natural sciences
Conference: 12th International Conference on Algebraic Methodology and Software Technology, USA, 01/01/2008
Source: orbit
Source-ID: 231162
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

A formal analysis for capturing replay attacks in cryptographic protocols

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Gao, H. (Intern), Bodei, C. (Ekstern), Degano, P. (Ekstern), Nielson, H. R. (Intern)
Pages: 150-165
Publication date: 2007

Host publication information
Title of host publication: 12th Asian Computing Science Conference, ASIAN 2007 : Lecture Notes in Computer Science
Volume: 4846
Publisher: Springer
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 231112
Publication: Research › Article in proceedings – Annual report year: 2007

Detecting and Preventing Type Flaws: a Control Flow Analysis with Tags

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of Pisa, Università degli Studi di Sassari
Authors: Bodei, C. (Ekstern), Degano, P. (Ekstern), Gao, H. (Intern), Brodo, L. (Ekstern)
Pages: 3-22
Publication date: 2007

Host publication information
Title of host publication: Electronic Notes in Theoretical Computer Science
Volume: 194
Main Research Area: Technical/natural sciences
Conference: 5th International Workshop on Security Issues in Concurrency, 01/01/2007
Source: orbit
Source-ID: 231155
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007

Analysis of LYSA-calculus with explicit confidentiality annotations
Recently there has been an increased research interest in applying process calculi in the verification of cryptographic protocols due to their ability to formally model protocols. This work presents LYSA with explicit confidentiality annotations for indicating the expected behavior of target protocols. A static analysis approach is developed for analyzing protocols specified in the extended LYSA. The proposed approach will over-approximate the possible executions of protocols while keeping track of all messages communicated over the network, and furthermore it will capture the potential malicious
activities performed by attackers as specified by the confidentiality annotations. The proposed analysis approach is fully automatic without the need of human intervention and has been applied successfully to a number of protocols.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Gao, H. (Intern), Nielson, H. R. (Intern)
Pages: 39-43
Publication date: 2006

Host publication information
Title of host publication: Proceeding of 20th International Conference on Advanced Information Networking and Applications
Volume: 2
Publisher: IEEE
ISBN (Print): 0-7695-2466-4
Main Research Area: Technical/natural sciences
Conference: 20th International Conference on Advanced Information Networking and Applications, 01/01/2006
Electronic versions: Gao.pdf
DOIs: 10.1109/AINA.2006.100

Bibliographical note
Copyright: 2006 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE
Source: orbit
Source-ID: 228993
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007

Projects:
Secure Communication Protocols
Department of Informatics and Mathematical Modeling
Period: 01/09/2004 → 29/05/2008
Number of participants: 5
Phd Student:
Gao, Han (Intern)
Main Supervisor:
Nielson, Hanne Riis (Intern)
Examiner:
Baumeister, Hubert (Intern)
Cortesi, Agostino (Ekstern)
Gilmore, Stephen (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Programbevilling
Project: PhD