

MODELING AND ANALYZING WEB PROTOCOLS FOR TRUST AND SECRECY

by

APURVA KUMAR

Department of Computer Science and Engineering

Submitted

in fulfillment of the requirements of the degree of

Doctor of Philosophy

to the



Indian Institute of Technology Delhi

December 2012

Certificate

This is to certify that the thesis titled “**Modeling and Analyzing Web Protocols for Trust and Secrecy**” being submitted by Apurva Kumar to the Indian Institute of Technology Delhi, for the award of the degree of Doctor of Philosophy, is a record of bona-fide research work carried out by him under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree/diploma.

December 2012

Dr. Pankaj Jalote
Department of Computer Science and Engineering
Indian Institute of Technology Delhi
New Delhi 110 016

Acknowledgements

I thank my advisor Professor Pankaj Jalote, for his continuous support during my Ph.D. program. Without his encouragement and positive influence, I could not have finished this thesis. He helped me define the problem and was always there to meet and discuss my ideas. His pointed questions invariably led to deeper investigation of the problem and improvement of the solution. He always provided useful suggestions that helped improve the quality of my papers and chapters.

I would like to thank Professor S. Arun-Kumar and Professor Sanjiva Prasad for their comments and suggestions on my work, which were really valuable.

I would like to thank my family, most of all my wife Deepali, for single-handedly running our lives for weeks and months when my workload was high. I would like to thank my son Arnav for his understanding and my daughter Navya for just lighting up our toughest days with her smile.

I would like to thank my management at IBM Research-India, especially Sougata Mukherjea and Ravi Kothari, for encouraging and supporting me during these years.

Apurva Kumar

Abstract

User management services were one of the first to be offloaded to third party cloud vendors. Today, a large number of service providers rely on trusted identity providers for managing users and their resources. At the core of these interactions involving multiple providers are a set of web-based workflows that have emerged as de-facto standards. Analyzing security of such web protocols is of immense importance to a large number of common business transactions on the web.

Designing cryptographic protocols is known to be highly error-prone due to the complex environment in which they must succeed. Thus not surprisingly web protocols that are additionally exposed to web-browser based attacks have proven to be even more challenging to design.

This thesis aims to advance techniques for cryptographic protocol analysis by proposing a framework that is especially designed for analyzing security of web protocols. To analyze trust between collaborating service providers on the web, we extend the well-known BAN logic. We include new primitives and inference rules which aid and simplify analysis of web protocols. In order to keep the complexity of the logic within reasonable limits, we also propose a hybrid approach based on augmenting belief logic analysis with a second stage that establishes secrecy properties through model checking. We illustrate the use of these approaches through analysis of several important web protocols. Not only does our analyses identify known issues, but we discover issues that have previously gone unnoticed.

Contents

Certificate	iii
Acknowledgements	v
Abstract	vii
List of Figures	xiii
List of Tables	xv
1 Introduction	1
1.1 Motivation	1
1.2 Summary of Prior Work	2
1.3 Overview of Proposed Approach	3
1.4 Structure of the Thesis	7
2 Background and Related Work	9
2.1 Definitions of Authentication	9
2.2 Adversary Model	10
2.3 Formalisms for Security Protocol analysis	12
2.3.1 Multiset Rewrite formalism and undecidability	12
2.3.2 Applied pi calculus formalism	13
2.3.3 The Strand formalism	14
2.3.4 Modal logics	14
2.4 Tools for security protocol analysis	15
2.4.1 The AVISPA tools	15
2.4.2 Proverif	16
2.4.3 Scyther	16
2.4.4 Tools for analyzing web protocols	16
2.5 Introduction to BAN Logic	17
2.5.1 BAN statements	17
2.5.2 Inference rules	18
2.5.3 Idealization	19
2.5.4 Analysis	20
2.6 Summary	20
3 Limitations of Belief Logic Analysis	21
3.1 Criticism of Belief Logics	21

3.1.1	Nessett's example and scope of BAN logic	22
3.1.2	Soundness issues with multiple session based attacks	22
3.2	Analysis of Needham Schroeder (Public Key) Protocol	23
3.2.1	Parallel session attack	23
3.2.2	Analysis in BAN paper	24
3.2.3	Observations and revised analysis	24
3.3	Analysis of Needham-Schroeder Lowe	26
3.3.1	Establishing Correspondence Property	27
3.3.2	Establishing Secrecy Property	29
3.3.3	Alternative resolution based on new inference rule	30
3.4	Summary	30
4	Belief Logic for Web Protocols	31
4.1	Need for Extending Belief Logic	31
4.1.1	A typical web-based workflow	31
4.1.2	Principals without identifying keys	32
4.1.3	Need to model secure channels	32
4.1.4	Browser-based attacker	32
4.1.5	Goals for web protocols	33
4.2	Belief Logic for the Web	33
4.2.1	Extended Syntax	33
4.2.2	Inference Rules	35
4.3	Semantics of Belief Logic for the Web	37
4.3.1	Semantics of secure channel	40
4.3.2	User Principals and Actions	41
4.3.3	Secret associated with action	41
4.3.4	Cookie associated with action	42
4.4	Soundness of extended logic	43
4.4.1	Soundness of R5	43
4.4.2	Soundness of R8	44
4.5	Analysis of SAML Browser SSO	45
4.6	Analysis of SAML Identity Linking	50
4.6.1	Protocol description	50
4.6.2	Modeling and Analysis	51
4.6.3	Fixing Identity Linking	52
4.7	Summary	54
5	Combining Belief Logic with Model Finding	55
5.1	Motivation for Hybrid Approach	55
5.2	Overview of the Approach	56
5.2.1	Static protocol model and constraints	57
5.2.2	Behavioral model and protocol simplification	58
5.2.3	Adversary model and Goal Assertion for web protocols	60
5.3	Modeling Web Protocols Using Alloy	60
5.3.1	Overview of Alloy	60
5.3.2	Modeling Principals	62
5.3.3	Protocol Session	63

5.3.4	Protocol Messages	64
5.3.5	Learning Rules	65
5.3.6	Protocol Flow	65
5.3.7	Adversary Model	66
5.4	Summary	67
6	Analyzing SAML based Web Single Sign-On	69
6.1	SAML Session and Request	69
6.1.1	New signatures	69
6.1.2	Constraints on SAML session	70
6.2	Modeling Response and SAML token	71
6.2.1	Token structure	71
6.2.2	Token generation	72
6.2.3	Token validation	73
6.3	Goal Assertion of SAML SSO	73
6.4	Result of Alloy analysis	74
6.5	Impact of Token validation	75
7	Analyzing Web-based Authorization Workflow of OAuth	79
7.1	Stage 1: Belief logic analysis of OAuth	80
7.2	Stage 2: Model finding using Alloy	83
7.2.1	OAuth Session and Request	83
7.2.2	The Verifier and its validation	85
7.2.3	Goal Assertion for OAuth	86
7.3	Result of Alloy analysis	86
7.4	Attack on OAuth 1.0	87
7.5	Summary	87
8	Conclusion	89
8.1	Future work	91
	Bibliography	93
	List of Publications	99
	Bio-data	101