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