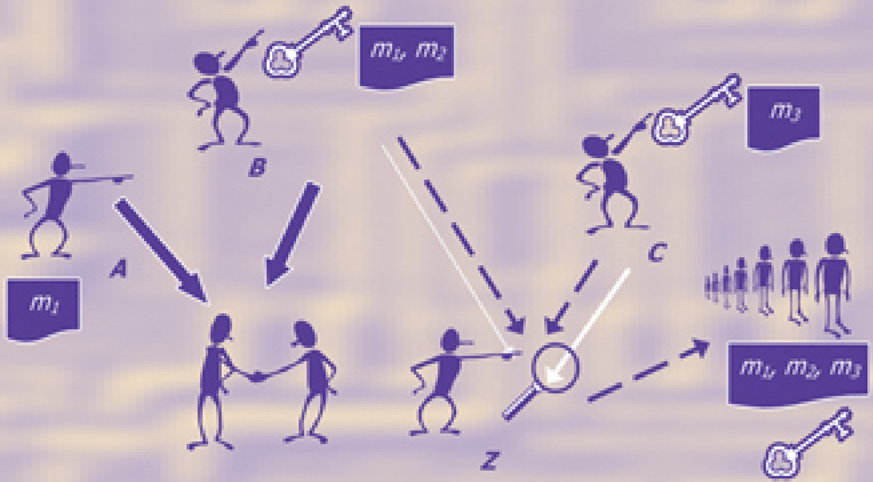
Qingfeng Chen
Chengqi Zhang
Shichao Zhang

LNCS 5111

Secure Transaction Protocol Analysis

Models and Applications



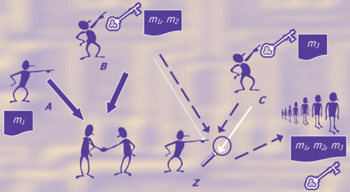
Springer

Qingfeng Chen
Chengqi Zhang
Shichao Zhang

LNCS 5111

Secure Transaction Protocol Analysis

Models and Applications



Springer

Lecture Notes in Computer Science 5111

Qingfeng Chen Chengqi Zhang Shichao Zhang

Secure Transaction Protocol Analysis

Models and Applications

Springer

Authors

Qingfeng Chen
Deakin University
School of Engineering and Information Technology
Melbourne, Australia
E-mail: qifengch@deakin.edu.au

Chengqi Zhang
University of Technology, Sydney
Faculty of Engineering and Information Technology
Centre for Quantum Computation and Intelligent Systems
Sydney, Australia
E-mail: chengqi@it.uts.edu.au

Shichao Zhang
Guangxi Normal University
College of CS and IT, Guilin, China
and
University of Technology, Sydney
Faculty of Engineering and Information Technology
Sydney, Australia
E-mail: zhangsc@mailbox.gxnu.edu.cn

Library of Congress Control Number: 2008931701

CR Subject Classification (1998): C.2, D.1.3, F.1.2, I.2.8, D.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-85073-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85073-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12327997 06/3180 5 4 3 2 1 0

Preface

The application of formal methods to security protocol analysis has attracted increasing attention in the past two decades, and recently has been showing signs of new maturity and consolidation. The development of these formal methods is motivated by the hostile nature of some aspects of the network and the persistent efforts of intruders, and has been widely discussed among researchers in this field. Contributions to the investigation of novel and efficient ideas and techniques have been made through some important conferences and journals, such as *ESORICS*, *CSFW* and *ACM Transactions in Computer Systems*. Thus, formal methods have played an important role in a variety of applications such as discrete system analysis for cryptographic protocols, belief logics and state exploration tools. A complicated security protocol can be abstracted as a manipulation of symbols and structures composed by symbols. The analysis of e-commerce (electronic commerce) protocols is a particular case of such symbol systems.

There have been considerable efforts in developing a number of tools for ensuring the security of protocols, both specialized and general-purpose, such as belief logic and process algebras. The application of formal methods starts with the analysis of key-distribution protocols for communication between two principals at an early stage. With the performance of transactions becoming more and more dependent on computer networks, and cryptography becoming more widely deployed, the type of application becomes more varied and complicated. The emerging complex network-based transactions such as financial transactions and secure group communication have not only brought innovations to the current business practice, but they also pose a big challenge to protect the information transmitted over the open network from malicious attacks. However, there has been no specialized monograph to consider these issues. Thus this book takes these interesting topics into account and offers innovative techniques for modelling e-commerce protocol, analyzing transaction data and testing the protocol performance in an intuitive way.

The present volume arose from a need for a comprehensive collection presenting the state of the art in security protocol analysis, and is aimed at serving as an overall course-aid and self-study material for researchers and students in formal methods theory and applications in e-commerce, data analysis and data mining. However, the volume can be useful to anyone else who is interested in secure e-commerce.

This book is organized into eight chapters that cover the main approaches and tools in formal methods for security protocol analysis. Having in mind that the book is also addressed to students, the contributors present the main results and techniques in an easily accessed and understood way together with many references and examples.

Chapter 1 is an introductory chapter that presents the fundamentals and background knowledge with respect to formal methods and security protocol analysis. Chapter 2 provides an overview of related work in this area, including basic concepts and terminology. Chapters 3 and 4 show a logical framework and a model checker especially for analyzing secure transaction protocols. Chapter 5 explains how to deal with uncertainty issues in secure messages, including inconsistent messages and conflicting beliefs in messages. Chapter 6 integrates data mining with security protocol analysis, and Chap. 7 develops a new technique for detecting collusion attack in security protocols. Chapter 8 presents a summary of the chapters and gives a brief discussion of some emerging issues.

Although it is not easy to cover all the relevant studies in this book, due to varied formal methods and increasingly complicated security protocols, we hope that it is comprehensive enough to provide a useful and handy guide for both beginners and experienced researchers.

We would like to express our sincere thanks to all colleagues who provided us with useful comments and support during our writing of this book. These include Yi-Ping Phone Chen and Zili Zhang from Deakin University, Li Liu from the University of Technology Sydney, Jeffrey Xu Yu from the Chinese University of Hong Kong, Shuo Bai from the Institute of Computing Technology of the Chinese Academy of Sciences, Xiaowei Yan from Guangxi Normal University and Kaile Su from Sun Yat-Sen University.

We also wish to especially thank Alfred Hofmann, Editor at Springer, for his enthusiasm, patience and great efforts in publishing this book, as well as his staff for their conscientious efforts of providing materials. We are very grateful to all of the reviewers for their useful and valuable feedback. We also thank our families for their persistent support throughout this project.

This work was partially supported by an Australian large ARC grant (DP0667060), a China NSF major research Program (60496327), a National Natural Science Fund for Distinguished Young Scholars of China under

Grant No. 60625204, a China NSF grant (90718020), a China 973 Program (2008CB317108), an Overseas-Returning High-level Talent Research Program of China Ministry of Personnel, and Guangxi NSF grants.

April 2008

Qingfeng Chen
Chengqi Zhang
Shichao Zhang

Contents

1 Introduction

Security protocols (cryptographic protocol) have been widely used to not only achieve traditional goals of data confidentiality, integrity and authentication, but also secure a variety of other desired characteristics of computer-mediated transactions recently. To guarantee reliable protocols, a great deal of formal methods has been undertaken not only to develop diverse tools with specialized purpose or general purpose, but also to apply them to the analysis of realistic protocols. Many of them have been proved to be useful in detecting some intuitive attacks in security protocols. In many cases, a useful feedback is supplied to designers in order to improve the protocol's security. For both beginners and experienced researchers, this book will present useful information on relevant technologies that can be extended or adapted. A comprehensive introduction to the basic concepts and core techniques will be presented. In this chapter, we explain what is security protocols and how they can be used to ensure secure transactions, what challenging issues in e-commerce (electronic commerce) are, why security protocol analysis important, how they are performed, and what are the ongoing efforts and relevant work. We will also explain the limitations in previous work and why it is important to develop new approaches. These questions will be briefly answered. In particular, we will focus on the discussion regarding secure transaction protocols. Finally, some emerging issues and the ways they are being met are also described.

1.1 What Is Security Protocol?

First, let us consider a financial transaction that is to send sensitive data such as *Alice*'s credit card numbers to a vendor like Dell Inc. Several occurring matters in this transaction are listed below.

- credit card number, ID
- encrypted credit card number, no ID
- encrypted credit card number, ID

Q. Chen, C. Zhang, S. Zhang: Secure Transaction Protocol Analysis, LNCS 5111, pp. 1–15, 2008.

The first case provides no encryption protection to the credit card number. An intruder can see the credit card number and masquerade as *Alice* to proceed the transaction using the ID. The credit card number is encrypted in the second case, whereas the vendor cannot authenticate the sender's identifier that might be missing, intercepted or tampered by malicious hackers. Only the last case may be safe since it encodes the credit card number and includes the ID.

In the past few years, researchers have sought to develop techniques for information security. One of the most effective and popular ways is the application of security protocols. A security protocol is a sequence of operations that perform a security-related function by using cryptographic methods. A protocol specifies how the cryptography should be used, and includes details about data structures and representations. For example, it is not easy for the intruder to see *Alice*'s credit card number without the right key.

There are a variety of protocols for different purposes, such as communication protocols. File transfer protocol (FTP) that is a protocol to describe file transfers between a host and a remote computer; hypertext transfer protocol (HTTP) is the set of rules for exchanging files (text, audio, video, and other multimedia files) on the World Wide Web; and electronic transaction protocols for secure e-commerce. Usually, a security protocol has to incorporate some of the following aspects to ensure secure data transport.

- *Entity authentication.* This means the authentication of principals, by which to ensure users are who they say they are. One familiar example is access control. A computer system supposed to be used only by those authorized must attempt to detect and exclude the unauthorized.
- *Key agreement or establishment.* This is to make two or more parties agree on a session key.
- *Encryption construction.* This is the process of converting information to make it unreadable without special knowledge. It has been widely used to protect communications. Although encryption can be used to ensure secrecy, other techniques are still needed to verify the integrity and authenticity of a messages.
- *Secure data transport.* This provides secure communication on the distributed systems in combination with various cryptographic mechanisms, such as public-key (asymmetric) cryptography, symmetric ciphers, one-way hash functions and so on. Furthermore, some new devices like timestamps and key-sharing are also used recently. We will give explanation to the above concepts in the next section.

Secure transaction protocol (e-commerce protocol) [55, 140] is one of the important security protocols, and has been mainly developed to secure financial transactions. It specifies transaction rules that must be conformed in each processing phase. To complete a transaction, for example, *Alice* needs to obtain a valid credit card number from a authorized financial institute, have the correct PIN to access the credit card, sends the encrypted credit card number along with relevant information such as identifier to the vendor; and the vendor must decrypt the message and send a response message to *Alice* to confirm the transaction.

With the rapid growth of online trading, the reliability of e-commerce protocols has received a great deal of attention. This book aims to present some innovative techniques for secure transaction protocol analysis. It considers the characteristic of financial transactions and focuses on building models for examining and evaluating the protocol performance using transaction data.

1.2 Needs of Formal Analysis for Secure Transaction Protocols

Most internet users may have experiences of buying products online such as shares, computers or foods, or transferring money by using internet banking. It is natural that they might be concerned about revealing their credit card numbers, personal details, or receiving wrong products. In other words, people wonder the transaction may be unsecured. The development of formal methods owes much to the security community. A number of formal security models, tools for reasoning about security, and applications of these tools to proving systems secure were developed in the 1970s and early 1980s. The wide use of the internet brings these security problems to the attention of the masses.

The emergence of e-commerce has caused innovation in current business practice, and has broken through conventional marketing barriers, as activities on the internet are no longer limited to time and geography. Unlike conventional business, the development of e-commerce is unprecedented. There has been a vast growth in retail e-commerce and in transactional use by small business. The following industry forecast should be sufficient to indicate the dynamic growth and potential of electronic commerce:

> *Forrester forecasts that the world total e-commerce (B2B and B2C) has been expected to reach 2.3 trillion by 2002 and to be on track to reach 13 trillion by 2006. The compound annual growth rate is around 53.6 per cent* [73].

Furthermore, e-commerce improves the efficiency of existing business models and enables the transformation of these models, which present reduced costs and increasing competitiveness, as well as bring new challenges. This has resulted in the development of a great many e-commerce systems. With the development of e-commerce systems, their security has become a key issue. For example, people may hesitate to send their credit card number or date of birth to an electronic transaction system when asked for it on-line. The vendor must be able to provide adequate protection from fraud and violation of privacy when trading on the Web. Currently, consumers can find a great variety of systems offered by vendors on the Internet, but secure payment capability has not been guaranteed. It is thus a high-profile problem for e-commerce systems to protect the information transmitted over the open network from malicious attacks.

In general, security in e-commerce is implemented by relying on a set of secure protocols that meet the user's expectation for secure transactions. However, existing security protocols are not always secure enough to meet people's expectation. Besides, the design of a security protocol is difficult and error-prone. In particular, some subtle flaws have been recognized in popular and widely-used security protocols. This generates a crucial requirement of identifying weakness and hidden flaws in security protocols.

The traditional ways of verifying security protocols are through human inspection, simulation, and testing. Unfortunately these approaches provide no guarantees about the quality of security protocols. Formal methods comprise a variety of mathematical modelling techniques for specifying and modelling the behaviour of a system, and may mathematically verify that the system design and implementation satisfy system functional and safety properties. One of the main applications of formal methods is to assist in security protocol analysis. Formal methods allow us to

- Specify the system's boundary: the interface between the system and its environment.
- Characterize a system's behaviour more precisely in handling both functional behaviour and real-time behaviour by a mathematical or logical model.
- Provide precise definition for the system's desired properties by formulating its requirements.
- Implement a thorough analysis of different paths which an intruder can utilize.
- Prove a system meets its specification by rigorous proofs. Some methods may offer counterexamples if it is not the case.

Clarke and Wing capture the three threads in the development of formal methods in their paper for 1996 *ACM Computing Surveys* [37]-model checking, theorem proving, and software specification. Model checking, in particular, is a proven success for hardware verification; companies such as Intel are establishing their own hardware verification groups, building their own verification systems, and hiring people trained in formal methods.

As more and more transactions are carried out via computer networks, however, and as cryptography is widely applied, the types of applications in which the security protocols need to be integrated becomes more varied and