Security enhanced agent systems

Qi Zhang

University of Wollongong

Follow this and additional works at: https://ro.uow.edu.au/theses

Recommended Citation
NOTE
This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING
You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
Security Enhanced Agent Systems

A thesis submitted in fulfillment of the requirements for the award of the degree

Master by Research

from

UNIVERSITY OF WOLLONGONG

by

Qi Zhang

School of Computer Science and Software Engineering
November 2009
Dedicated to

my parents ...  
with love and gratitude
Declaration

I, Qi Zhang, declare that this thesis is wholly my own work unless otherwise referenced or acknowledged below. The document has not been submitted for qualifications at any other academic institution.

Qi Zhang
November 18, 2009
Certification to Thesis
Examination Committee

I (with my co-authors) wrote three research papers (as listed on page ix) during my study. The contents of these papers were used in my thesis. I declare that I have made the major contribution to these papers. As co-authors, Associate Professors Yi Mu and Minjie Zhang were also my thesis supervisors and Professor Robert H Deng is my external advisor. They provided their professional advices and guidance to me during my study. These advices and guidance were indeed very helpful and led to the success of our study. I would like to declare that I have contributed around 80% of the work, which captures the major development of the schemes and security proofs.

Qi Zhang
November 18, 2009
Abstract

Software agents are useful for distributed systems and electronic commerce. However, to fully deploy software agents in practice, a number of challenging issues, especially security and privacy, need to be addressed. In general, software agents can be classified into mobile agent and multi-agent, which have different security requirements.

Mobile agents are mobile in the sense that they can move in the defined computer network. Due to this nature, security and privacy become critical. When a mobile agent travels in a hostile environment or migrates to an untrusted platform, its security and privacy can be easily compromised. In particular, the remote hosts in which agents visit and get services are not considered to be trusted. Existing solutions suggest that remote hosts together with the agent’s home jointly sign the service agreement. Therefore, proxy-based signing model was utilized. We observe that this actually poses a serious problem: a host which should be excluded from the desirable hosts could also generate a signed service agreement. In order to solve this problem, we propose a secure mobile agent transaction scheme which achieves host authentication with designated hosts. In our scheme, only selected hosts can be included in the agent network and hence generate a valid signed service agreement. We also propose a variant of our scheme that provides a shorter signature size.

Multi-agent systems are different from mobile agents systems in that they are not mobile. Although multi-agent systems do not have the security risks stemming from mobility, they have other security problems. Unfortunately, security and privacy issues have not been adequately addressed. Most proposed schemes only concern with security protection rather than privacy protection. Privacy issues have not drawn adequate attention and actually been ignored or mistreated in most proposed multi-agent protocols. We argue that privacy issues are indeed not trivial and cannot be resolved with traditional security mechanisms. If agents do not trust each other, their privacy must be protected. In order to solve the issue, we
propose a novel secure multi-agent protocol which captures several most important security properties including data confidentiality, agent privacy and authenticity. In our scheme, privacy protection is applied to both negotiating parties (agents). The security protection in our scheme satisfies the most stringent security level, i.e., indistinguishability against adaptive chosen ciphertext attacks.
First of all, I am very grateful to my supervisor, A/Prof. Yi Mu, who gave me this opportunity to study cryptography. He was always very patient to answer my questions and provide professional guidances. I also would like to express my gratefulness to my co-supervisor, A/Prof. Minjie Zhang, who gave me her professional advices on improving my knowledge of software agents.

Another great gratitude goes to my parents. When I encounter problems, their encouragement always helps me to move forward.

I am very grateful to my beloved girlfriend Yidan, for her love and sacrifice. During my thesis writing, she took most of the housework to make sure I can concentrate on my thesis.

I would like to express my appreciation to Dr. Xinyi Huang. It is a pleasure to discuss research with him. I appreciate his clear explanations on some cryptographic topics and critical comments on my papers. I would like to thank Ms Wei Wu, for her time and patient discussions on the research topics.

I thank the administrative staff and the technical support staff of School of Computer Science and Software Engineering, Faculty of Informatics, for their supports.

Qi Zhang
Wollongong, August 2009


Qi Zhang, Yi Mu, and Minjie Zhang. Secure mobile agents with less communication overhead. (draft)
# Contents

Certification to Thesis Examination Committee .......... v

Abstract .......................................................... vi

Acknowledgement .................................................. viii

Publications ........................................................ ix

1 Introduction ....................................................... 1

   1.1 Security Issues in the World of Agents ..................... 1

   1.2 Existing Works ............................................... 3

   1.3 Challenging Issues and Motivations ....................... 3

   1.4 Proposed Solutions ......................................... 5

   1.5 Overview of the Thesis ....................................... 6

2 Background ..................................................... 7

   2.1 Preliminaries ............................................... 7

      2.1.1 Miscellaneous Notations .............................. 7

      2.1.2 Random Oracle Model ................................... 8

      2.1.3 Polynomial Time (Complexity Theory) ................. 8

      2.1.4 Bilinear Map ............................................ 8

   2.2 Number-Theoretic Problems ................................ 9

      2.2.1 The Discrete Logarithm Problem ....................... 9

      2.2.2 The Diffie-Hellman Problem .......................... 10

      2.2.3 The Bilinear Diffie-Hellman Problem .................. 10

      2.2.4 The q-Strong Diffie-Hellman Problem ................ 11

   2.3 Hash Function ............................................... 11

   2.4 Public Key Encryption ...................................... 12
2.4.1 Identity-Based Encryption ........................................... 13
2.5 Digital Signatures ....................................................... 14
2.6 Proxy Signatures ......................................................... 15
2.7 Accumulators ............................................................. 17
2.8 Secret Handshakes ....................................................... 18
2.9 Oblivious Signature-Based Envelope ................................. 19
2.10 Proxy-Based Mobile Agents ........................................... 20
2.11 Multi-Agents ............................................................. 24

3 Secure Mobile Agents with Designated Hosts .......................... 25
3.1 Task Execution Procedure of Proposed Mobile Agent .............. 26
3.2 Security Model .......................................................... 27
  3.2.1 Existential Unforgeability Against Malicious Hosts .......... 27
  3.2.2 Existential Unforgeability Against Malicious Customer .... 29
  3.2.3 Complexity Definitions ......................................... 30
3.3 Our Scheme ............................................................. 30
3.4 Security Analysis ....................................................... 32
  3.4.1 Existential Unforgeable Against Adversary A1 ............... 32
  3.4.2 Existential Unforgeable Against Adversary A2 .............. 37
  3.4.3 Existential Unforgeable Against Adversary A3 .............. 39
3.5 Summary ............................................................... 40

4 Secure Mobile Agents with Less Communication Overhead ............ 41
4.1 Security Model .......................................................... 41
  4.1.1 Complexity Assumptions ........................................ 42
4.2 Our Scheme ............................................................ 42
4.3 Security Analysis ....................................................... 44
  4.3.1 Existential Unforgeable Against Malicious Host within Desi-
  gnated List ............................................................... 44
  4.3.2 Existential Unforgeable Against Malicious Host without in-
  Designated List .......................................................... 48
  4.3.3 Existential Unforgeable Against Malicious Customer ....... 49
4.4 Comparison .............................................................. 49
4.5 Summary ............................................................... 50
5 Attribute-based Authentication for Multi-Agent Systems with Dynamic Groups 51

5.1 Model and Definitions ........................................ 51
  5.1.1 A High-Level Description of Our Scheme ............... 51
  5.1.2 Outline of Our Scheme ................................ 53
  5.1.3 Security Definitions ..................................... 54
  5.1.4 Complexity Assumptions ................................. 60

5.2 The Proposed Scheme ........................................ 61

5.3 Security Analysis ............................................ 63

5.4 Summary ....................................................... 77

6 Conclusion ....................................................... 78

Bibliography ....................................................... 80
List of Tables

4.1 Bandwidth Comparison Between Two Schemes. . . . . . . . . . . . . 49
4.2 Performance Comparison Between Two Schemes. . . . . . . . . . . . 49
List of Figures

3.1 Agent-based Online Application Architecture . . . . . . . . . . . . . . 27

5.1 Attribute-based Information Exchange in the Multi-agent System . . 52