ACCESS MANAGEMENT IN ELECTRONIC COMMERCE SYSTEM

By

Hua Wang

A thesis submitted to

The Department of Mathematics and Computing

University of Southern Queensland

for the degree of

Doctor of Philosophy
Statement

I hereby declare that the work presented in this dissertation is my own and is, to the best of my knowledge and belief, original except as acknowledged in the text. It has not previously been submitted either in whole or in part for a degree at this or any other university.

Hua Wang
Acknowledgement

I express my sincere gratitude and appreciation to my PhD supervisor Dr Yanchun Zhang of University of Southern Queensland (USQ) for his invaluable advice, teaching and encouragements during the realization of this research. It is his love for his students and dedication to research that made them available whenever I needed during all these years. If it was not for him I may not be getting my PhD.

I also express my gratitude and appreciation to my PhD co-supervisor Dr Jinli Cao of La Trobe University for all her valuable guidance, encouragement and support in every aspect during my PhD study.

I sincerely thank the Department of Mathematics and Computing, Faculty of science and High Degree Committee of the USQ for providing the excellent study environment and the financial support. I highly appreciate the great support from Professor Tony Roberts and Associate Professor Chris Harman during my study at the USQ. It is a great pleasure to study at the Department of Mathematics and Computing.
I thank Mrs Ruth Hilton for their support in many aspects. Thanks also goes to my friends at USQ and abroad for their friendship, valuable advice and encouragements that made my stay a memorable one.

I also acknowledge all the help from those who carefully read the dissertation and made the English corrections.

Finally, my appreciation goes to my mother Jiqi, my wife Lili and daughter Haina for their love and affection. I could not be able to complete my PhD study without their encouragement and support.
Abstract

The definition of Electronic commerce is the use of electronic transmission mediums to engage in the exchange, including buying and selling, of products and services requiring transportation, either physically or digitally, from location to location. Electronic commerce systems, including mobile e-commerce, are widely used since 1990. The number of world-wide Internet users tripled between 1993 and 1995 to 60 million, and by 2000 there were 250 million users. More than one hundred countries have Internet access. Electronic commerce, especial mobile e-commerce systems, allows their users to access a large set of traditional (for example, voice communications) and contemporary (for example, e--shop) services without being tethered to one particular physical location. With the increasing use of electronic service systems for security sensitive application (for example, e-shop) that can be expected in the future, the provision of secure services becomes more important. The dynamic mobile environment is incompatible with static security services. Electronic service access across multiple service domains, and the traditional access mechanisms rely on cross-domain authentication using roaming agreements starting home location. Cross-domain authentication involves many complicated
authentication activities when the roam path is long. This limits future electronic commerce applications.

Normally, there are three participants in an electronic service. These are users, service providers, and services. Some services bind users and service providers as well as services such as flight services; other services do not bind any participants, for instance by using cash in shopping services, everyone can use cash to buy anything in shops. Hence, depending on which parts are bound, there are different kinds of electronic services.

However, there is no scheme to provide a solution for all kinds of electronic services. Users have to change service systems if they want to apply different kind of electronic services on the Internet. From the consumer's point of view, users often prefer to have a total solution for all kinds of service problems, some degree of anonymity with no unnecessary cross authentications and a clear statement of account when shopping over the Internet. There are some suggested solutions for electronic service systems, but the solutions are neither total solution for all kinds of services nor have some degree of anonymity with a clear statement of account.
In our work, we build a bridge between existing technologies and electronic service theory such as e-payment, security and so on. We aim to provide a foundation for the improvement of technology to aid electronic service application. As validation, several technologies for electronic service system design have been enhanced and improved in this project. To fix the problems mentioned above, we extend our idea to a ticket based access service system.

The user in the above electronic service system has to pay when s/he obtains service. S/He can pay by traditional cash (physical cash), check, credit or electronic cash. The best way to pay money for goods or services on the Internet is using electronic cash. Consumers, when shopping over the Internet, often prefer to have a high level of anonymity with important things and a low level with general one. The ideal system needs to provide some degree of anonymity for consumers so that they cannot be traced by banks. There are a number of proposals for electronic cash systems. All of them are either too large to manage or lack flexibility in providing anonymity. Therefore, they are not suitable solutions for electronic payment in the future.
We propose a secure, scalable anonymity and practical payment protocol for Internet purchases. The protocol uses electronic cash for payment transactions. In this new protocol, from the viewpoint of banks, consumers can improve anonymity if they are worried about disclosure of their identities. An agent, namely anonymity provider agent provides a higher anonymous certificate and improves the security of the consumers. The agent will certify re-encrypted data after verifying the validity of the content from consumers, but with no private information of the consumers required. With this new method, each consumer can get the required anonymity level.

Electronic service systems involve various subsystems such as service systems, payment systems, and management systems. Users and service providers are widely distributed and use heterogeneous catalog systems. They are rapidly increasing in dynamic environments. The management of these service systems will be very complex. Whether systems are successful or not depends on the quality of their management. To simplify the management of e-commerce systems \cite{Sandhu97}, we discuss role-based access control management. We define roles and permissions in the subsystems. For example, there are roles TELLER, AUDITOR, MANAGER and permissions teller (account operation), audit operation,
managerial decision in a bank system. Permissions are assigned to roles such as permission teller is assigned to role TELLER. People (users) employed in the bank are granted roles to perform associated duties. However, there are conflicts between various roles as well as between various permissions. These conflicts may cause serious security problems with the bank system. For instance, if permissions teller and audit operation are assigned to a role, then a person with this role will have too much privilege to break the security of the bank system. Therefore, the organizing of relationships between users and roles, roles and permissions currently requires further development.

Role based access control (RBAC) has been widely used in database management and operating systems. In 1993, the National Institute of Standards and Technology (NIST) developed prototype implementations, sponsored external research, and published formal RBAC models. Since then, many RBAC practical applications have been implemented, because RBAC has many advantages such as reducing administration cost and complexity.
However, there are some problems which may arise in RBAC management. One is related to authorization granting process. For example, when a role is granted to a user, this role may conflict with other roles of the user or together with this role; the user may have or derive a high level of authority. Another is related to authorization revocation. For instance, when a role is revoked from a user, the user may still have the role.

To solve these problems, we present an authorization granting algorithm, and weak revocation and strong revocation algorithms that are based on relational algebra. The algorithms check conflicts and therefore help allocate the roles and permissions without compromising the security in RBAC. We describe the applications of the new algorithms with an anonymity scalable payment scheme.

In summary, this thesis has made the following major contributions in electronic service systems:

1. A ticket based global solution for electronic commerce systems;
   A ticket based solution is designed for different kinds of e-services.
   Tickets provide a flexible mechanism and users can check charges at anytime.
2. Untraceable electronic cash system;

An untraceable e-cash system is developed, in which the bank involvement in the payment transaction between a user and a receiver is eliminated. Users remain anonymous, unless she/he spends a coin more than once.

3. A self-scalable anonymity electronic payment system;

In this payment system, from the viewpoint of banks, consumers can improve anonymity if they are worried about disclosure of their identities. Each consumer can get the required anonymity level.

4. Using RBAC to manage electronic payment system;

The basic structure of RBAC is reviewed. The challenge problems in the management of RBAC with electronic payment systems are analysed and how to use RBAC to manage electronic payment system is proposed.

5. The investigation of recovery algorithms for conflicting problems in user-role assignments and permission-role assignments.
Formal authorization allocation algorithms for role-based access control have developed. The formal approaches are based on relational structure, and relational algebra and are used to check conflicting problems between roles and between permissions.
Publications Based on this Thesis


15. H. Wang, H, Ming. A MultiSignature Scheme for Integrity of Database. The Fifth International Conference for Young Computer Science, International Academic Publisher, pages: 627-630, Nanjing, P. R. China, 1999.
Contents

1 Introduction

1.1 Overview and Motivation ........................................ 1

1.1.1 Mobile service system ...................................... 1

1.1.2 Electronic payment .......................................... 6

1.1.3 Role based access control .................................. 10

1.2 Objectives of the Thesis ....................................... 13

1.3 Organization of the Thesis ..................................... 14

2 Electronic Commerce Items and Related Technology ............ 17

2.1 Introduction ...................................................... 17

2.2 Items in Electronic Commerce ................................ 18

2.2.1 Trust and privacy .......................................... 18

2.2.2 Electronic payment systems ................................ 20

2.2.3 Security ...................................................... 20

2.3 A framework for electronic commerce ......................... 23
2.4 Conclusions ........................................... 29

3 A ticket-based access scheme for mobile users ........................................... 31

3.1 Introduction ........................................... 31

3.2 Basic ticket model ........................................... 34

3.3 Single signature scheme for ticket group 1 ........................................... 38

3.3.1 Initialization of the system ........................................... 41

3.3.2 The single signature scheme ........................................... 42

3.3.3 The usage of tickets in ticket group 1 ........................................... 45

3.4 Multi-signature scheme for ticket group 2 ........................................... 46

3.4.1 Initialization of the system ........................................... 48

3.4.2 The Multi-signature scheme ........................................... 49

3.4.3 Usage of tickets in ticket group 2 ........................................... 51

3.5 Security analysis and the related work ........................................... 53

3.5.1 Security threats ........................................... 53

3.5.2 Related work ........................................... 55

3.5 Conclusion ........................................... 57

4 Untraceable Off-line Electronic Cash Flow in E-Commerce ........................................... 59

4.1 Introduction ........................................... 59

4.1.1 Electronic cash and its properties ........................................... 59
4.1.2 Off-line Electronic Cash Overview ........................................... 62
4.1.3 Outline of the chapter ................................................................. 62
4.2 Some Basic Definitions ................................................................. 63
  4.2.1 Random oracle model ............................................................... 63
  4.2.2 Cut-and-Choose technique ......................................................... 64
  4.2.3 DLA ...................................................................................... 65
  4.2.4 Blind signature ................................................................... 66
4.3 Basic model ................................................................................ 67
4.4 New off-Line Untraceable Electronic Cash
  Scheme .......................................................................................... 68
  4.4.1 System Initialization ................................................................. 69
  4.4.2 New Untraceable Electronic Cash Scheme .............................. 70
4.5 Security Analysis .......................................................................... 73
4.6 A simple example ......................................................................... 75
4.7 Comparisons ................................................................................ 77
4.8 Conclusion ................................................................................... 80

5 Building a consumer scalable anonymity payment protocol for Internet purchases ................................................. 81
  5.1 Introduction .................................................................................. 82
  5.2 Some Basic Definitions ................................................................. 84
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>ElGamal encryption system</td>
<td>84</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Undeniable signature scheme and Schnorr signature scheme</td>
<td>84</td>
</tr>
<tr>
<td>5.3</td>
<td>Basic model and new payment model</td>
<td>86</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Basic payment model</td>
<td>86</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Anonymity Provider Agent</td>
<td>87</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Proof of ownership of a coin</td>
<td>89</td>
</tr>
<tr>
<td>5.4</td>
<td>Self-scalable anonymity payment scheme</td>
<td>90</td>
</tr>
<tr>
<td>5.4.1</td>
<td>System Initialization</td>
<td>90</td>
</tr>
<tr>
<td>5.4.2</td>
<td>New off-line payment scheme</td>
<td>91</td>
</tr>
<tr>
<td>5.5</td>
<td>Security Analysis</td>
<td>95</td>
</tr>
<tr>
<td>5.5.1</td>
<td>Payment scheme security</td>
<td>95</td>
</tr>
<tr>
<td>5.6</td>
<td>Comparisons</td>
<td>98</td>
</tr>
<tr>
<td>5.7</td>
<td>An example</td>
<td>99</td>
</tr>
<tr>
<td>5.7.1</td>
<td>An example</td>
<td>100</td>
</tr>
<tr>
<td>5.7.2</td>
<td>Purchase procedures</td>
<td>101</td>
</tr>
<tr>
<td>5.8</td>
<td>Conclusions</td>
<td>103</td>
</tr>
<tr>
<td>6</td>
<td>Role Based Access Control and its applications</td>
<td>105</td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>105</td>
</tr>
<tr>
<td>6.2</td>
<td>Administrative issues in RBAC</td>
<td>109</td>
</tr>
<tr>
<td>6.2.1</td>
<td>User-role assignments</td>
<td>109</td>
</tr>
</tbody>
</table>
6.2.2 Permission-role assignments ................................. 112
6.2.3 Role-role assignment ........................................ 113
6.2.4 Duty separation constraints ................................. 114
6.3 User-role assignments for a flexible payment scheme ........ 116
6.4 Permission-role assignments with the payment scheme ........ 124
6.5 Related work ....................................................... 129
6.6 Conclusions ......................................................... 131

7 Formal Authorization Allocation Approaches for URA Based on
Relational Algebra Operations ......................................... 133

7.1 Introduction ....................................................... 134
7.2 Problem Definitions ............................................. 135
7.3 Authorization granting and revocation algorithms ................ 139
7.4 Algorithms for URA with the mobility of user-role relationship .......... 146
  7.4.1 Introduction of mobility .................................. 146
  7.4.2 Authorization granting and revocation algorithms .......... 149
7.5 Applications of the relational algebra algorithms ................ 163
  7.5.1 An application of the authorization granting algorithm .......... 163
  7.5.2 Application of the authorization revocation algorithm .......... 164
7.6 Related work ....................................................... 167
7.7 Conclusions ......................................................... 169
8 Formal Authorization Allocation Approaches for PRA Based on Relational Algebra Operations

8.1 Introduction .......................................................... 171
8.2 Authorization granting and revocation algorithms for PRA ........ 175
8.3 Extensions of the algorithms with mobility of permissions .......... 184
8.4 Illustration of the relational algebra algorithms with permission-role assignments ................................................. 195
8.5 Related work ............................................................ 200
8.6 Conclusions ............................................................. 201

9 Conclusions and future work ........................................... 203

9.1 Contributions .......................................................... 203

9.1.1 Enhancements on ticket-based access control scheme for mobile user .......................................................... 204
9.1.2 Enhancements on anonymity payment scheme ............... 204
9.1.3 Enhancements on formal authorization approaches for role based access control .......................................... 205

9.2 Future work ............................................................. 206

9.2.1 Improvement of the payment scheme ......................... 206
9.2.2 Extension of formal authorization approaches for role based access control ........................................... 207
9.2.3 Electronic commerce with RBAC .............................. 207
9.2.4 Implementation issues .......................... 208

10 Index ............................................. 215

11 Bibliography ..................................... 219
Contents

1 Introduction .................................................. 1
   1.1 Overview and Motivation .............................. 1
   1.1.1 Mobile service system ............................ 1
   1.1.2 Electronic payment .................................. 6
   1.1.3 Role based access control ......................... 10
   1.2 Objectives of the Thesis ............................ 13
   1.3 Organization of the Thesis .......................... 14

2 Electronic Commerce Items and Related Technology ........ 17
   2.1 Introduction ........................................... 17
   2.2 Items in Electronic Commerce ....................... 18