

Secure Multi-Party Non-Repudiation Protocols and Applications

Secure Multi-Party Non-Repudiation Protocols and Applications

by

José A. Onieva
*University of Malaga
Spain*

Javier Lopez
*University of Malaga
Spain*

Jianying Zhou
*Institute for Infocomm Research
Singapore*

 Springer

Authors:

José A. Onieva
University of Malaga
Computer Science Dept.
E.T.S. Ingenieria Informaica
Campus de Teatinos
29071 Malaga, Spain
onieva@lcc.uma.es

Javier Lopez
University of Malaga
Computer Science Dept.
E.T.S. Ingenieria Informaica
Campus de Teatinos
29071 Malaga, Spain
jlm@lcc.uma.es

Jianying Zhou
Institute for Infocomm Research (I2R)
21 Heng Mui Keng Terrace
Singapore 119613, Singapore
jyzhou@i2r.a-star.edu.sg

ISBN-13: 978-0-387-75629-5

e-ISBN-13: 978-0-387-75630-1

Library of Congress Control Number: 2008938604

© 2009 Springer Science+Business Media, LLC.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

springer.com

To my parents, for being always there.
– Jose A. Onieva.

Preface

Currently, it seems that each day the world is less reluctant to accept the truth: communications will be shifted to Internet (whatever the generation is when it takes place). Doubtlessly, this will result in a large number of advantages, speeding up the way we have to make businesses and be in touch with each other. Some solutions are already part of our lives and either enhance or provide new methods for communicating, purchasing, selling, reporting and in general transmitting information. Some of these are: VoIP, Instant Messaging, E-Mail, E-commerce, Internet Payment methods, P2P for file sharing, etc.

In some of these methods efficiency and functionality are of major concern. Furthermore, tools (or protocols) providing this functionality have gained a place or become a de-facto standard because they perform better at providing this key components. Nevertheless, other solutions need to consider security as a key component from the very beginning of their design. Moreover, fulfilling this important and at the same time difficult to achieve property, some solutions have failed to accomplish their purpose as users are still unenthusiastic about adopting new solutions if either security is important or otherwise this is not provided with a 100% assurance. In other words, trust is not easily assumed by users in e-payment methods, e-commerce, e-banking, contract signing applications, Internet biddings, etc.

But as security practitioners learn from the very beginning of their career, there's no unconditional and complete secure system. What's more, it will never exist. There is always something that could not work in the system, be broken up, accessed without authorization, leaked information, etc. And if not, the human component (which will be present as long as we do) would need to be totally trusted not to put in risk all the implemented security measures.

This is the reason for which in traditional paper-based procedures (as with contract signing, money transfers, etc.) accountability as a means to solve possible disputes among users has always played part of the procedure itself. Here the hand-written signature plays the main role. It allows for (non-)repudiation of acts such that, for instance, a bank cannot transfer our money from one account to another if it does not have an application with our consent (signature). And of course, it exists

the digital counterpart: the digital signature. And even better, most of the countries already (or are in the way to) have legislated its use.

But unfortunately, the network communication grounds (and among them, distance and lack of trust) make translation of paper-based procedures to networked digital ones hard to achieve. Thus, in order to realize security in Internet (or any other networked including mobile) applications, special protocols are needed to ensure that any dispute could be solved between users if the network fails or an entity misbehaves. In the computer security field, these protocols are known as non-repudiation protocols.

Research oriented to non-repudiation protocols has been active since late 90's; considering in most occasions Alice and Bob as the players of the protocol design scenario. It is time to give a step forward and realize that in many applications there are more than two entities and that two-party protocols are not appropriate for scenarios in which multiple entities are involved. This is the main aim of this book.

This book is mainly targeted to professional audiences with in-depth knowledge of information security and a basic knowledge of applied cryptography. This book briefly settles the state of the art in non-repudiation protocols and gives insight of its applicability to e-commerce applications. It organizes the existing scant literature regarding non-repudiation protocols with multiple entities' participation. It provides to the reader with sufficient grounds to understand the non-repudiation property and its applicability to real applications. Security practitioners will find it very useful in the design of secure applications with multiple entities, helping them to envisage the basics of multi-party non-repudiation as a necessary tool when trust is not present among players. Additionally it could serve as text book for postgraduate students who wish to understand the non-repudiation service and mechanisms in the presence of an undefined number of players.

Malaga,
September 2008

Javier Lopez
Jianying Zhou
Jose A. Onieva

Contents

Part I Introduction and Fundamentals

1	Introduction	3
1.1	Introduction to E-commerce	3
1.2	Security Issues in E-commerce	6
1.3	Security Services and Protocols	8
1.4	The Non-repudiation Service	10
1.5	Challenges and Goals of this Book	12
	Appendix	14
2	Fundamentals of Non-repudiation	17
2.1	Specific Non-repudiation Services	17
2.2	Evidence	19
2.3	Roles of the TTP	21
2.4	Non-repudiation Phases	23
2.5	Non-repudiation Requirements	25
2.6	Analysis of Standards	27
2.7	Supporting Legal Framework	29

Part II Multi-Party Non-repudiation

3	Multi-Party Non-repudiation: Analysis	35
3.1	General MPNR Problem	35
3.1.1	Definitions	35
3.1.2	State of the Art Analysis	40
3.2	1-N MPNR Problem and State of the Art	47
3.3	General Contribution to Multi-Party Problem	50
3.3.1	Model Definition	53
3.3.2	Cryptographic Primitives	54
3.4	Summary of MPNR Protocol Properties	57

4	New Design Approaches for MPNR	59
4.1	MPNR Protocol for Different Messages	60
4.1.1	On-line MPNR Protocol for Distribution of Several Messages	60
4.1.2	Optimistic MPNR Protocol for Exchange of Different Messages	64
4.1.3	Fairness vs. Collusion	71
4.1.4	Further Discussions	71
4.2	Agent-Mediated Non-repudiation Protocols	74
4.2.1	Model	75
4.2.2	First Solution	75
4.2.3	Simple Agent-Mediated Protocol	77
4.2.4	Extension to Multiple Recipients	80
4.2.5	Further Extension to Multiple Messages	84
4.2.6	Applications	87
4.2.7	Requirements Fulfillment	88
4.3	Event-Oriented Simulation	89
4.3.1	Protocol	89
4.3.2	Simulation Model	90
4.3.3	Main Model Simulation Events	94
4.3.4	Output Analysis	98

Part III Applications

5	Multi-Party Non-repudiation Applications	109
5.1	Multi-Party Optimistic Fair CEM	109
5.1.1	A Protocol for Fair CEM with Deadline Time	110
5.1.2	Extension to Fair CEM with Asynchronous Timeliness	111
5.1.3	Extension to Multi-Party Fair CEM	113
5.1.4	Requirements Fulfillment	116
5.2	Multi-Party Contract Signing	119
5.2.1	A New Synchronous MPCs Protocol	120
5.2.2	Requirements Fulfillment	123
5.2.3	Achieving Abuse-Freeness	125
5.2.4	Achieving Timeliness	127
6	Scenarios Supported by MPNR Services	131
6.1	Extension of an OMA-based DRM Framework	132
6.1.1	Protocol	135
6.1.2	Design and Implementation	140
6.1.3	Requirements Fulfillment	142
6.2	Practical Service Charge for P2P Content Distribution	145
6.2.1	Scenario and Requirements	145
6.2.2	P2P Payment Protocol	147
6.2.3	A New Approach	148

- 6.2.4 Requirements Fulfillment 152
- 6.2.5 Practical View 155
- 6.3 Free Roaming Agent Result-Truncation Defense 157
 - 6.3.1 Security Requirements 158
 - 6.3.2 Cheng-Wei Protocol 159
 - 6.3.3 Security Analysis 162
 - 6.3.4 Amendments 164
 - 6.3.5 Security Requirements Analysis 166

Part IV

- 7 Conclusions 171**
- References 177**
- Index 183**

List of Figures

1.1	Conglomerate of Applications	5
1.2	Security Architectural Elements in X.805 ITU-T Recommendation	9
2.1	Models of Message Transfer	18
3.1	n2n Scenario	36
3.2	Non-repudiation Service	38
3.3	Ferrer et al. Solution for Multi-party Certified Email	49
3.4	E-commerce Scenario	50
3.5	Layered Architecture of Non-repudiation Protocols	54
4.1	Protocol for Distribution of Different Messages	61
4.2	Optimistic Protocol with Different Messages	66
4.3	E-commerce Scenario with an Active Intermediary Agent	75
4.4	An Intuitive Solution to Non-repudiation	76
4.5	Virtual Shopping	87
4.6	Simulation Events	91
5.1	Deadline Time Intervals	111
5.2	CEM-ZOL Protocol	114
6.1	Content Distribution	133
6.2	DRM	134
6.3	Right Object Acquisition	135
6.4	HTTP Communication Flow	140
6.5	P2P Service and Payment Scenario	146
6.6	Application Scenario	156
6.7	Agent Transmission	162
6.8	Attack Scenario	163
6.9	Amended Agent Transmission	166

List of Tables

3.1	Multi-party Protocols' Properties Summary	58
3.2	New Solutions' Properties Summary	58
4.1	O's Computation Complexity	64
4.2	R'_i 's Computation Complexity	64
4.3	TTP's Computation Complexity	64
4.4	General Off-line Solution Comparison	70
4.5	Public Key Operations Comparison	70
4.6	Simulator Entity	93
4.7	Message Entity	93
4.8	Originator Entity	94
4.9	Recipient Entity	94
4.10	TTP Entity	95
4.11	Input Test for P1	101
4.12	Output Results for P1	101
4.13	Input Test for P2	104
4.14	Output Results for P2	105
6.1	Model Notation	160
6.2	Cryptographic Notation	160

Acronyms

Lists of abbreviations, symbols.

ANX	Automotive Network Exchange
API	Application Programming Interface
B2B	Business-to-Business
B2C	Business-to-Consumer
C2C	Consumer-to-Consumer
CA	Certification Authority
CEM	Certified Electronic Mail
CEMBS	CERTificate of a Message Being a Signature
CRL	Certificate Revocation List
DES	Data Encryption Standard
DoS	Denial of Service
DRM	Digital Rights Management
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EOD	Evidence of Delivery
EOO	Evidence of Origin
EOR	Evidence of Receipt
ERP	Enterprise Resource Planning
EU	European Union
FTP	File Transport Protocol
GPRS	General Packet Radio Service
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IN	Intermediary ageNt
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Standarization Organization

IT	Information Technology
ITU	International Telecommunications Union
L2TP	The Layer Two Tunneling Protocol
LAN	Local Area Network
MPNR	MultiParty Non-Repudiation
MAC	Message Authentication Code
MNO	Mobile Network Operator
MPCS	Multi-Party Contract Signing
NRD	Non-repudiation of Delivery
NRO	Non-Repudiation of Origin
NRR	Non-Repudiation of Receipt
NRS	Non-repudiation of Submission
OCSP	On-line Certificate Server Protocol
ODR	On-line Dispute Resolution
OMA	Open Mobile Alliance
OS	Operating Systems
OSI	Open System Interconnection
P2P	Peer-to-Peer
PC	Personal Computer
PCS	Private Contract Signature
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
PRAC	Partial Result Authentication Code
QES	Qualified Electronic Signature
QoS	Quality of Service
RSA	Rivest, Shamir and Adelman
RO	Right Object
RI	Rights Issuer
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
SSH	Secure SHell
S/MIME	Secure/Multipurpose Internet Mail Extensions
TSA	Time-Stamp Authority
TCP	Transport Control Protocol
TLS	Transport Layer Security
TPD	Trusted Personal Device
TTP	Trusted Third Party
URL	Uniform Resource Locator
VPN	Virtual Private Network
WEP	Wireless Equivalent Privacy
WTLS	Wireless Transport Layer Security
XML	eXtensible Markup Language