



Source Authentication in Group Communication

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

Doctor of Philosophy

from

MACQUARIE UNIVERSITY

by

Mohamed Hussain Al-Ibrahim, (MEngSc - UNSW)

Computing Department - Algorithms and Cryptography
March 2005

© Copyright 2005

by

Mohamed Hussain Al-Ibrahim, (MEngSc - UNSW)

All Rights Reserved

Dedicated to
My Parents

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Mohamed Hussain Al-Ibrahim, (MEngSc - UNSW)
March 25, 2005

Abstract

This is a thesis in the area of *Applied Cryptography and Network Security*, where we investigate the problem of *Source Authentication in Group Communication* in the context of multicast environment.

Multicast is a relatively new and emerging communication mode in which a sender sends a message to a group of recipients in just one connection establishment. The main benefits behind this technique is apparent in reducing bandwidth overhead and increasing resource utilization in the already congested and contented network. This makes multicast technology a perfect option for group communication. The focus of the research in this area has been in two directions: first, building an efficient routing infrastructure and, secondly, building a sophisticated security infrastructure. The focus of this work is on the second issue.

In general, building a secure system requires providing a number of services. These services includes confidentiality, integrity, authenticity and non-repudiation. As a rule of thumb, some systems have special characteristics; consequently, construction of their associated security environment has special characteristics as well. This is also true in multicast security. One of the distinguishing issues in securing multicast environment is providing source authentication.

A typical multicast operation is one in which a host tries to join a multicast environment using membership protocol and becomes a member of a group. Based on a successful membership, the host is able to send or receive messages to or from other members of the group. When a sender sends a message to a group of recipients, the operation takes the form of one-to-many communication. Consequently, receivers would send their acknowledgments back to the sender in many-to-one mode. Usually, traffic passes through intermediate nodes in the network, between the sender and receiver, as transit flows. An *ideal authenticated multicast environment* is the one which provides authenticity for all the communication operations in the system.

In this thesis, we focus on the source authentication in multicast communication and propose a *comprehensive* solution to the problem of authentication in multicast communication which tackles the problem for its all possible operations.

We have divided the authentication process in a multicast environment into four stages:

1. one-to-one (or joining mode)
2. one-to-many (or broadcast mode)
3. many-to-one (or concast mode)
4. intermediate (or transit mode)

For each of the above stages, we study and propose new authentication scheme(s).

In addition, we study the authentication problem in the multicast-related communication mode known as anycast, in which a server is selected from a group of servers.

Further, we develop several authentication schemes for group-based communication exploiting the distinct features of one-time signatures. The schemes cover situations when a threshold number of participants are involved and situations where a proxy signer is required.

Thesis Related Publications

1. Mohamed Al-Ibrahim and Josef Pieprzyk, “Authenticating Multicast Streams in Lossy Channels Using Threshold Techniques,” In the proceedings of the *First International Conference in Networking: ICN’01*, Colmar: France, Lecture Notes in Computer Science *vol. 2094*, pp. 239–249, P. Lorenz (Eds), Springer-Verlag, July 2001.
2. Mohamed Al-Ibrahim and Josef Pieprzyk, “Authentication of Transit Flows and k -Sibling One-time Signatures,” In the proceedings of the *Sixth IFIP Communication and Multimedia Security Conference: CMS’02*, Portroz: Slovenia, pp. 41–55, Kluwer Academic Publisher, September 2002.
3. Mohamed Al-Ibrahim, Hossein Ghodosi and Josef Pieprzyk, “Authentication of Concast Communication,” In the proceedings of the *Third International Conference on Cryptology in India: INDOCRYPT’02*, Hyderabad: India, Lecture Notes in Computer Science *vol. 2551*, pp. 185–198, A. Menezes and P. Sarkar(Eds), Springer-Verlag, December 2002.
4. Mohamed Al-Ibrahim, “An Authentication Scheme Using A Secret Sharing Technique,” In the proceedings of the *International Conference on Information Networking: ICOIN’03*, Jeju island: Korea, *vol. II*, pp. 923–929, February 2003.
5. Mohamed Al-Ibrahim and Anton Cerny, “Authentication of Anycast Communication,” In the proceedings of the *Second International Workshop in Mathematical Methods, Models and Architectures for Computer Networks Security: MMM-ACNS 2003*, Saint-Petersburg: Russia, Lecture Notes in Computer Science *vol. 2776*, pp. 419–423, Springer-Verlag, September 2003.

6. Mohamed Al-Ibrahim, “A Signcryption Scheme based on Secret Sharing Technique,” In the proceedings of the *Second International Workshop in Mathematical Methods, Models and Architectures for Computer Networks Security: MMM-ACNS 2003*, Saint-Petersburg : Russia, Lecture Notes in Computer Science *vol. 2776*, pp. 279–288, Springer-Verlag, September 2003.
7. Mohamed Al-Ibrahim and Anton Cerny, “Proxy and Threshold One-time Signatures,” In the proceedings of the *First MiAn International Conference in Applied Cryptography and Network Security: ACNS’03*, Kunming: China, Lecture Notes in Computer Science *vol. 2846*, pp. 123–136, J. Zhou, M. Yung, and Y. Han (Eds), Springer-Verlag, October 2003.

Acknowledgements

Firstly, I would like to extend my regards and thanks to my supervisor, Prof. Josef Pieprzyk, without whose invaluable assistance this study would not have been possible. Secondly, I wish to thank my co-supervisor A/Prof. Anton Cerny from Department of Mathematics and Computer Science at Kuwait University for his invaluable support.

I am also grateful for the help and assistance that the staff, and colleagues in the Centre for Computer Security Research at the University of Wollongong provided to me, where this work was initially established. Also, I don't forget to expand my thanks to Mr. Dick Pond for English language consultations.

Finally, I would like to express my gratitude to my father, mother, brothers and other anonymous friends for their encouragement and support throughout my study.

Basic Notation

Most of the notation used in this thesis is defined in the text. Here are listed notation for which this is not done.

\oplus	Exclusive-or (of Booleans)
\vee	Or (of Booleans)
\wedge	And (of Booleans)
$/$	Not (e.g., \neq denotes “not equal”)
\cup	Set union
\cap	Set intersection
\in	Set membership
$\mathcal{P} \setminus \mathcal{A}$	The set of elements in \mathcal{P} but not in \mathcal{A}
$\mathcal{A} \subset \mathcal{P}$	\mathcal{A} is a subset of \mathcal{P} , $\mathcal{A} \neq \mathcal{P}$
$\mathcal{A} \subseteq \mathcal{P}$	\mathcal{A} is a subset of \mathcal{P}
$ $	Such that (set notation)
$a \mid b$	a divides b ($a, b \in \mathbb{N}$)
$ \mathcal{A} $	The cardinality of set \mathcal{A}
$\mathbb{N}, \mathbb{Z}, \mathbb{R}$	The set of natural numbers, integers and reals, respectively
\parallel	Concatenation
$2^{\mathcal{A}}$	The set of all subsets of set \mathcal{A}
2^x	Raising 2 to power x
$\lceil x \rceil$	Smallest integer greater than x
$\lfloor x \rfloor$	Greatest integer smaller than x
$[a]$	A reference (used in bibliography)
$[x, y]$	An interval (a subset of set \mathbb{R})
\mathbb{Z}_a	The set of integers modulo a
\log_a	Logarithm to base a
\sum	Summation
\prod	Multiplication

\rightarrow	Mapping
$\binom{n}{t}$	The number of subsets of cardinality t of a set of cardinality n
\equiv	Congruence
$!$	Factorial (e.g., $n! = 1 \times 2 \times \cdots \times n$)
$GF(p)$	The Galois field with p elements
\mathcal{K}	a set of possible keys
\mathcal{M}	a set of possible messages
\mathcal{C}	a set of possible cryptogram

Acronyms

ATM: Asynchronous Transfer Mode

BiBa: BIns & BALLs

CBT: Core Base Tree

DVMRP: Distance Vector Multicast Routing Protocol

DVS: Designated Verifier Signature

GMR: Goldwaser, Micali , Rackoff

PIM-DM: Protocol Independent Multicast - Dense Mode

PIM-SM: Protocol Independent Multicast - Sparse Mode

IGMP: Internet Group Multicast Protocol

IP: Internet Protocol

LNCS: Lecture Notes in Computer Science

MAC: Message Authentication Code

MOSPF: Multicast Open Shortest Path First

SBIBD: Symmetric Balanced Incomplete Block Design

SEALS: Self Authenticating Values

SIFF: Sibling Intractable Function Family

Contents

Thesis Related Publications	ii
Acknowledgements	iv
Basic Notation	v
Acronyms	vii
1 Introduction	1
1.1 Multicast	2
1.2 Multicast Security	3
1.3 Motivation and Methodology	4
1.4 Organization of the Thesis and Contributions	6
2 Cryptographic Essentials	9
2.1 Terminology	10
2.2 Primitives	12
2.3 Private Key Cryptosystems	13
2.4 Public Key Cryptosystems	14
2.4.1 The RSA Cryptosystem	16
2.4.2 The ElGamal Cryptosystem	17
2.5 Digital Signatures	19
2.5.1 Digital Signature Schemes with Appendix	20
2.5.2 Digital Signature Schemes with Message Recovery	22
2.5.3 One-time Signatures	22
2.5.4 Other Types of Digital Signatures	23
2.5.5 Performance of Digital Signatures	24
2.6 Hashing	24
2.6.1 Properties	24

2.6.2	Keyed Hashing	26
2.6.3	Digital Signatures vs. Message Authentication Codes	28
2.7	Secret Sharing Schemes	28
2.7.1	Basic Concepts	28
2.7.2	Shamir Threshold Scheme	30
2.7.3	Verifiable Secret Sharing Scheme	31
2.8	Cryptographic Protocols	33
3	Multicast: Structure and Security	35
3.1	Multicast Illustrated	35
3.2	Multicast Evolution	37
3.3	Multicast Security	41
3.3.1	Multicast group characteristics	42
3.3.2	Group key management and distribution	43
3.3.3	Source authentication	48
4	Authentication of Multicast Streams	52
4.1	Introduction	52
4.2	Related Work	54
4.3	The Model	56
4.4	Stream Authentication Based on Linear Equations	58
4.4.1	Scheme 1	59
4.4.2	Scheme 2	61
4.5	Stream Authentication Based on Combinatorial Designs	64
4.5.1	Balanced Incomplete Block Design	64
4.5.2	Rotational Designs	66
4.6	Comparative Analysis	67
4.6.1	Linear Equations method	67
4.6.2	Combinatorial Design method	68
4.7	Summary	71
5	Authentication of Concast Communication	72
5.1	Introduction	72
5.1.1	Related Work	73
5.1.2	Concast Scenario	74

5.2	The Model	75
5.3	Components of the System	75
5.3.1	Communication Channel	75
5.3.2	Signature Scheme	76
5.3.3	An Approach to Digital Multisignature	77
5.4	Concast Signatures	78
5.4.1	Warm-up Solution	78
5.4.2	The Concast Scheme	79
5.4.3	Stinson Attack	80
5.4.4	Secured Concast	81
5.5	Fast Screening for a Non-RSA Signature Scheme	83
5.5.1	Model of Security	84
5.5.2	The Screening Scheme	85
5.5.3	Security Analysis	86
5.6	Summary	89
6	Authentication of Transit Flows	90
6.1	Introduction	90
6.2	<i>K</i> -Sibling Intractable Hashing	91
6.2.1	Hashing with a Single Polynomial	92
6.2.2	Hierarchical Sibling Intractable Hashing	93
6.3	Authentication of Packets	93
6.3.1	Authentication with Single Hashing	95
6.3.2	Authentication with Hierarchical Hashing	97
6.3.3	Security Issues	99
6.4	<i>K</i> -Sibling One-time Signature	100
6.4.1	The Scheme	101
6.4.2	Security Issues	104
6.4.3	Performance Issues	106
6.5	Summary	107
7	One-time Signatures for Authenticating Group Communication	108
7.1	Introduction	108
7.2	Related work	110
7.3	A class of one-time signature schemes	110
7.4	A simple one-time proxy signature scheme	112

7.5	A (t, n) threshold one-time signature scheme	116
7.5.1	A scheme with a trusted party	116
7.5.2	A scheme without a trusted party	119
7.6	A (t, n) threshold proxy one-time signature scheme	121
7.6.1	Special case: $t = 1$	124
7.7	Summary	124
8	Authentication of Anycast Communication	125
8.1	Introduction	125
8.2	Related work	126
8.2.1	The Schnorr signature	127
8.2.2	Schnorr-based proxy signatures	127
8.3	Anycast Scenario	128
8.3.1	The Model	128
8.3.2	Security Requirements	130
8.4	The Anycast Scheme	131
8.4.1	Security Issues	133
8.4.2	Performance Issues	135
8.5	Summary	136
9	Authentication of Joining Operation	137
9.1	Introduction	137
9.2	Related Work	138
9.3	Theoretical Description and Construction	139
9.4	Designated Verifier Signature	141
9.4.1	Formal Definition of DVS scheme	141
9.4.2	Security Notions	142
9.4.3	The DVS Scheme	144
9.4.4	Security Analysis	146
9.4.5	Performance Issues	149
9.5	Digital Signcryption	150
9.5.1	Model of Security	151
9.5.2	Formal Definition	152
9.5.3	Description	153
9.5.4	The SC Scheme	154
9.5.5	Security Issues	155

9.5.6 Performance Issues	157
9.6 Summary	158
10 Conclusion and Future Directions	159
10.1 Summary	160
10.2 Future Directions	161
Bibliography	163

List of Tables

2.1	Special signature schemes	23
4.1	Distribution of message digests using SBIBD	66
4.2	A Comparison of multicast authentication schemes	69

List of Figures

1.1	Group-based communication modes	5
3.1	Hierarchical Tree key distribution	47
6.1	Hierarchical Sibling Hashing	94
6.2	Authenticating messages with Hierarchical Sibling Hashing	98
7.1	One-time signature polynomials interpolation	117
8.1	Anycast Model	129