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

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)
$\bigvee$	Or (of Booleans)
$\bigwedge$	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 $\mathcal{P}$
$\mid$	Such that (set notation)
$a \mid b$	a divides b (a, $b \in \mathbb{N}$)
$\lvert\mathcal{A}\rvert$	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
$\left(\begin{array}{c} \mathrm{n} \\ \mathrm{t} \end{array} \right)$	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

List of Tables

List of Figures