AIN SHAMS UNIVERSITY
FACULTY of ENGINEERING
Electronics and Communications Engineering Department

Multicast Authentication Protocol

A Thesis Submitted in partial fulfillment of the requirements for
The Degree of Doctor of Philosophy in Electrical Engineering
(Electronics and Communications Engineering)

Submitted by

Reham Abdellatif Abou Hogail Esmail

M.Sc. in Electrical Engineering
(Electronics and Communications engineering)
Cairo University, 2004)

Supervised by

Prof. Dr.

Slawa Hussein Elramly

Department of Electronics and Communications Engineering
Faculty of engineering, Ain Shams University

Assoc. Prof.

Heba Kamal Aslan

Electronics Research Institute

Cairo, Egypt
2008

AIN SHAMS UNIVERSITY
FACULTY of ENGINEERING

Electronics and Communications Engineering Department

Judgment Committee

Presented by: Reham Abdellatif Abou Hogail

Thesis Title: Multicast Authentication Protocol

Degree: Doctor of philosophy in Electrical Engineering

Name, Title and Affiliation	**Signature**
Prof. Dr. Abdelrahman Hussein El-Sawy Electronics and Communication Engineering Dept. Faculty of Engineering, Helwan University	(Examiner)
Prof. Dr. Hadia Mohammed El-Hennawy Electronics and Communication Engineering Dept. Faculty of Engineering, Ain Shams University	(Examiner)
Prof. Dr. Salwa Hussein El-Ramly Electronics and Communication Engineering Dept. Faculty of Engineering, Ain Shams University	(Supervisor)
Assoc. Prof. Dr. Heba Kamal Aslan Informatics Dept. Electronic Research Institute	(Supervisor)

Date:30-10-2008

ACKNOWLEDEMENTS

الحمد لله رب العالمين

I thank God, my country, and my supervisors Prof. Salwa Hussein Elramly and Associated prof. Heba Kamal Aslan for great effort in this study.

Prof. Dr. Salwa El Ramly gave me the valuable suggestions, guiding and advices, which raises my thinking way.

I thank my supervisor Associate prof. Heba Kamal Aslan for her great effort in many stimulating discussions. The reading of many references and the corrections led to improve the presented work.

I would like to thank Prof. Dr. Ibrahim Metawie, the professor in the National Institute of Standard for his encouragement.

I am indebted to my parents, my sister, my brothers, the rest of my family, and all my friends for keeping my morals high.

Special thanks to my mother, the most compassionate person in the world.

My deep thanks to my husband, for his help, support, and understanding. He was the friend, the father, the brother, and the husband.

Many thanks to my darling daughter, and my darling son.

STATEMENT

This dissertation is submitted to Ain Shams University for the degree of Philosophy Doctor in Electrical Engineering (Electronics and Communication Engineering).

The work include in this thesis was carried out by the author at the Electronics and Communications Engineering Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt.

No part of this thesis was submitted for a degree or a qualification at any other university or institution.

Name: Reham Abdellatif Abou Hogail.

Contents

List of Figures

List of Tables

List of Abbreviations

AAPA	Automatic Authentication Protocol Analyzer
BAN	Burrows, Abadi, and Needham
CAPSL	Common Authentication Protocol Specification Language
FDR	Failures Divergences Refinement Checker
HOL	Higher Order Logic
IDA	Information Dispersal Algorithm
IGMP	Internet Group Membership Protocol
IP	Internet Protocol
ISL	Interface Specification Language
LOTOS	Language of Temporal Ordering Specification
MAC	Message Authentication Code
MBMAEC	MAC-Based Multicast Authentication using Erasure Code
MD5	Message Digest version5
MuCAPSL	Multicast Common Authentication Protocol Specification Language
PRABS	Pollution Resistant Authenticated Block Streams
TRNG	True Random Number Generator
RSA	Rivest-Shamir-Adelman
SAIDA	Signature Amortization using IDA

List of Symbols

Count	Counter length
E	The erasure code function
Edec	The erasure decoding function
EncLen	Length of the symmetric encryption
F	A pseudo random function
H	The hash function
Hout	Length of the hash function
K_a^{-1}	Private key of *A*
K_g	The group key
KeyLen	Key length
MAC	Length of the MAC
P_i	Packet number *i*
R	The loss rate
RN	Length of the random number
Sig	The signature length
UMACout	Length of the UMAC function output

Thesis Abstract

Multicast gives professional large-scale content distribution by providing an efficient transport mechanism for one-to-many and many-to-many communication. Over the years, multicast has been the topic of many research, and development efforts. These efforts have continued to transform multicast into a technology that can be trusted by a large number of applications. Therefore, security in multicast content distribution is an important issue.

There is a number of security issues in multicast communication directly related to the specific nature of multicast. There has been many researches that provide solutions to many of these security issues. Some of these solutions are ready for operation, some are still under development, and others are in the primary phases of research.

In this thesis, we concentrate on the multicast authentication problem. two methods are described for authenticating multicast packets. Erasure code function is used to amortize a single signature operation over multiple packets. This technique is especially efficient in terms of communication overhead, because the essential elements needed for authentication are one MAC per packet and one signature per group of packets.

The first proposed protocol is concerned with the real time applications; it is based on the idea of dividing the stream into blocks of m packets.

The UMAC of each packet is calculated, and then the signature is calculated over the concatenation of all UMAC of the packets. The proposed scheme resists packet loss by using erasure code functions over the signature and the UMAC of the packets. To resist pollution attacks, our scheme computes the UMAC of the erasure code output. To resist replay attacks, a counter number is added to each packet. The proposed scheme is compared to other multicast authentication protocols. The comparison shows that the proposed scheme has the following advantages: first, it has low computation and communication overheads; second it has reasonable buffer requirements. Furthermore, it resists packet loss, pollution attacks, and replay attack. This protocol assumes that the group members are trusted entities and are not likely to be disturbing the system themselves.

The second proposed protocol is for general applications, different types of group members. It is based on the idea of dividing the stream into blocks of *m* packets. The digital signature is calculated over a generated random number. The proposed scheme resists packet loss by using erasure code functions over the signature. To resist pollution attacks, our scheme computes the UMAC of the erasure code output. To resist replay attacks, the generated random number is changed with every block. The proposed scheme is compared to other multicast authentication protocols. The comparison shows that the proposed scheme has the following advantages: first, it has low computation and communication overheads and it has reasonable buffer requirements. Furthermore, it resists packet loss, pollution attacks and replay attacks.

To evaluate the correctness of our scheme, we analyze our two techniques with a known logical analysis technique. First, we give a survey of the formal methods that are used in the analysis of cryptographic protocols. We use Meadows's classification which divides the analysis techniques into four types.

The Type I approach models and verifies a protocol using specification languages and verification tools not specifically developed for the analysis of cryptographic protocols. In Type II, a protocol designer develops expert systems to create and examine different scenarios, from which one may draw conclusions about the security of the protocols being studied. Type III approach develops a formal model based on the algebraic term-rewriting properties of cryptographic systems. Finally, the IV approach models the requirements of a protocol family using logics developed specifically for the analysis of knowledge and belief.

Most of the research and the most interesting results are in Type IV approach, such as Burrows, Abadi and Needham logic; we present this technique and its language. We make verification of the two presented protocols using the BAN logic. The verification results show that these protocols achieve their goals.