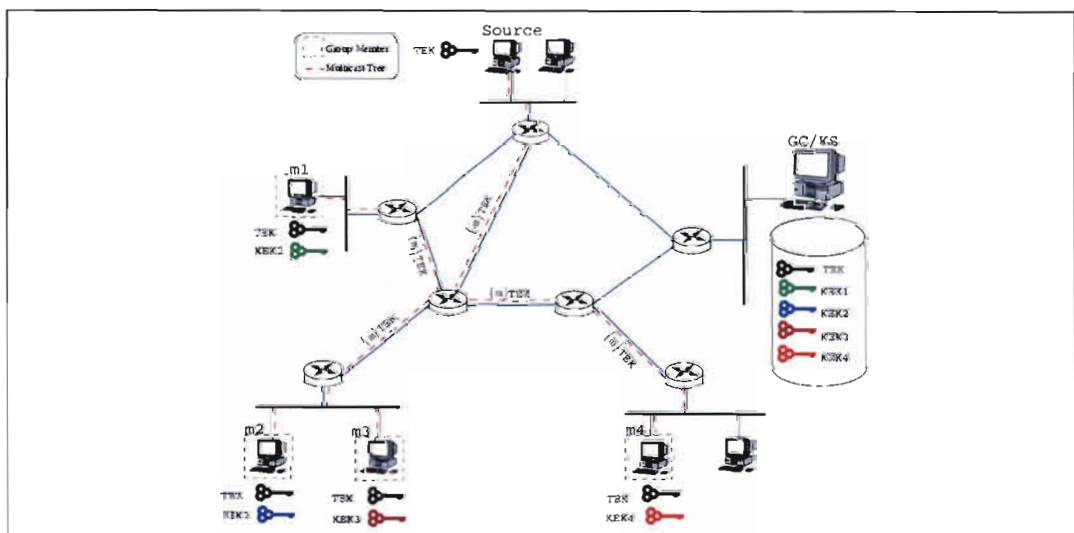


Par Yacine CHALLAL

Sécurité dans les communications de groupe.

Thèse présentée
pour l'obtention du grade
de Docteur de l'UTC.



Soutenu le : 13 mai 2005

Spécialité : Technologies de l'Information et des Systèmes

Group Communication Security

Yacine Challal

► **To cite this version:**

Yacine Challal. Group Communication Security. Networking and Internet Architecture [cs.NI]. Université de Technologie de Compiègne, 2005. English. tel-01308756

HAL Id: tel-01308756

<https://hal.archives-ouvertes.fr/tel-01308756>

Submitted on 28 Apr 2016

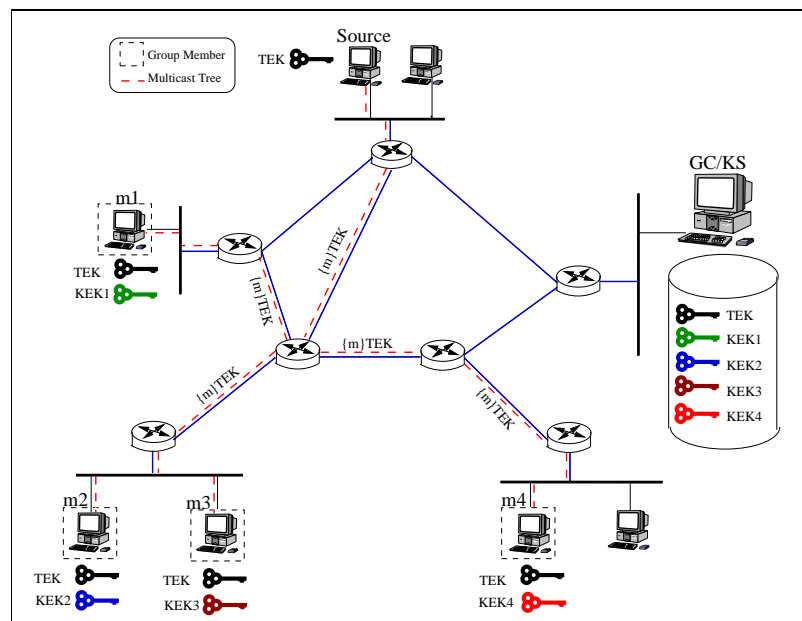
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

by Yacine Challal

Group Communication Security

Ph.D. Thesis



Thesis defense: May, 13th 2005

Abstract

THE advantages of IP multicast in multi-party communications, such as saving bandwidth, simplicity and efficiency, are very interesting for new services combining voice, video and text over Internet. This urges the effective large scale deployment of multicasting to satisfy the increasing demand for multicasting from both Internet Service Providers (ISPs) and Content Distributors. Unfortunately, the strengths of IP multicast are also its security weaknesses. Indeed, the open and anonymous membership and the distributed nature of multicasting are serious threats to the security of this communication model. Much effort has been conducted to address the many issues relating to securing multicast data transmission, such as: *access control, confidentiality, authentication and watermarking*.

In this thesis we deal with the two keystone security issues of any secure multicast architecture: *data origin authentication and confidentiality*. For each theme, we present a detailed analysis of the problem while highlighting special features and issues inherent to the multicast nature. Then, we review existing solutions in the literature and analyze their advantages and shortcomings. Finally, we provide our own original proposals, depicting their advantages over the previous solutions.

Acknowledgments

MY first and most heartfelt thanks go to my supervisor, M. Abdelmadjid Bouabdallah, Professor at Compiegne University of Technology for invaluable discussions and advice throughout the course of this research, and for many helpful comments and concise and constructive criticism without which this dissertation would not have been achieved.

Particular thanks go to M. Hatem Bettahar, Assistant Professor at Compiegne University of Technology, for inestimable advice and fruitful discussions during my research. Each time I faced difficulties, I had always found Hatem next to me for encouragements and solutions.

I would like also to thank the reviewers of my thesis, M. J. William Atwood, Professor at Concordia University and M. Serge Fdida, Professor at Paris VI University, who took time out of their busy schedules to send valuable comments and feedback about this work. My thanks go also, to M. Prosper Chemouil, Research Director at France Telecom R&D, and M. Ahmed Serhrouchni, Assistant Professor at ENST-Paris, for having accepted to be in the jury of my thesis defense.

Next, a note of gratitude to my colleagues of the Networking group (Heudiasyc Lab.), Imed Romdhani, Mounir Kellil, Hamida Seba, Hani Ragab, Yoann Hinard, Yacine Khaled, Hamid Menouar, David Savourey, Linh Doan, François Clautiaux and Farid Sayeh for their help and encouragement.

I would like to thank our colleagues at Algiers University of Technology (USTHB-Algeria), Professor Nadjib Badache and Mahfoud Benchaiba, and the folks at the Research Centre on Technical and Scientific Information (CERIST-Algeria), Djamel Tandjaoui, Djamel Djenouri, Wahid Derhab for many stimulating discussions of ideas of mutual interest during their visits to our lab.

I wish to thank Said Gharout and Abdelaziz Babakhouya; master students at Bejaia University for the many interesting exchanges during their internship.

I am grateful to the Algerian and French governments for supporting my research with the Algerian-French Cooperation Scholarship.

Special thanks go to Samir Kohil, Ali Khouas, Kamel Merdes, Youcef and the folks at ETM-Ibnrochd for their support and encouragements.

My deep gratitude to my parents, and my family, for supporting me all this time, and to my fiancée, for her support and patience.

Contents

Committee Members	iii
Dedication	v
Abstract	vii
Acknowledgments	ix
Author Publications List	xi
Glossary	xiii
Contents	xv
List of Tables	xxi
List of Figures	xxiii
Introduction	1
1 Multicast Security Background	5
1.1 Multicasting: strengths and motivations	5
1.2 Security and Multicasting: a Complex Deal	6
1.2.1 Security threats and countermeasures	6
1.2.2 Challenges to overcome	8
1.3 The IETF multicast security reference framework	9
1.4 Conclusion	11

I	Group Communication Confidentiality	13
2	Definitions and Requirements	15
2.1	Data confidentiality	15
2.1.1	Symmetric-key Encryption	15
2.1.2	Public-key Encryption	16
2.2	Group Communication Confidentiality	16
2.3	Group Key Management Requirements	17
2.4	Conclusion	19
3	A Taxonomy of Group Key Management	21
3.1	Common TEK Approach	21
3.1.1	Centralized Protocols	21
3.1.2	Decentralized Architectures	28
3.1.3	Distributed Key-agreement Protocols	32
3.2	Independent TEK per sub-group	37
3.2.1	Membership-driven re-keying	37
3.2.2	Time-driven re-keying	40
3.2.3	Comparison	40
3.2.4	Conclusion	41
4	Scalable and Adaptive Group Key Management	43
4.1	Overview of SAKM Architecture	44
4.2	SAKM Analytic Model	45
4.2.1	Preliminaries and nomenclature	45
4.2.2	Multicast Dynamism Model	47
4.2.3	Application of the analytic model to actual re-key strategies	50
4.3	SAKM problem statement	52
4.3.1	Illustrative example	52
4.3.2	SAKM problem formalization	53
4.4	SAKM Protocol	54

4.4.1	Overview of SAKM protocol	56
4.4.2	Merge / Split Protocol	57
4.4.3	Membership change protocol	59
4.4.4	Agent's dynamic behavior	60
4.5	Simulation results	63
4.5.1	Simulation model	63
4.5.2	Split / merge criteria	64
4.5.3	Simulation results and discussion	64
4.6	Conclusion	67
II	Data Origin Authentication in Group Communication	69
5	Definitions and Requirements	71
5.1	Data integrity	71
5.2	Data origin authentication	72
5.3	Non-repudiation with proof of origin	74
5.3.1	Certification	75
5.3.2	One-time signing	75
5.4	Multicast Data Origin Authentication Issues and Requirements	76
5.5	The bursty packet loss model	77
5.6	Group Authentication vs. Data Origin Authentication	78
5.7	Conclusion	79
6	A Taxonomy of Multicast Data Origin Authentication	81
6.1	Multicast Data Origin Authentication	82
6.1.1	Secret-Information Asymmetry	82
6.1.2	Time Asymmetry	85
6.1.3	Comparison	88
6.2	Multicast Data Origin Authentication with Non-repudiation	89
6.2.1	Signature propagation	90

6.2.2	Signature Dispersal	94
6.2.3	Differed signing	96
6.2.4	Comparison	98
6.3	Conclusions	99
7	Source driven Adaptive Hash-chaining	101
7.1	H_2A : Hybrid Hash-chaining scheme for Adaptive multicast data origin authentication	102
7.1.1	Terminology	102
7.1.2	Redundant and Hybrid Hash-chaining scheme	102
7.1.3	Adaptive Redundancy Degree	103
7.1.4	H_2A protocol	104
7.2	A^2Cast : Adaptive source Authentication protocol for multiCAST streams	107
7.3	Simulations and performance evaluation	108
7.3.1	Simulation parameters	108
7.3.2	Adaptation of redundancy degree	108
7.3.3	Results	110
7.4	H_2A Security and Performance Comparison	111
7.5	Conclusion	113
8	Receiver driven Layered Hash-chaining	115
8.1	RLH: Receiver driven Layered Hash-chaining for multicast data origin authentication	115
8.1.1	Layered Hash-chaining scheme	116
8.1.2	RLH protocol	118
8.2	Simulations and performance evaluation	119
8.2.1	Simulation parameters	120
8.2.2	Updating the membership to authentication layers	121
8.2.3	Simulation Results	122
8.2.4	RLH security and other performance criteria	131
8.2.5	Comparison	132
8.3	Conclusion	132

9 Conclusions and Future Work	135
--------------------------------------	------------

Bibliography	139
---------------------	------------