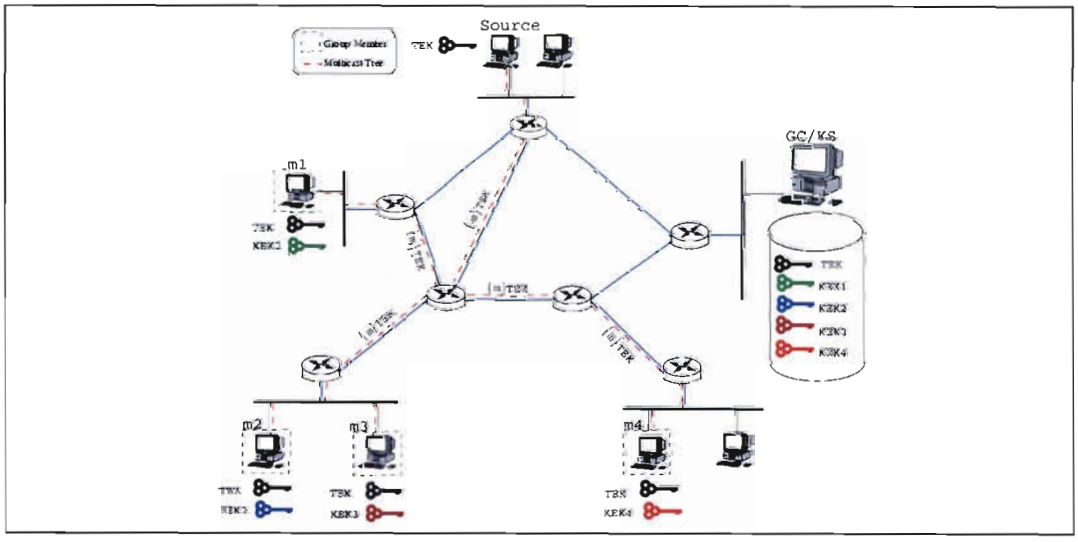
Par Yacine CHALLAL

Sécurité dans les communications de groupe.

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



Soutenue le : 13 mai 2005
Spécialité : Technologies de l'Information et des Systèmes

D1561

Group Communication Security

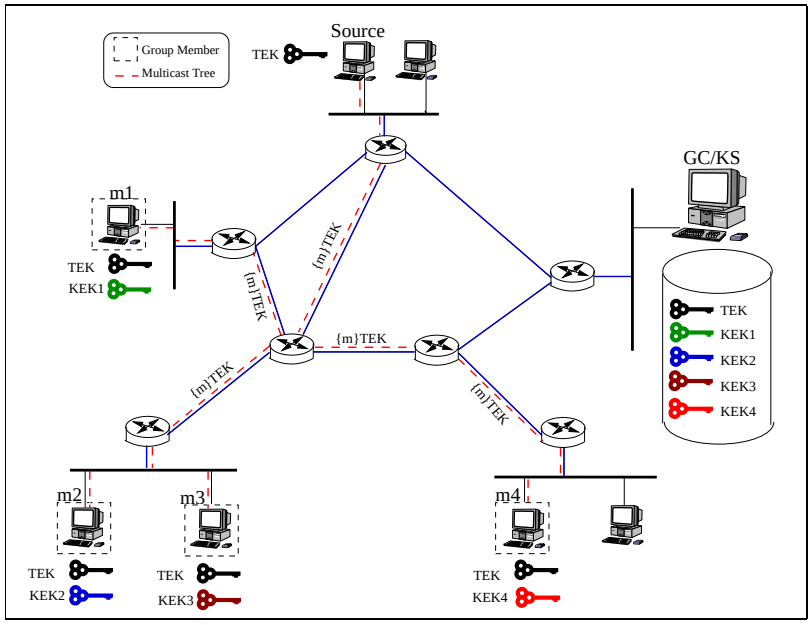
Yacine Challal

utc
Université de Technologie
Compiègne

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 fiancee, for her support and patience.

Contents