Multimedia Encryption, Transmission and Authentication

Edited by

Othman Omran Khalifa, B.Sc. ,M.Sc., Ph.D
International Islamic University Malaysia

Aisha-Hassan Abdulla, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

Teddy Surya Gunawan, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

IIUM PRESS

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Multimedia Encryption, Transmission and Authentication

Edited by

Othman Omran Khalifa, B.Sc. ,M.Sc., Ph.D
International Islamic University Malaysia

Aisha-Hassan Abdulla, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

Teddy Surya Gunawan, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

IIUM Press

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Cataloguing-in-Publication Data Perpustakaan Negara Malaysia

ISBN: 978-967-418-160-4

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Contents

Chapter 30

Multicast Security: *Issues and Solutions*

MOHAMMAD QABAJEH[1], AISHA-HASSAN A. HASHIM[2], OTHMAN O. KHALIF[3]

ECE Dept, Fac. of Eng., International Islamic Univ. Malaysia (IIUM), Jalan Gombak, 53100 Kuala Lumpur, Malaysia.

m_qabajeh@yahoo.com[1], aisha@iiu.edu.my[2], Khalifa@iiu.edu.my[3], liana_tamimi@ppu.edu[4]

30.1. Introduction

The rapid growth of multicast communications has lead to wide use of the Internet for both individual and commercial distributed applications. Multicast communication is defined as an efficient way to distribute rich media to multiple users or participants simultaneously over the Internet. This is efficient in many applications including Internet video transmissions, news feeds, stock quotes, software updates, live multiparty conferencing, on-line video games and shared whiteboards. Thus, the need for secure transmission of multicast streams is considered as an important issue. However, potential security threats to multicast communications are similar to those encountered in unicast transmissions. These threats include the unauthorized creation, alteration ,destruction and illegitimate use of data. In case of multicast traffic, the inherent broad scope of a multicast session, the potential for attacks may be greater than that countered in unicast traffic. It is required to secure these services while maintaining the trade-off between efficiency and performance.

The field of multicast networking and related security issues is an important issue, which requires more efforts from research community. Multicast communication is becoming the basis for a growing number of applications. Therefore, it is important to provide security mechanisms for this type of applications. Various techniques to support multicast security have been proposed. The most common types of encryption are conventional (symmetric or single key) and public-key (asymmetric or two-key) encryption. The most popular symmetric encryption algorithms are data encryption standard (DES) and triple data encryption. The public-key encryption algorithms provide message authentication and integrity in addition to message confidentiality. The most popular public-key encryption algorithms are the RSA, Diffie-Hellman, digital signature standard (DSS) and the elliptic curve algorithms. In this chapter, a brief background about security threats facing multicast technology is provided.