



This chapter appears in the book, *Web and Information Security*
edited by Elena Ferrari and Bhavani Thuraisingham © 2006, Idea Group Inc.

Chapter XI

A Multimedia-Based Threat Management and Information Security Framework

James B. D. Joshi, University of Pittsburgh, USA

Mei-Ling Shyu, University of Miami, USA

Shu-Ching Chen, Florida International University, USA

Walid Aref, Purdue University, USA

Arif Ghafoor, Purdue University, USA

Abstract

This chapter focuses on the key challenges in the design of multimedia-based scalable techniques for threat management and security of information infrastructures. It brings together several multimedia technologies and presents a conceptual architectural framework for an open, secure distributed multimedia application that is composed of multiple domains employing different security and privacy policies and various data analysis and mining tools for extracting sensitive information. The challenge is to integrate such disparate components to enable large-

scale multimedia applications and provide a mechanism for threat management. The proposed framework provides a holistic solution for large-scale distributed multi-domain multimedia application environments.

Introduction

Security of information infrastructures, both in public or private sectors, is vital to overall national security goals. Such infrastructures provide capabilities for gathering, managing, and sharing vital information among numerous organizations that can form large e-enterprises and generally interoperate in the form of a federation of autonomous domains (Joshi, Ghafoor, Aref, & Spafford, 2001; Thuraisingham, 2003). Information shared among multiple domains can come in various forms including text, audio, video, and images which can increase the complexity of security and privacy management. The key security challenges include integration of diverse security policies of collaborating organizations into a coherent capability for protecting information and using collaborative knowledge for detecting and responding to any emerging threats. In addition, information privacy is generally an overriding concern (Adams & Sasse, 1999). Furthermore, a plethora of data analysis and mining tools have emerged that cyber defenders can use to extract sensitive information from public and private multimedia applications and detect patterns and activities indicating potential threats to an infrastructure. Thus, two key challenges to the design of multimedia-based scalable techniques for threat management and security of information infrastructures are *data mining* and *security*, which we briefly overview in the next section.

Key Issues in Data Mining and Multimedia Security

Multimedia Data Analysis and Mining

Emerging multimedia applications require large-scale integration, mining, and analysis of multimedia data that is generally distributed over multiple security domains. Most of these applications use sensitive information for identifying

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/multimedia-based-threat-management-information/31090

Related Content

Secure Two-Party Association Rule Mining Based on One-Pass FP-Tree

Golam Kaosar and Xun Yi (2011). *International Journal of Information Security and Privacy* (pp. 13-32).

www.irma-international.org/article/secure-two-party-association-rule/55377

Balanced Scheduling Method of Network Information Resources for Cloud Storage

Xiang Ma and Zhan Li (2022). *International Journal of Information Security and Privacy* (pp. 1-17).

www.irma-international.org/article/balanced-scheduling-method-of-network-information-resources-for-cloud-storage/310514

Spatial and Temporal Position Information Delivery to Mobile Terminals Using Audio Watermarking Techniques

Toshio Modegi (2013). *Multimedia Information Hiding Technologies and Methodologies for Controlling Data* (pp. 182-207).

www.irma-international.org/chapter/spatial-temporal-position-information-delivery/70289

ICS Software Protection

Peter H. Jenney (2013). *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection* (pp. 217-239).

www.irma-international.org/chapter/ics-software-protection/73126

Can Community Resilience to Disaster Be Taught?

Bernard Anthony Jones (2021). *International Journal of Risk and Contingency Management* (pp. 58-68).

www.irma-international.org/article/can-community-resilience-to-disaster-be-taught/289398