Chapter 3.18
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 complex threat actions that cannot be detected via real-time monitoring as such actions can take place over relatively long timeframes. Examples of such applications include detecting the spread of an epidemic and monitoring deterioration of the environment. However, today, data no longer appears in the text form only. Instead, the information from different sources may be in the form of text, image, video, audio, or multimedia documents consisting of several multimedia objects that are tightly synchronized both in space and time (Little & Ghafoor, 1990). Unlike mining the relational data, multimedia data mining is a more complex issue due to the sheer volume and heterogeneous characteristics of the data and the spatial and/or temporal relationships that may exist among multimedia data objects.

Mining multimedia data has recently been addressed in the literature (Chen et al., 2003a; Chen et al., 2004; Thuraisingham, 2003). Most of the existing approaches, however, provide limited capabilities in terms of content analysis and generally do not exploit correlations of multiple data modalities originating from diverse sources and/or sensors. Real-time mining and correlating of multi-modality data from distributed sources and using security-oriented spatio-temporal knowledge can assist in identifying potential threats and ensuring security of large-scale infrastructures (e.g., in command and control environments). In a broader perspective, both *long-ranged* and *real-time* data analysis and mining techniques are needed to allow multi-level content analysis and representation of multimedia data at different levels of resolution to facilitate information classification that has security and privacy implications.

Security Policy and Privacy Management

The multi-modality nature of data and the unique synchronization and *quality of service* (QoS) requirements of multimedia information systems