Chapter 3.8
Security of Mobile Devices for Multimedia Applications

Göran Pulkkis
Arcada University of Applied Sciences, Finland

Kaj J. Grahn
Arcada University of Applied Sciences, Finland

Jonny Karlsson
Arcada University of Applied Sciences, Finland

Nhat Dai Tran
Arcada University of Applied Sciences, Finland

INTRODUCTION

Users of the Internet have become increasingly more mobile. At the same time, mobile users want to access Internet wireless services demanding the same quality as over a wire. Emerging new protocols and standards, and the availability of WLANs, cellular data and satellite systems are making the convergence of wired and wireless Internet possible. Lack of standards is however still the biggest obstacle to further development. Mobile devices are generally more resource constrained due to size, power, and memory. The portability making these devices attractive greatly increases the risk of exposing data or allowing network penetration.

Multimedia applications in mobile devices require support for continuous-media data types, high network and memory bandwidth, low power consumption, low weight and small size, and QoS (quality of service). Also security features like authentication and authorization for multimedia content as well as secure connectivity to multimedia sources with possibilities to verify the integrity and guarantee the confidentiality of delivered multimedia content are required (Havinga, 2000). A mobile user must also be able to roam between different networks, also between different types of networks (WLAN, cellular, etc.), and still maintain an ongoing secure multimedia application session.

A standard for a mobile multimedia system architecture has also been proposed (MITA, 2002). Two technologies, MBMS (Multimedia Broadcast/Multimedia Service [see MBMS, 2004]), and DVB-H (digital video broadcasting handheld [see ETSI EN 302 304, 2004]), are being developed for delivery of multimedia content to mobile devices.

To fulfill all security requirements for multimedia applications in a mobile environment, while still maintaining QoS, is a challenging issue. In this chapter, the security requirements and proposed solutions for fulfilling these requirements are discussed. Attention is paid to ongoing related research. However, in order to achieve a secure mobile multimedia environment, also basic mobile device security issues must be seriously taken into account.

BACKGROUND

A mobile computer is a computing device intended to maintain its functionality while moving from one location to another. Different types of mobile computers are:

- Laptops
- Sub-notebooks
- PDAs (personal digital assistants)
- Smartphones

These devices can be divided in two groups: handheld devices and portable PCs. Handheld devices, such as PDAs and smartphones, are pocket-sized computing devices with smaller computing, memory, and display capacity compared to basic desktop computers. Portable PCs such as laptops and sub-notebooks, however, don't significantly differ from the desktops on this area.

Mobile computing and mobility are generic terms for describing the ability to use mobile devices for connecting to and using centrally located applications and/or services over a wireless network. Mobile multimedia can be defined as a set of protocols and standards for exchanging multimedia information over wireless networks. Mobile multimedia user services are usually divided in three categories (MBMS, 2004):

- streaming services like real-time video and audio streams, TV and radio programs, and on-demand video services;
- file download services; and
- carousel services, for example, news delivery with timed updating of text, image, and video objects.

For setup of sessions using multimedia streaming services in IP-based networks is used a signaling protocol, the Session Initiation Protocol (SIP), which is an Internet standard adopted by the Internet Engineering Task Force (IETF). SIP is a text-based client server protocol, in which servers respond to SIP requests sent by clients. SIP entity types are user agents (SIP clients), proxy servers, redirect servers, and registrar servers. Two or more participants can establish a session consisting of multiple media streams. SIP also provides application level mobility, which includes personal, terminal, session, and service mobility. *Personal mobility* means that a user ID provides global accessibility. *Terminal mobility* means that a mobile end-user device can maintain streaming media sessions while moving within and between IP subnets. *Session mobility* means users can change terminals during streaming media sessions and still maintain their sessions. *Service mobility* means that users maintain their streaming media session while moving, changing terminal devices, and changing network service providers (Rosenberg et al., 2002).

SIP does not define any protocol for media transport. However, streaming services typically use the Real-time Transport Protocol (RTP) over UDP. RTP defines a standardized packet format for delivering audio and video over the Internet (Schulzrinne, Casner, Frederick, & Jacobson, 2003).

Related Content

Multimedia Transcoding in Mobile and Wireless Networks: Secure Multimedia Transcoding for Scalable Video Streams
Shiguo Lian (2009). *Multimedia Transcoding in Mobile and Wireless Networks (pp. 258-280).*
www.irma-international.org/chapter/multimedia-transcoding-mobile-wireless-networks/27205

Tertiary Storage Devices
Phillip K.C. Tse (2008). *Multimedia Information Storage and Retrieval: Techniques and Technologies (pp. 145-155).*
www.irma-international.org/chapter/tertiary-storage-devices/27009

Landmark Dataset Development and Recognition
Min Chenand Hao Wu (2021). *International Journal of Multimedia Data Engineering and Management (pp. 38-51).*
www.irma-international.org/article/landmark-dataset-development-and-recognition/301456

Logo Matching and Recognition Based on Context
Tapan Kumar Das (2018). *Feature Dimension Reduction for Content-Based Image Identification (pp. 164-176).*
www.irma-international.org/chapter/logo-matching-and-recognition-based-on-context/207233

Improving Auto-Detection of Phishing Websites using Fresh-Phish Framework
Hossein Shirazi, Kyle Haefnerand Indrakshi Ray (2018). *International Journal of Multimedia Data Engineering and Management (pp. 1-14).*
www.irma-international.org/article/improving-auto-detection-of-phishing-websites-using-fresh-phish-framework/196249