

Chapter XLVIII

Evaluation of Security Architectures for Mobile Broadband Access

Symeon Chatzinotas

University of Surrey, UK

Jonny Karlsson

Arcada University of Applied Sciences, Finland

Göran Pulkkis

Arcada University of Applied Sciences, Finland

Kaj Grahm

Arcada University of Applied Sciences, Finland

ABSTRACT

During the last few years, mobile broadband access has been a popular concept in the context of fourth generation (4G) cellular systems. After the wide acceptance and deployment of the wired broadband connections, such as DSL, the research community in conjunction with the industry have tried to develop and deploy viable mobile architectures for broadband connectivity. The dominant architectures which have already been proposed are Wi-Fi, universal mobile telecommunications system (UMTS), WiMax, and flash-orthogonal frequency division modulation (OFDM). In this chapter, we analyze these protocols with respect to their security mechanisms. First, a detailed description of the authentication, confidentiality, and integrity mechanisms is provided in order to highlight the major security gaps and threats. Subsequently, each threat is evaluated based on three factors: likelihood, impact, and risk. The technologies are then compared taking their security evaluation into account. Flash-OFDM is not included in this comparison since its security specifications have not been released in public. Finally, future trends of mobile broadband access, such as the evolution of WiMax, mobile broadband wireless access (MBWA), and 4G are discussed.

INTRODUCTION

During the last decade, wireless network technologies have greatly evolved and have been able to provide cost-efficient solutions for voice and data services. Their main advantages over wired networks are that they avoid expensive cabling infrastructure and they support user mobility and effective broadcasting. As a result, mobile wireless networks have managed to take over a large percentage of the “voice” market, since the global system for mobile communications (GSM) cellular technology has promoted the worldwide expansion of mobile telephony. Furthermore, nowadays broadband Internet has become a necessity for many home and business users. Moreover, in the context of all-IP network convergence, an increasing share of telephony subscribers is migrating towards VoIP solutions mainly due to the decreased cost compared to fixed telephony. Therefore, the main challenge is to find spectrum- and cost-efficient solutions for the provision of mobile broadband services. In this direction, a large research community of academic and industrial origin has dedicated considerable effort on designing, implementing, and deploying systems for mobile broadband access, such as Wi-Fi, universal mobile telecommunications system (UMTS), WiMax, and flash-orthogonal frequency division modulation (OFDM). According to the predictions, in the years to come, more and more of our voice samples and data packets will be carried over wireless broadband links through the Internet. Therefore it becomes imperative that these messages are secured from malicious eavesdroppers and attackers. Especially in applications such as e-banking, e-commerce, and e-government the revelation of sensitive data to unauthorized persons, unauthorized data submission, and/or the interruption of system availability can cause financial damage, user preferences’ surveillance, industry espionage, and/or administrative overhead.

The purpose of this chapter is to analyze and compare the security architectures of the dominant mobile broadband technologies. More specifically, the objectives are to:

- Describe and analyze the security architectures of mobile broadband technologies.
- Identify the strong and weak points of each technology in terms of access control based on authentication, confidentiality, integrity, and physical layer resilience.
- Compare the investigated security architectures based on a risk evaluation of the identified security vulnerabilities.

MOBILE BROADBAND TECHNOLOGIES

This section discusses the mobile technologies Wi-Fi, UMTS, WiMax, and flash-OFDM. Authentication performance, confidentiality, and integrity mechanisms for each technology are analyzed.

Wi-Fi

Wi-Fi was the first widely-deployed technology for wireless computer networks. It was originally designed to provide portability support in local area networks (LANs). However, Wi-Fi has also been utilized in other scenarios, such as wireless metropolitan area networks (WMANs), since it was the first wireless technology with support for mobile communication and for a wide range of portable and mobile devices.

The Wi-Fi radio interface is based on the IEEE 802.11 standard and is available in three versions:

- **802.11a**
 - **Frequency:** 5.5 GHz,
 - **Modulation:** OFDM
 - **Bandwidth:** 54 Mbps
- **802.11b**
 - **Frequency:** 2.4 GHz
 - **Modulation:** Direct sequence spread spectrum (DSSS)
 - **Bandwidth:** 11 Mbps
- **802.11g**
 - **Frequency:** 2.4 GHz
 - **Modulation:** OFDM
 - **Bandwidth:** 54 Mbps

15 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/evaluation-security-architectures-mobile-broadband/22083

Related Content

Authentication, Authorization, and Accounting (AAA) Framework in Network Mobility (NEMO) Environments

Sangheon Pack, Sungmin Baek, Taekyoung Kwon and Yanghee Choi (2008). *Handbook of Research on Wireless Security* (pp. 395-411).

www.irma-international.org/chapter/authentication-authorization-accounting-aaa-framework/22060

Critical Evaluation of RFID Security Protocols

Azam Zavvari and Ahmed Patel (2012). *International Journal of Information Security and Privacy* (pp. 56-74).

www.irma-international.org/article/critical-evaluation-rfid-security-protocols/72724

An Integrated Security Governance Framework for Effective PCI DSS Implementation

Mathew Nicho, Hussein Fakhry and Charles Haiber (2011). *International Journal of Information Security and Privacy* (pp. 50-67).

www.irma-international.org/article/integrated-security-governance-framework-effective/58982

Blockchain-Based Educational Management and Secure Software-Defined Networking in Smart Communities

Bin Fang (2022). *International Journal of Information Security and Privacy* (pp. 1-20).

www.irma-international.org/article/blockchain-based-educational-management-and-secure-software-defined-networking-in-smart-communities/308314

Large Key Sizes and the Security of Password-Based Cryptography

Kent D. Boklan (2011). *Security and Privacy Assurance in Advancing Technologies: New Developments* (pp. 60-66).

www.irma-international.org/chapter/large-key-sizes-security-password/49495