An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions

Taeshik Shon and Wook Choi

IP Lab, Telecommunication R&D Center, Samsung Electronics
Dong Suwon, P.O. BOX 105, 416, Maetan-3dong, Suswon-si, Gyeonggi-do, 442-600, Korea
{ts.shon,to.choi}@samsung.com

Abstract. The IEEE 802.16 Working Group on Broadband Wireless Access Standards released IEEE 802.16-2004 which is a standardized technology for supporting broadband and wireless communication with fixed and nomadic Access. The standard has a security sublayer in the MAC layer called, Privacy Key Management, which aims to provide authentication and confidentiality. However, several researches have been published to address the security vulnerabilities of 802.16-2004. After the IEEE 802.16-2004 standard, a new advanced and revised standard was released as the IEEE 802.16e-2005 amendment which is foundation of Mobile WiMAX network supporting handoffs and roaming capabilities. In the area of security aspects, Mobile WiMAX adopts improved security architecture, PKMv2, including Extensible Authentication Protocol (EAP) authentication, AES-CCM-based authenticated encryption, and CMAC or HMAC based message protection. However, there is no guarantee that PKMv2-based Mobile WiMAX network will not have security flaws. In this paper, we first describe an overview of security architecture of IEEE 802.16e-based Mobile WiMAX and its vulnerabilities. Based on the related background research, we focus on finding new security vulnerabilities such as a disclosure of security context in initial entry and a lack of secure communication in network domain. We propose possible solutions to prevent these security vulnerabilities.

1 Introduction

More and more, our life is closely related to a variety of networking environments for using Internet-based services and applications. The ever-changing trends of our lifestyle require faster speed, lower cost, and more broadband capacity as well as nomadic and mobility support. Due to these reasons and demands, the Institute of Electrical and Electronics Engineers (IEEE) 802.16 working group on broadband wireless metropolitan area networks has created new standards with mobility Access called the IEEE 802.16e-2005 amendment. It has also been developed by many working groups of the Worldwide Interoperability for Microwave Access (WiMAX) Forum, similar to Wi-Fi in IEEE 802.11 standards. The WiMAX Forum tries to coordinate the interoperability and compatibility of various company products as a field standard. Mobile WiMAX means system profiles and network architectures from WiMAX Forum based on IEEE 802.16e-2005 standards. Specifically, Mobile WiMAX technology is

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 88–97, 2007.

considered as one of the best next-generation wireless technologies because it can support high-speed, broadband data transmission, fully-supported mobility, and wide coverage and high capacity. Of these, Mobile WiMAX has many advantages and unique characteristics such as superior performance (multiple handoff mechanisms, power-saving mechanisms, advanced Quality of Service and low latency, advanced Authentication, Authorization, Accounting functionality), flexibility (global roaming, deployment from the edge infrastructure to overlay/complement networks, various spectrum usage), advanced IP-based architecture (fully support Internet Multimedia Subsystem, 3GPP2, and Multichannel Multipoint Distribution), attractive economics (open standards, mass adoption of subscriber units, attractive Intellectual property rights structure) [1-4]. From a security viewpoint, the Mobile WiMAX system based on the IEEE 802.16e-2005 amendment has more enhanced security features than the existing IEEE 802.16-based WiMAX network system. The improved core part of the security architecture in Mobile WiMAX, called Privacy Key Management version 2 (PKMv2), is operated as a security sublayer in a Medium Access Control (MAC) layer like PKMv1 in IEEE 802.16-2004. The PKMv2 in a security sublayer provides a message authentication scheme using HMAC/CMAC (Hash-based Message Authentication Code/Cipher-based Message Authentication Code), device/user authentication using Extensible Authentication Protocol (EAP) methods, and confidentiality using AES-CCM (Advanced Encryption Standard – Counter with CBC Mode) encryption algorithm. Moreover, user credentials exist including: Username/Password, SIM/USIM (Subscriber Identity Module/Universal SIM) Cards, Smart Cards, Universal Integrated Circuit Card (UICC), Removable User Identity Module (RUIM), and Digital Certificate [3-4]. Even though Mobile WiMAX uses more enhanced security schemes supported by PKMv2, it can not guarantee the reliability of the whole Mobile WiMAX systems and network architectures. In addition, open architecture and various applications of Mobile WiMAX could cause much more risks to try to compromise Mobile WiMAX network than existing systems.

Among many potential risks in Mobile WiMAX network, this paper focuses on two security vulnerabilities according to security requirements of each Mobile WiMAX network domain. Mobile WiMAX network has a link range domain(access network) and network domain. Therefore, in order to deal with the security vulnerabilities from the various network domains, we propose enhanced security approaches applying well-known cryptographic methods such as Diffie-Hellman (DH) key agreement [5] and Public Key Infrastructure (PKI).

The rest of this paper is organized as follows. In section 2, we study an overview of Mobile WiMAX security and analyze known security vulnerabilities and attacks. In section 3, new security threats in Mobile WiMAX network are examined. In section 4, we propose possible solutions in order to cope with the new threats we mention in section 3. In section 5, we describe a reliable Mobile WiMAX architecture including our proposed solutions. In the last section, we conclude with a summary and discussion of future work.

2 Background: Known Vulnerabilities and Attacks

The security architecture of Mobile WiMAX is partially originated from wireless networks based on IEEE 802.11. In the case of IEEE 802.11-based wireless networks,