Chapter XLVII
End-to-End (E2E) Security Approach in WiMAX:
A Security Technical Overview for Corporate Multimedia Applications

Sasan Adibi
University of Waterloo, Canada

Gordon B. Agnew
University of Waterloo, Canada

Tom Tofigh
WiMAX Forum, USA

ABSTRACT

An overview of the technical and business aspects is given for the corporate deployment of services over worldwide interoperability for microwave access (WiMAX). WiMAX is considered to be a strong candidate for the next generation of broadband wireless access; therefore its security is critical. This chapter provides an overview of the inherent and complementary benefits of broadband deployment over a long haul wireless pipe, such as WiMAX. In addition, we explore end-to-end (E2E) security structures necessary to launch secure business and consumer class services. The main focus of this chapter is to look for a best security practice to achieve E2E security in both vertical and horizontal markets. The E2E security practices will ensure complete coverage of the entire link from the client (user) to the server. This is also applicable to wireless virtual private network (VPN) applications where the tunneling mechanism between the client and the server ensures complete privacy and security for all users. The same idea for E2E security is applied to client-server-based multimedia applications, such as in Internet protocol (IP) multimedia subsystem (IMS) and voice over IP (VoIP) where secure client/server communication is required. In general, we believe that WiMAX provides the opportunity for a new class of high data rate symmetric services. Such services will require E2E security schemes to ensure risk-free high data-rate uploads and downloads of multimedia applications. WiMAX provides the capability for embedded security functions through the 802.16 security architecture standards. IEEE 802.16 is further subcategorized as

802.16d (fixed-WiMAX) and 802.16e (mobile-WiMAX). Due to the mobility and roaming capabilities in 802.16e and the fact that the medium of signal transmission is accessible to everyone, there are a few extra security considerations applied to 802.16e. These extra features include: privacy key management version 2 (PKMv2), PKM-extensible authentication protocol (EAP) authentication method, advanced encryption standard (AES) encryption wrapping, and so forth. The common security features of 802.16d and 802.16e are discussed in this chapter, as well as the highlights of the security comparisons between other broadband access, third-generation (3G) technologies, and WiMAX.

INTRODUCTION

The E2E security structure is transparent from the user's point of view and requires dedicated overhead and processing power. In the case of Wi-Fi, the overhead is a relatively large percentage of the total bandwidth, which makes Wi-Fi infeasible for most E2E security structures. However, in worldwide interoperability for microwave access (WiMAX), the security overhead is nominal and may not be an issue.

Today's enterprise customers are forced to use dedicated physical circuits such as leased lines to realize business class E2E security. With inherent WiMAX security features, a secured virtual private network (VPN) can easily be achieved over public networks. Instead of such dedicated leased line circuits, WiMAX users could enjoy VPN connectivity with up to 10 Mbps bandwidth to access the public backbones.

Personal broadband access technologies have undergone many challenges, one of which was digital subscriber line (DSL). DSL is a high-speed connection that utilizes the same wiring system as a regular telephone line uses. The advantages of DSL include: voice/data on the same line and higher data rates than regular modems. There are, however, a few downsides to DSL, including distance dependence (between users and the service provider) of data rate, unbalance rates for uploading and downloading of data, and having no complete physical area coverage.

All of the downsides of DSL technology appear in other personal broadband products. This is due to the physical limitations of wired technologies. WiMAX, on the other hand, is a wireless technology with very high bandwidth for voice/data applications, which does not appear to have any of the downsides of the wired technologies. WiMAX also has advantages over Wi-Fi technology in terms of longer range and larger bandwidth. This allows WiMAX to support a variety of broadband services.

Wi-Fi technology was not suited for personal broadband services due to a number of limitations, especially security. WiMAX, on the other hand, enjoys an all-IP open platform infrastructure with the benefit of its inherent security functions and features. This allows for faster and inexpensive provisioning of E2E secured services based on open standards. In addition WiMAX can be configured for self-installed services of multimedia VPN with enhanced end-to-end user control signalling.

The security aspect of WiMAX is an important issue: this includes state-of-the-art security mechanisms, such as very strong authentication with per station keys and higher-level security mechanisms. WiMAX's security strength is normally found in add-on products, such as in wired VPNs and virtual local area networks (VLANs), which are usually built into each of the WiMAX's base stations (BSs).

This chapter will present the characteristics of WiMAX security and how it fits into both consumer and business class structures. We believe that strong E2E security can be achieved with WiMAX without compromising performance.