A Survey of WiMAX and Mobile Broadband Security

Emily Yang, emy1@cec.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract

This paper covers the security mechanisms and issues in WiMAX, as well as universal threats to wireless networks. It also examines similar wireless and mobile broadband technologies, WLAN, MBWA, and 3G and the security measures that are taken. Awareness is raised of the current as well as future security implications of an increasingly wireless world.

Table of Contents

1.0 Introduction

Consider a scenario in which a person wakes up and walks around with her laptop connected to a local area network in her house as she gets ready, checking email, and using it to read the news as she eats breakfast. On the bus on her way to work, she pulls out her iPhone to browse the internet, check the scores of her favorite sports teams, watch some funny YouTube videos, and call a friend. She then stops at Starbucks, connects to the Wi-Fi, and answers some email while sipping some coffee. Once at work, she pulls out her laptop to connect to the WLAN at the office and starts work.

The fact that this scenario sounds fairly normal and typical is interesting, not only because of how technology and internet-centered our lives have become, but because every network connection that this person used was wireless. Most people use multiple types of wireless internet every day without even realizing it. It's fast and convenient, but how do we know that the data we send and receive is secure? As it turns out, there are many

mechanisms in place to provide security, but there are also many weaknesses and threats, especially since wireless and mobile broadband service is a fairly new and still developing technology. The IEEE 802.16 standard and its implementation, WiMAX, provide an interesting case of the evolving nature of mobile broadband use and security as well as problems that are continuously being found.

In this paper we discuss the inherent and fairly universal weaknesses and security threats of wireless networks, take a thorough look at WiMAX's security mechanisms and issues, and then examine some similar wireless and mobile broadband technologies and their security. Through discussion of common security problems as well as in-depth study of real world examples, like WiMAX, we can come to a better understanding of the threats we face now and the implications for the future of mobile broadband security.

2.0 Background on Wireless Security

There are several security concerns and development implications that arise from the varying nature of mobile communication and the fast-paced increase in usage of mobile devices for m-commerce, email, and other functionality that require secure connections. Mobile security poses an interesting problem, largely because it requires an enormous amount of compatibility over different access media, as well as a wide range of end user devices, with different capacities and capabilities. Users expect to be able to use their mobile devices spontaneously in many different environments, and sometimes continuously while going through multiple types of access points, for example, in a moving car. Despite the frequent need for even more security than is provided to their counterparts that are within a fixed network, mobile devices have much less processing ability and also need to comply with reasonable cost, size and weight restrictions as well as usability requirements. To make matters even more complicated, mobile devices are also often lost or stolen, which calls for even higher protection of sensitive information. Through more detailed discussion of the security challenges it becomes clear that there are many hurdles that engineers must consider when designing mobile communication architectures. [Raghunathan03]

Figure 1: Major Mobile Security Concerns

2.1 Mobile Security Concerns

Several issues have been identified that must be taken into account when evaluating the security of mobile communication. Some of the most important and universal ones are discussed below (also seen above in Figure 1).

2.1.1 Authorization Techniques

Especially because the devices are mobile, there is a large risk that they might fall into the wrong hands. Here, a usability issue arises where people expect to be able to conveniently and frequently use their devices, which often rules out the idea of a login procedure. Also, there are a variety of data types flowing to and from the devices, both public and private, that need different types of authentication, such as encryption, Message Authentication Codes (MAC), or digital signatures. It may even be the case that different network levels require different authentication. [Jurjens08]

2.1.2 Storage of Sensitive Information

There is an increasing amount of sensitive information that can be stored on mobile devices, from passwords, to credit card information, to certificates that must be secure. The performance and physical capabilities of the device can make it hard or impossible to sufficiently encrypt data. [Jurjens08]

2.1.3 Application Environment

Like any computer, mobile devices must be able to defend against software attacks such as viruses, but unlike