Chapter XLI
Evaluating Security Mechanisms in Different Protocol Layers for Bluetooth Connections

Georgios Kambourakis
University of the Aegean, Greece

Angelos Rouskas
University of the Aegean, Greece

Stefanos Gritzalis
University of the Aegean, Greece

ABSTRACT

Security is always an important factor in wireless connections. As with all other existing radio technologies, the Bluetooth standard is often cited to suffer from various vulnerabilities and security inefficiencies while attempting to optimize the trade-off between performance and complementary services including security. On the other hand, security protocols like IP secure (IPsec) and secure shell (SSH) provide strong, flexible, low cost, and easy to implement solutions for exchanging data over insecure communication links. However, the employment of such robust security mechanisms in wireless realms enjoins additional research efforts due to several limitations of the radio-based connections, for example, link bandwidth and unreliability. This chapter will evaluate several Bluetooth personal area network (PAN) parameters, including absolute transfer times, link capacity, throughput, and goodput. Experiments shall employ both Bluetooth native security mechanisms, as well as the two aforementioned protocols. Through a plethora of scenarios utilizing both laptops and palmtops, we offer a comprehensive in-depth comparative analysis of each of the aforementioned security mechanisms when deployed over Bluetooth communication links.

INTRODUCTION

Without doubt, the Bluetooth specification (IEEE 802.15) (Bluetooth SIG, 2003; IEEE, 2002) is gradually becoming the de-facto standard for replacing short range wired communications using radio technology. According to estimations, devices incorporating Bluetooth are predicted to

quadruple in number between now and 2008, from under 100 million to about 440 million. Bluetooth enabled devices are used in several different environments and cover a wide range of applications. For instance, for mobile applications, the device periodically connects to the network to download music, to transfer files, or to synchronize with one's desktop on calendar and other files. Consequently, the safety and security of these applications, for instance, the security of the private information stored on the devices, becomes a major issue. By attacking actively or passively the communication link, aggressors could obtain personal and also important business data. However, security features (Gehrmann, Persson, & Smeets, 2004) must be carefully considered and analyzed in order to decide whether Bluetooth technology indeed provides the right answer for any particular task or application.

The Bluetooth standard has been long criticized for various vulnerabilities and security inefficiencies, as its designers are trying to balance between performance and complementary services including security. So far, both the Bluetooth Special Interest Group (SIG) (Bluetooth SIG, 2003) and several researchers have made significant contributions on Bluetooth security aspects, discovering numerous vulnerabilities and potential weaknesses and proposing solutions (Adam, 2003; Gehrmann, & Nyberg, 2002; Jacobson & Wetzel, 2001; Persson & Manivannan, 2003; Shaked & Wool, 2005). For example, the Bluetooth pairing procedure has been anticipated to be weak under certain circumstances. Moreover, other categories of threats, either active or passive, have also been investigated, including ad hoc security issues, malicious software like "Cabir," war-nibbling, and so forth.

An obvious choice for any Bluetooth application would be to use Bluetooth encryption provided at link layer. Virtually all Bluetooth devices support this feature, and it is, in most cases, considered to be adequately secure. However, this may not be applicable for all deployment scenarios. In order to establish a secure channel with another Bluetooth device, a preshared secret called PIN is required. A symmetric key is generated from this PIN. On customer devices this PIN typically consists of four or five digits. Supposing a whole piconet network would utilize this PIN to encrypt its communication, anyone acquiring this PIN could theoretically decrypt all communication. On top of that, in applications like VoIP that mandate IP connectivity to access points (APs), the encryption would end at the AP, which means that the AP, or any host that can manipulate the communication between the Mobile Device and the other end, can expose the data (see Figure 1). Thus, it is obvious that Bluetooth encryption is not well suited for all applications which may exploit Bluetooth connections.

Under these circumstances and for certain classes of security sensitive applications deployed in Bluetooth PAN networks, the investigation of complementary and advanced security protocols apart from Bluetooth's native security mechanisms, even if deployed as an interim countermeasure, is an interesting research issue. On the other hand, as Bluetooth wireless technology is targeting devices with particular needs and constraints (e.g., processing power and battery consumption) the trade-offs between security services and performance must be carefully considered. Furthermore, considering that radio links in general suffer from limited bandwidth and are unreliable by nature, performance issues must be thoroughly investigated to make a decision whether certain security protocols and their mechanisms are advantageous over Bluetooth connections, delivering robust and agile security services within tolerable service response times.

Figure 1. Sample scenario that mandates upper layer security