SECURITY COMPARISON: BLUETOOTH COMMUNICATIONS vs WI-FI

Mahendra Maheta

Abstract

Bluetooth and WiFi wireless technology came into focus in few years would be an understatement. It was a time of tremendous progress – a time of refining, improving and making strides towards perfecting Bluetooth and WiFi wireless technology. In this paper we will check that how Bluetooth and WiFi technology came into focus for users worldwide. With over four million products shipping every week, member companies saw a significant increase in both brand recognition and product demand. Even more importantly, increased consumer understanding of Bluetooth capabilities has resulted in a growing demand for applications that best fit lifestyles and needs. Members focused strongly on developing and marketing their Bluetooth enabled products.

Keywords : Bluetooth, WI-Fi, 802.11, Network Security

1. Introduction

Several attacks on IEEE 802.11b have been described in the media. It has been shown that the WEP security framework used in IEEE 802.11 is susceptible to both attacks on library data content and library user authentication. These exposures allow an attacker to both inappropriately intercept data and also gain access to a library network by impersonating a valid user.

Bluetooth and IEEE 802.11b are different, complementary technologies. IEEE 802.11b is largely applied to LAN access, while Bluetooth LAN access is only one of many applications, most of which focus on smaller personal area networks (PANs). Different target applications and technology dictate different security architectures. With the differences between Bluetooth technology and IEEE 802.11b in mind, one may question the validity of comparing the security architectures of the two technologies. We feel, however, that such a comparison is valid. Indeed, from a user perspective the two technologies are really quite similar. Both are methods which allow computers to communicate to other devices, both using wireless technology; both operate in the 2.4 GHz spread spectrum band, etc. Due to these similarities, the public sometimes confuses Bluetooth communications with IEEE 802.11b. In addition, 802.11b security concerns have been unjustifiably applied to Bluetooth communications. However, these attacks do not apply to Bluetooth technology.

In this paper we discuss the two main attacks on 802.11b that have been described in the literature. We also explain why these attacks are not effective with Bluetooth wireless communications.

2. 802.11b Eavesdropping

When a user sends data over a wireless network, he has a reasonable expectation that such data is not easily readable by unauthorized persons. Unlike a wired network, which requires a physical intrusion, wireless data packets can be received by anyone nearby with an appropriate receiver, potentially outside of the physical security barriers of an organization. This allows, so called parking lot attacks, in which an attacker sits in a car in the parking lot of the intended victim. Accordingly, both Bluetooth and 802.11 technologies utilize data encryption in lower network layers.

The 802.11b specification utilizes a security framework called wireless equivalent privacy (WEP) protocol. A key component of WEP is the use of the stream cipher RC4. RC4 is a well-known and commonly used stream cipher, but its use in 802.11b is questionable owing to the nature of a wireless packet network.

3. 802.11b False Authentication

To gain access to a network, a user must be authenticated. While authentication is typically done at a higher network level, 802.11b and Bluetooth technologies also support device authentication. In 802.11b authentication is performed by a challenge response procedure using a shared secret. After requesting authentication, the authenticator sends the initiator a 128-octet random number challenge. The initiator encrypts the challenge using the shared secret and transmits it back to the authenticator. Encryption is performed the challenge with a pseudo-random string formed by the shared secret and a public IV. Note that the only thing that changes from authentication to authentication with a specific user is the plaintext message.

4. Device Authentication in Bluetooth Technology

Like 802.11b, Bluetooth technology provides a method for authenticating devices. Device authentication is provided using a shared secret between the two devices. The common shared secret is called a link key. This link key is established in a special communications session called pairing. All paired devices (devices that have had a previous connection to establish security procedures) share a common link key. There are two types of link keys defined in the: unit keys and combination keys.

A device using a unit key uses the same secret for all of its connections. Unit keys are appropriate for devices with limited memory or a limited user interface. During the pairing procedure the unit key is transferred (encrypted) to the other unit. Note that only one of the two paired units is allowed to use a unit key. Combination keys are link keys that are unique to a particular pair of devices. The combination key is only used to protect the communication between these two devices. Clearly a device that uses a unit key is not as secure as a device that uses a combination key. Since the unit key is common to all devices with which the device has been paired, all such devices have knowledge of the unit key.

5. Data Eavesdropping, 802.11

The Bluetooth standard does not use RC4 but rather the stream cipher E0, which is specifically designed to run over a Bluetooth wireless packet network. A unique encryption key is generated for each session, from which per-packet keys are derived, in a manner that avoids the problem in 802.11b caused by frequent reuse of per-packet keys.

Direct attacks on the E0 cipher are known but are of significant complexity. Like RC4, E0 required a ciphering key. The ciphering key is computed as a hash of a random number, the link key and a byproduct of the authentication procedure the Authentication Ciphering Offset (ACO). While the link key is also used to generate a ciphering key used for data encryption, it is not used for data encryption itself. This is a significant advantage over 802.11b in which the same key is used for authentication and encryption.

In summary the known attacks on the E0 cipher used in Bluetooth are far more computationally complex then corresponding attacks on RC4 used in 802.11b. As yet, no practical direct attack has been reported. Also, unlike 802.11b, different keys are used for authentication and encryption. Accordingly practical studies on Bluetooth security have been focused on methods to guess or steal the key (or at least a portion of it). The most logical time to attempt this is during the pairing procedure.

6. Bluetooth Pairing

As discussed in Section 4.0 pairing is the procedure where a relationship (link key) is established between two previously unknown devices. The link key is derived when the devices are initially paired (i.e. the link key does not exist before the pairing procedure). Pairing is facilitated with yet another key, the initialization key. This key is computed by a pair of devices using the Bluetooth addresses of each device, a random number, and a shared secret (PIN). Since it is only used in the initial pairing, the initialization key is only used once.

The initial pairing is the most profitable area of attack on a Bluetooth device. If the attacker can guess or steal the PIN during the initial pairing, then he can perform a much more efficient search to derive the link key. This search is further simplified if the communications occurring while the devices are paired is recorded. For this reason the Bluetooth SIG strongly encourages the use of long, random PINs and suggests that pairing be performed only in a private place. Assuming that both devices have a man-machine interface (such as a keypad) it is also suggested that the PIN be manually entered into both devices and in any case communicated out-of-band (not transmitted over the Bluetooth wireless link). Thus, long PINs provide improved security since the PIN cannot be received over-the-air. To steal the PIN an attacker must guess or record it by some other means such as direct observation of the user, a more difficult procedure if the PIN is long and the pairing is performed in private.

7. Conclusion

The known attacks on 802.11b security have been discussed and found not to apply to Bluetooth wireless technology. In particular

a) 802.11b authentication is highly susceptible to impersonation by recording only one authentication procedure. This is facilitated because a plaintext/ciphertext pair is transmitted. Bluetooth communications do not share this limitation.

b) 802.11b encryption is not very secure. The RC4 implementation used in 802.11b has several well-known direct attacks. Currently known direct attacks on the Bluetooth encryption are computationally complex and of little practical value.

From the preceding discussion it is clear that the weakest link in the Bluetooth security architecture is the initial pairing especially if a weak PIN is used. Accordingly the Bluetooth SIG strongly encourages pairing in a private place and the use of robust PINs. In addition, simple devices that use unit keys should not be relied upon to communicate highly secure data.

As a communication standard, Bluetooth security focuses on the link level. It provides both entity authentication and link privacy. Since these functions are focused at the lower network layers, message authentication and secure end-to end links are not provided. However, many applications, such as e-mail and browser transactions require end-to-end security. As with other communication standards, this function is expected to be provided at higher network layers by specific application providers. Accordingly, the Bluetooth SIG encourages the reuse of existing transport, session and application layer security. Regarding the security limitations that have been reported for 802.11b; the WLAN community is currently examining these issues. We expect them to be resolved with subsequent revisions of the standard. In addition several 802.11b vendors have added proprietary authentication and encryption procedures at higher network layers.

References

1. W. A. Arbaugh, “Wireless Research”, available from, http://www.cs.umd.edu/~waa/wireless.html last visited on October 10, 2007.
2. J. Walker, “Unsafe at any key size; An analysis of the WEP encapsulation”, available from http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0- 362.zip, last visited on October 16, 2007.

3. N. Borisov, I. Goldberg, and D. Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11.” available from http://www.issac.sc.berkley.edu/issac/wep-faq.html., last visited on October 14, 2007.
4. S. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, in the Workshop Record of SAC 2001
5. W. Arbaugh, N. Shankar, Y.C.J. Wan, “Your 802.11 Wireless Network has No Clothes” available from http://www.cs.umd.edu/~waa/wireless.pdf, last visited on October 13, 2007.
6. M. Jakobsson and S. Wetzel, “Security Weaknesses in Bluetooth” available from http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/bluetooth.pdf, last visited on October 14, 2007.
7. S. Fluhrer and S. Lucks, “Analysis of the E0 Encryption System” available from S. Lucks’ web site at http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz , a gnu-zipped Postscript file.
8. Bluetooth SIG, Specification of the Bluetooth system, Profiles”,, Version 1.1, 1 February 22, 2001, available at http://www.bluetooth.com/. Last visited on October 10, 2007.
9. Bluetooth SIG, Specification of the Bluetooth system, Core “, Version 1.1, 1 February 22, 2001, available at http://www.bluetooth.com/. Last visited on October 13, 2007.
10. B. Miller, “IEEE 802.11 and Bluetooth wireless technology” available from http://www-106.ibm.com/developerworks/wireless/library/wi-phone. Last visited on October 13 2007.

ABOUT AUTHOR

Mr. Mahendra Maheta is working as a Chief Librarian at Vivekananda institute of Hotel and Tourism Management, Rajkot - 360005 (Gujarat).
E-mail: librarian007@rediffmail.com