Overview of IEEE 802.11b Security

Sultan Weatherspoon, Network Communications Group, Intel Corporation

Index words: 802.11b, wireless, WLAN, encryption, security

ABSTRACT

There is much regulatory and standards work in the area of security, especially in wireless. The wireless LAN standard IEEE 802.11b provides a mechanism for authentication and encryption. This paper describes the 802.11b security protocols and the implications they have for user privacy, ease of use, and import/export issues.

INTRODUCTION

Because wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted. Encryption and authentication are always considered when developing a wireless networking system. The goal of adding these security features is to make wireless traffic as secure as wired traffic. The IEEE 802.11b standard provides a mechanism to do this by encrypting the traffic and authenticating nodes via the Wired Equivalent Privacy (WEP) protocol.

Whenever encryption and authentication are implemented in any system, three things must be considered:

1. *The customers need for privacy*. How strong do the protocols need to be and how much should they cost (MIPS, dollars, and time).
2. *Ease of use*. If the security implementation is too difficult to use, then it will not be used.
3. *Government regulations*. Encryption is viewed as munitions by many governments, including the US, so all encryption products are export controlled.

The WEP protocol used in 802.11b balances all the above-mentioned considerations.

WIRED VS. WIRELESS IMPLICATIONS

The main security issue with wireless networks, especially radio networks, is that wireless networks intentionally radiate data over an area that may exceed the limits of the area the organization physically controls. For instance, 802.11b radio waves at 2.4GHz easily penetrate building walls and are receivable from the facility's parking lot and possibly a few blocks away. Someone can passively retrieve all of a company's sensitive information by using the same wireless Network Interface Card (NIC) from a distance without being noticed by network security personnel.

This problem also exists with wired LAN networks, but to a lesser degree. Current flow through the wires emits electromagnetic waves that someone could receive by using sensitive listening equipment. However, a person would have to be much closer to the cable to receive the signal.

Most LAN adapters, wired and wireless, on the market today offer a "promiscuous mode" that, with off-the-shelf software, enables them to capture every packet on their segment of the LAN.

Many of the security issues facing wireless LANs are also issues facing wired LANs. Data transmitted on the wired LAN are incorrectly assumed to be protected because one needs to be physically in the building to access the network. This is largely untrue with corporate access to the Internet. Often, if users from inside can get out to the Internet, then hackers from outside can get into a network if proper precautions are not taken. There is also remote access for corporate travelers and telecommuters.

These examples illustrate that both wireless and wired networks are subject to the same security risks and have the same issues. These include the following:

- Threats to physical security of a network (e.g., denial of service and sabotage).
- Unauthorized access and eavesdropping.
- Attacks from within the network's (authorized) user community, (e.g., disgruntled, current, and ex-employees have been known to read, distribute, and alter valuable company data).

In addition, measures taken to ensure the integrity and security of data in the wired LAN environment are also applicable to the wireless LAN's as well. Wireless

LAN's, such as 802.11b, include an additional set of security elements, namely WEP, which are not available in the wired world. Therefore, some people are of the opinion that a properly implemented protected wireless LAN is more protected than a wired LAN.

802.11 WEP Protocol

The WEP algorithm was selected to meet the following criteria:

- *Reasonably strong*. It must meet customers' needs.
- *Self-synchronizing*. Stations quite frequently go in and out of coverage.
- *Computationally efficient*. The WEP algorithm may be implemented in hardware or software. If it is efficient, it allows low-MIPS devices to still implement it in software.
- *Exportable*. It can be exported outside the US and imported to other countries.
- *Optional*. It is an option not required in an 802.11-compliant system.

The same key is used to encrypt and decrypt the data. The WEP encryption algorithm (see Figure 1) works as follows:

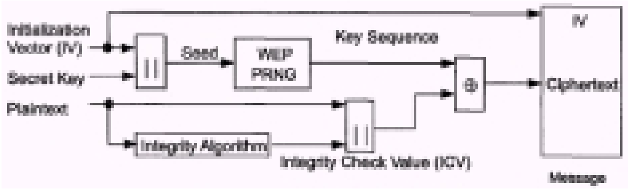

Figure 1: WEP encryption

Two processes are applied to the plaintext data. One encrypts the plaintext; the other protects against unauthorized data modification.

The secret key (40-bits) is concatenated with an initialization vector ("IV", 24-bits) resulting in a 64-bit total key size. The resulting key is input into the pseudorandom number generator (PRNG). The PRNG (RC4) outputs a pseudorandom key sequence based on the input key. The resulting sequence is used to encrypt the data by doing a bitwise XOR. This results in encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus 4 bytes. This is because the key sequence is used to protect the integrity check value (ICV, 32-bits) as well as the data.

To protect against unauthorized data modification, an integrity algorithm (CRC-32) operates on the plaintext to produce the ICV. The ciphertext is accomplished by doing the following. See Figure 3 for an example.

1. Compute the ICV using CRC-32 over the message plaintext.
2. Concatenate the ICV to the plaintext.
3. Choose a random initialization vector (IV) and concatenate this to the secret key.
4. Input the secret key+IV into the RC4 algorithm to produce a pseudorandom key sequence.
5. Encrypt the plaintext+ICV by doing a bitwise XOR with the pseudorandom key sequence under RC4 to produce the ciphertext.
6. Communicate the IV to the peer by placing it in front of the ciphertext.

The IV, plaintext, and ICV triplet forms the actual data sent in the data frame.

In decryption, the IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message (see Figure 2). Combining the ciphertext with the proper key sequence yields the original plaintext and ICV. The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received message is in error, and an error indication is sent to the MAC management and back to the sending station. Mobile units with erroneous messages (due to inability to decrypt) are not authenticated.

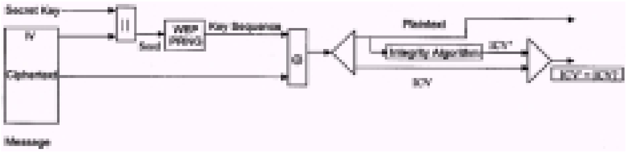

Figure 2: WEP decryption

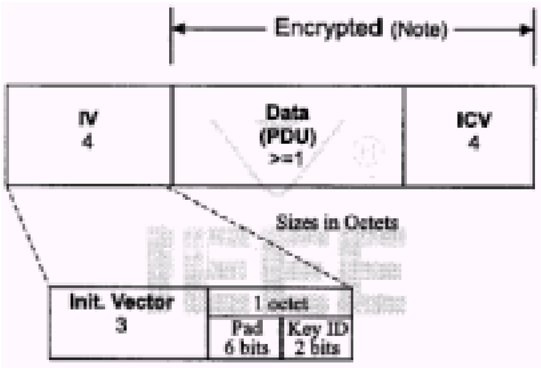

Figure 3: WEP data frames

The same shared key used to encrypt/decrypt the data frames is also used to authenticate the station. It is considered a security risk to have the encryption and authentication keys be the same. There is also a method where stations and AP's can utilize WEP alone without shared key authentication, essentially using WEP as an encryption engine only. This is done in open system mode. This is considered to be the most protected implementation in 802.11 thus far, and it still enables reasonable authentication.

There are two types of 802.11 authentication:

- *Open system authentication*. This is the default authentication service that doesn't have authentication.
- *Shared key authentication*. This involves a shared secret key to authenticate the station to the AP.

The open system authentication is "null" authentication. The station can associate with any access point and listen to all data that are sent plaintext. This is usually implemented where ease-of-use is the main issue, and the network administrator does not want to deal with security at all.

The shared key authentication approach provides a better degree of authentication than the open system approach. For a station to utilize shared-key authentication, it must implement WEP. Figure 4 illustrates the operation of shared-key authentication. The secret shared key resides in each station's MIB in a write-only form and is therefore only available to the MAC coordinator. The 802.11 standard does not specify how to distribute the keys to each station, however.

The process is as follows:

1. A requesting station sends an Authentication frame to the access point ("AP").
2. When the AP receives an initial Authentication frame, the AP will reply with an Authentication frame containing 128 bytes of random challenge text generated by the WEP engine in standard form.
3. The requesting station will then copy the challenge text into an Authentication frame, encrypt it with a shared key, and then send the frame to the responding station.
4. The receiving AP will decrypt the value of the challenge text using the same shared key and compare it to the challenge text sent earlier. If a match occurs, the responding station will reply with an authentication indicating a successful authentication. If not, the responding AP will send a negative authentication.

The WEP PRNG (RC4) is the critical component of the WEP process, since it is the actual encryption engine. The IV extends the useful lifetime of the secret key and provides the self-synchronous property of the algorithm. The secret key remains constant while the IV changes periodically. Each new IV results in a new key sequence, thus there is a one-to-one correspondence between the IV and the output. The IV may change as frequently as every message, and since it travels with the message, the receiver will always be able to decrypt any message. Therefore the data of higher layer protocols (e.g., IP) are usually highly predictable. An eavesdropper can readily determine portions of the key sequence generated by the (Key, IV) pair. If the same pair is used for successive messages, this effect may reduce the degree of privacy. Changing the IV after each message is an easy way to preserve the effectiveness of WEP.

RC4 was developed in 1987 by Ron Rivest for RSA Data security. RC4 is a stream cipher that takes a fixed length key and produces a series of pseudorandom bits that are XOR'ed with the plaintext to produce ciphertext and vice versa. RC4 is used in the popular SSL Internet protocol and many other cryptography products. The benefits of using RC4 are as follows:

- The keystream is independent of the plaintext.
- Encryption and decryption are fast, about 10 times faster than DES.
- RC4 is simple enough that most programmers can quickly code it in software.
- RSADSI claims that RC4 is immune to differential and linear cryptoanalysis.

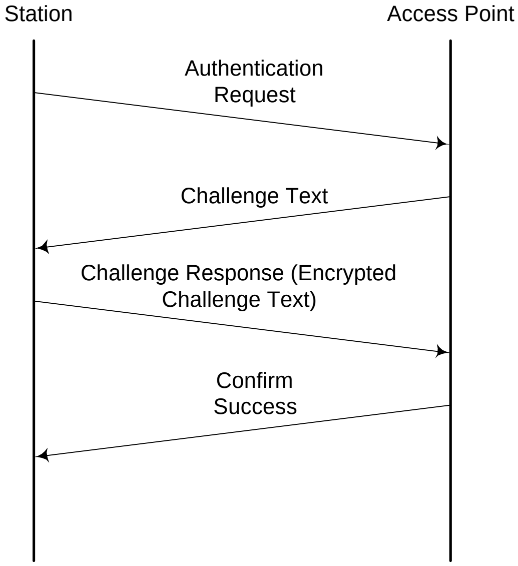

Figure 4: Shared-key authentication

SECURITY IMPLEMENTATION FOR BLUETOOTH[*]

Intel is a key contributor and supporter of the Bluetooth standard. This is a brief description of the implementation of its security system.

Bluetooth Security Implementation

Bluetooth technology provides three modes of security:

- *Security mode 1 (non-secure).* A device does not initiate any security procedure such as encryption or authentication.
- *Security mode 2 (service-level enforcement security).* A device does not initiate security procedures before channel establishment at the L2CAP (service) level. This mode allows different and flexible access policies for applications, and is used especially for running applications with different security requirements in parallel.
- *Security mode 3 (link-level enforced security).* A device allows only authenticated connections.

Bluetooth technology has three security attributes: authorization, authentication, and encryption.

Since there are many services that a Bluetooth device might have, there is a database of which services a device has authorization to use. The user can choose to “auto” trust devices or “manually” trust devices.

Since the identity of the remote device is used as a condition for authorization, authentication is performed. Authentication is accomplished using a challenge-response scheme using symmetric link keys. If the devices do not share a link key, one is created through a process called “pairing” and it is based on a shared secret association, such as a PIN code. If a device does not have a mechanism to enter a PIN, a restricted form link key, called a unit key, is generated based on the device’s address and random number.

Encryption can only be activated after authentication. Encryption is based on a stream cipher easily implemented in hardware or software.

SPREAD SPECTRUM

Both 802.11b and Bluetooth operate in the worldwide available 2.4GHz spectrum and use spread spectrum technologies. Spread spectrum was initially developed by the US military to send unbreakable codes that were either hard to detect or hard to jam. Some vendors might say their systems are secure because they use spread spectrum technology but when the spreading sequence is known to everyone, there is very little security gained from spread spectrum by itself.

Impact on Ease of Use

For 802.11b and Bluetooth, ease of use was always considered to be a key factor in choosing the implementation. As mentioned before, if security is not transparent to the application and easy to use, it won’t be used. This is proven by the fact that both 802.11b and Bluetooth security implementations have encryption as an option. There are clearly scenarios where encryption is not required nor wanted and others where encryption is needed.

Both of these implementations also have varying levels of security. The greater the level of security, the more complex the implementation seems to be. If users want very strong security, they will need to possess some knowledge of security mechanisms (shared secret entered by hand). If users do not want any security, they need not possess any knowledge of the underlying security, because there is none.

Another issue that affects ease of use is how to distribute the initial shared secret key. The shared secret in 802.11b is 40-bits. Shared secret keys are normally passwords or the like. They either need to be told to everyone in the peer group or distributed in a secure fashion.

Regulatory Issues

The United States government is constantly changing its export laws. The laws on encryption are no different. An interesting note is that the US government will let a company export any sort of product with authentication without regulation. Up to this point, the US government views encryption as munitions, similar to a nuclear bomb!

However, the government has recently relaxed the rules on export. Now a company can export an encryption product with an infinite size encryption key as long as the company complies with the following rules:

- It must have a one-time technical review with the Department of Export.
- It must not sell to terrorist countries.
- It must not sell directly to foreign governments. (However, if the product obtains “retail” classification, then the company can sell to foreign governments.)

The law used to be that one could only export up to 56-bit encryption. The 802.11b standard specified up to only

[*] Bluetooth is a trademark owned by its proprietor and used by Intel under license.

40-bit solely for export reasons. When exporting, though, one also needs to comply with a country's import rules.

Many of the encryption algorithms are well known and thus implemented outside the US. So some of the export/import rules can inhibit a US company from competing effectively in the world market.

FUTURE WORK

Intel and other companies are working together to propose increased security extensions to the 802.11 standard to increase the authentication, encryption, and key exchange.

From a security point of view it is more secure to have separate keys for encryption and authentication. It is even suggested that a different encryption key be used for sending and receiving.

Since 802.11 is a true wireless LAN, meaning it is designed to connect to the wired LAN, many of the security protocols applied to the wired LAN's are directly applicable to 802.11.

Here are some of the security mechanisms that will likely be implemented:

- 128 bit WEP encryption. This is already implemented by all of the major vendors but has not been standardized yet. It is a 104-bit key with a 24-bit IV.
- Standard key exchange and key distribution. Currently, 802.11 uses shared secrets that are physically entered. This can be done by a number of different protocols like RADIUS, Kerberos, SSL, and IPSEC.
- Improved data integrity via keyed MAC. This is a mechanism to ensure each packet of data has not been tampered with and is authentic. The CRC in 802.11b was designed to detect errors in a data frame while a keyed MAC will provide better authenticity and integrity.
- Compatibility with existing wired LAN infrastructure standards such as manageability and wake on LAN.

CONCLUSION

When defining a security system, companies need to first define what type of attacks to protect against and what they are willing to pay in MIPS, dollars, and time. As users' needs change and the requirements for security become more aggressive, 802.11 is poised to accept the challenge.

ACKNOWLEDGMENTS

The author acknowledges the help of Duncan Kitchin, Jesse Walker, and Jon Inouye.

REFERENCES

[1] Jim Geir, *Wireless LANs: Implementing Interoperable Networks*, MacMillan Technical Publishing, USA, pp. 25-26, 138-142.

[2] Wireless LAN Security White Paper, http://www.wlana.com.

[3] HomeRF Technical Committee, "Shared Wireless Access Protocol Specification," Revisions 1.09.

[4] Bluetooth White paper, "Bluetooth Security Architecture," Version 1.0.

[5] IEEE Standards Board, "802 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications."

[3] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, Inc, USA and Canada, pp. 397-398.

AUTHOR'S BIOGRAPHY

Sultan Weatherspoon is a technical marketing engineer with the Wireless LAN Operation in Intel Oregon. He is one of the original members of WLO that investigated WLAN, which eventually lead to the formation of the group and a $100 million investment in Symbol Technologies. He earned his B.S. degree in electrical engineering from the University of Michigan. His e-mail is sultan.weatherspoon@intel.com.