Global Information Assurance Certification Paper

Jorgen Ellingson
Version 1.2e

Layers One &Two of 802.11 WLAN Security

The ubiquity and convenience of wireless LANs (WLAN) is both enticing for the users and attackers alike, and as it turns out, equally accessible too. Physical controls of your environment represent a much bigger challenge when someone from the parking lot can gain access to even the most highly secured parameter defense. Like it or not this is the nature of WLANs and unless strong defense measures are taken i.e. encrypting all your company's digital assets or in an extreme case electro magnetically shielding your office, then you are leaving several potential doors wide open for attackers.

Today the most widely used WLAN protocol is called 802.11 administered by IEEE. A more secure derivative of the 802.11 protocol is called 802.11b with many more in the pipeline e.g. 802.11e, 802.11g. The standard encryption algorithm behind 802.11 is called Wireless Equivalent Privacy (WEP) and uses RSA's RC4 encryption engine. Just recently Nikita Borisov, Ian Goldberg, and David Wagner of UC Berkeley cracked WEP's 40-bit algorithm in less than four hours using 250 workstations. They proved that no matter what the size of the key bit, WEP is susceptible to attacks. They cracked both the 40 bit and the 128 bit versions equally well. The following attacks:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic. [1]

As far as a standard, 802.11 is still very much in a development phase and companies considering implementing WLAN need to find ingenious ways of securing against 'war driving' (hackers accessing WLANs from a corporate parking lot), and rely less on industry standard organizations to come up with an omnipotent solution.

So what does this mean to the existing 802.11 standard and what should I know before implementing my first WLAN? In this paper I will address most of the fundamental security concerns by examining closely OSI layers one and two of the 802.11 standard, media access control (Layer two) and physical layer (Layer one). This will provider you, the reader, with a foundation to implement more secure WLAN environments and avoid existing security holes. I will begin by introducing a figure, on the following page, representing the two layers; MAC and physical, where most of our WLAN security

concerns remain.

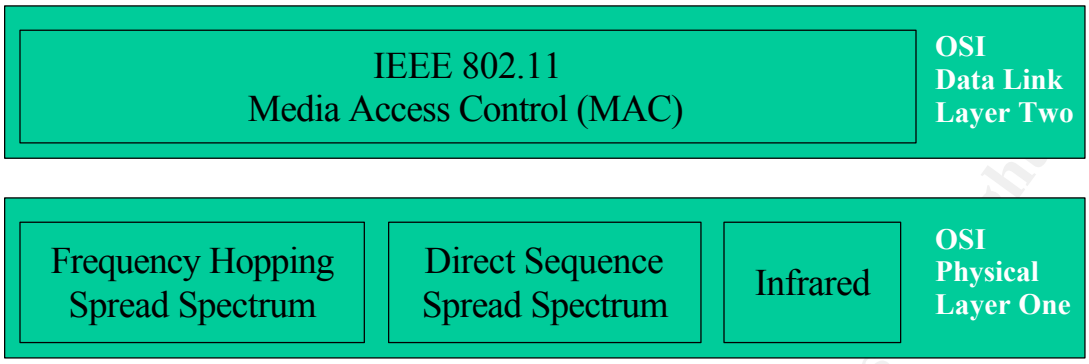

Figure 1: The OSI model according to IEEE 802.11 protocol.

1. Media Access Control (OSI Layer Two)

The MAC layer provides a set of services e.g. data transfer, association, re-association, authentication, privacy, and power management that control the communications between the wireless stations (e.g. laptops connected to the network via a wireless network interface card) and access points (AP) over a shared medium. However for discussion in this paper I will only look at authentication and encryption, and their current inherent insecurities to eavesdropping.

User Authorization

802.11 supports two methods of authentication: Open Systems and Shared Key or WEP (wired equivalent privacy). Open system is a default null authentication algorithm that involves a two-step process consisting of an identity assertion and request for authentication followed by authentication result.[2] For example before communication can take place, all mobile units must associate themselves with an access point (AP) by using Extended Service Set ID (ESSID) or a list of MAC addresses, but these are limited somewhat by most PC Cards' ability to change their MAC address.[6] Shared Key or WEP authentication supports authentication of wireless stations as either a member of those who know a shared secret key or a member of those who do not. The standard currently assumes that the shared key is delivered to the authenticating wireless station over a secure channel (e.g. RADIUS, Kerberos, SSL, IPv6 and IPSec) that is autonomous of the 802.11 wireless communication channels. If not, then the shared key is susceptible to attacks, and as the group from UC Berkeley has already proven, WEP is indeed crackable. Here is how the share key exchange works:

1. A requesting station sends an authentication frame to the access point or 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 indication a successful authentication. If not, the responding AP will send a negative authentication.[11]

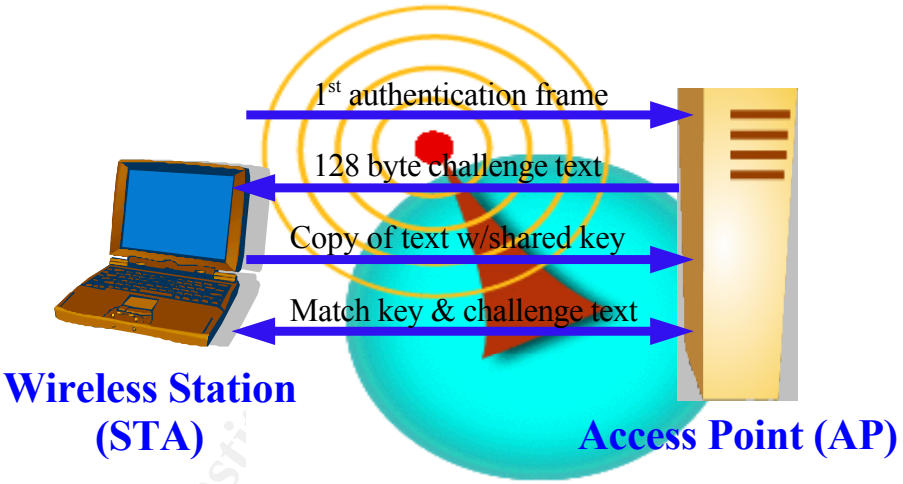

Figure 2: Graphical illustration of the shared key authentication process.

Encryption

A call has gone out loud and clear for a new encryption algorithm. As it stands WEP is standing naked with its 40-bit secret keys for authentication and encryption. Many 802.11 implementations also allow 104 and 128 bit secret keys, but no matter how large the key is, the WEP algorithm is unsafe at any bit level as proved by the Berkeley trio. This brings into question the shared key authentication method. If the encryption can be compromised then what good is our authentication method? Cisco's Aironet solution

creates per user, per-session, dynamic WEP key tied to the network logon, thereby addressing some of the limitations associated with the above mentioned shared static key system. Cisco's solution proposes five additional methods to secure 802.1b networks that serve as an immediate alternative to out of the box 802.11 implementations.

1. **Secure key derivation—**The original shared secret secure key derivation is used to construct responses to the mutual challenges. It undergoes irreversible one-way hashes that make password-replay attacks impossible. The hash values sent over the wire are useful for one-time at the start of the authentication process, and therefore, never after.

2. **Dynamic WEP keys—** Cisco believes that one of the biggest security exposures in WLANs is primarily due to static WEP and the tremendous administrative burden it imposes. With the Cisco Aironet solution, session keys are unique to the users and are not shared among them. Also, with LEAP authentication, the broadcast WEP key is encrypted using the session key before being delivered to the end client. By having a session key unique to the user, and by tying it to the network logon, the solution also eliminates vulnerabilities due to stolen or lost client cards or devices.

3. **Reauthentication policies—**Aironet administrators can also set policies for reauthentication at the back-end RADIUS server ACS2000. This will force users to reauthenticate more often and get new session keys. Because the vulnerability window can be configured to be very small, it can minimize attacks where traffic is injected during the session.

4. **Initialization Vector changes—**The Cisco Aironet wireless security solution also changes the initialization vector (IV) on a per-packet basis so that hackers can find no predetermined sequence to exploit. This capability, coupled with the reduction in possible attack windows, greatly mitigate exposure to hacker attacks due to frequent key rotation. In particular, this makes it difficult to create table-based attacks based on the knowledge of the IVs seen on the wireless network.

Also other adaptations of 802.11 will add 128-bit AES encryption to shore up 802.11 encryption battles. For more information about all the different flavors of 802.11, refer to http://www.ieee802.org/1/pages/802.1x.html for all the gory details.

Eavesdropping

Eavesdropping is very easy in the radio environment, when one sends a message over the radio path, everyone equipped with a suitable transceiver in the range of the transmission can eavesdrop.[4] 802.11 uses frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), or infrared radio transmission types (described below). FHSS and DSSS operate in the 2.4 to 2.4835 GHz range that can be easily transmitted through walls at distances of around a few hundred feet. Furthermore the 802.11 protocol inherently leaves the physical layer header unencrypted, providing critical information to

the attacker. Therefore data encryption is the critical layer of defense, but in many out of the box implementations the data transmitted is unencrypted altogether, or they have already passed that loop by decrypting the algorithm like the group from UC Berkeley. Next I will explain how the physical layer plays a critical role in defending 802.11 WLAN from attacks.

2. Physical Layer (OSI Layer One)

Data on the physical layer can be relayed using three different transmission types:

1. Direct Sequence Spread Spectrum (DSSS)
2. Frequency Hopping Spread Sequence (FHSS)
3. Infrared

Similar to today's microwave ovens, the 802.11 technology functions in frequency bands, but to eliminate interference and allow large numbers of users access to the same frequencies, WLAN engineers have developed a new way to transmit data by radio. Traditional radio is transmitted over a single frequency. But with FHSS implementations, data is transmitted in a pseudo-random way over a broad frequency band. Similarly, DSSS injects random bits into the data stream in a pseudo-random pattern in addition to hopping frequencies. This makes WLANs comparatively less susceptible to certain attacks because FHSS and DSSS make it virtually impossible to comprehensively gather enough packets to decipher messages or data. The attacker would have to know the hopping patterns (FHSS), dwell time (seconds between hops on the alternate channels), and the number of channels to assemble enough data to be worth anything. These techniques depend on both the transmitter and the receiver using matching algorithms to create and predict the correct frequency or correct bit of data in the data stream. In addition, these non-interference and frequency-sharing techniques provide a physical layer that's actually more secure than a wired infrastructure. The data stream is hard to locate or decipher, making it very difficult to detect and decipher during transmission.

But mishaps can happen and usually do. Here is an example of one out of the box DSSS implementation that serves as a benchmark when implementing not only DSSS WLANs but also all configurations. Because finding alternative and layered security methods is becoming du jour of WLAN implementations.

"Lucent released a new 'secure' wireless LAN card called the 'WaveLan'. It uses Direct Sequence Spread Spectrum as its modulation method, which could be very secure, but this security was crippled by the use of the same spreading code on all WaveLan cards. This means that although it is fairly difficult for a random eavesdropper to find, let alone decode, a WaveLan signal, it is very easy for another WaveLan user to do so. If you are thinking of that you could change the spreading code, be aware that it is inside one of the proprietary chips itself, and is virtually impossible to modify. This was probably done at the insistence of the US Government, which wants to be able to listen to all of its citizen's

transmissions. While Lucent does provide a selectable Network ID, there are only 65,280 possible codes, and it would be fairly easy to write a program that tries all codes in quick succession until the proper Network ID is found. Hence, the radio link-layer of the WaveLan is not very secure. Some cards come with a DES or AES implementation, of unknown key length and robustness. Our cards did not. So we suggest implementing some encryption and authentication on top of the WaveLan architecture, such as IPv6."

3. Conclusion

Although the 802.11 has been widely accepted in several vertical markets as a viable replacement to wired LANs, it is still in its infant stages as far as security is concerned. One way to improve your chances of a secure WLAN is to upgrade to 802.11b (Cisco's Aironet) or in the near term you will be able to use 802.11e with a 128-bit key AES encryption and of course, install a layered defense plan similar to one used on your wired LAN network i.e. password policies, file access controls, and encrypt all critical data on hard drives and in extraordinary circumstances, electromagnetic shielding can be install to lock down the parameters i.e. wall out 'war driving' hacks from the company's parking lot. The defense in depth theory once again reins supreme, particularly with 802.11 WLAN deployments.

4. Bibliography

1. Borisov, Nikita; Goldberg, Ian; Wagner, David. "Security of the WEP algorithm." UC Berkeley. URL:
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

2. Microsoft. "Enabling IEEE 802.11 Networks with Windows "Whistler"." November 30, 2000. URL:
http://www.microsoft.com/hwdev/wireless/IEEE802Net.htm

3. Durkin, Brian. "Wireless Local Area Networking." Fall 1999. URL:
http://polaris.umuc.edu/~bdurkin/wireless_lan.htm

4. Uskela, Sami. "Security in Wireless Local Area Networks." Helsinki U. of Technology. Dec. 1997. URL:
http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html

5. Intelligraphics. "Introduction to IEEE 802.11" URL:
http://www.intelligraphics.com/articles/80211_article.html

6. Fairleigh Dickinson University. "Wireless Local Area Network IEE 802.11." URL:
http://alpha.fdu.edu/~anandt/security.html

7. Cisco. "Cisco Aironet Security Solution Provides Dynamic WEP to Address Researchers' Concerns." Product Bulletin No. 1281. Apr. 2001. URL
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm

8. Adventure Publishing. "WLAN Security." 2000. URL:
http://www.cco.com/jour0009.htm

9. Dr. Who. "WaveLAN." URL:
http://www.l0pht.com/~oblivion/radionet/reference/wavelan/sin_wavelan.html

10. Somogyi, Stephen. "802.11 and swiss cheese." ZDNet. Apr. 2001. URL:
http://www.zdnet.com/zdnn/stories/comment/0,5859,2707262,00.html

11. Weatherspoon, Sultan."Overview of IEEE 802.11b Security." URL:
http://developer.intel.com/technology/itj/q22000/pdf/art_5.pdf