Wireless Networks

Securing Wireless Networks and Biometric RFID (Radio Frequency Identification)

Case Communications

TECHNICAL NOTES

Wireless networks are very common, both for organisations and individuals. Many laptop computers have wireless cards pre-installed for the buyer. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into non-wireless networks.

In this article we explore traditional wireless security and touch on the new Biometric and RFID methods of providing security to our data.

In traditional wireless networks we have different types of authentication like MAC ID Filtering, WEP Encryption, WPA, WPA2, 802.1X, LEAP, PEAP, TKIP, radius, Smart Cards, USB Tokens and Software Tokens etc. The paragraphs below provide an overview of these technologies, before we look at the emerging Biometric RFID technology.

MAC ID filtering

Most wireless access points contain some type of MAC ID filtering that allows the administrator to only permit access to computers that have wireless functionalities that contain certain MAC IDs. This can be helpful; however, it must be remembered that MAC IDs over a network can be faked. Cracking utilities such as SMAC are widely available, and some computer hardware also gives the option in the BIOS to select any desired MAC ID for its built in network capability.

WPA (Wi-Fi Protected Access)

WPA was created by the Wi-Fi Alliance, an industry trade group, which owns the trademark to the 'Wi-Fi ' name and certifies devices that carry that name.

WPA is designed for use with an IEEE 802.1X authentication server, which distributes different keys to each user; however, it can also be used in a less secure "pre-shared key" (PSK) mode, where every user is given the same pass-phrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard.

The Wi-Fi Alliance created WPA to enable the introduction of standard-based secure wireless network products prior to the IEEE 802.11i group finishing its work. The Wi-Fi Alliance at the time already anticipated the WPA2 certification based on the final draft of the IEEE 802.11i standard, therefore the tags on the frame fields (Information Elements or IEs) are intentionally made different from 802.11i to avoid the confusion in unified WPA/WPA2 implementations.

Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger IV, this defeats the well-known key recovery attacks on WEP.

In addition to authentication and encryption, WPA also provides vastly improved payload integrity. The cyclic redundancy check (CRC) used in WEP is inherently insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key. A more secure message authentication code (usually known as a MAC, but here termed a MIC for "Message Integrity Code") is used in WPA, an algorithm named "Michael". The MIC used in WPA includes a frame counter, which prevents replay attacks being executed. By increasing the size of the keys and IVs, reducing the number of packets sent with related keys, and adding a secure message verification system, WPA makes breaking into a Wireless LAN far more difficult. The Michael algorithm was the strongest that WPA designers could come up with that would still work with most older network cards. Due to inevitable weaknesses of Michael, WPA includes a special countermeasure mechanism that detects an attempt to break TKIP and temporarily blocks communications with the attacker.

WPA2 (Wi-Fi Protected Access V2)

WPA2 implements the mandatory elements of 802.11i. In particular, in addition to TKIP and the Michael algorithm, it introduces a new AES-based algorithm, CCMP, that is considered fully secure. Note that from March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be Wi-Fi certified.

Vendor support:

- Official support for WPA2 in Microsoft Windows XP was rolled out on 1 May 2005. Driver upgrades for network cards may be required.
- Apple Computer supports WPA2 on all AirPort Extreme-enabled Macintoshes, the AirPort Extreme Base Station, and the AirPort Express.
- Firmware upgrades needed are included in AirPort 4.2, released July 14, 2005.

IEEE 802.11i (also known as WPA2)

IEEE 802.11i is an amendment to the 802.11 standard specifying security mechanisms for wireless networks The draft standard was ratified on 24 June 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher.

The 802.11i architecture contains the following components:

- 802.1X for authentication (entailing the use of EAP and an authentication server).
- RSN for keeping track of associations.
- AES-based CCMP to provide confidentiality, integrity and origin authentication.

Another important element of the authentication process is the four-way handshake, explained below.

The Four-Way Handshake

The authentication process leaves two considerations:

- The access point (AP) still needs to authenticate itself to the client station (STA).
- Keys to encrypt the traffic need to be derived.

The earlier EAP exchange has provided the shared secret key PMK (Pairwise Master Key). This key is however designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address. The product is then put through a cryptographic hash function.

1. The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the AP together with a MIC.
3. The AP sends the GTK and a sequence number together with another MIC. The sequence number is the sequence number that will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP.

As soon as the PTK is obtained it is divided into five separate keys: PTK (Pairwise Transient Key – 64 bytes)

1. 16 bytes of EAPOL-Key Encryption Key (KEK) – AP uses this key to encrypt additional data sent (in the ‘Key Data’ field) to the client (for example, the RSN IE or the GTK)
2. 16 bytes of EAPOL-Key Confirmation Key (KCK) – Used to compute MIC on WPA EAPOL Key message
3. 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
4. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP
5. 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.

IEEE 802.1X

IEEE 8021X standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is used for certain closed wireless access points, and is based on the EAP, Extensible Authentication Protocol (RFC 2284). RFC 2284 has been obsoleted by RFC 3748.

802.1X is available on certain network switches, and can be configured to authenticate hosts which are equipped with supplicant software, denying unauthorized access to the network at the data link layer. Some vendors are implementing 802.1X for wireless access points, to be used in certain situations where an access point needs to be operated as a closed access point, addressing the security vulnerabilities of WEP (see 802.11i). The authentication is usually done by a third-party entity, such as a RADIUS server. This provides for client-only authentication, or more appropriately, strong mutual authentication using protocols such as EAP-TLS.

In many cases, the public is invited to the premises but not invited to connect to the network. In the case of a wired network, it is possible to control access through physical security on all network ports. As this does not apply to an IEEE 802.11 wireless signal, operators of closed access points can instead use 802.1X or other network admission controls at the data link layer. This correlation between wireless networking and use of 802.1X authentication has led some to mistakenly call the standard “802.11x” when it is used in a wireless network.

Upon detection of the new client (supplicant), the port on the switch (authenticator) will be enabled and set to the “unauthorized” state. In this state, only 802.1X traffic will be allowed; other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator will send out the EAP-Request identity to the supplicant, the supplicant will then send out the EAP-response packet that the authenticator will forward to the authenticating server. The authenticating server can accept or reject the EAP-Request; if it accepts the request, the authenticator will set the port to the “authorized” mode and normal traffic will be allowed. When the supplicant logs off, he will send an EAP-logoff message to the authenticator. The authenticator will then set the port to the “unauthorized” state, once again blocking all non-EAP traffic.

LEAP Lightweight Extensible Authentication Protocol

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary EAP method developed by Cisco Systems.

Cisco has since made efforts to entrench the protocol by allowing other vendors to produce LEAP-compliant products through the CCX (Cisco Certified Extensions) program. There is no native support for LEAP in any Windows operating system but is supported by third party supplicants (IEEE term for client software). The protocol has been known from the beginning to be vulnerable to dictionary attacks just like EAP-MD5 but it wasn’t until the release of ASLEAP by Joshua Wright in 2003 that people began to argue that LEAP was a serious security liability. Cisco still maintains that LEAP can be secure if sufficiently complex passwords are used, but complex passwords are rarely used in the real world because of the difficulty they pose for average users. Newer protocols like EAP-TTLS and PEAP do not have this problem because they create a secure TLS tunnel for the MS-CHAPv2 user authentication session and can operate on Cisco and non-Cisco Access Points.

PEAP (Protected Extensible Authentication Protocol)

PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.

As of May of 2005, there were two PEAP sub-types certified for the updated WPA and WPA2 standard. They are:

- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC

PEAPv0/EAP-MSCHAPv2

PEAPv0/EAP-MSCHAPv2 is the technical term for what people most commonly refer to as "PEAP". Whenever the word PEAP is used, it almost always refers to this form of PEAP since most people have no idea there are so many flavors of PEAP. Behind EAP-TLS, PEAPv0/EAP-MSCHAPv2 is the second most widely supported EAP standard in the world. There are client and server implementations of it in Microsoft, Cisco, Apple, Linux, and open source. PEAPv0/EAP-MSCHAPv2 is natively supported in Mac OS 10.3 and above, Windows 2000 SP4, Windows XP, Windows Mobile 2003 and above, and Windows CE 4.2. The server side implementation of PEAPv0/EAP-MSCHAPv2, called IAS (Internet Authentication Service), is also included in Windows 2003 server. PEAPv0/EAP-MSCHAPv2 enjoys universal support and is known as the PEAP standard. This version of PEAP was defined in Internet Draft "draft-kamath-pppext-peapv0".

PEAPv1/EAP-GTC

PEAPv1/EAP-GTC was created by Cisco as an alternative to PEAPv0/EAP-MSCHAPv2. It allows the use of an inner authentication protocol other than Microsoft's MSCHAPv2. EAP-GTC (Generic Token Card) is defined in RFC 3748. It carries a text challenge from the authentication server, and a reply which is assumed to be generated by a security token. EAP-GTC does not protect the authentication data in any way.

Even though Microsoft (along with RSA and Cisco) co-invented the PEAP standard, Microsoft never added support for PEAPv1 in general, which means PEAPv1/EAP-GTC has no native Windows OS support. Since Cisco has always favored the use of its own less secure proprietary LEAP and EAP-FAST protocols over PEAP and markets them as simpler certificate-less solutions, standardized PEAP is rarely promoted by Cisco. With no interest from Microsoft to support PEAPv1 and little interest from Cisco to promote PEAP in general, PEAPv1 authentication is rarely used. There is no native OS support for this EAP protocol.

Although there is no in-built support for PEAP-GTC in MS Windows, it is supported by the Cisco CCX extensions program. CCX compatibility is enabled by default on many vendor-provided 802.11A/B/G clients.

Note: The PEAP standard was created by Microsoft, Cisco, and RSA after EAP-TTLS had already come on the market. Even with its late start, Microsoft's and Cisco's size allowed them to quickly overtake EAP-TTLS in the market. Microsoft and Cisco parted ways when Microsoft only supported the PEAPv0 standard while Cisco supported both PEAPv0 and PEAPv1. PEAPv0 and PEAPv1 both refer to the outer authentication method and is the mechanism that creates the secure TLS tunnel to protect subsequent authentication transactions while EAP-MSCHAPv2, EAP-GTC, and EAP-SIM refer to the inner authentication method which facilitates user or device authentication. From Cisco's perspective, PEAPv0 supports inner EAP methods EAP-MSCHAPv2 and EAP-SIM while PEAPv1 supports inner EAP methods EAP-GTC and EAP-SIM. Since Microsoft only supports PEAPv0 and doesn't support PEAPv1, Microsoft simply calls PEAPv0 PEAP without the v0 or v1 designator. Another difference between Microsoft and Cisco is that Microsoft only supports PEAPv0/EAP-MSCHAPv2 mode but not PEAPv0/EAP-SIM mode. However, Microsoft supports another form of PEAPv0 (which Microsoft calls PEAP-EAP-TLS) that Cisco and other third-party server and client software don't support. PEAP-EAP-TLS does require a client-side digital certificate located on the client's hard drive or a more secure smartcard. PEAP-EAP-TLS is very similar in operation to the original EAP-TLS but provides slightly more protection due to the fact that portions of the client certificate that are unencrypted in EAP-TLS are encrypted in PEAP-EAP-TLS. Since few third-party clients and servers support PEAP-EAP-TLS, users should probably avoid it unless they only intend to use Microsoft desktop clients and servers. Ultimately, PEAPv0/EAP-MSCHAPv2 is the only form of PEAP that most people will ever know. PEAP is so successful in the market place that even Funk Software, the inventor and backer of EAP-TTLS, had no choice but to support PEAP in their server and client software for wireless networks.

This version of PEAP is defined through the IETF internet draft "draft-josefsson-pppext-eap-tls-eap-05." Note that this is an individual submission and not standardized in the IETF.

TKIP (Temporal Key Integrity Protocol)

In cryptography, TKIP is a security protocol used in Wi-Fi Protected Access (WPA). WPA is used for WiFi networks to correct deficiencies in the older Wired Equivalent Privacy (WEP) standard. TKIP (pronounced “tee-kip”) was designed to replace WEP without replacing legacy hardware. This was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and the solution to this problem could not wait for the replacement of deployed hardware. For this reason, TKIP, like WEP, uses a key scheme based on RC4, but unlike WEP, TKIP provides per-packet key mixing, a message integrity check and a rekeying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key.

Key mixing increases the complexity of decoding the keys by giving the cracker much less data that has been encrypted using any one key. The message integrity check prevents forged packets from being accepted. Under WEP it was possible to alter a packet whose content was known even if it had not been decrypted. Also TKIP hashes the initialization vector (IV) values, which are sent as plaintext, with the WPA key to form the RC4 traffic key, addressing one of WEP’s largest security weaknesses. WEP simply concatenated its key with the IV to form the traffic key, allowing a successful related key attack.

CCMP (Counter Mode with Cipher Block Chaining Messaging Authentication Protocol)

CCMP is an IEEE 802.11i encryption protocol, created to replace, together with TKIP, an earlier, insecure WEP protocol. CCMP uses the Advanced Encryption Standard (AES) algorithm. In the CCMP, unlike TKIP, key management and message integrity is handled by a single component built around AES.

Smart Cards

A smart card, chip card, or integrated circuit(s) card (ICC), is defined as any pocket-sized card with embedded integrated circuits which can process information. This implies that it can receive input which is processed – by way of the ICC applications – and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components.

USB Tokens

A security token (or sometimes a hardware token, authentication token or cryptographic token[1]) may be a physical device that an authorized user of computer services is given to aid in authentication. The term may also refer to software tokens.

Hardware tokens are typically small enough to be carried in a pocket or purse and often are designed to attach to the user’s keychain. Some may store cryptographic keys, such as a digital signature, or biometric data, such as a fingerprint. Some designs feature tamper resistant packaging, other may include small keypads to allow entry of a PIN.

Biometric Authentication

Another commonly known form of authentication process is biometric authentication. In the biometric identification process , authentication is carried out by eyes retina and iris scan: hand or fingers scan: facia; pattern scan or by voice analysys. A Case Communications customer based in Moscow developed a biometric footprint based on the distance between a mans eyes and the tip of his nose, as they said this was unique to each man. We never discovered what would happen if the man had broken his nose.

RFID (Radio Frequency Identication)

Among the most interetsing concept is RFID (radio frequency identification). Basically Radio frequency identification, or RFID, is an identification process using radio waves to automatically identify objects. In the radio frequency identification process, information is stored and retrieved using a device called an RFID tag or RFID transponder. This is a combination of a microchip and antenna (The RFID tag receices retransmits and amplifies a signal inresponse to a predefined received signal). The antenna enables the chip to transmit the identification information to a reader in the form of radio waves. The reader converts the radio waves reflected back from the RFID Tag into digital informaiton, which is transferred to a computer.

There are three types different types of RFID Tag: passive, semi-passive and active.

Passive RFID Tags

Passive tags don't use batteries, but draw current from signals passed by the tags antenna and transmits a signal back. Since passive RFID's don't use an internal power source, they can be very small and have a very long life span. The range of a passive RFID tag of about 2mm depending on the radio frequency

Semi-Passive Tags

Semi-passive tags use an additional power supply in the form of a battery, which allows the tag circuit to be constantly powered. However, semi-passive tags communicate by taking power from the RFID reader.

The advantages of using a semi-passive tag are:

- Antennas can be used to optimise signals which are sent back.
- The use of batteries allow semi passive RFID tags are faster and stronger to respond back on receiving a signal compared to passive tags.
- Active RFID tags have an internal power source, which is used to run the microchips circuitry and to broadcast a signal to a reader.

Active RFID tags

Active tags have an internal power source, which is used to run the microchip's circuitry and to broadcast a signal to a reader.

Benefits of an active RFID tag:

- They cover a greater range compared to a passive and semi passive tag
- They have a larger memory compared to a passive and semi passive tag
- Active and semi-passive tags can be used for tracking high-value gods that require scanning over long ranges, such as railway carriages on tracks. The only problem with active tags is the cost involved in manufatcuring making them too expensive for use on lower cost items.
- Compared to active tags, passive UHF tags cost less than 0.25p each to manufacture today once your into volume production.

Typical uses for RFID Tags

By implanting low frequency RFID tags in an animals body or their outer skin, it is possible to track them. Hence low frequency RFID tags could be used to find lost pets.

High frequency RFID tags can be used for any number of applications a few that spring to mind are:

- Keeping track of items withina store, clothes or trainers for example, or books withina library or book store
- Maintaining tight security withina building
- Tracking airline baggage
- Microwave RFID tags are used in long range access control for vehicles.

RFID and Biometric Systems

By combining the benefits of RFID and biometric technology, a foolproof security system could be built. In fact, such systems have already been started. A newly proposed system, converts the fingerprint minutiae into integers, these integers are stored in the database instead of the templates of the finger-print-minutiae. This data is compared with the RFID tag and if both data sets are similar, then access is granted. The biometric-based RFID system seems to be trust worthier as it prevent misue of RFID tags. The reliability of RFID biometric bonds comes from the fact that biometric details are not stored in an easy to readformat; instead they are converted into integers, preventing the risk of the data being stolen.

Within Great Britain there is already a firm that has developed an RFID system which goes into animals at birth and which tracks them through to joints of meat in the supermarket (Presumably by injecting a die with some form of radio activation into the animal). This system has yet to be put into use, but the technology has been proven to work.

Acknowledgements

We would like to give our thanks and acknolwedgement to the following organisations for information contained within this article.

- Wikepedia
- Jim Trade