WIRELESS SECURITY DESIGN OVERVIEW

Nidal Aboudagga, Damien Giry*, Jean-Jacques Quisquater
UCL Crypto Group - Place du levant, 3 - 1348 Louvain-la-Neuve Belgium
aboudagg@dice.ucl.ac.be, giry@dice.ucl.ac.be, quisquater@dice.ucl.ac.be
(*Extended version available on author's website*)

Today, Wireless Network has become more and more present in open area or large companies and security enhancement is needed to control authentication and confidentiality. The 802.11 Working Group introduced the 802.11i amendment as the final stage of the Robust Security Network standard, superseded the old WEP technology. This paper describes the technical evolution of wireless security and introduces the future 802.11i with the most recent IEEE draft.

1. INTRODUCTION

Wireless systems (IEEE Standard 802.11 [1]) are expected to become significantly used in many open environments like train stations or universities. The principal aspect of this new technology is mobility and simplicity regarding user manipulation. It opened a wide range of new commercial areas for hardware vendors, at low cost.

In 1999, the IEEE 802.11 working group defined the 802.11b standard [2], designing the communication between a client and an Access Point. Wireless network appeared to be the elegant network solution as it provides easy LAN access and low cost solution. This system is becoming popular for home network but security concerns have slowed wireless deployment at professional level.

2. WIRED EQUIVALENT PRIVACY (WEP)

The 802.11b introduced the concept of Wired Equivalent Privacy (WEP). It tried to ensure confidentiality, integrity and authenticity in wireless communication. At the beginning, implementing WEP required hardware resources and modifications to existing wireless card. With security at low cost in mind, vendors decided to introduce the so-known MAC-address filtering instead of the 802.11b. It prevented connection from unknown users to the wireless system. This authentication technique could be practical for a home network but maintaining a good address list quickly became a nightmare for IT departments. Moreover, an

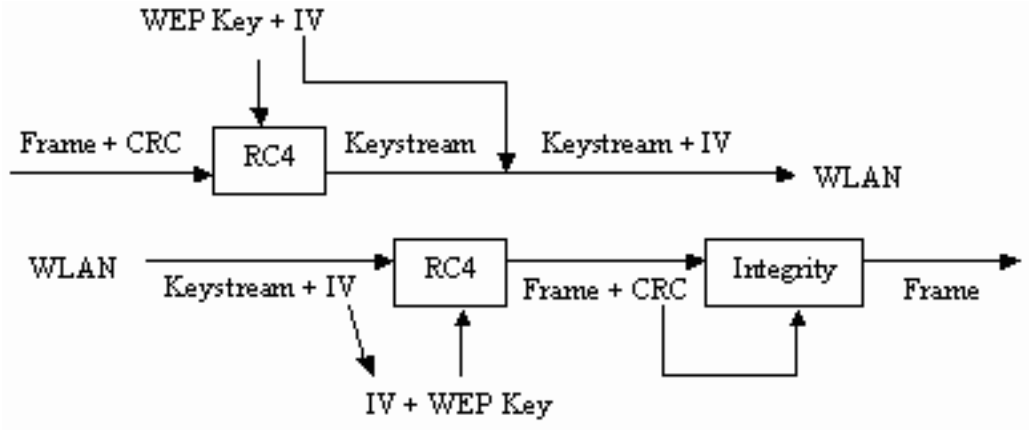

Figure 1: WEP Data Processing

attacker could use spoofing techniques as the authentication referred to MAC-addresses, not the user himself.

Address filtering was never part of the standard and vendors finally implemented 802.11b WEP specification in hardware. It used RC4 stream cipher and Cyclic Redundancy Check (CRC) integrity algorithm as described in figure 1. A basic challenge-response protocol is used for authentication.

WEP can used up to four default keys and it can create pairwise keys related to MAC-address (describe in the 802.11 management information base, MIB). It specified a 40-bit secret key, combined with a 24-bit Initialization Vector (IV).

The 802.11 Working Group focussed on the early stage of the wireless protocol and did not implement real security measures. Here is a list of WEP problems:

- No specification for the construction of the Initial Vector. A IV collision could occur [3] and compromises the key.
- Key distribution remains a problem in case of compromising or when a user must be deleted from the authorization list.
- Message injection attack [3], which allows Authentication spoofing.
- Brute Force Attack: The 40-bit secret key is too small for encryption.
- All network users use the same authentication keys.
- No replay protection.
- Pairwise keys are not user dependant but relative to MAC-address.
- The CRC integrity check algorithm detects single-bit alterations but is not cryptographically secure: As it does not use a hash function, an attacker can easily forge messages.

The final break has been done in "Weaknesses in the Key Scheduling Algorithm of RC4" [4] and is specifically adapted for WEP in another paper [5].

The 802.11 Working Group adopted the 802.1X standard to address the shortcomings of WEP authentication scheme. It is based on the IETF Extensible Authentication Protocol (EAP). EAP was designed with flexibility in mind and has been used in a lot of network authentications.

3. 802.1X: NETWORK PORT AUTHENTICATION

The IEEE has proposed long-term security architecture for 802.11, which they called Robust Security Network (RSN). It utilized the IEEE 802.1X standard [6] as basis for access control, authentication, and key management. 802.1X had three components: a client (user), an authenticator (AP) and an authentication server.

802.1X is not a Wireless LAN related protocol but IEEE adapted it to the 802.11 structures in RSN. Network connectivity is provided through the concept of open (controlled) and close (uncontrolled) ports. In IEEE 802.11b, a network port is an association between a client and an Authenticator.

The IEEE 802.1X standard combines a 128-bit WEP keys and the Extensible Authentication Protocol EAP (RFC2284), which permits the use of various authentication methods such as certificate, smartcards, one-time passwords and public key authentication. Usually the authentication server is a Remote Authentication Dial-In User Service (RADIUS) but the standard did not specifically require it.

EAP is built around the challenge-response paradigm. The authenticator must allow first EAP network transaction to the uncontrolled port before any other traffic (in controlled port).

1. The client sends a request for authentication to the uncontrolled port of the authenticator.
2. The authenticator replies with a request for the client to provides identification and blocks all other traffic until it can verify the client's identity using the authentication server.
3. The client sends a response containing the identity to the authenticator. This last one forwards it to the authentication server.

4. The authentication server receives the request and uses an appropriate authentication algorithm (like POP, SMTP, KERBEROS, etc...) to verify the client's identity. If the user can be identified, an accept message is sent, otherwise it is a reject message.
5. In case of acceptation, the authenticator will convert the client's port to an authorized mode and optionally it could send a secret key to protect future transaction.

802.1X enhances security and addresses WEP authentication vulnerabilities. It allowed computer and network to authenticate each other with a central server. It provided dynamic 128-bit WEP keys management: per-user and per-session keys and ability to change them at frequent intervals.

4. 802.1X / EAP: METHODS AND PROBLEMS

EAP allowed developers to construct their own algorithm and consequently a lot of wireless vendors implemented their own 802.1X adaptation. They provided significant modifications to the authentication system but, as there was no general specification, this enhancement was frequently platform dependent. Moreover, these adaptations often relied on external systems like Radius server, PKI and Certificates. All this solutions have some problems related to attacks on 802.1X [7]:

1. Man-in-Middle attack: the one-way authentication exposed to the man-in-middle attack where adversary becomes an authenticator for the client and a client for the real authenticator.
2. Session Hijacking: A hacker waits until a valid user authenticates himself, then he pretends to be this user and blocks the valid user traffic.

Here is a list of the most common EAP implementations:

- EAP-MD5, Message Digest 5 (or CHAP Protocol) (RFC1994): Vulnerable to a lot of attacks and did not support dynamic WEP keys. Only use this implementation in a small private network.
- EAP-TLS, Transport Layer Security (RFC2716): Open standard, using X.509 certificates complex architecture for servers and users. It relies on PKI and TLS. It allowed manipulation of dynamic WEP keys. It resists to most 802.1X attacks except Man-in-Middle and the user's identity is revealed.

- EAP-TTLS, Tunnelled TLS: very similar to EAP-TLS. This protocol simplifies the PKI structure by using server's Certificate only. It also protects the user's identity.
- PEAP, Protected EAP: Very similar to EAP-TTLS, this solution is used by Cisco and Microsoft in their products.
- LEAP, Lightweight EAP: Proprietary Cisco solution, it is vulnerable to a lot of attacks like dictionary, man-in-middle and session hijacking (Cisco answer to dictionary attack by EAP-FAST[1]).
- There is also EAP-SIM, EAP-SPEKE, etc...

802.1X / EAP resolved most WEP authentication problems, but RC4 and EAP attacks conducted the 802.11 Working group to reveal a part of the future 802.11i standard. The Wi-Fi Alliance used this information to build a new standard, the Wireless Protected Access protocol (WPA).

5. INTERIM SOLUTION: WI-FI PROTECTED ACCESS (WPA)

WPA is a subset of IEEE 802.11i security specification currently under development. It took some ready parts of 802.11i draft to enhance security structure of wireless network and it only required a software upgrade of actual wireless devices.

WPA supported a mixed environment of client devices using either WPA or WEP. It used 802.1X EAP-TLS to authenticate users and addressed WEP vulnerabilities by using a new Temporal Key Integrity Protocol (TKIP) and 128-bit RC4 key. TKIP is a suit of four algorithms with minimum computing cost:

1. The cryptographic Message Integrity Code (MIC), called Michael, to defeat forgeries. It replaces CRC with providing true cryptographic hash function.
2. A new Initial Vector sequencing discipline, to prevent replay attacks.
3. A key mixing function, to have a per-packet key.
4. A re-keying mechanism, to provide fresh keys to the key mixing function.

Michael Algorithm used a tagging function and a 64-bit secret key, shared only between sender and receiver. It ensured the message integrity without preventing replay attacks. To enhance and prevent the lake of MIC in replay, the sender appended a sequence number to the packet.

[1] http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

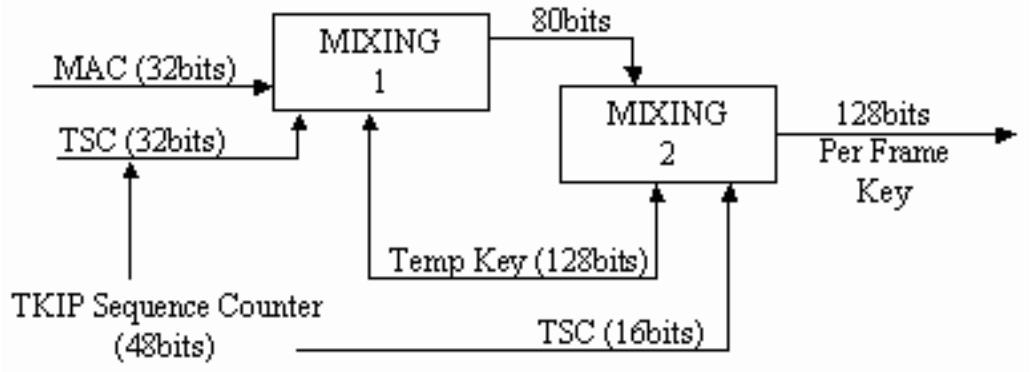

Figure 2: TKIP Key Mixing

The Initial Vector (IV) took the role of this TKIP Sequence Number (TSC). It is based on an extended 48-bit WEP IV field. WPA associated TSC with the encryption key as it will be initialized to zero whenever a new TKIP key is set. The sender incremented the TSC after each packet sent. TKIP prevented replay attack by discarding packets out of order.

The key mixing function enables TKIP to give a different key for each packets. The figure 2 represents the mixing process.

WPA associated the temporal key (user dependant) and the MAC-address (computer dependant) to prevent packet forgery.

In most cases, WPA used the infrastructure 802.1X to authenticated and obtained two fresh master keys for global and per-user communication. By derivation, the client and the authenticator acknowledge themselves of a temporal key, which is regularly refreshed.

In home environment and small network, TKIP use a shared secret passphrase to generate per-station encryption key or mutually entered keys without the need of an authentication server. This WPA mode suffering from dictionary attack if the user did not use a strong one (more then 20 characters) [8].

The WPA is an intermediate solution. It discards all known attacks from WEP architecture but it preserves the RC4 Algorithm to ensure compatibility and simple update of actual hardware. Even if WPA structure consolidates WEP, the 802.11 Working Group decided to change it as it could be the only Achilles' heel for the future.

6. THE FUTURE: 802.11I / ROBUST SECURITY NETWORK (RSN)

The 802.11 Working Group seems to be ready to release 802.11i in late 2004. We will refer to Draft 9 [9] as reference for 802.11i description. It will be part of the Robust Security Network (RSN), the IEEE security standard for wireless network.

RSN and WPA have a lot in common: same security protocol, key distribution and key renewal but compatibility is optional. They both need RADIUS server and 802.1X protocol as they rely on several components to produce an overall security system. Contrary to WPA, RSN had no recommendation for the choice of EAP. The support for older systems like WEP needed the utilization of traditional specifications described in Transitional Security Network (TSN).

Let us describe the RSN main aspects (not present in WPA):

- Utilization of the AES (Advanced Encryption Standard).
- Support of Quality of Service with a dedicated place in the header of RSN packet.
- Support of pre-authentication to enhance the roaming in wireless network. The client can authenticate with more than one authenticator and quickly switch his traffic from one to another.

The apparition of AES could be a serious update problem to current hardware. Most of WEP compatible Wi-Fi cards did not have enough computational power to be easily transformed in an RSN card.

CCMP is to RSN what TKIP is to WPA. CCMP is based on AES-CCM described in RFC3610. CCM mode combines Counter Mode (CTR) for encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) for authentication and integrity. It requires a fresh Temporal Key for every session and a unique nonce for each frame protected by a given Temporal Key.

CCMP fixed some parameters of CCM:

- The M parameter (see RFC3610) to 8 octets MIC.
- The L parameter (see RFC3610) to 2 octets length field.
- A unique AES 128-bit key for encryption / authentication.
- A 48-bit Packet Number as nonce.

The CCM process takes four inputs: the CCMP Temporal Key, the nonce, the frame body (payload) and some additional data taken from the frame body header. It provides authentication / integrity for the payload and the header as well as confidentiality for the payload.

CCMP has a replay protection as it transfers an authenticated Packet Number. Furthermore, forgeries can be easily detected with the CBC-MAC Message Integrity Code, protecting the source and destination.

7. CONCLUSION

Today, the future seems to be in the 802.11i standard. This new vision of wireless transactions extends the 802.11b to the security area. The only remaining problem seems to be the roaming efficiency. For Real time protocol, like Voice IP, pre-authentication system did not comply with sufficient fast authenticator switching. A key passing architecture will be, perhaps, the next major evolution of RSN.

REFERENCES

[1] Wireless LAN Medium Access Control and Physical Layer Specifications, IEEE Std 802.11-1999 Edition.

[2] IEEE Std 802.11b-1999 and IEEE Std 802.11b-1999-Cor1-2001, Amendment to IEEE Std 802.11-1999 Edition.

[3] Intercepting Mobile Communications: The Insecurity of 802.11; *Borisov, Goldberg and Wagner*; 7th Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.

[4] Weaknesses in the Key Scheduling Algorithm of RC4; *Fluhrer, Mantin and Shamir*; SAC 2001.

[5] Attacks on RC4 and WEP; *Fluhrer, Mantin and Shamir*; Cryptobytes 2002.

[6] Port-Based Network Access Control, IEEE Std 802.1X, 2001 Edition.

[7] An Initial Security Analysis of the IEEE 802.1X Standard; *Mishra and Arbaugh*; University of Maryland; `http://www.cs.umd.edu/~waa/1x.pdf`.

[8] WLAN Testing Reports "PSK as the Key Establishment Method"; *Moskowitz*; ICSA Labs WLAN Security Whitepapers; `http://www.icsalabs.com/html/communities/WLAN/wp_PSKStudy.pdf`.

[9] IEEE P802.11i/D9.0, March 2004, Amendment to ANSI/IEEE Std 802.11-1999 Edition as amended by IEEE Std 802.11g-2003 and IEEE Std 802.11h-2003.