
Indoor WLAN Design

Part VI: An Introduction to Wi-Fi Protected Access

Kjell Jørgen Hole
UiB

Last updated 28.01.09
Mail: Kjell.Hole@ii.uib.no
URL: www.kjhole.com

Outline

KJhole.com

- Introduction to *Wi-Fi Protected Access*
 - overview
 - missing pieces
 - protocols (EAP, IEEE 802.1X, TKIP)
 - key hierarchy

WPA *Wi-Fi Protected Access*. Specification of security enhancements that increase the level of *authentication, access control, replay prevention, message integrity, message privacy, and key distribution* for legacy Wi-Fi systems

- applicable for both home and enterprise users
- designed to run on original Wi-Fi hardware as a software upgrade
- forward-compatible with the 802.11i standard*

*The Wi-Fi Alliance refers to 802.11i as WPA2

6.3

Enhanced Message Protection

- To improve the message protection, WPA utilizes its *Temporal Key Integrity Protocol (TKIP)*. TKIP adds four algorithms to WEP:
 1. *Extended initialization vector with sequencing rules*, to defend against replay attacks
 2. *Message Integrity Code (MIC)*, to detect message modification
 3. *Per-packet key mixing function*, to de-correlate the public IVs from weak keys
 4. *Re-keying mechanism*, to avoid key reuse

6.4

Improved Authentication and Access Control

- To improve user authentication and access control, WPA implements the **IEEE 802.1X** standard for port-based access control and the *Extensible Authentication Protocol* (**EAP**)
- This framework utilizes a central authentication server, such as *RADIUS* (Remote Authentication Dial-In User Service) defined in RFC 2865 and RFC 2869, to authenticate each user on the network before they join it
- *Mutual* authentication is employed so that the wireless user does not accidentally join a rogue network

6.5

What is Missing from WPA?

KJhole.com

- WPA is a subset of the IEEE 802.11i standard that was approved in June of 2004
- The main pieces of the 802.11i standard not included in WPA are
 - secure IBSS (independent BSS)
 - secure fast handoff
 - secure de-authentication and disassociation
 - enhanced encryption protocols

6.6

WPA consists of three main pieces organized into three layers:

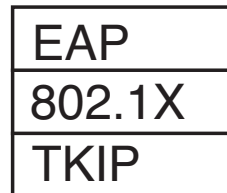


Figure 1 WPA security layers

6.7

Extensible Authentication Protocol—EAP

- EAP, defined by RFC 3748 and RFC 4017, is not an authentication protocol per se, but rather a transport protocol tailored to the needs of *Upper Layer Authentication (ULA)* protocols
- It provides a “plug-in” architecture for concrete ULAs
- ULA protocols are not specified in WPA or 802.11i, but are an integral part of the security system in many deployments

6.8

EAP Details (1)

- Eases manageability by centralizing
 - authentication decisions
 - authorization decisions
- Well matched economically to 802.11:
 - minimizes MS cost by moving ULA to authentication server
 - BS unaware of the ULA protocol, only 802.1X is implemented on BS

6.9

EAP Details (2)

- Authentication server initiates all transactions
 - request/response protocol
 - MS can't recover from authentication server or BS problems
- Authentication server tells the MS which authentication protocol to use
 - MS must decline if asked to use weak methods it can't support

6.10

EAP Details (3)

KJhole.com

- Authentication server sends EAP-Success to MS if authentication succeeds
 - MS breaks off if authentication fails
- Authentication server breaks off communication if authentication fails

6.11

EAP's Requirements for ULAs

KJhole.com

- New ULA methods must satisfy security requirements stated in RFC 4017
- The ULA documentation must state which of the security requirements apply and which do not
- Must provide “proofs” that the relevant requirements are satisfied

6.12

Security Claims for ULAs (1)

KJhole.com

Security claim	Requirement level	Explanation
Key derivation	Mandatory	Ability of the ULA to derive exportable key material
Key strength	Mandatory	Measure of the strength of the key derivation algorithm
Mutual authentication	Mandatory	MS authenticates auth. server and vice versa
Dictionary attack resistance	Mandatory	Requirement for password-based ULA

6.13

Security Claims for ULAs (2)

KJhole.com

Security claim	Requirement level	Explanation
Man-in-the-middle attack resistance	Mandatory	
Protected ciphersuite negotiation	Mandatory	Negotiation of a cryptographic algorithm and key
Packet fragmentation and reassembly	Recommended	
Confidentiality	Recommended	Encryption of EAP messages

Not complete list

6.14

- There are a number of popular ULA protocols in use today, primarily in the enterprise environment where the network infrastructure is in place to support their use
- The ULA protocols are used to provide a mutual authentication exchange between the MS and an authentication server residing on the network and to generate *cryptographic keys* to be used between the MS and the BS over the wireless link

6.15

- **EAP-TLS** (Extensible Authentication Protocol—Transport Layer Security) is defined in RFC 2716
 - TLS is described in RFC 2246 (successor to SSL)
 - mutual authentication between MS and authentication server
 - public-key certificates for both parties
 - provides encrypted channel
- Most secure ULA, but requires a public-key infrastructure

6.16

PEAP (1)

- **PEAP** (Protected Extensible Authentication Protocol)
 - developed by Microsoft, Cisco Systems, and Extundo
 - Windows provides native support
 - built into Cisco clients

6.17

PEAP (2)

- Mutual authentication:
 - server authenticated with certificate
 - MS authenticated with other method (like username/password)
- Two-phase approach:
 1. *Privacy without authenticity*: establish secure commun. between MS and PEAP authenticator using TLS with server certificate
 2. *Authentication via private connection*: tunnel authentication information between MS and authenticator

6.18

- 802.1X (www.ieee802.org/1/pages/802.1x.html) defines a standard framework for **port-based** network access control
 - the term port is an abbreviation of network access port
- 802.1X is used in conjunction with EAP to perform *user authentication* and *generation of encryption keys*. 802.1X defines how to pass EAP over a network
- Designed to scale to handle large networks (not originally designed for wireless networks)

6.19

802.1X in the Enterprise

- There are three primary roles played by enterprise equipment in an 802.1X system:
 - the **supplicant** (typically the MS in an 802.11 network) is the port requesting access to the network
 - the **authenticator** (usually the BS) is the port that enforces the authentication process and routes the traffic to the appropriate entities on the network
 - the **authentication server** is an entity (e.g. RADIUS server) that performs the authentication of the credentials supplied by the supplicant

6.20

- BS generates a **logical port** for each new wireless connection. The logical port is the point at which an MS connects to a BS to obtain access to the wired network
 - there is a one-to-one relationship between a supplicant (MS) and a logical port on the BS
 - each logical port has an associated authenticator to control its state
 - a single authentication (RADIUS) server is responsible for many logical ports

6.21

Architecture Overview

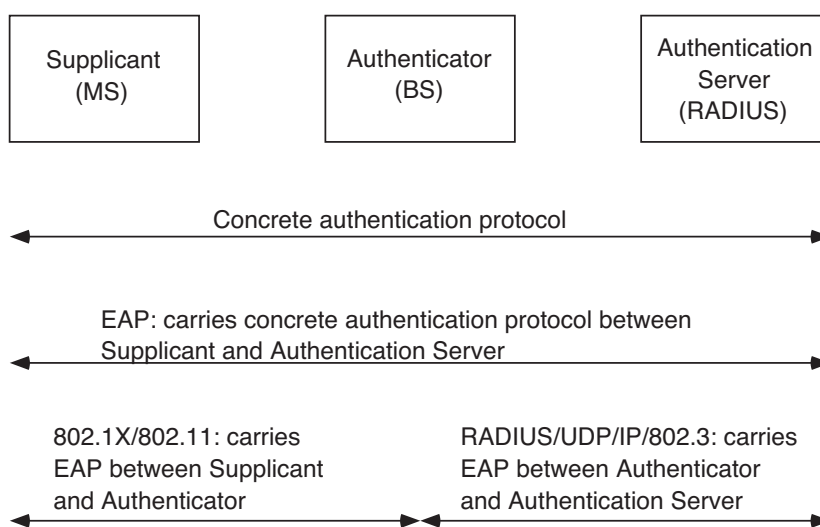


Figure 2 802.1X/EAP architecture overview

6.22

The Controlled/Uncontrolled Port Concept

- 802.1X operation can be understood using the concept of a *controlled port* and *uncontrolled port*
- The controlled and uncontrolled ports are logical entities and are the same physical connection to the network
- Whether a frame traveling through the BS is routed through the controlled or uncontrolled port is determined by the authentication state of the MS

6.23

Controlled/Uncontrolled Ports

KJhole.com

- Prior to authentication by the authentication server the BS will only allow the MS to communicate with the authentication server through the *uncontrolled port*
- After successful authentication by the authentication server, the BS will also allow the MS to access other services available on the network using the *controlled port*

6.24

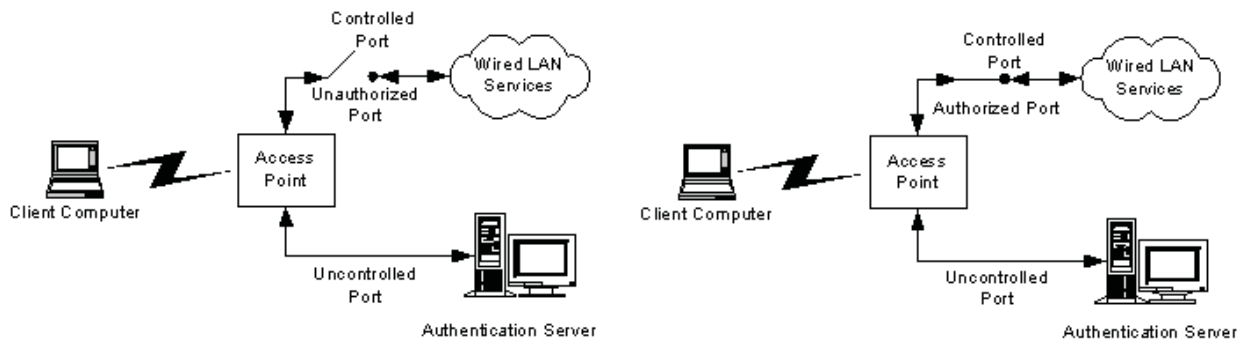


Figure 3 802.1X state before (left) and after (right) successful mutual authentication

6.25

802.1X—EAPOL

- EAP does not specify how messages should be passed around
- 802.1X defines a protocol *EAP over LAN* (**EAPOL**) to get EAP messages passed between the supplicant (MS) and the authenticator (BS)
- Four types of EAPOL messages are used (see following pages)

6.26

EAPOL Messages (1)

KJhole.com

- EAPOL-Start message:
 - supplicant sends EAPOL-Start message to special group-multicast MAC address reserved for 802.11 authenticators
 - the authenticator respond with an EAP-Request Identity message using the EAPOL-Packet message
- EAPOL-Key message:
 - Authenticator sends key material to the supplicant in an EAPOL-Key message after it has decided to admit the supplicant to the network

6.27

EAPOL Messages (2)

KJhole.com

- EAPOL-Packet message:
 - used to send actual EAP messages
- EAPOL-Logoff message:
 - message indicates that that the supplicant wishes to be disconnected from the network

6.28

EAP/802.1X in the Enterprise

- EAP/802.1X enhances the enterprise security model by providing the following improvements over WEP:
 - support for a centralized security management model
 - cryptographic keys are unique to each link so the traffic on any single key is significantly reduced
 - support for strong upper layer authentication
 - the authentication server ensures that the integrity (MIC) and encryption keys are generated dynamically (no network administrator is needed)

6.29

802.1X for Home/SOHO

KJhole.com

- In a home or *Small Office/Home Office* (SOHO) environment, where there are no central authentication servers or EAP framework, WPA runs in a special home mode
- This mode, also called *Pre-Shared Key*, allows the use of a manually-entered password to ensure that
 - only MSs with the correct password can join the network
 - session keys are provided and TKIP encryption is started
- Upper-layer authentication is not supported

6.30

TKIP—Temporal Key Integrity Protocol

- TKIP was designed to address all the known attacks and deficiencies in the WEP algorithm while still maintaining backward compatibility with legacy hardware
- It was designed to be made available as a firmware or software upgrade to existing hardware (millions of units)
- TKIP provides an upgrade path by offering an additional protocol and a wrapper around WEP

6.31

Extended IV

KJhole.com

- TKIP utilizes an 48-bit *Initialization Vector (IV)*, also called TKIP sequence counter
- IV has secondary role as a sequence counter to avoid replay attacks
- IV is constructed from the first and second bytes from the original WEP IV and 4 additional bytes (one byte of the old IV is not used)
- Since the IV is updated with each packet, 2^{48} packets can be exchanged using a single temporal key (key with limited lifetime) before key reuse would occur

6.32

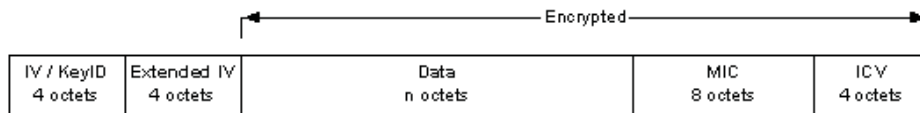


Figure 4 TKIP packet structure

6.33

MIC (1)

- A MIC (Message Integrity Code) provides a keyed cryptographic checksum to detect forgeries (also called Message Authentication Code, or MAC)
 - The MIC function is a one-way cryptographic hash function
 - The MIC is calculated over the source and destination MAC addresses and the plaintext after being seeded by the 64-bit MIC key

6.34

- Must be implemented on both MS and BS
- Additional MIC bytes added to packets *before* encryption
- Recipient checks MIC for integrity
- If there is no match, packet is dropped
- Works with TKIP which forces a rekey if there is a MIC validation error

6.35

- Per-packet key mixing is used to break up the correlation between weak keys and the first few bytes of encrypted data
- Two-phase key mixing function combines
 - Temporal key
 - sender's MAC address
 - 48-bit IV (TKIP sequence counter)to generate a per-packet key to seed WEP engine
- The key mixing results in different keys for each direction of communications over each link

6.36

- The per-packet key is 128 bits long and is split into a 104-bit RC4 key and a 24-bit IV for presentation to the WEP engine
- Temporal encryption and MIC keys are used, which are generated as part of the 802.1X exchange
- The TKIP encapsulation process is shown in Figure 5

6.37

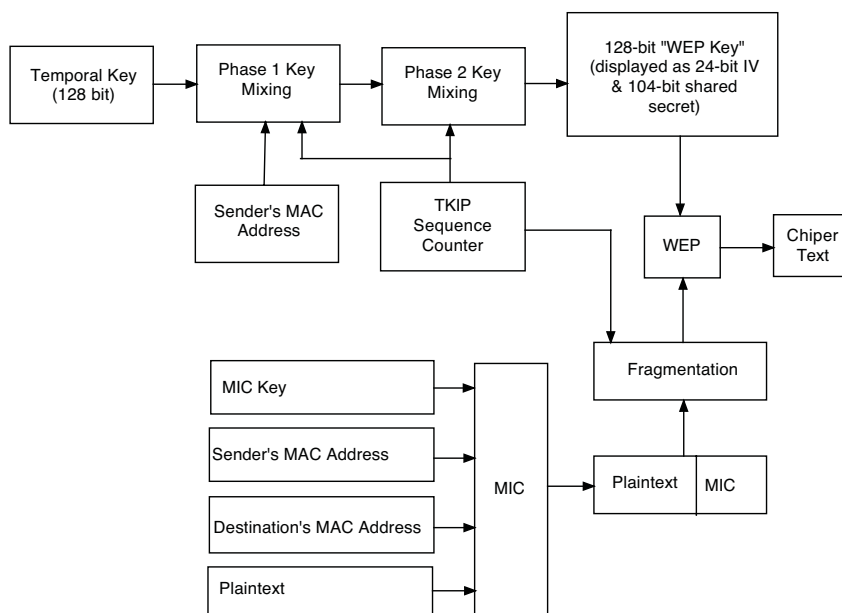


Figure 5 TKIP encapsulation process

6.38

Cryptographic Key Requirements

- Randomly generated to reduce the probability that they can be determined by an adversary or that they will be reused
- Changed frequently to reduce the possibility of discovery through sophisticated cryptanalysis
- Protected while in storage, so that previous communication cannot be deciphered
- Protected during transmission
- Erased completely when no longer needed

6.39

Pairwise Key Hierarchy: Master Session Key

- For unicast communication, a *Master Session Key* (**MSK**), also called *authentication, authorization, and accounting key*, is generated by the EAP framework and the authentication server
 - used for the duration of a user's session
 - 256 bits long

6.40

Pairwise Key Hierarchy: Pairwise Master Key

- The *Pairwise Master Key* (**PMK**), is generated from the MSK
 - MS must store one PMK
 - BS must store one PMK for each associated MS (!)
 - all PMKs are 256 bits long

6.41

Group Key Hierarchy

- Consists of a single key, the *Group Temporal Key* (GTK)
- Generated by BS
- Transmitted to all MSs connected to BS
- 256 bits long for TKIP and 128 bits for WPA2

6.42

Pairwise Transient Keys (1)

KJhole.com

- *Integrity* (or MIC) keys and *encryption* keys are generated from the PMK and some random numbers transported between MS and BS by 802.1X
 - Temporal Key (TK): data encryption key
 - MIC key: data integrity key
 - EAPOL-Key Encryption key
 - EAPOL-Key Integrity key

6.43

Pairwise Transient Keys (2)

KJhole.com

- Pairwise transient keys are unique to each association between an individual MS and the BS

6.44

- Security is one of the largest issues facing the Wi-Fi industry
- WPA is a significant improvement over WEP, but 802.11i is needed to attain a high level of security

Remark : This lecture was partly based on NIST SP 800-97, *Guide to IEEE 802.11i: Establishing Robust Security Networks*