
Indoor WLAN Design

Part VIII: RADIUS, TLS, and Known WPA Attacks

Kjell Jørgen Hole

UiB

Last updated 08.06.08

Mail: Kjell.Hole@ii.uib.no

URL: www.kjhole.com

- Remote Access Dial-In User Service (**RADIUS**)
- Transport Layer Security (**TLS**)
- Known WPA attacks:
 - Man-in-the-Middle (MiM) attacks using ARP spoofing and management frames
 - passphrase vulnerable to offline dictionary attack
 - Denial-of-Service (DoS) attacks

- RADIUS defines:
 - set of common functionality for all authentication servers used with WPA
 - a protocol that allows other devices to access those capabilities
- RADIUS is specified by IETF (Internet Engineering Task Force) and is designed for use with TCP/IP type networks, i.e, a device must use an IP network to talk to a RADIUS server

- RFC-2865: Remote Authentication Dial-In User Service (RADIUS)
- RFC-3579: RADIUS Support For Extensible Authentication Protocol (EAP)
 - contains information on how to use EAP over RADIUS

RFC = Request For Comments

RADIUS Mechanics

KJhole.com

- WPA uses RADIUS to communicate between BS (authenticator) and authentication server
- In RADIUS terms, the BS is the *Network Access Server* (NAS) and the authentication server is the RADIUS server
- RADIUS utilizes encryption and adds integrity check values to transmitted data

RADIUS and WPA

KJhole.com

- In a WPA system, the RADIUS server holds (or has access to) user credentials (e.g., user names and passwords) and authenticates wireless users before they gain access to the network
- RADIUS delivers the *Master Session Key* (**MSK**) to the NAS (remember that the MSK is generated by an ULA protocol, e.g., TLS)

- *Secure Sockets Layer (SSL)*, invented by Netscape, provides a reliable end-to-end security service
 - digital certificates may be used to authenticate both server and client
 - often, only the server has a certificate and the client must provide a password or credit card details
- SSL authenticates one or both parties and then opens a private communication channel with encryption and integrity checking

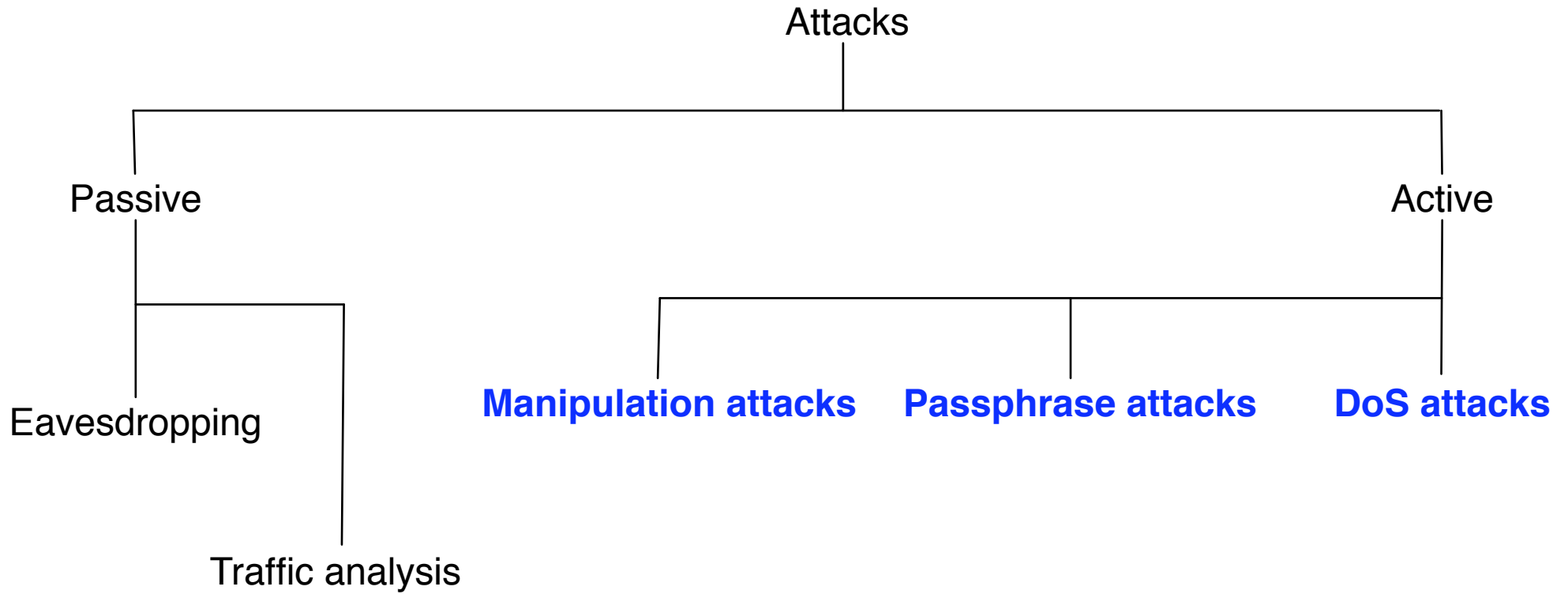
- TLS is:
 - based on the SSL 3.0 Protocol Specification, standardized by IETF in RFC-2246
 - a transport layer protocol utilizing a TCP/IP connection
 - an ULA protocol encapsulated in EAPOL/EAP and RADIUS
 - default authentication method for WPA
- WPA uses TLS between MS and authentication server

WPA and TLS

KJhole.com

- WPA only utilizes the initial authentication/key generating phase of TLS
 - TLS utilizes public key cryptography (certificates) during the initial handshake period to carry out the authentication
 - A symmetric encryption key, i.e. the Pairwise Master Key (PMK), is agreed upon during the public-key phase

Attack Overview



Manipulation Attacks

ARP Spoofing (1)

- *Man-in-the-Middle* (**MiM**) attacks were first introduced in Part V. *Address Resolution Protocol* (**ARP**) spoofing is a type of MiM attack that is difficult to defend against:
 - ARP identifies the MAC address for a given IP address (RFC 826)
 - An MS or BS wanting to communicate with an IP address issues an ARP-Request as a broadcast packet to learn the MAC address corresponding to the IP address
 - Because ARP packets do not have any integrity protection, it is possible to answer with incorrect information, poisoning the ARP cache

ARP Spoofing (2)

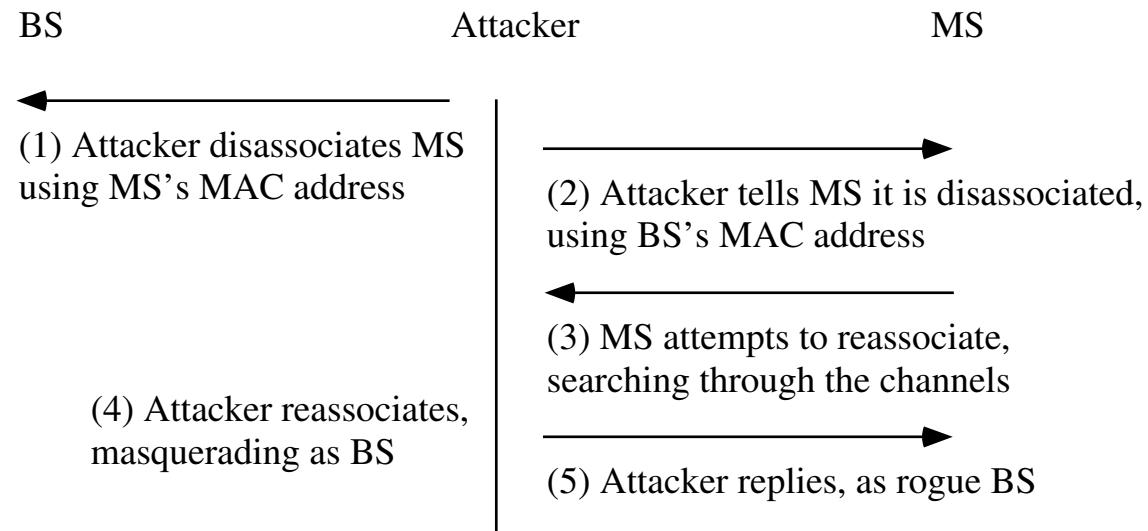
KJhole.com

- The poisoning of the ARP cache causes the traffic to go to the attacker rather than the real recipient
 - as a result, the attacker can obtain passwords, capture sensitive data, and even interface with corporate servers
- Note however that an attacker must have access to the link layer. If encryption is used, the attacker must first break the encryption. With WPA this task may be difficult

Management Frame Attacks

- MiM attacks based on the fact that management frames lack encryption and integrity protection were first described in Part V
 - these attacks can also be carried out against networks utilizing WPA or 802.11i (WPA2)
- The attacker obtains complete control over the traffic stream between an MS and its valid BS
 - if encryption is not used, then the attacker can modify packets before forwarding
 - if encryption is used, packets can be denied or delayed

MitM Attack



Offline Dictionary Attack

www.wifinetnews.com/archives/002452.html

Pre-Shared Key

- In home mode, WPA provides for a *Pre-Shared Key* (**PSK**) as an alternative to 802.1x based key establishment
 - A PSK is a 256 bit number or a passphrase 8 to 63 bytes long
- Each MS may have its own PSK, tied to its MAC address. So far, vendors only provide for one PSK for an entire ESS (?)
- The PSK is the PMK. A formula exists for converting a passphrase PSK to the 256-bit value needed for the PMK

Passphrase Conversion

- A 256 bit PSK is used directly as the PMK. When the PSK is a passphrase, the PMK is derived from the passphrase as follows:

$$\text{PMK} = \text{PBKDF2}(\text{passphrase}, \text{SSID}, \text{SSIDlength}, 4096, 256)$$

- The PBKDF2 method is from PKCS #5 v2.0: Password-based Cryptography Standard
 - the concatenated string of the passphrase, SSID, and the SSID-length is hashed 4096 times to generate a value of 256 bits

Key Hierarchy Revisited (1)

- The PMK is used to generate the following 128 bits long *encryption* and *Message Integrity Code* (MIC) keys:
 - Data Encryption key (Temporal key)
 - Data Integrity key (MIC key)
 - EAPOL-Key Encryption key
 - EAPOL-Key Integrity key (MIC key)
- The EAPOL keys are used to protect the communications between the BS and MS during the initial 4-way handshake

Key Hierarchy Revisited (2)

KJhole.com

- The MIC keys are used during the calculation the MIC function, a cryptographic hash function
- All four keys are referred to as the *temporal keys* because they are recomputed every time an MS associates to the BS
- The collection of all four temporal keys is also called the *Pairwise Transient Key (PTK)* hierarchy

PTK Hierarchy Computation

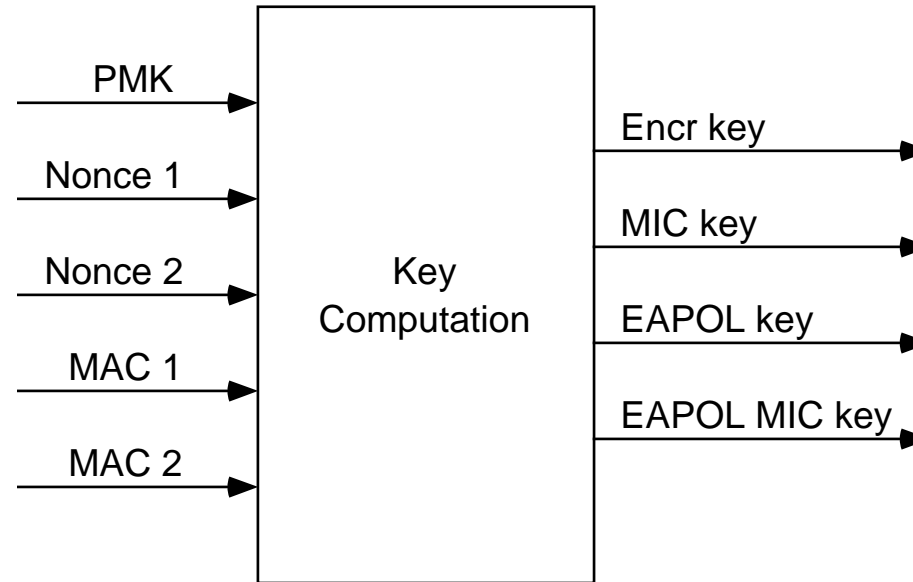


Figure 1: The PTK hierarchy is a keyed-HMAC function using the PMK on the two MAC addresses and the two nonces from the first two packets of the 4-way handshake

PTK Hierarchy Weaknesses

- An attacker can passively listen for the cleartext MAC addresses and nonces available in the first two packets of the 4-way handshake
- !!! As a result, the whole PTK hierarchy falls into the hands of anyone possessing the PSK (i.e. the PMK)
- !!! Even though each MS-BS pairing in the ESS has unique keys (PTK) there is nothing private about these keys to any other device in the ESS

Offline PSK Dictionary Attack (1)

- A passphrase typically provides a relatively low level of security, with keys generated from short passwords subject to dictionary attack
- An attacker that does not know a passphrase-based PSK can attack it with an offline attack (after passively intercepting initial key exchange messages). This is effective for
 - an outsider where there is a single PSK in the ESS
 - an insider where there are unique PSKs

Offline PSK Dictionary Attack (2)

- There exist many dictionary-based cracking programs, and little modification is needed to turn one of those into a weak-WPA-key attack
- A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks. This is considerably longer than most people will be willing to use.
- This offline attack should be easier to execute than the WEP attacks

Use Random Values for the PSK

- Remember that the PSK may be a 256-bit random number. This is a large number for human entry
- Given the nature of the attack, a PSK with only 128 bits of security is really sufficient, 96 bits should be adequate
- Using a relatively small random value represented in hexadecimal, and entering it as a passphrase will expand it to a proper 256-bit PSK

Summary and Consequences

KJhole.com

- Anyone with knowledge of the PSK can determine any PTK in the ESS through passive sniffing of the wireless network
- If a weak passphrase is used, for example, a short passphrase, an offline dictionary attack can readily guess the PSK
- Since the common usage will be a single PSK for the ESS, once this is learned by the attacker, the attacker is now a member of the ESS. He can read and forge any traffic in the ESS

Risks and Recommendation

KJhole.com

- Pre-Shared Keying is provided to simplify deployments in small, low risk, networks
 - the risk of using PSK is relatively high
- !!! PSK can only offer a satisfactory level of security if truly random keys are used
 - PSK should only be used if this is fully understood by the implementors

Denial-of-Service Attacks

Denial-of-Service Attacks

KJhole.com

- *Denial-of-Service* (**DoS**) attacks were first described in Part V
- We saw that DoS attacks at the physical (RF) layer are very difficult to protect against
- In the following we describe a **cryptographic DoS attack** on WPA. We first need to study the MIC

Michael the MIC

- Remember that WPA computes a MIC called Michael. The MIC depends on the MIC key and is computed over the entire (unencrypted) data in a frame
- Since Michael has only 20 bits of security, a randomly chosen MIC value has about one in a million chance of being accepted as valid
- WPA contains **countermeasures** on both the MS and BS to defend against the MIC weakness

Countermeasures on MS (1)

KJhole.com

- MIC failure on a *unicast* message:
 1. Drop any received frames and block any transmitted frames except for 802.1x messages (to allow new key exchange)
 2. Request new pairwise keys by sending an EAPOL message to the authenticator
 3. Log the event and notify the operator if possible

Countermeasures on MS (2)

KJhole.com

- MIC failure on a *multicast* message:
 1. Delete the local copy of the group key
 2. Request a new copy of the group key from authenticator using an EAPOL message (indicates MIC failure)
 3. Log the event and inform system manager if possible

Countermeasures on BS (1)

- MIC failure on a *unicast* message:
 1. Log the event and notify the system operator
 2. Drop any received frames and block any transmitted frames except for 802.1x messages (to allow new key exchange)
 3. If there has been another MIC failure within the last 60 seconds, wait until the 60-second blackout period expires
 4. Initiate a four-way key exchange to establish new pairwise keys

Countermeasures on BS (2)

- When an MS detects a MIC failure on a *multicast* message, it sends an EAPOL message to the BS. The BS carries out the following steps:
 1. Delete the existing group key and stop sending multicast messages
 2. Log the event and notify the system operator
 3. If there has been another MIC failure within the last 60 seconds, wait until the 60-second blackout period expires
 4. Create a new group key and distribute to all stations

Forged Message

- It may look like an attacker only needs to transmit a forged multicast message every 59 seconds to take down the BS and all its MSs
- However, it is more difficult to forge a frame that result in a MIC failure because
 1. A frame must be forged where the TSC (TKIP sequence counter) is correct so the frame is not immediately dropped as "out of sequence"
 2. The TSC is also the IV, and the IV is mixed into the per-packet encryption key. So if the TSC is changed, the frame will not decrypt correctly; the ICV will not give a good value and the frame will be deleted

Cryptographic DoS Attack (1)

KJhole.com

- Hence, to mount a cryptographic DoS attack, it is necessary to:
 1. Capture a valid frame during transmission
 2. Prevent it being delivered to the intended BS
 3. Modify the MIC to make it invalid
 4. Recompute the ICV so that it matches the changed MIC value
 5. Deliver the modified message to BS (before BS receives message with higher IV) to trigger a MIC failure

Cryptographic DoS Attack (2)

KJhole.com

- It seems hard to mount a DoS attack using the Michael countermeasures
 - however, if a MiM attack is established, then the steps 1, 2, 3 and 5 can easily be carried out. Step 4 may also be achieved because the ICV function is a linear CRC

Cryptographic DoS Attack (3)

KJhole.com

- Note that holding someone responsible for this attack could prove difficult because:
 - Physically locating the attacker is made much more difficult than finding an ordinary radio frequency jammer by the fact that only a couple of packets per minute need be transmitted
 - Also the equipment required has innocent uses (unlike a jammer) so prosecuting an apprehended suspect would be more difficult

Conclusions

KJhole.com

- MitM attacks using management frames constitute a real problem
- Offline dictionary attacks on WPA in home mode is also a problem