
Indoor WLAN Design

Part V: 802.11 Security and the Failure of WEP

Kjell Jørgen Hole
UiB

Last updated 25.01.09
Mail: Kjell.Hole@ii.uib.no
URL: www.kjhole.com

Outline

KJhole.com

- Review of two security mechanisms
- Problems with 802.11 security
- Different types of possible attacks
- MS and BS security
- Alternatives to 802.11 security: Captive portals and Virtual Private Networks (VPNs)

Review

5.3

Security Mechanisms

KJhole.com

- **Message Privacy** Protecting the data
- **Key Management** Distribution and protection of secret keys
- **Authentication** Who are you? (Discussed in Part IV)
- **Message Integrity** Preventing modification and insertion
- **Access Control** Should you be allowed to access the network?

5.4

WEP (Wired Equivalent Privacy) A form of wireless security. Encrypts packets at the MAC (Media Access Control) layer. Only MSs with the “secret key” can associate with a BS

- any MS without the key may be able to see network traffic, but every packet is encrypted
- since the encryption takes place at the MAC layer, only the wireless link is protected

5.5

WEP Encryption Details

- Plaintext is encrypted using a stream cipher called RC4. The cipher is *symmetric*, i.e., same key encrypts and decrypts the data
 - a new RC4 key is generated for *each* new packet to avoid synchronization problems caused by lost packets
 - standard specifies 40-bit keys. Vendors have also implemented 104-bit keys (a 24-bit vector is added to obtain a RC4 key)
 - pseudorandom sequence, determined by RC4 key, is XOR'ed with data stream
- The SSID and, in general, management packets are not encrypted

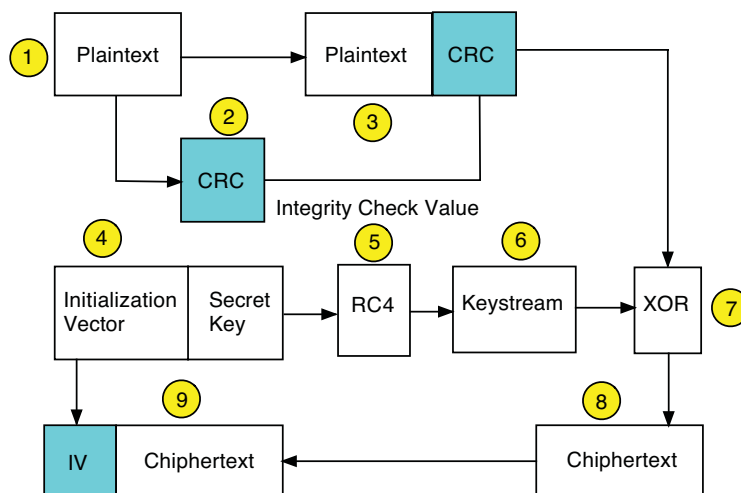
5.6

WEP Integrity

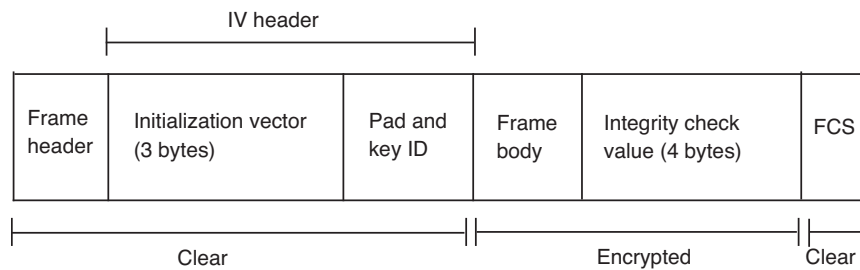
- To protect against tampering, an *Integrity Check Value* (ICV), in the form of a *Cyclic Redundancy Check* (CRC) sum, is computed on the message
- The message and ICV are concatenated *before* encryption
- The receiver recomputes the CRC and verifies that it matches the received CRC value

5.7

WEP Encryption Process



5.8



- A 24-bit IV (Initialization Vector) is combined with the 40-bit key to create a 64-bit RC4 key
- The 2-bit key ID usually specifies that the default pre-shared key is used
- The ICV (Integrity Check Value) is a 4-byte CRC added *before* encryption
- The FCS (Frame Check Sequence) is a 4-byte CRC added *after* encryption

5.9

WEP Decryption

- Decryption is the reverse process of the encryption:
 - IV (in the clear) is prepended to secret key and plugged into RC4 cipher to regenerate key stream
 - key stream is XOR'ed with cipher text
 - ICV is recalculated to detect tampering

5.10

Security Problems

5.11

Integrity (ICV) Problem

KJhole.com

- The idea behind the ICV is to prevent anyone from tampering with the message in transit
- Unfortunately, since a CRC is a *linear* function of the message, it is possible to make controlled modifications to a ciphertext without disrupting the checksum
- *Cryptographically secure* integrity checks are based on (non-linear) keyed hash functions, which are “unpredictable”
- **Remark:** The FCS is only used to detect transmission errors

5.12

Replay Problem

KJhole.com

- WEP has no protection against replay attacks because no IV sequencing rules are implemented
- WEP will accept a packet with a smaller IV value than the IV value in the previous received packet

5.13

Key Management Problem

KJhole.com

- WEP ignores issue of key management. Most vendors do not implement any key distribution mechanism
- Keys must be statically entered into either the driver software or the firmware
- All MSs accessing the same BS use the same pre-shared key—denoted the *default key* in the standard—and can therefore decrypt each others packets

5.14

IV Reuse Leads to Reuse of RC4 Keys

- Weakness in implementation of RC4. Can be cracked if enough traffic can be intercepted:
 - the pre-shared key is static and rarely changed
 - randomness of RC4 key stream depends on IV
 - early implementations reset IV to 0 and increment by 1 for each packet
 - only 2^{24} possible IVs, so repeated after 17 million packets
 - two packets sharing the same IV are likely to use the same RC4 key

5.15

RC4 Weak Keys (1)

KJhole.com

- There exists large class of weak RC4 keys: A small part of a key determines a large number of the initial bits that result in the pseudo-random output of the RC4 cipher
 - can determine weak keys from (cleartext) IVs
- If many packets encrypted with weak RC4 keys can be captured, then—since IV part of keys are known—it is possible to derive the (static) secret part of the RC4 keys with relatively little work
 - must know the first byte of the plaintext

5.16

RC4 Weak Keys (2)

KJhole.com

- The time it takes to crack WEP only grows linearly (not exponentially) with key length because the attack recovers each key byte individually
 - a longer keys is not an efficient defense against a key recovery attack
- **Remark:** many vendors avoid using IVs identifying weak keys

5.17

Message Privacy Problem (1)

KJhole.com

- There are several freely available programs to crack RC4 keys in WEP, including *AirSnort* (<http://airsnort.shmoo.com/>) and *KisMAC* (<http://kismac.macpirate.ch/>)
- AirSnort requires approximately 5-10 million encrypted packets to be gathered. It can then guess the encryption password in under a second

5.18

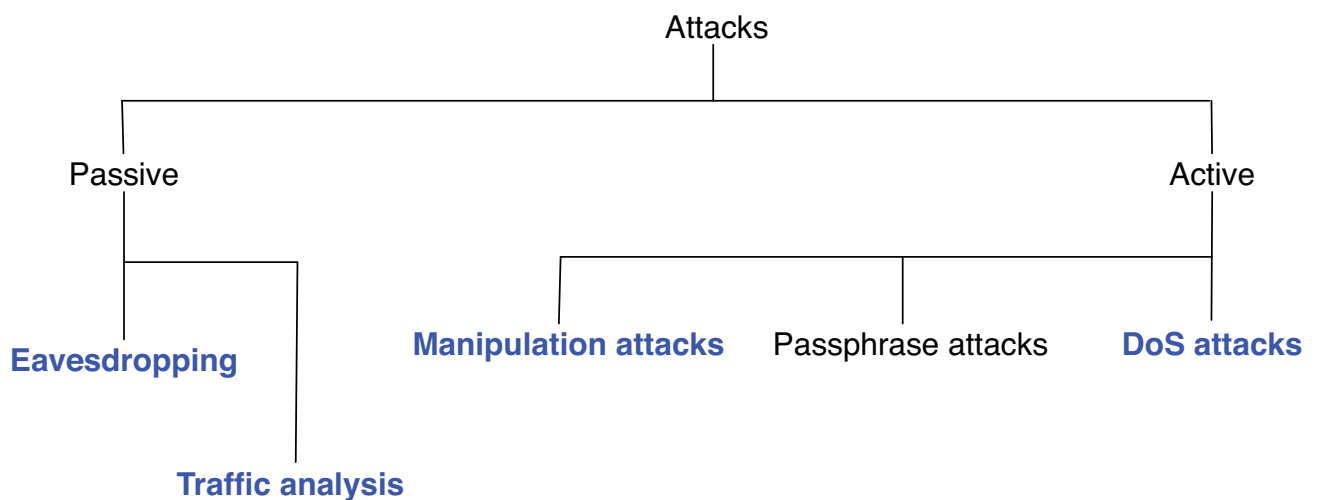
Message Privacy Problem (2)

KJhole.com

- FBI (Federal Bureau of Investigation) demonstrated in 2005 that an active attack only needed 50.000–200.000 packets to crack a 40 bit WEP key
- Only 200.000–700.000 packets were needed to crack a 104 bit key
- Do not rely on WEP because it has been soundly defeated

5.19

Attack Overview



5.20

Eavesdropping Defined

KJhole.com

Eavesdropping Occurs when a nearby attacker can receive the radio waves from a nearby network and reconstruct the frames. All frames can then be examined in real time or stored for later examination

- Because WEP has several flaws, it can be cracked. A user who accesses his mail using the POP or IMAP protocols is then at risk because these protocols often pass the mail over the wireless network without any form of extra encryption

5.21

Traffic Analysis Defined

KJhole.com

- Attacker passively monitors traffic on wireless network to identify communication patterns and participants
- Analysis of traffic patterns can aid in determining the content of the communications
 - short traffic bursts may indicate terminal emulation or instant messaging
 - steady traffic streams may indicate video conferencing or downloading of movies

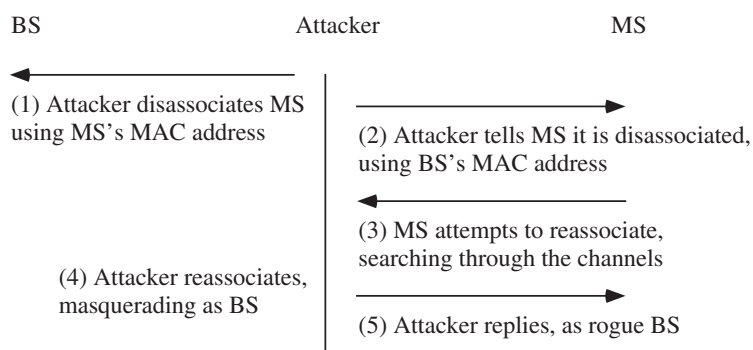
5.22

Manipulation Occurs on a wireless link when an attacker

1. is able to receive the victim's encrypted data, manipulate it, and retransmit the changed data to the victim. The attacker may change emails, instant messages, or database transactions
2. intercepts packets with encrypted data and is able to change the destination address to forwarded the packets across the Internet. While the data is encrypted on the wireless link, the received data over the Internet is decrypted

5.23

Man-in-the-Middle Attack



5.24

Denial-of-Service (DoS) attacks aim to prevent access to network resources by flooding the network with traffic choking the transmission lines. DoS attacks can target different layers of the network

- *Application layer*: Large amounts of requests are transmitted to a network-aware application, e.g. a web server, swamping the server process. The goal is to prevent other users from accessing the service

5.25

- *Transport layer*: Many connection requests are sent to a host. The attack is targeted against the operating system of the victim's computer. A typical attack involves sending an excessive number of TCP connection requests
- **Remark**: At the application and transport layers, there is nothing fundamentally different between DoS attacks on wireless and wired networks. The same is not true for the *network*, *data-link*, and *physical layers*

5.26

802.11 Physical DoS Attacks

KJhole.com

- Attacker can be outside building containing 802.11 network
- Possible to create device that saturates the 802.11 frequency bands with noise and reduce the *signal-to-noise ratio* to an unusable level
- The attacker may also use common commercial devices:
 - 2.4GHz cordless phones
 - large scale Bluetooth deployments

5.27

802.11 Data-Link DoS Attack

KJhole.com

- MSs are programmed to connect to the BS with the strongest signal
- It may be possible for an attacker to install a “malicious” BS with the correct SSID (network name)
- If the “malicious” BS has the strongest signal, then an MS will connect to this BS
- A signal amplifier or directional antenna may be used to create a very strong signal

5.28

- Since an 802.11 network is a *shared medium*, a malicious user can flood the network with traffic, denying access to users associated to the affected BS
- As an example, an attacker can generate a ping (ICMP) flood to saturate the BS
- Given the relatively slow speed of 802.11 networks, a network DoS may happen due to large file transfers or bandwidth-intense applications

5.29

MS and BS Security

5.30

- **Prevent access to MS** through the use of a *firewall* on the MS
 - monitors all data going in and/or out of your computer
 - blocks any suspicious attempts to access your computer
 - provides software switches that block network sharing
- Firewall software is available from a number of companies and is built into some operating systems

5.31

Upper Layer Tunnels: SSL and SSH

- *Secure Sockets Layer* (**SSL**) is a public-key, cryptography-based confidentiality mechanism
 - used in HTTPS to enable secure access to web pages
 - used by some mail clients (POP3 or IMAP over SSL)
- *Secure Shell* (**SSH**) is a secure replacement for *rlogin*. SSH utilizes public-key cryptography like SSL, but does not rely on a trusted authority to issue public-key certificates

5.32

The BS controls access to the wireless network using:

Closed network —BSs do not broadcast SSID in the Beacon frames. Hence, an MS must specify the “name” of the wireless network to associate with a BS

MAC address filtering —An MS attempting to access a wireless network must have its MAC address listed in tables contained in the BSs

Closed network and MAC address filtering are not part of the 802.11 standard. However, these techniques are implemented by vendors

5.33

- The SSID is broadcast in the clear by MSs wanting to join the network
- An attacker only has to sniff packets waiting for a probe request containing the SSID

5.34

Do Not Trust MAC Filtering

KJhole.com

- The MAC address is broadcast in the clear with each frame, even when WEP is enabled
- Many wireless cards allow the MAC address to be changed by the user
- The change can be made via the driver GUI in Windows or the *ifconfig* command in Linux/BSD

5.35

Alternative: Captive Portal

KJhole.com

- A captive portal is a router or gateway host that will not allow traffic to pass until *authentication conditions* are met. The operation of a portal is:
 1. Assign a new MS on the network an IP address through DHCP
 2. Block traffic, except to the captive portal server
 3. Redirect any web traffic to the captive portal
 4. Display terms of use and/or login screen
 5. Allow access after user has accepted terms and/or logged in

5.36

Closed and Open Portals

KJhole.com

Closed Portal Used to limit the access to a known set of users with user names and passwords

Open Portal Requires acceptance of terms before access is granted

- The *NoCat* portal (<http://nocat.net>) supports both closed and open modes. When running in closed mode *NoCat* uses encrypted communications with a central authentication server to validate passwords

5.37

Disadvantages of Portals

KJhole.com

- Each time a laptop is turned on, the web browser must be loaded before a new connection can be established
- The web browser must run in the background at all times
- It is difficult to keep the connection alive on some platforms

5.38

- A **Virtual Private Network** (VPN) uses authentication and/or encryption to connect users to a private network over a public network, usually the Internet (see <http://www.vpnc.org>)
- VPN is often based on the Point-to-Point Tunneling Protocol (PPTP) made by Microsoft
- PPTP may be used to set up an encrypted connection over TCP/IP links, typically between a person and his home office
 - PPTP also supports several authentication protocols

5.39

- When an MS first connects to a BS:
 1. the MS receives a “private” IP address from DHCP server
 2. the MS connects to a VPN server using the private IP address and transmits the user’s login name and password
 3. the VPN server verifies the login name and password and returns a “real” routable IP address

5.40

Wireless VPN (2)

KJhole.com

- All outgoing traffic from the MS passes through a PPTP tunnel to the VPN server which transmits the traffic to its final destination. The return traffic is first received by the VPN server and then transmitted through the PPTP tunnel to the MS
- A VPN client must be installed on the MS. There exist VPN clients for many different operating systems

5.41

Disadvantages of VPN

KJhole.com

- Because interoperability between vendor's VPN products is not assured, you must buy server and client software from the same company
- VPN clients can sometimes be intrusive, slowing down communication and limiting the types of operations that can be performed on an MS
- If you have many VPN users, then you need a high-capacity VPN server

5.42

- IPsec is a trio of extensions that provide added security for IP packets
 - AH (Authentication Header) for integrity
 - ESP (Encapsulating Security Payload) for encryption
 - ISAKMP (Internet Security Association and Key Management Protocol) for authentication and key management—part of Internet Key Exchange (IKE)
- Extension to layer 3

5.43

- IPsec is a very powerful protocol
- IPsec can offer a high degree of security
- IPsec can be difficult to set up
- IPsec will eventually become universal

5.44

- Do not rely on the WEP encryption, there exist several programs to crack keys
- Many attacks are possible
- MSs should employ firewalls and use encryption (SSL, SSH)
- Possible to use captive portals or VPN for authentication, access control, and encryption
- For more information, see www.nowires.org/Wi-Fi/