

WLAN Technologies and IT-Security

From 1G to 4G
Using
the Family of IEEE 802.1X standards

Outline

- Goals of WLAN Technologies from a users' perspective
- The IEEE 802.1X family of WLAN protocols
- Generations
 - 1G (first generation)
 - Basic operations in a WLAN
 - Forms of attacks (passive/active)
 - 2G (second generation)
 - WEP and RC4
 - The IEEE 802.11g standard
 - 3G (third generation)
 - The IEEE 802.11i standard
 - Authentication and (implemented) encryption methods
 - WiFi Alliance
 - Comparison of WEP, WAP and RSN
- Needs and perspectives of the fourth generation (4G)

Goals of WLAN Technologies

- Access to information infrastructure
- Flexibility
- Support ubiquitous computing
- From a user-perspective: quickly installed in an ad hoc configuration
 - without pre-planning and
 - without supporting backbone network(s)

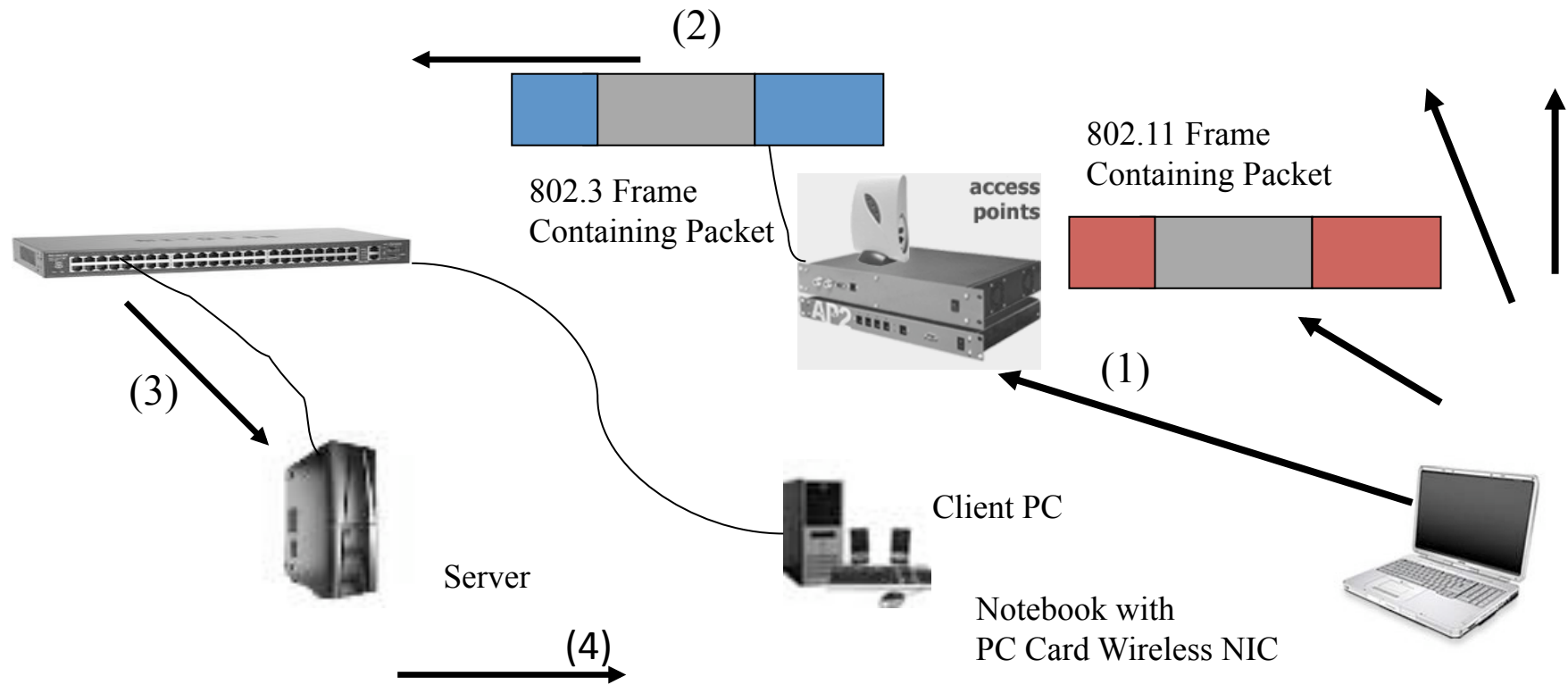
WLAN 802.11 Standard

- IEEE Std 802.11a™-1999 (Amendment 1)
 - IEEE Std 802.11b™-1999 (Amendment 2)
 - IEEE Std 802.11b-1999/Corrigendum 1-2001
 - IEEE Std 802.11d™-2001 (Amendment 3)
 - IEEE Std 802.11g™-2003 (Amendment 4)
 - IEEE Std 802.11h™-2003 (Amendment 5)
 - IEEE Std 802.11i™-2004 (Amendment 6)
 - IEEE Std 802.11j™-2004 (Amendment 7)
 - IEEE Std 802.11e™-2005 (Amendment 8)
 - IEEE Std 802.11n™-2007 (Super Fast WLAN)
-
- IEEE Std 802.1X – latest version 2007 on the Web
<http://standards.ieee.org/getieee/download/802.11-2007.pdf>

1G – First Generation WLAN Technology

- Related (quasi-)standards
 - IEEE Std 802.11a™-1999 (Amendment 1)
 - IEEE Std 802.11b™-1999 (Amendment 2)
 - IEEE Std 802.11b-1999/Corrigendum 1-2001
- A WLAN consists of a set of wireless stations (STx) called a Basic Service Set (BSS), an Access Point (AP) [former: Point Connector (PC)] which arbitrates the access of the wireless stations
- 1998/99: Specification of WLAN connections
 - No security issues
 - Designed for stations to find and hear another one
 - Simple authentication via session key
 - Examples: e.g. GPS-standards and TCP/IP implementations
- A basic architecture implements the WLAN connection

Basic architectures of 802.11 WLANs



- (1) When a wireless station has a message to send, it places a packet in an 802.11 frame and transmits the frame to the access point.
- (2) The access point removes the packet from the 802.11 frame, and places the packet in an Ethernet frame, and
- (3) sends the Ethernet frame to the server.
- (4) When the server replies, its packet contained in the Ethernet frame goes to the access point. The access point removes the packet from the Ethernet frame, and places the packet in the 802.11 frame, and transmits the 802.11 frame.

802.11 Wireless LAN family of standards

- Basic operation (see Figure above)
 - Main wired network for servers
 - Wireless stations with wireless NICs (Network Interface Card)
 - Access point
 - Access point and bridges
 - Propagation distance: Farther for attackers than users
 - Handoffs as wireless stations move from one access point to another

802.11 Wireless LAN family of standards

Standard	Rated Speed (a)	Unlicenced Radio Band	Effective Distance (b)
802.11b	11 Mbps	2.4 GHz	~ 30 - 50 meters
802.11a	54 Mbps	5 GHz	~ 10 - 30 meters
802.11g	54 Mbps	2.4 GHz	Outdoor More than 1000 meters

a) Actual speeds are much lower and decline with distance

b) These are distances for good communication; attackers can read some signals and attack frames from longer distances.

WLAN Technologies and Known Problems

- Classification of active and passive attacks
 - Active attacks, e.g.
 - replay messages,
 - denial-of-service attacks,
 - man-in-the-middle,
 - spoofing,
 - sniffing
 - Passive attacks, e.g.
 - eye-dropping,
 - traffic analysis,
 - man-in-the-middle,
 - sniffing

WLAN Problems – Passive Attacks

- Passive attacks
 - An existing signal is needed
 - Decryption, if needed
 - Get data from signal and traffic, e.g. spoofing a MAC address
 - Spoofing from outside the building
 - Access points coverage outside the buildings is seldom taken into account for IT-security
 - Check the applied direction attendance

WLAN Problems – Active Attacks

- Active attacks
 - Denial-of-Service attack: Radio signal
 - Microwave method for making noise
 - Flooding an access point (AP)
 - Spoofing MAC-address
 - Send a disconnect message to access point
 - Problem
 - Replay attack
 - SSID (to access the AP)
 - Message modification
 - Rogue access points

2G – Second Generation WLAN Technologies

- IEEE Std 802.11d™-2001 (Amendment 3)
- IEEE Std 802.11g™-2003 (Amendment 4)
- Authorization and privacy matters
- Watch out: Privacy = protection in our terminology

2G – Security Aspects

- Wired Equivalent Privacy (WEP)
 - RC4 algorithm (64-bit / 128-bit key)
 - WEP is unusable for high security applications
 - Problem: insecure key exchange
 - First step: React to specific computers using MAC addresses of the network adapter
 - Second step: Packets are encrypted with private key(s) before sending and an integrity check

RC4 Stream Cipher (Rivest 1987)

Short overview

- Byte-oriented operations
- Use of a random permutation
- 8-16 machine operations are required per output byte
- Cipher runs quickly in software
- RC4 is implemented in
 - SSL/TLS (for Web communications)
 - WEP
 - Newer WiFi Protected Access

RC4 in brief

- A variable-length key of 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S , with elements $S[0], \dots, S[255]$
- At all times, S contains a permutation of all 8-bit numbers from 0 through 255
- For encryption and decryption a k -byte is generated from S by selecting one of the 255 entries in a systematic fashion; e.g. in cycles
- As each value of k is generated, the entries in S are once permuted.
- RC4 consists of
 - An initialization of S and
 - A stream generation phase

RC4 – Initialization of S

- To begin, the entries of S are set equal to the values from 0 to 255 in ascending order; that is $S[0]=0$, $S[1]=1$, ..., $S[255]=255$.
- A temporary vector T is also created.
 - If the length of the key k is also 256 bytes, the K is transferred to T.
 - Otherwise, for a key of length keylen, the first keylen elements of T are copied from k and then k is repeated as many times as necessary to fill out T.
- These preliminary operation can be summarized as follows
for i=0 **to** 255 **do**
S[i]=i; T[i] = k (i mod keylen);

RC4 – Initialization of S

- We use T to produce the initial permutation of S
 - This involves starting with S[0] and going through S[255], and, for each S[i], swapping S[i] with another byte according to the scheme in T[i]

- The initial permutation can be summarized as follows

j=0;

for i=0 **to** 255 **do**

 j=(j+S[i]+T[i]) mod 256

 swap(S[i],S[j])

RC4 – Stream Generation

- Once the vector S is initialized, the input key is no longer used.
- Stream generation involves cycles through all elements of $S[i]$, and, for each $S[i]$, swapping $S[i]$ with another byte in S according to a dictated by the current configuration of S
- After $S[255]$ is reached, the process continues over again $S[0]$
- The stream generation phase can be summarized as follows

RC4 – Stream Generation

$i, j = 0;$

while (true)

$i = (i + 1) \bmod 256;$

$j = (j + S[i]) \bmod 256;$

swap($S[i], S[j]$);

$t = (S[i] + S[j]) \bmod 256;$

$k = S[t]$

RC4 – Encryption and Decryption

- To encrypt, XOR the value k with the next byte of the plaintext
- To decrypt, XOR the value k with the next byte of ciphertext

2G – 802.11g Standard

- Security issues
 - Authentication with key exchange (symmetric encryption)
 - More expensive devices
 - asymmetric encryption and
 - Message integrity
 - RC4 algorithm
 - RC4 is not enabled by default
 - 40-bit encryption key are to small
 - suitable length of keys will be discussed later, when we consider applied encryption methods
 - Non-standard 128-bit, really 104-bit (with 24-bit initialization vectors), (256-bit resp. 232-bits) are reasonable interoperable
 - AES is limited by bandwidth and computational power and is impractical in this stage.

3G – Third Generation WLAN Technologies

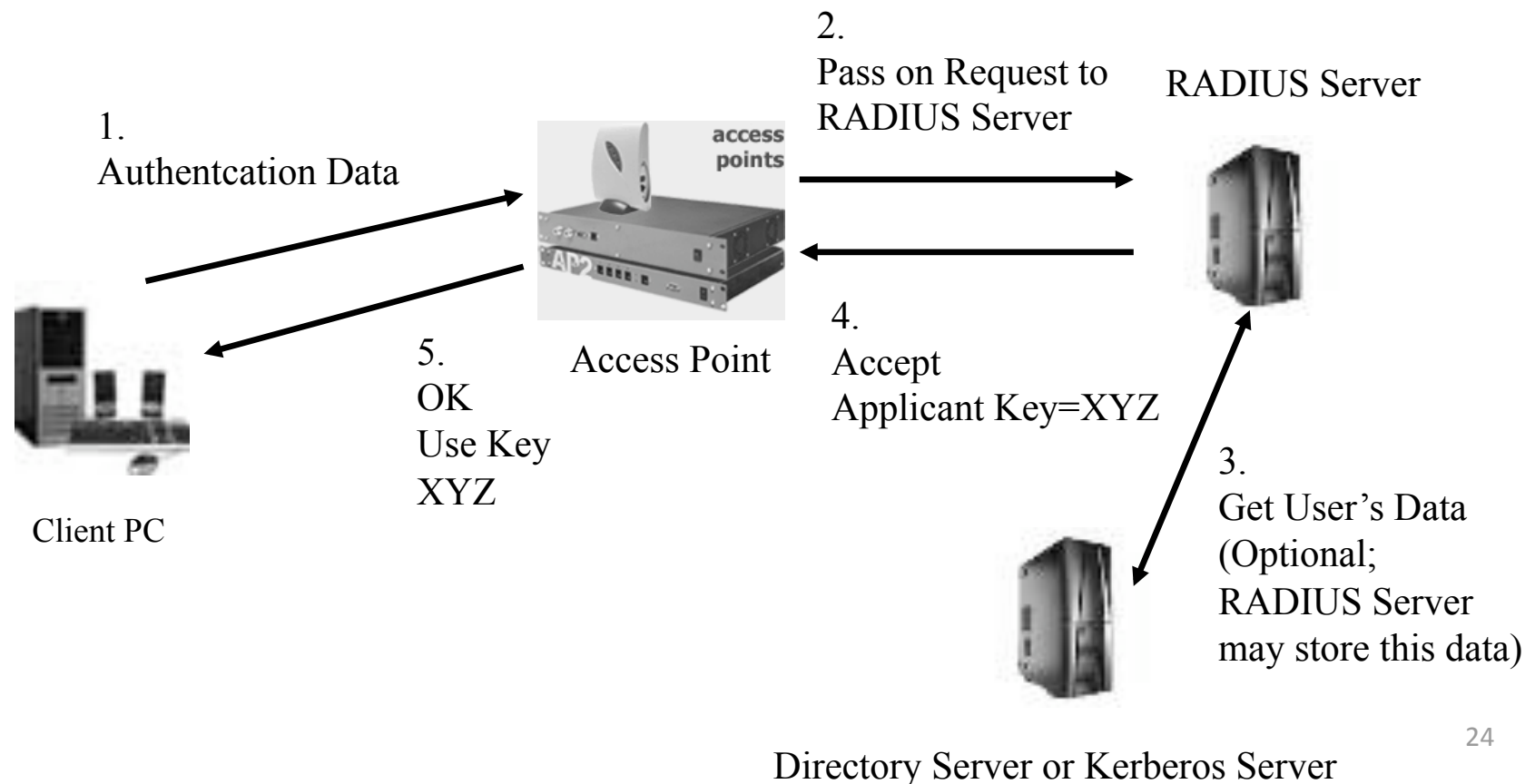
- IEEE Std 802.11hTM-2003 (Amendment 5)
- IEEE Std 802.11iTM-2004 (Amendment 6)
- Extension of 802.11g concerning security issues
- Problems solved: bandwidth and computational power

3G – 802.11i Standard

- The 802.11i standard standardizes wireless encryption protocols
 - Extensible Authentication Protocol (EAP)
 - Protected EAP (PEAP)
 - Tunneled Transport Layer Security (TTLS)
 - Temporal Key Integrity Protocol (TKIP)
 - Advanced Encryption Standard (AES)
 - WiFi Protected Access (WPA)
- „Frazed” standard (2006)

802.11i Standard

- 802.11i specifies modifications in the WLAN infrastructure by adding
 - An authentication server and
 - A user data server (e.g. for supporting PEAP)
- Authentication for 802.11i WLANs



802.11i Standard and Encryption

- Individual keys given out to access point
- Multiple authentication options (see above encryption protocols)
 - Uses the Extensible Authentication Protocol (EAP), for instances, or
 - TLS
 - In strongest option, both client and access point must have digital certificates
 - Difficult to create public key infrastructure for digital certificates
 - Option for only access point to have a digital certificate
 - Still no authentication for a certain station
 - TTLS (Tunneled TLS))
 - Access point must have digital certificate
 - Station authenticated with password or other weak approach
 - MD5 CHAP
 - Authenticates only wireless station, with reusable password,
 - but MD5 can be insecure (see practical exercises)

802.11i Standard and Encryption

- Temporal Key Integrity Protocol (TKIP)
 - Temporary stopgap method; many older systems must be upgraded
 - Key changed every 10'000 frames to foil data collection for key guessing
- Wireless Fidelity Alliance (“Wi-Fi”)
 - Wireless Protected Access (WPA) will require the phased implementation of TKIP

WiFi Alliance (www.wi-fi.org)

- To act against security features deficits of WEP
 - Improved data encryption through TKIP
 - User authentication
 - (Message) Integrity
- Problems in WEP in more detail
 - Master keys are used directly in WEP
 - WPA – hierarchy of keys is used
 - Key management and updating is poorly provided for in WEP
 - IV values can be reused / IV length is too short
 - Weak IV values are susceptible to attack
 - Message integrity checking is ineffective
- Drawback associated with WPA
 - 802.11i passwords are too short
 - Passwords with more than 20 characters are requested that are too long for keeping in mind for many users
 - As a consequence an offline attack would be easier to execute than the WEP attacks
- WiFi certifies products in respect of the (current) 802.11i standard

Comparison of WEP Mechanism, WPA and RSN Security Protocols (802.11i)

Table-1. Comparison of WEP Mechanism, WPA and RSN Security Protocols.

Features of Mechanism	WEP	WPA	RSN
Encryption Cipher Mechanism	RC4 (Vulnerable - IV Usage)	RC4 / TKIP	AES / CCMP CCMP / TKIP
Encryption Key Size	40 bits *	128 bits	128 bits
Encryption Key Per Packet	Concatenated	Mixed	No need
Encryption Key Management	None	802.1x	802.1x
Encryption Key Change	None	For Each Packet	No need
IV Size	24 bits	48 bits	48 bits
Authentication	Weak	802.1x - EAP	802.1x - EAP
Data Integrity	CRC 32 - ICV	MIC (Michael)	CCM
Header Integrity	None	MIC (Michael)	CCM
Replay Attack Prevention	None	IV Sequence	IV Sequence
(*) Some vendors apply 104 and 232 bits key, where the 802.11 requires a 40 bits of encryption key.			

4G – Fourth Generation of WLAN Technologies

- IEEE Std 802.11e™-2005 (Amendment 8)
- IEEE Std 802.11n™-2007 (Super Fast WLAN, current standard)
 - 3G enhancement of computable power
 - 4G wider bandwidth
 - To support a variety of security-sensitive applications, like m-banking and m-commerce
- E.g. AES can now be implemented in an effective manner or
- Robust end-to-end security solutions (E2E) as known from the “traditional” networks
- On-going process!

Some References

- Barka, S.B.; Mohammed, E.E.; Hayawi (2006): End-to-End Security Solutions for WLAN: A Performance Analysis for Underlying Encryption Algorithms in Lightweight Devices. IWCMC '06, July 3-6, 2006, Vancouver, British Columbia, Canada, p. 1295-1300.
- Bhagyavati; Summers, W. S.; DeJoie A (2004): Wireless Security Techniques: An Overview. InfoSecCD Conference '04, September 17-18, 2004, Kennesaw, GA, USA, p. 82-87.
- Bulbul, H.H.; Batmaz, I.; Ozel, M. (2008): Network Security Comparison of WEP, Mechanism, WPA, and RSN Security. E-Forensics 2008, January 21-23, 2008, Adelaide, Australia.
- Eckert, C. (2007): IT-Sicherheit: Konzepte, Verfahren, Protokolle. 5. überarbeitete Auflage.
- Gill, R.; Smith, J.; Clark, A. (2006): Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks. AISW-NetSec 2006, Hobart, Australia Conferences in Research and Practice in Information Technology (CR-PIT), Vol. 54. R.Buyya, T.Ma, R. Safavi-Naini. C. Steketee and W. Susilo (Eds.)
- Panko, R.R.(2004): Cooperate Computer and Network Security. Pearson Education. Upper Saddle River.
- Park, S.H; Ganz, A.; Ganz, Z (1998): Security protocol for IEEE 802.11 wireless local area network. Mobile Networks and Applications 3, p.237-246