FACULTEIT INGENIEURSWETENSCHAPPEN

Network and Computer Security

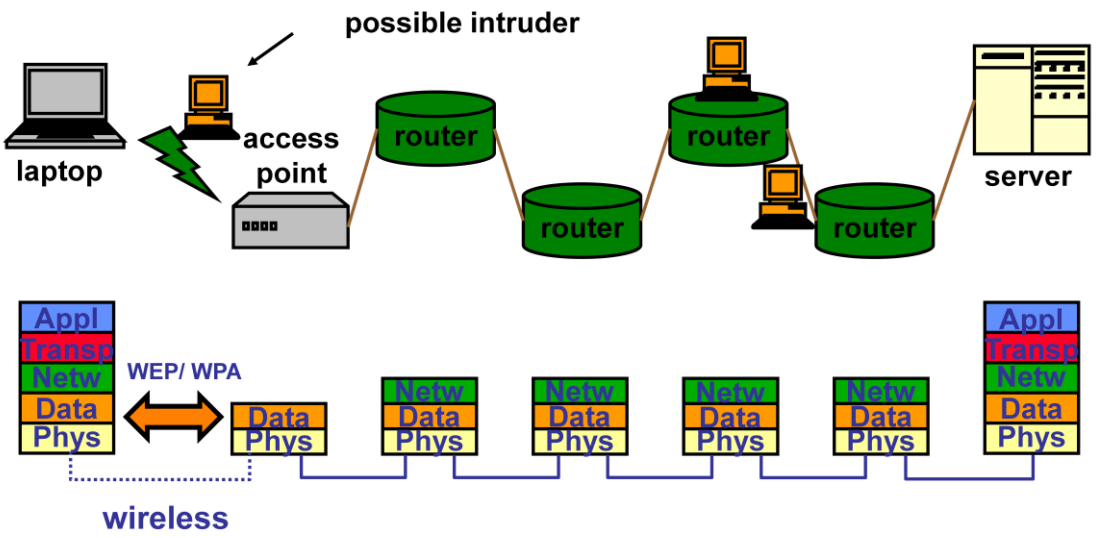
Chapter 3 – Network and communication security

Prof. dr. ir. Eli De Poorter

Overview

- Network model
- Secure configuration of devices
- Exchanging keys
- Secure networking protocols
  - Transport layer: TLS & SSL
  - Network layer: IPSec & VPN
  - **Data link layer: WEP & WPA**
- Firewalls

Datalink security



Data link security

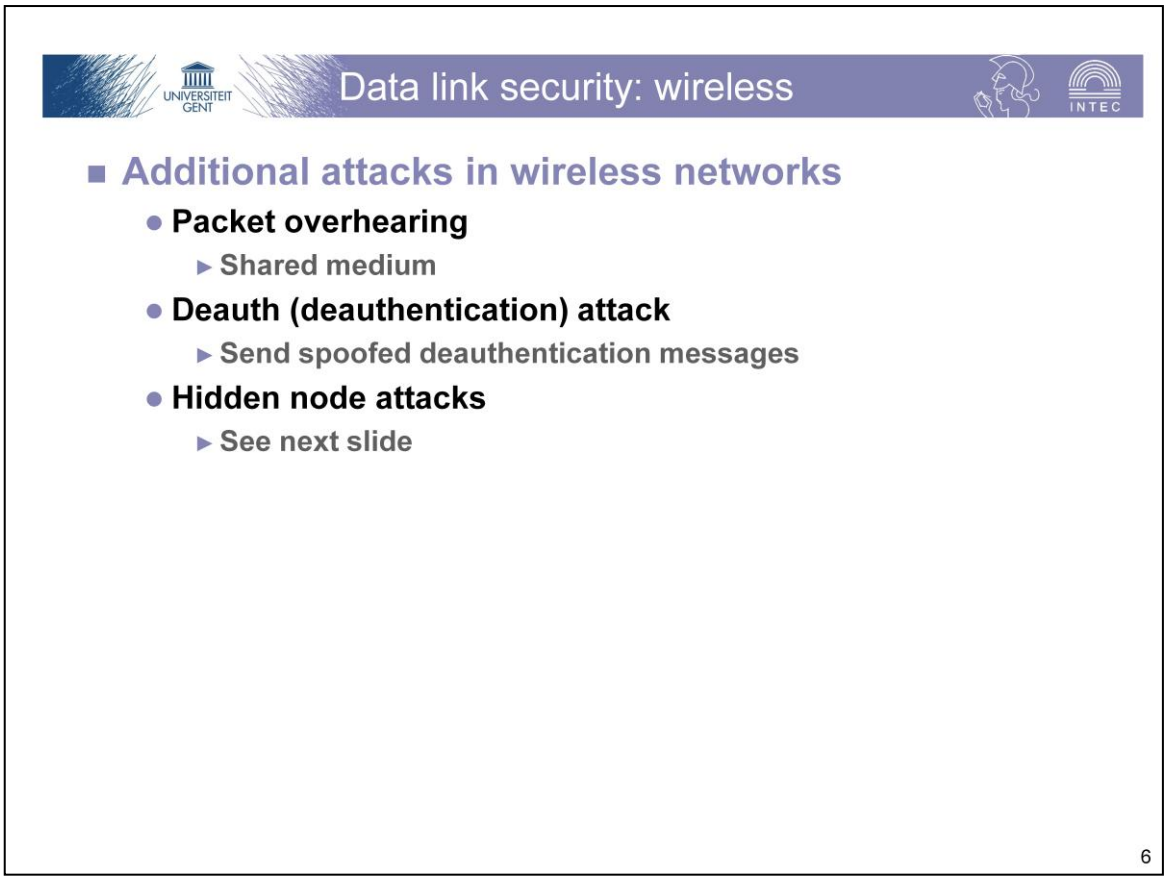
- **Common attacks**
  - **Content Address Memory (CAM) table exhaustion attack**
    - Through flooding, fill the CAM table that stores which device should be contacted through each switch port
    - Device defaults to broadcasting
    - Turns a switch into a hub
  - **Address Routing Protocol (ARP) spoofing**
    - Data link layer is responsible for mapping logical (IP) to physical (MAC) addresses
    - Broadcast spoofed IP packets
  - **Dynamic Host Configuration Protocol (DHCP) starvation**
    - Continue sending DHCP requests

4

The network interface layer, commonly referred to as the data link layer, is the physical interface between the host system and the network hardware. It defines how data packets are to be formatted for transmission and routings. Some common link layer protocols include IEEE 802.2 and X.25. The data link layer and its associated protocols govern the physical interface between the host computer and the network hardware. The goal of this layer is to provide reliable communications between hosts connected on a network.

Data link security

- **Example data layer security protocols**
  - **CHAP**
  - **PPTP**
  - **L2F**
  - **ECP**
  - **EAP**



Packet overhearing

Due to the shared nature of the wireless medium, all packets can be overheard

Hidden node attacks

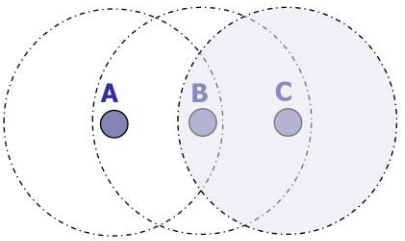
In a wireless network many hosts or nodes are sharing a common medium. If nodes A and B are both wireless laptop computers communicating in an office environment their physical separation may require that they communicate through a wireless access point. But only one device can transmit at a time in order to avoid packet collisions. Prior to transmitting, Node A sends out a Ready to Send (RTS) signal. If it is not receiving any other traffic the access point will broadcast a Clear to Send (CTS) signal over the network. Node A will then begin transmitting while Node B knows to hold off transmitting it's data for the time being. Even though it cannot directly communicate with Node A, i.e. Node A is hidden, it knows to wait based on its communication with the access point. An attacker can exploit this functionality by flooding the network with CTS messages. Then every node assumes there is a hidden node trying to transmit and will hold its own transmissions, resulting in a denial of service. Preventing hidden node attacks requires a network tool. Such a tool monitors access point traffic and develops a baseline level of traffic. Any spikes in CTS/RTS signals are assumed to be the result of a hidden node attack and are subsequently blocked.

Deauth (deauthentication) attack

Any client entering a wireless network must first authenticate with an access point (AP) and is thereafter associated with that access point. When the client leaves it sends a deauthentication, or deauth, message to disassociate itself with the access point. An attacker can send deauth messages to an access point tied to client IP addresses thereby knocking the users off-line and requiring continued re-authenticate, giving the attacker valuable insight into the reauthentication handshaking that occurs. To mitigate this attack, the access point can be set up to delay the effects of deauthentication or disassociation requests (e.g., by queuing such requests for 5–10 seconds) thereby giving the access point an opportunity to observe subsequent packets from the client. If a data packet arrives after a deauthentication or disassociation request is queued, that request is discarded since a legitimate client would never generate packets in that order

Data link security: hidden node

- **Hidden node problem**

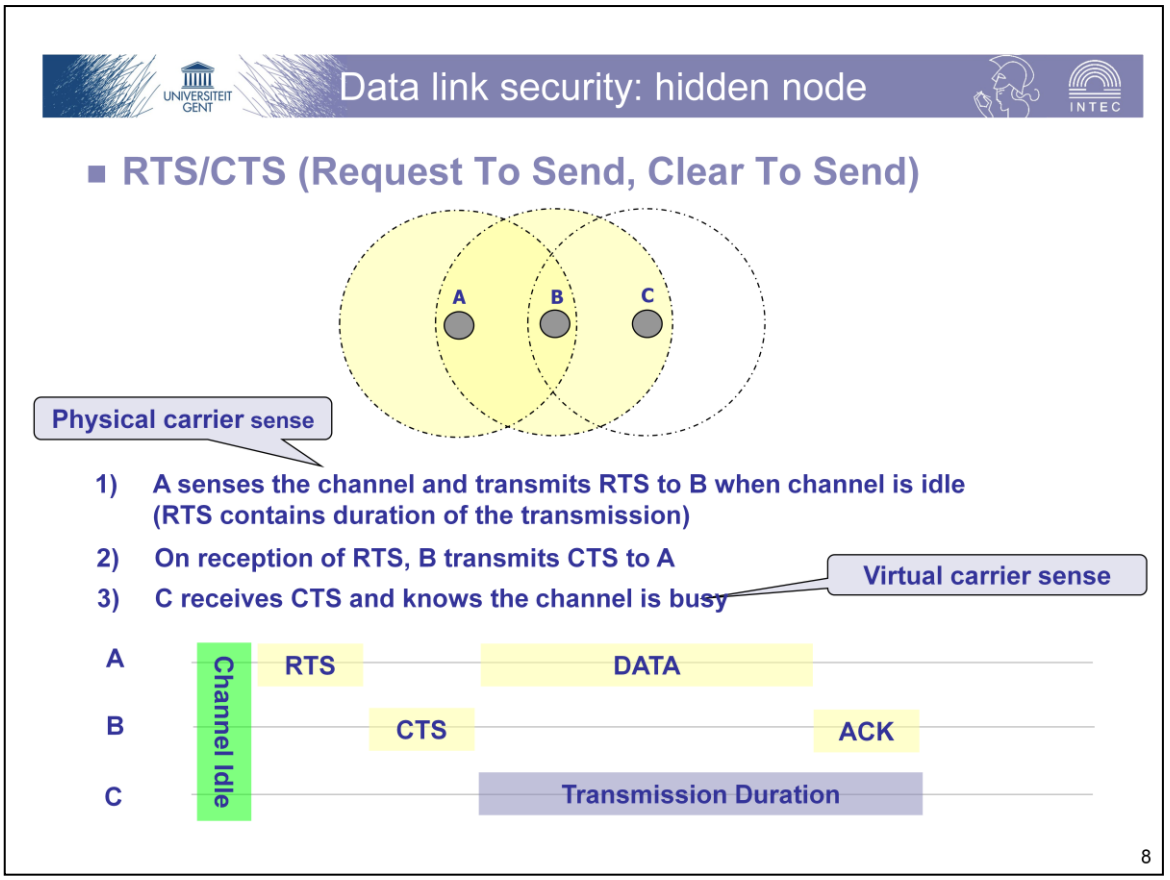


1) **A senses the channel (CS) and transmits to B when channel is idle**
2) **C cannot detect the transmission of A and thinks the channel is idle (CS fails)**
3) **C transmits and a collision occurs at B (CD fails at A ➔ A is hidden for C)**

➔ **Reduced throughput**

7

Consider the scenario with three wireless devices as shown in the figure. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission range of C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa. A starts sending to B, C does not receive this transmission. C also wants to send something to B and senses the medium. The medium appears to be free, the carrier sense fails. C also starts sending causing a collision at B. But A cannot detect this collision at B and continues with its transmission. A is hidden for C and vice versa.



This slide shows the same scenario as previously shown in the slide on **hidden terminals**. Remember, A and C both want to send to B. A has already started the transmission, but is hidden for C, C also starts with its transmission, thereby causing a collision at B.

A frequently used solutions is to ensure A does not start its transmission at once, but sends a **request to send (RTS)** first. B receives the RTS that contains the name of sender and receiver, as well as the length of the future transmission. This RTS is not heard by C, but triggers an acknowledgement from B, called **clear to send (CTS)**. The CTS again contains the names of sender (A) and receiver (B) of the user data, and the length of the future transmission. This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission. After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS toward B. A collision cannot occur at B during data transmission, and the hidden terminal problem is solved – provided that the transmission conditions remain the same. (Another station could move into the transmission range of B after the transmission of CTS.) Still, collisions can occur during the sending of an RTS. Both A and C could send an RTS that collides at B. RTS is very small compared to the data transmission, so the probability of a collision is much lower. B resolves this contention and acknowledges only one station in the CTS (if it was able to recover the RTS at all). No transmission is allowed without an appropriate CTS.

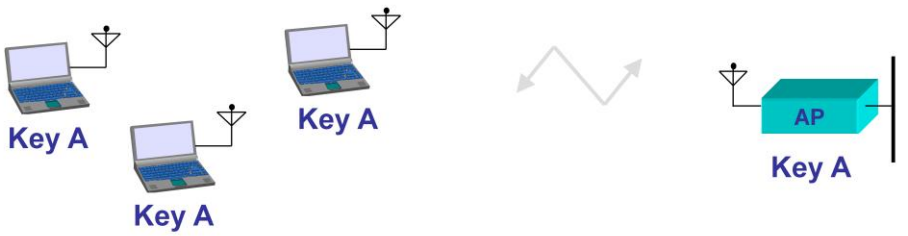
Data link security: wireless

- Need for additional security mechanisms
- WLAN security solutions
  - **Wired Equivalent Privacy (WEP):**
    - Part of the original 802.11 standard. No key management, also several other weaknesses.
  - **WiFi Protected Access (WPA):**
    - Interim solution offers key management using the 802.1X authentication framework, plus improved encryption and integrity checking.
  - **IEEE 802.11i (WPA2):**
    - Same as WPA, except improved encryption (AES).

WEP

- IEEE 802.11 specifies **as an option** the use of WEP which can take care of the following security mechanisms:
  - **Authentication ("shared key" user authentication)**
  - **Confidentiality (RC4 stream cipher encryption)**
  - **Integrity checking (CRC-32 integrity mechanism)**
- It lacks
  - **key management**
  - **protection against replay attacks**

- No key management in WEP



No key management in WEP ⇔ every wireless station and AP has the same "preshared" key that is used during authentication and encryption. This key is distributed manually (=> insufficient for enterprise applications).

- Problems with preshared keys

Manual key management is not very flexible

Same key for everybody:

In a large network, users may wish to have independent secure connections. Just a single non-honest WLAN user can break the security.

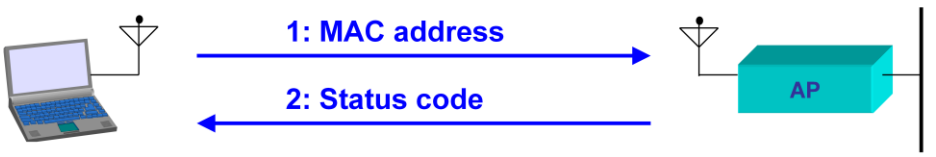
Static key:

Since it is relatively easy to crack WEP encryption in a reasonably short time, the keys should be changed often, but the preshared key concept does not support this.

WLAN authentication methods

- Open system authentication (specified in WEP)
  - actually no authentication at all
- Shared key authentication (specified in WEP)
  - weak due to non-existing key management
- Authentication using SSID of AP
- MAC address filtering
- IEEE 802.1X authentication (specified in WPA)
- SIM/AuC authentication (in operator-based network)

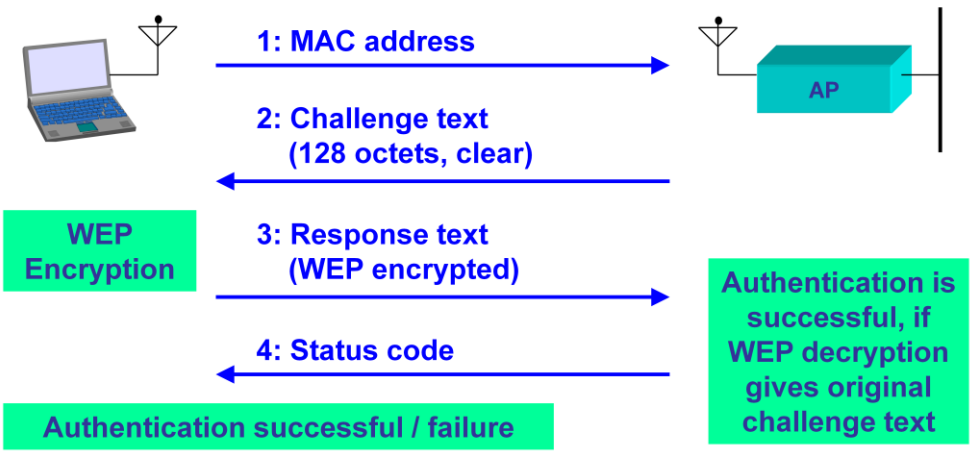
- Open system authentication



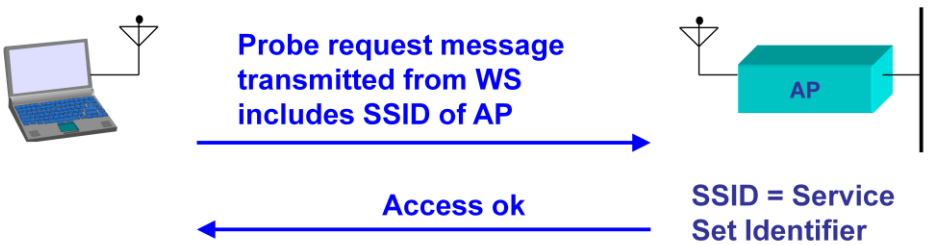
Status codes are defined in IEEE 802.11

Status code	Meaning
0	Successful
1	Unspecified failure
:	:
15	Authentication rejected (cause x)
:	:

- Shared-key authentication

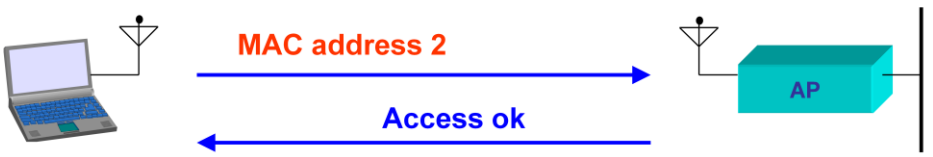


- Authentication using SSID of AP



Not very secure: SSID is transmitted unencrypted over the wireless network and can be easily captured by an attacker.

- MAC address filtering



Accepted MAC addresses:

MAC address 1
MAC address 2
MAC address 3
MAC address 4
:

Not very secure: Attacker can read MAC address of a wireless station attached to the WLAN and replace own MAC address with this stolen MAC address.

WEP Vulnerabilities

- **Small and static keys :**
  - **Actual keyspace is 40 bits**
  - **No easy way to exchange and distribute keys.**
  - **Key change involves manually changing the key on each AP and Client.**
- **Use of small, plaintext initialization vector (IV)**
  - **IV is sent out in clear text usually at the starting of the packet.**
  - **Dictionary of IVs and keystreams**
    - **Only 2^24 possibilities**
    - **Can be stored in 24GB disk space**
    - **Can be intercepted in a very short period of time on high traffic wireless networks.**
- **Weak encryption algorithms**

WEP Vulnerabilities

- **Small and static keys :**
  - **Actual keyspace is 40 bits**
  - **No easy way to exchange and distribute keys.**
  - **Key change involves manually changing the key on each AP and Client.**
- **Use of small, plaintext initialization vector (IV)**
  - **IV is sent out in clear text usually at the starting of the packet.**
  - **Dictionary of IVs and keystreams**
    - **Only 2^24 possibilities**
    - **Can be stored in 24GB disk space**
    - **Can be intercepted in a very short period of time on high traffic wireless networks.**
- **Weak encryption algorithms**

WEP Vulnerabilities

- **Cracking the WEP key**
  - **Attacker sets NIC drivers to Monitor Mode**
  - **Begins capturing packets with Airsnort**
  - **Airsnort quickly determines the SSID**
  - **Sessions can be saved in Airsnort, and continued at a later date so you don't have to stay in one place for hours**
  - **A few 1.5 hour sessions yield the encryption key**
  - **Once the WEP key is cracked and his NIC is configured appropriately, the attacker is assigned an IP, and can access the WLAN**

WPA

- **WLAN security using WPA**
  - **Precursor of IEEE 802.11i**
- **Features**
  - **Key management (using the 802.1X framework, it is also possible to use preshared keys)**
  - **Authentication (using the 802.1X framework)**
  - **Confidentiality (TKIP encryption)**
  - **Integrity checking**
  - **Protection against replay attacks.**

WPA: encryption

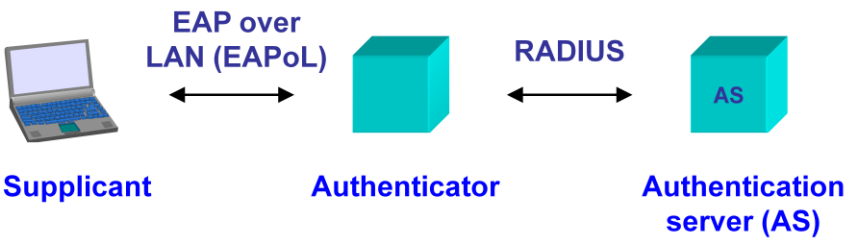
- **RC4 stream cipher, just like WEP encryption, with the following differences:**
  - **The length of the initialization vector is 48 bit (instead of 24 bit in WEP)**
  - **TKIP uses 104-bit per-packet keys, derived from a master secret and different for each packet (instead of a 40-bit or 104-bit static preshared key in WEP).**

WPA: authentication

- **The 802.1X authentication framework protects wired and wireless networks from unauthorised use in open environments**
  - **802.1X uses EAP (Extensible Authentication Protocol) to handle authentication requests. As the name implies, EAP is extensible and therefore should be future proof.**
  - **802.1X also uses RADIUS (Remote Authentication Dial-in User Service) for handling secure signalling between AP and authentication server.**
    - **Use of a key distribution centre**

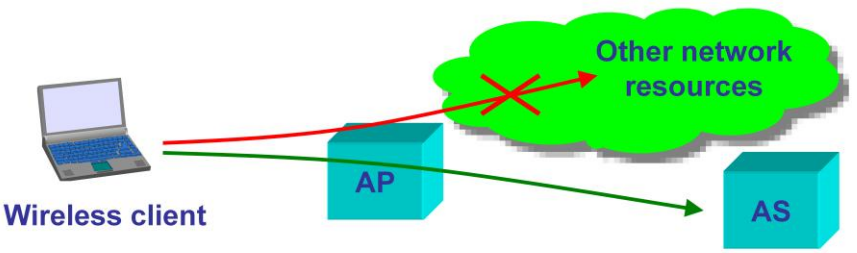
802.1X architecture

802.1X defines three network entities: **Supplicant** (the wireless client in the wireless station), **authenticator** (in a WLAN usually the AP) and **authentication server** (containing user-related authentication information).



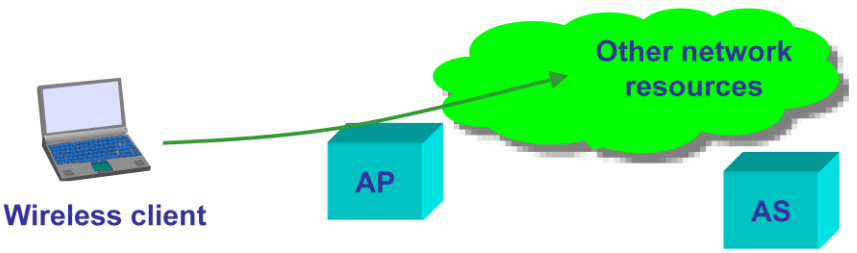
802.1X authentication procedure (1)

With 802.1X, authentication occurs after association. However, prior to successful authentication, a wireless client is only allowed access to the AS. All other traffic is blocked at the AP.



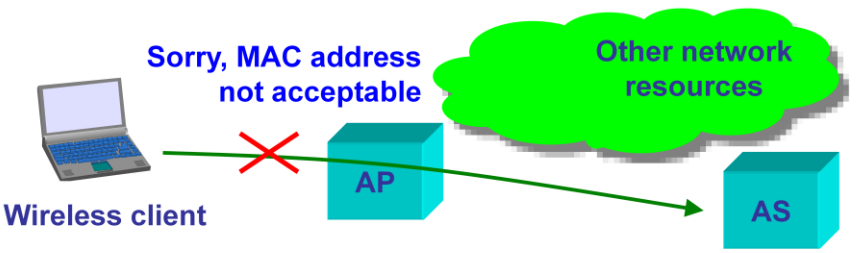
802.1X authentication procedure (2)

After successful authentication, the wireless client is granted access to other network resources by the AP.



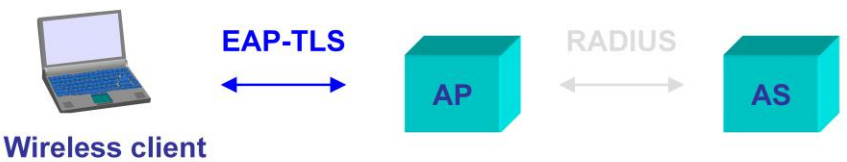
802.1X authentication procedure (3)

The authenticator (AP) can also perform authentication based on MAC address filtering (for preventing denial-of-service = DoS attacks) before starting the 802.1X authentication.

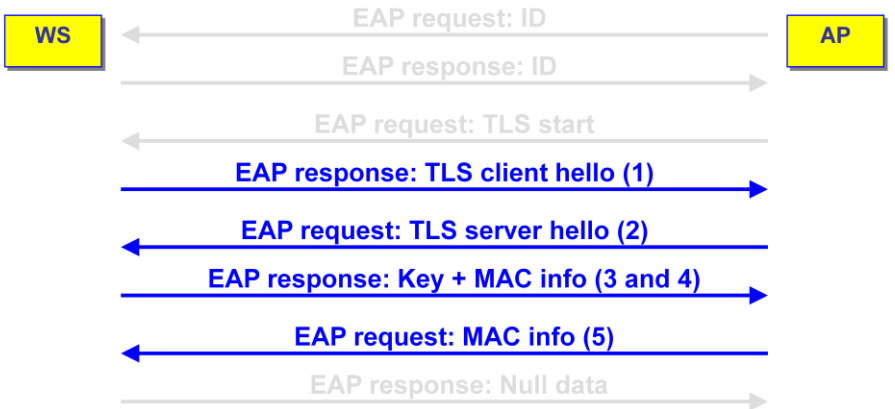


Example: EAP-TLS

As an example, SSL/TLS is one of the various options defined to be used over EAP. The next two slides show how the SSL/TLS handshake sequence is embedded into a corresponding EAP sequence.



EAP-TLS signalling sequence



Authentication in operator-based network

802.11 networks offer new possibilities when the wireless station includes a SIM (Subscriber Identity Module) that is provided by a certain network operator / service provider.

Through the SIM, operators can offer WLAN users added value applications such as secure authentication, nation-wide or worldwide roaming, and user-tailored charging solutions.

Overview

- Network model
- Secure configuration of devices
- Exchanging keys
- Secure networking protocols
  - Transport layer: TLS & SSL
  - Network layer: IPSec & VPN
  - **Data link layer: WEB & WPA**
- Firewalls

Besides the lecturers' own material, many third party, often copyrighted, material is reused within this lecture (e.g. in the notes) under the 'fair use' approach, for sake of educational purpose only, and very limited edition. As a consequence, the current slide set presentation usage is restricted, and is falling under usual copyrights usage.

At the end of every lecture, appropriate references to used materials are included.

References

- This work contains content adapted from, amongst others, the following sources (in no particular order)
  - **Books**
    - William Stallings, "Cryptography and Network Security, principles and practices", 6th (international) edition, Prentice Hall, 2010;
    - Matt Bishop, "Computer Security: Art and Science", Addison Wesley, Pearson Education, 2003, ISBN-13: 978-0-201-44099-7
  - **Lecture slides:**
    - "Informatiebeveiliging", Universiteit Gent, Eric Laermans & Thom Dhaene
    - Stallings, 2014, Lecture slides by Lawrie Brown
    - Slides Teknillinen Korkeakoulu, S-72.3240 Wireless Personal, Local, Metropolitan and Wide Area Networks
  - **Wikipedia**
    - Note page descriptions
  - **Websites**