**IS ZA Secure Communication and Layer 2 Security**

Gefahren Kommunikation:

* Eavesdropping (reading data in transit)
* Manipulating data (modifying data in transit)
* Injecting data (adding data to an ongoing communication relationship)
* Replaying data (sending previously recorded data again)
* Getting unauthorized access (using a system without privileges, after having obtained credentials by eavesdropping)
* Masquerading (pretending to be somebody else, a person or a system)

Secure communication protocols do not solve all security problems:

* Software vulnerabilities on the endpoints => buffer overflow attacks, API => SQL Injection, cross-site scripting
* Malware
* DDoS (Distributed Denial of Service)

Protocols => implemented at all layers

**Higher layers**:

* Easier to deploy
* Typically provides end-to-end protection
* Less generally applicable => often optimized for an application

**Lower layers**:

* Difficult to deploy
* Layer 2 => hop-to-hop protection
* More generaly applicable => protects all layers on top of it

Application Layer => S/MIME, PGP

Transport Layer => SSL/TLS

Network Layer => IPSec

Data Link Layer => EAP, 802.1x, WEP

Physical Layer => Quantum Cryptography

EAP => **Extensible Authentication Protocol**

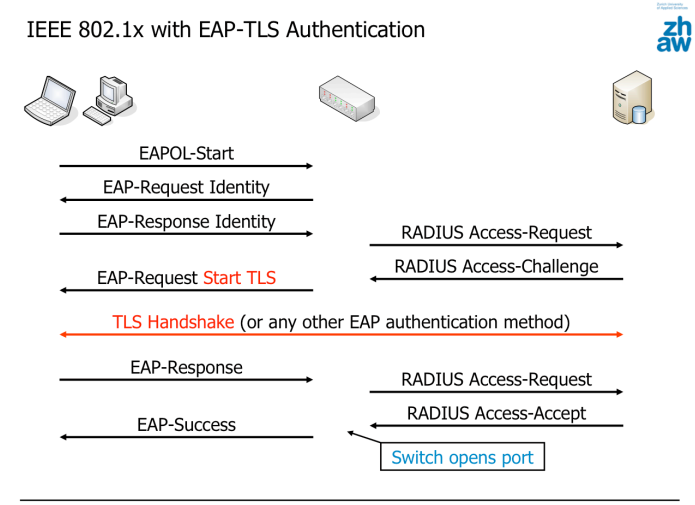
* In wireless networks, layer 2 encryption is very important
* Holds various authentications methods

**Port-based network access control=> protect access to LANs**

* Most widely used standard **IEEE 802.1x**
  + One of the most important applications of EAP
* LAN ports are not open per default
* Client => authenticated for access to the network
* **EAP is used as the authentication protocol**
* IEEE 802.1x => defines how EAP messages are encapsulated withing Ethernet/WLAN frames => EAP over LAN (EAPOL)
* Authentication is usually not done on the Ethernet switch/access point, but **delegated to an authentication server** => **RADIUS server** (Remote Authentication Dial-In User Service (RADIUS)
  + Switch/access point merely relays the EAP protocol messages

**Sequence**:

* Client connecting => first blocked => only EAP messages are accepted
* **Authenticator (ethernet switch)** relays all EAP messages **between the client and the radius server**
  + Radius protocol is secured using **pre-shared keys** **=> authenticity and confidentiality between authenticator and RADIUS-Server**
* **A client gets full network access** when the authenticator has received the “**authentication successful” messag**e from the RADIUS Server



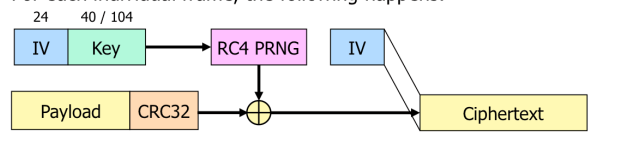
**WLAN:**

* **Sniffing** packets is very easy => data should be encrypted
  + Encryption at layer 2

**WEP** (Wired Equivalent Privacy):

* **AP** and all **clients** share a **preconfigured long-term key**
  + Key is used to encrypt individual frames
  + Every user (who knows this key) can read the traffic of every other user
* Length : **40 – 104 bits**, **RC4**
* 5 – 13 **character** , 10 – 26 hex symbols

WEP Frame protection:



* **CRC checksum** => protects payload **integrity**
* **40 bits – 104 bits => insecure**
* 24-bit IV and a constant key, the RC4 PRNG generates **too few keystreams**
  + **Attack the different keystreams!**

WEP 1st attack:

* **Sniff all frames and wait until the IVs are repeated**
* Two ciphertexts with the same IV
  + XOR-ing the ciphertexts gives the XOR-ed plaintexts => derive from the structure => two plaintexts => derive keystream
* After a while, all 2^24 possible keystreams will be known => allows to read all data and inject own data
  + The actual key is never uncovered, but the keystreams are enough
  + Depending on the trafiic, takes several hours to a few days to execute

WEP 2nd attack:

* **Exploit a weakness of RC4**
  + Knowing a small number of key bits allows to determine several bits of the keystream with probability > 50 %
  + IV as the first part of the key => one always knows the first 24 bits of the RC4 key

WEP was heavily driven by **performance optimizations** => to maximize the available bandwith and to minimize costs of access points

Using a «real» hash function such as SHA-2 or SHA-3 instead of a CRC wouldn't increase security.  
Integrity protection can only be achieved with a MAC (e.g.. the combination of a hash function with  
a key) or by other means, e.g. digital signatures

WIFI protected access

* WPA and WPA2

**Fundamental difference WEP ⬄ WPA/WPA2 => client first have to authenticate themselves at AP**

Two options to authenticate clients:

* Port-based network access control => IEEE 802.1x
  + Using RADIUS server and EAP
* Pre-shared key (PSK) among all clients and Aps
  + Suited for small and home offices (SOHO)

During authentication, a key exchange takes place between the client and the AP => each client uses its own key material

* Users cannot read the unicast data of other users

**Key exchange between client and AP:**

* **Two 128 bit unicast keys** for encryption and integrity protection => unique per client and session
* **Two 128 bit broadcast keys** for encryption and integrity protection => the same for all clients
* Periodic re-keying, typically after one hour (avoid IV wrap around)

**Encryption modes:**

* **TKIP** 
  + For each frame, generates and individual encryption key
  + This key is used to initialize **RC4**, which used to encrypt the frame
  + **Authenticity/integrity: A Mac** using the **Michael algorithm** is appended
    - **Michael is not a one-way function!**
      * Attacker can learn the integrity key if he knows the plaintext and the MAC
  + Several practical attacks
    - Injection of frames that have a valid MAC after decryption
    - Attack to decrypt all traffic towards the client
    - DOS attack requiring 2 packets per minute only
  + Main reason for using RC4 and Michael :
    - **Performance**
    - Backwards compatibility with devices designed for WEP
* **CCMP** (Counter Mode CBC-MAC Protocol)
  + **Based on AES**
  + Guarantees **confidentiality and authenticity/integrity**
  + Cipher mode => block cipher => encryption
    - Authenticated encryption mode
  + In WPA/WPA2 => CCMP is used with AES and 128-bit keys
  + **Protects the frame header** => very important to prevent some attacks => integrity!!

Two ways for clients and AP to get **master key**

* Port-based network access control according to IEEE 802.1x
* PSK (pre-shared key) among all clients and Aps

Client Authentication with master key => includes exchanging key material to protect the frames

* This process is typically repeated every hour to make sure the key material is periodically refreshed

