WLAN security

BMEVITMAV52

Information and Network Security

feher.gabor@tmit.bme.hu

Wireless technologies

- WiFi - Wireless Fidelity
  - Maximum: 800Mbps/3.2Gbps – 3.5Gbps/14Gbps (ax)
  - World Record: unamplified 11Mbps, 125 miles!
- WiMAX – Worldwide Interoperability for Microwave Access
  - Maximum: 50 km, 75 Mbps
- Bluetooth
  - Maximum: 100 (10) m, 768 Kbps

- Other wireless technologies
  - GPRS, UMTS, 3G/4G/5G, Wireless USB, …

Wireless networks

- Benefits compared to traditional wired networks
  - Users
    - One wire minus (Laptop, PDA)
    - Internet access in frequent places (HOTSPOT)
  - Administrators
    - Easy deployment, easy maintenance
      - No wires
    - Network in places where it is hard to get cables
  - Business
    - Cheap maintenance

WiFi network standards

- IEEE 802.11
- Current transfer standards

– IEEE 802.11b	11Mbps	2.4 GHz
– IEEE 802.11g	54Mbps	2.4 GHz
– IEEE 802.11a	54Mbps	5 GHz
– IEEE 802.11n	300Mbps	2.4, 5 GHz
– IEEE 802.11ac		
– IEEE 802.11ax		

IEEE 802.11 standard family

IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
IEEE 802.11d - International (country-to-country) roaming extensions (2001)
IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
IEEE 802.11f - Inter-Access Point Protocol (2003)
IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
IEEE 802.11i - Enhanced security (2004)
IEEE 802.11j - Extensions for Japan (2004)
IEEE 802.11k - Radio resource measurement enhancements
IEEE 802.11l - (reserved, typologically unsound)
IEEE 802.11m - Maintenance of the standard; odds and ends.
IEEE 802.11n - Higher throughput improvements
IEEE 802.11o - (reserved, typologically unsound)
IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1q VLAN trunking)
IEEE 802.11r - Fast roaming
IEEE 802.11s - ESS Mesh Networking
IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
IEEE 802.11v - Wireless network management
IEEE 802.11w - Protected Management Frames
IEEE 802.11y - 3650-3700 MHz Operation in USA
IEEE 802.11z - Extensions to Direct Link Setup

IEEE 802.11aa - Video Transport Streams (2012)
IEEE 802.11ac - Very High Throughput 6GHz (2013)
IEEE 802.11ad - Very High Throughput 60GHz (2012)
IEEE 802.11ae – Prioritization of Management Frames (2012)
IEEE 802.11af - TV White Spaces (2014)
IEEE 802.11ah -Sub 1 GHz
IEEE 802.11ai - Fast Initial Link Setup
IEEE 802.11aj - China Millimeter Wave
IEEE 802.11ak – General Link
IEEE 802.11aq - Pre-Association Discovery
IEEE 802.11ax – High Efficiency WLAN
IEEE 802.11ay – Next Generation 60GHz
IEEE 802.11az: Next Generation Positioning
IEEE 802.11ba: Wake Up Radio
IEEE 802.11bb: Light Communications

Devices on a WiFi network

- Wireless network client device
  - Usually mobile devices
    Laptop, PDA and TablePC
    - New fields: cameras, game consoles, mobile phones …
  - Built in devices, PCMCIA, CF card, US, etc…
  - Unique MAC address – just like Ethernet

- Access Point – AP
  - Infrastructure mode: Wireless clients are in connection with the Access Point

HOTSPOT

- Places where lots of potential WiFi users are expected
  - Airport terminals
  - Hotels
  - Café’s, Restaurants

- Users pay for the Internet Access

Challenges of wireless networks

- Main challenges
  - Interference of radiowaves
    - Deploying many access points to the same place
    - Channels disturbing other channels
    - Terrain effects
  - Power consumption
    - Optimizing radio transmissions
  - Movement between access points
    - Handover
    - Changing service-povider
  - **Security**

Security of wireless networks

- In the case of wired networks the inaccessibility of the wires already stops many potential hackers
- In the case of wireless networks hackers can access the network invisibly
  - Sent and received packets can be captured easily
  - Walls of the building does not border the wireless network

Security of wireless networks 2.

- Security
  - Authentication
    - Authentication of the user
    - Authentication of the service provider
    - Protecting the authentication
  - Data confidentiality after successful authentication
  - Anonymity (usually it is not a goal)

Authentication issues

- Challenge-response based authentication
  - Works well in wired environment
    - The user can trust in the service provider
  - Not perfect solution in wireless environment
    - The hacker can capture both the challenge and the response
    - In the case of weak passwords (or protocols) it is an easy attack

Authentication issues 2.

- Man-in-the-middle attacks
  - In wired environment there are no hackers in the wire
  - In wireless environment the attacker can personate others
    - Fake access points
    - Problems with key agreement protocols
      - Diffie-Hellman protocol

Service provision issues

- Fake access points (rogue AP – evil twin)
  - Easy to deploy – even a PDA can be an AP!
  - The user does not necessarily know the AP
    - HOTSPOT
- Denial of Service attacks
  - Bandwidth exhaustion attack using the wired connection (usually higher speed)
  - Jamming

Wireless access control

Access filtering

- Access filtering based on MAC addresses
  - The AP has a list of the acceptable MAC addresses
    - It can be a blacklist also
  - Not safe!
    - MAC addresses can be captured on the network and later the hacker can use this MAC address
    - One who gets the device also gets access to the network
    - Managing many access points is not easy
  - Unfortunately it is still popular even today

SSID hiding

- Hiding the access points
  - The access point does not advertise it own name (Service Set ID - SSID)
  - Those users can connect only who knows the name of the service (SSID)
  - BAD: The hacker can eavesdrop on the network and get know the SSID

WEP

- Protecting data communication using the WEP protocol
  - WEP: Wired Equivalent Privacy
    - The target is to be as secure as wired networks

- Authentication and ciphering
  - Ciphering in the first place
    - RC4 cipher, 40 and 104 bit long keys (4 keys can be set at the same time), 24 bit long Initialization Vector (IV)
    - One key for the whole network
  - Integrity protection
    - CRC value
    - Not a cryptographic hash value!
  - Authentication
    - Clear challenge and ciphered response
    - Only optional

Header	IV	KA	Message	ICV

WEP - Ciphering

- Static keys
  - Using a Vernam cipher
    - Using the key twice should be avoided!
  - The IV is 24 bit long, so there is a sure collision after 2^{24} packets
    - There is no need for that much packet, since drivers usually reset the IV to 0
    - Due to the „Birthday paradox” there is a high change for collision after 2^{12} packets!
  - Cracking the 40 bit key is not a problem
    - Usually the key is generated form a password, so dictionary attack is possible
- RC4 flaw
  - The output of the RC4 cipher is not as safe as they thought once

WEP integrity and authentication

- The CRC value is good to detect and repair bit errors
  - Protection against the noise
  - But can not protect from intentional overwriting
    - CRC value can be recalculated without the key
- Authentication can be cracked also
  - The hacker can know a challenge and its good and ciphered response
    - The keystream is known from these messages
    - For a new challenge he or she can create the correct response using the keystream

WEP security

- There is no WEP security
  - Even worse: the users have a false sense of security

- As a patch to WEP, they increased the key size to 104 bits
  - This was not the error!
  - All the other weakness remained

HOTSPOT protection

- Protecting HOTSPOTs
  - The user should be authenticated
    - It is required to create the bill
    - Authentication in the IP layer
      - The user’s traffic is blocked and its first web request is redirected to a secure authentication site
  - The user’s traffic is not protected!
    - Usually the user has secure connections (TLS) to the servers

IEEE 802.11i

- The goal of the 802.11i is to create secure wireless networks
  - The standard came in 2004
  - Until 2004 there was a need to something that is better than WEP and converges to 802.11i
    - WPA – WiFi Protected Access
      - In parallel with 802.11i
  - That is why 802.11i got the name WPA2

WPA - Wi-Fi Protected Access

- WPA form Wi-Fi Alliance to fix WEP problems (2003)
  - Strong confidentiality
  - Authentication
  - Works in all environment (SOHO and Enterprise)
  - Should need a firmware upgrade only
  - Compatibility with the upcoming 802.11i standard
- Replace WEP as fast as possible

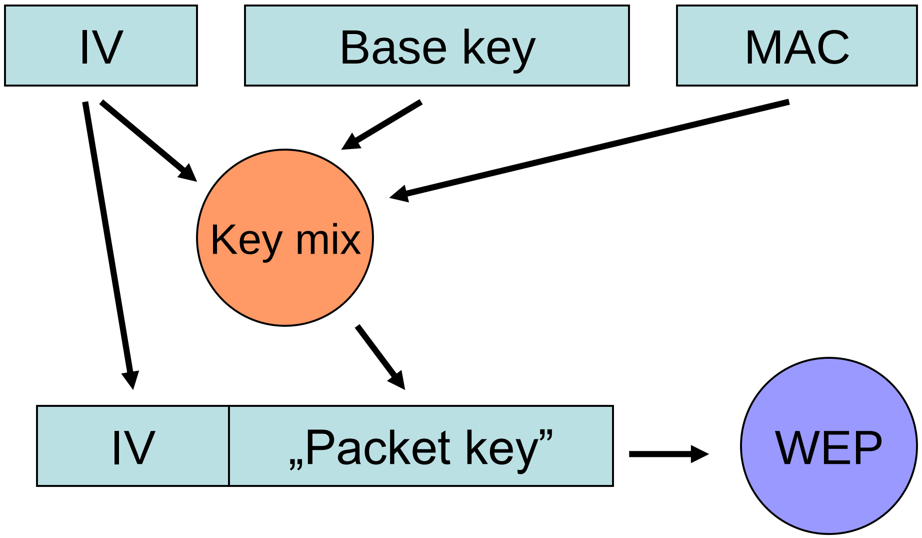
WPA - TKIP

- Fix WEP problems while keep the WEP infrastructure
- Ciphering: Temporal Key Integrity Protocol (TKIP)
  - Per-packet key mixing (not just concatenation)
  - Message Integrity Check (MIC) - Michael
  - Extended initialization vector (48 bit IV)
  - Strict IV counting rules
  - Periodically refreshed keys (must)
- Authentication: 802.1X and EAP
  - Securing the authentication
  - Authentication can be mutual (EAP-TLS)
  - Authentication strength can depend on the environment needs (SOHO <> Enterprise <> HOTSPOT)

TKIP

- Per Packet Keying

- Each new IV results a new key
- Due to the inclusion of the MAC address, each terminal has own keys
- Using “packet key” instead of the WEP key



TKIP – key mixing

- 128 bit long temporal key (Result of the authentication)
- Creating the packet key in two phases
  - Feistel based cipher (Doug Whiting and Ron Rivest)
  - 1. phase
    - Mix of the source MAC address, the temporal key and the highest 32 bit of the IV
    - The result is stored temporary, it is good for 2^{16} more packet keys
  - 2. phase
    - Cancel the dependency of the IV and the key

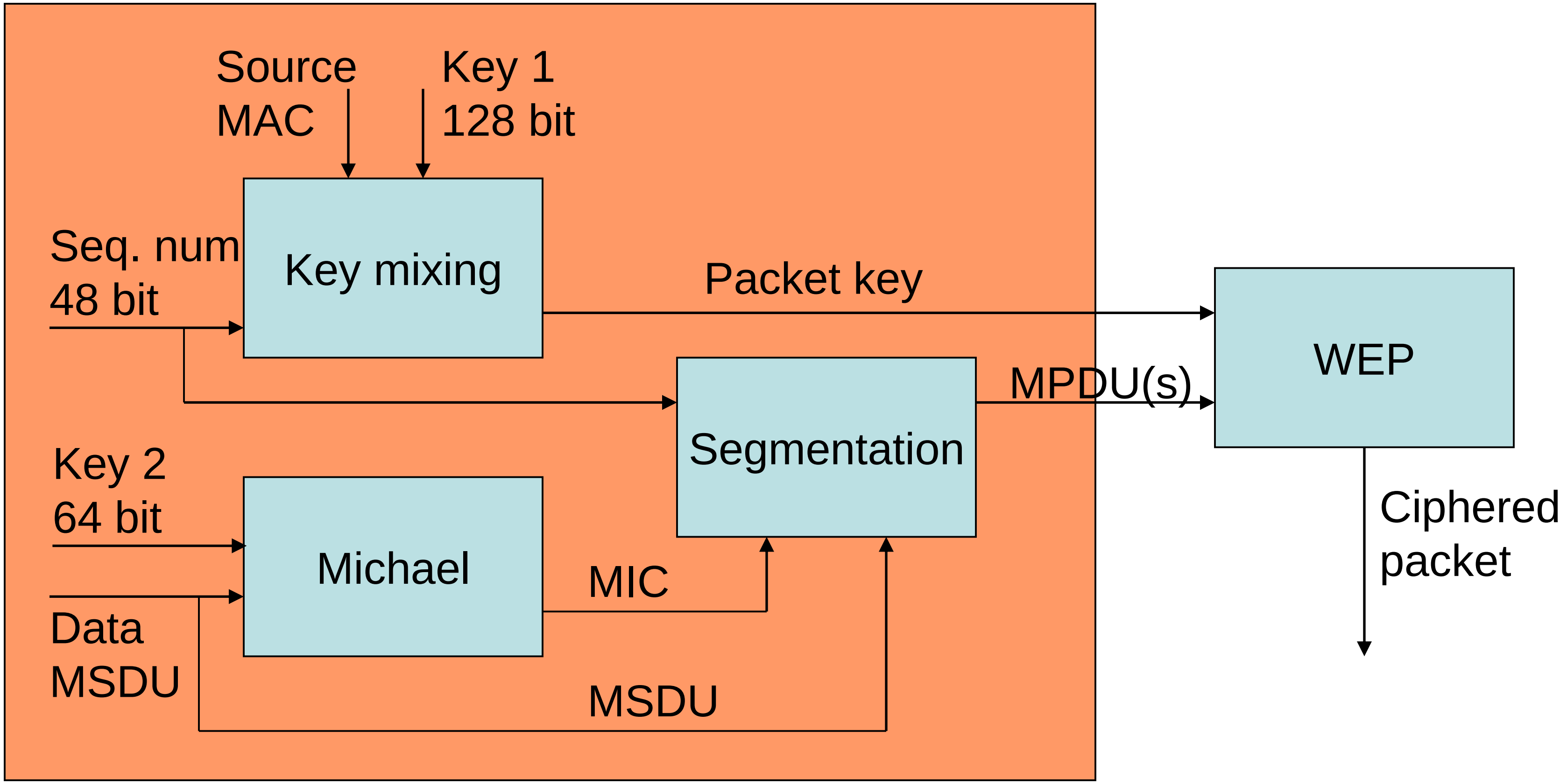
IV sequencing

- IV sequencing rules
  - Always starts from 0
    - Unlike WEP, it is not a problem, since we always have a fresh key!
  - Each packet increase the IV value by one
    - If not increased the drop the packet
- 48 bit long IV is not exhausted normally
  - If it would happen then there comes a new fresh key

MIC

- Message Integrity Code
- Michael algorithm (Neils Ferguson)
  - 64 bit key 64 bit long authentication check
  - However the strength is 30 bit only
    - Capturing 2^{31} messages is enough to create a correct message
    - Not considered as a strong protection
    - However other algorithms, such as HMAC-SHA-1 or CBC-MAC would degrade the performance
    - additional protection: if observing an active attack the change the key and lock the key for one minute
  - Protects the MC addresses as well
  - There is no separate IV for the authentication, but the MIC value is encrypted

TKIP in work

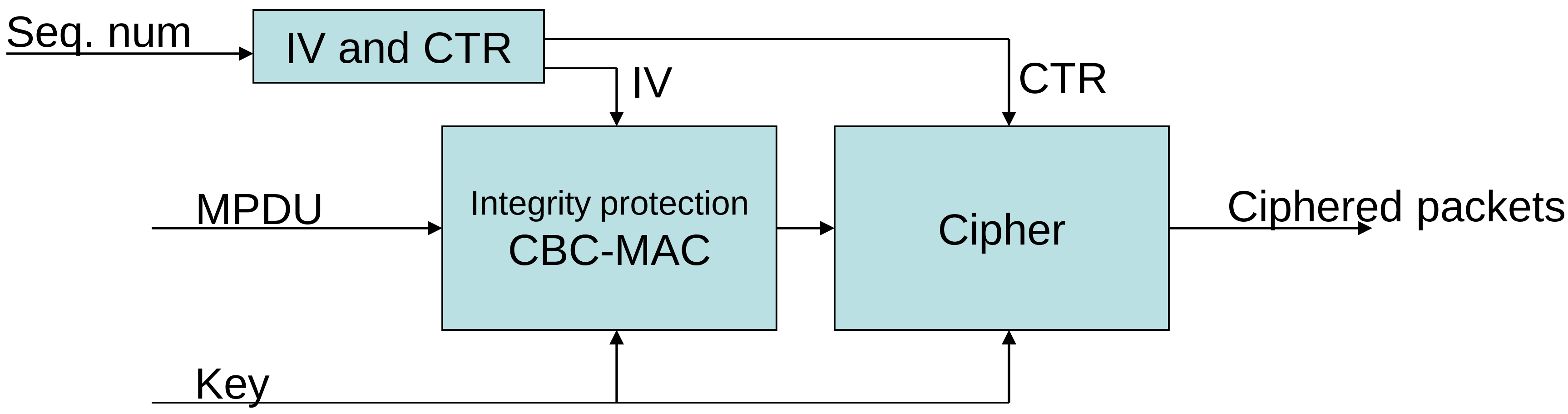

Source
MAC
Key 1
128 bit
Seq. num
48 bit
Key mixing
Packet key
WEP
Segmentation
MPDU(s)
Key 2
64 bit
Michael
MIC
Ciphered
packet
Data
MSDU
MSDU

802.11i (WPA2)

- Standardized in 2004
  - WPA +
    - Secure IBSS
    - Secure and fast handovers
    - De-authentication
    - New ciphers: AES-CCMP, (*WRAP)*
  - The new cipher requires to build new hardware
    - Slow deployment

CCMP

- Counter Mode CBC-MAC Protocol
- Using AES cipher



CBC-MAC

- Cipher Block Chaining Message Authentication Code

- Procedure
  - 1. Ciphering the first block
  - 2. XOR the result with the next block and perform ciphering
  - 3. Repeat the 2. step

  - Padding is necessary!

CCMP advances

- Only one key is needed
  - The same key goes for ciphering and authentication
  - Usually it is not good, but in this case it is not a problem
- AES benefits
  - Precalculation possible
  - Multithread supports
  - Strong security (lots of experiences)
- Without any patents
  - WRAP failed because of existing patents

802.1X

- IEEE standard to increase (W)LAN security (2001)
  - Protocols to protect the authentication and help data confidentiality
  - RADIUS (de facto)
    - Authentication outside of the access point
    - RADIUS is well known and accepted
  - EAP and EAPoL (EAP over LAN)
    - Transport protocol for the 802.1X messages
    - EAP-MD5 Challenge, EAP-TLS, LEAP (EAP-Cisco Wireless), PEAP
  - Suits to the WLAN needs:
    - Authentication based on the users
    - The access point is not affected (remains cheap)
    - Centralized management

802.1X protocols

Supplicant (STA)

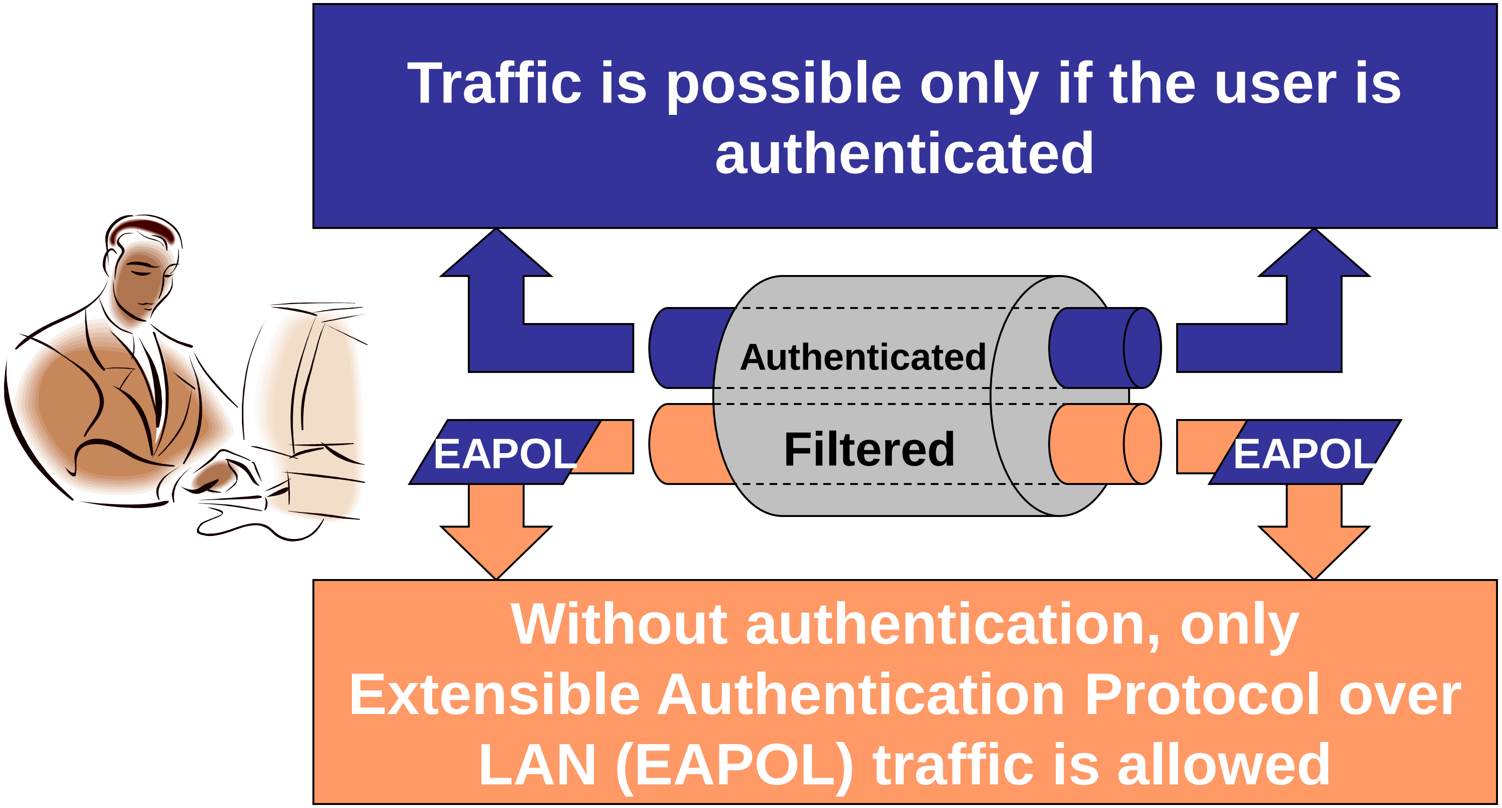
Authenticator (AP)

Authentication server (AS)

<table>
<tr><td>EAP-TLS</td><td colspan="2"></td><td>EAP-TLS</td></tr>
<tr><td colspan="4">EAP</td></tr>
<tr><td colspan="2" rowspan="2">EAPol</td><td colspan="2">RADIUS</td></tr>
<tr><td colspan="2">IP/UDP</td></tr>
<tr><td colspan="2">802.11</td><td colspan="2">Ethernet</td></tr>
</table>

Access control

- At the beginning only EAPoL traffic is allowed



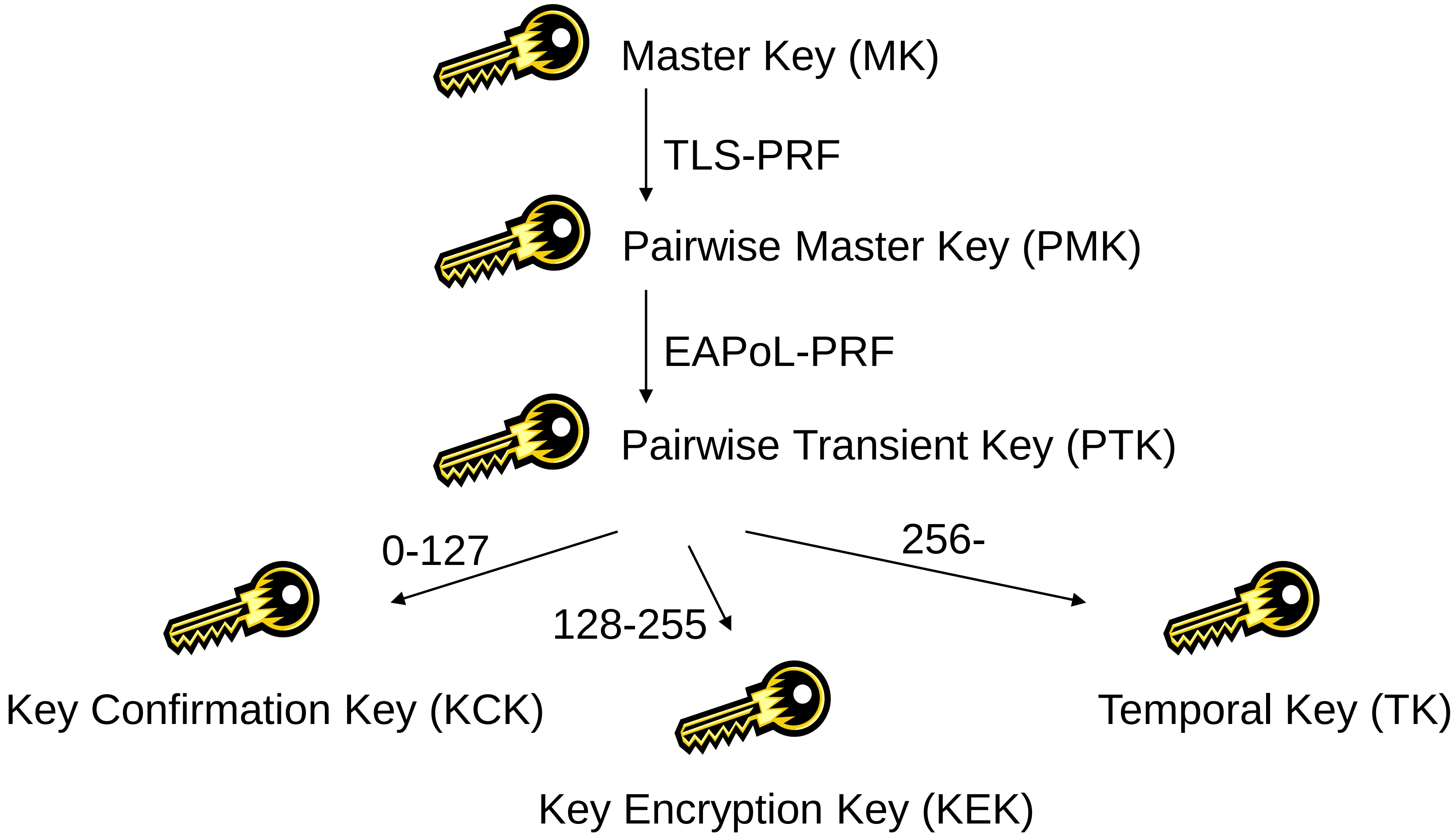
Keys

- Master Key (MK)
  - Symmetric key between supplicant and authenticaton server during the session
  - Only they posses this key (STA and AS)
  - Every other key is derived from this one
- Pairwise Master Key (PMK)
  - Fresh symmetric key between the supplicant and the access point
  - The supplicant generates this key from the MK
  - The access point gets this key from the authentication server

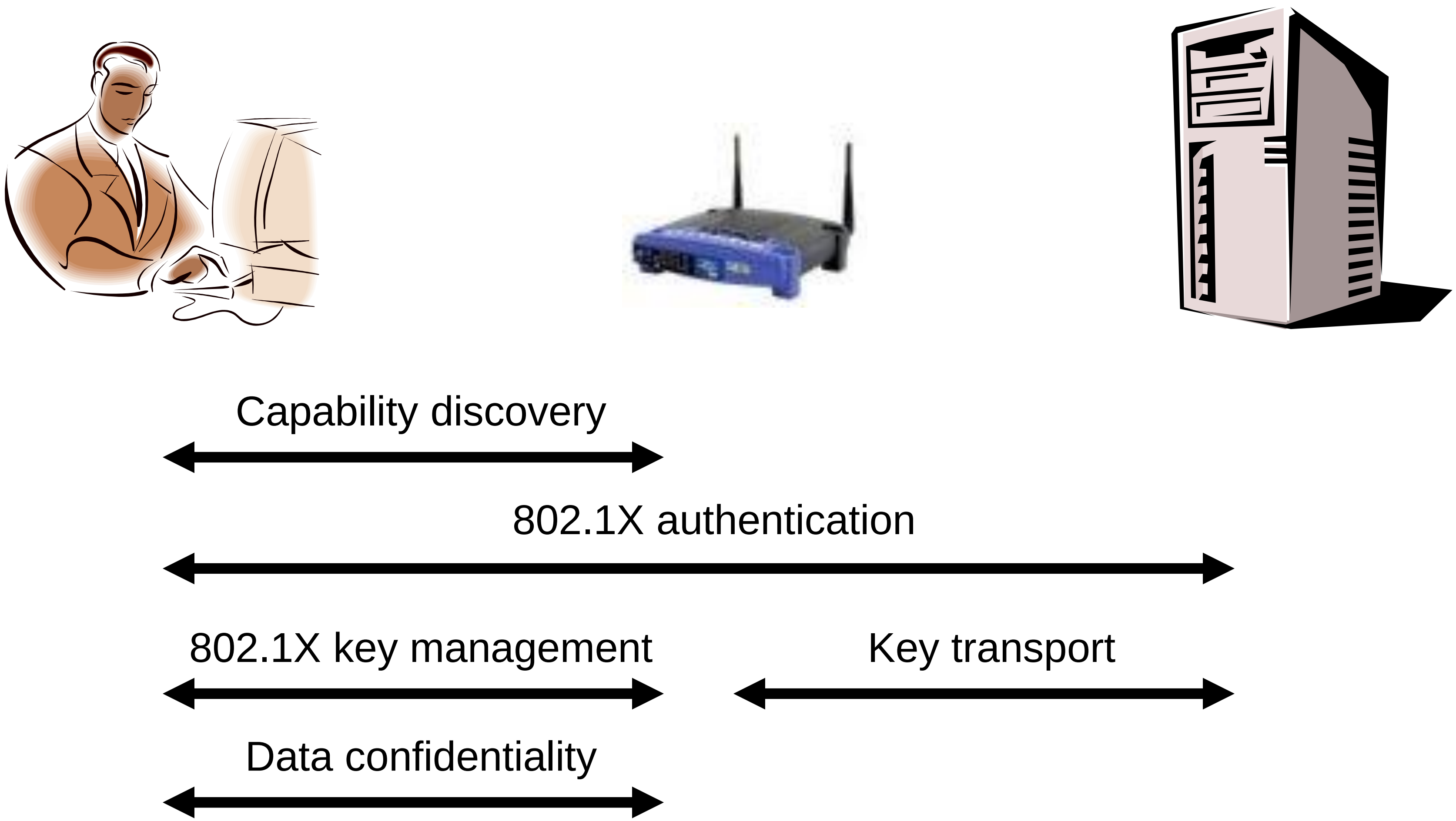
Keys (cont.)

- Pairwise Transient Key (PTK)
  - The fresh keys
  - Key Confirmation Key (PTK bits 1-128)
    - Key to provde the knowledge of PMK
  - Key Encryption Key (PTK bits 129-256)
    - Issuing or refreshing other keys
  - Temporal Key (TK) (PTK bits 257-..)
    - Provides date confidentiality

Key hierarchy



802.1X Work phases



802.1X work phases (cont.)

- Capability discovery
  - Negotiate the cooperating peers (STA and AP)
  - Advertisement about the AP capabilities
- 802.1X authentication
  - Centralized authentication at the AS
  - The user (STA) decides about the connection
  - Mutual authentication of the peers (STA and AS)
    - EAP based authentication
  - Generating Master Key (MK) and Pairwise Master Key (PMK)

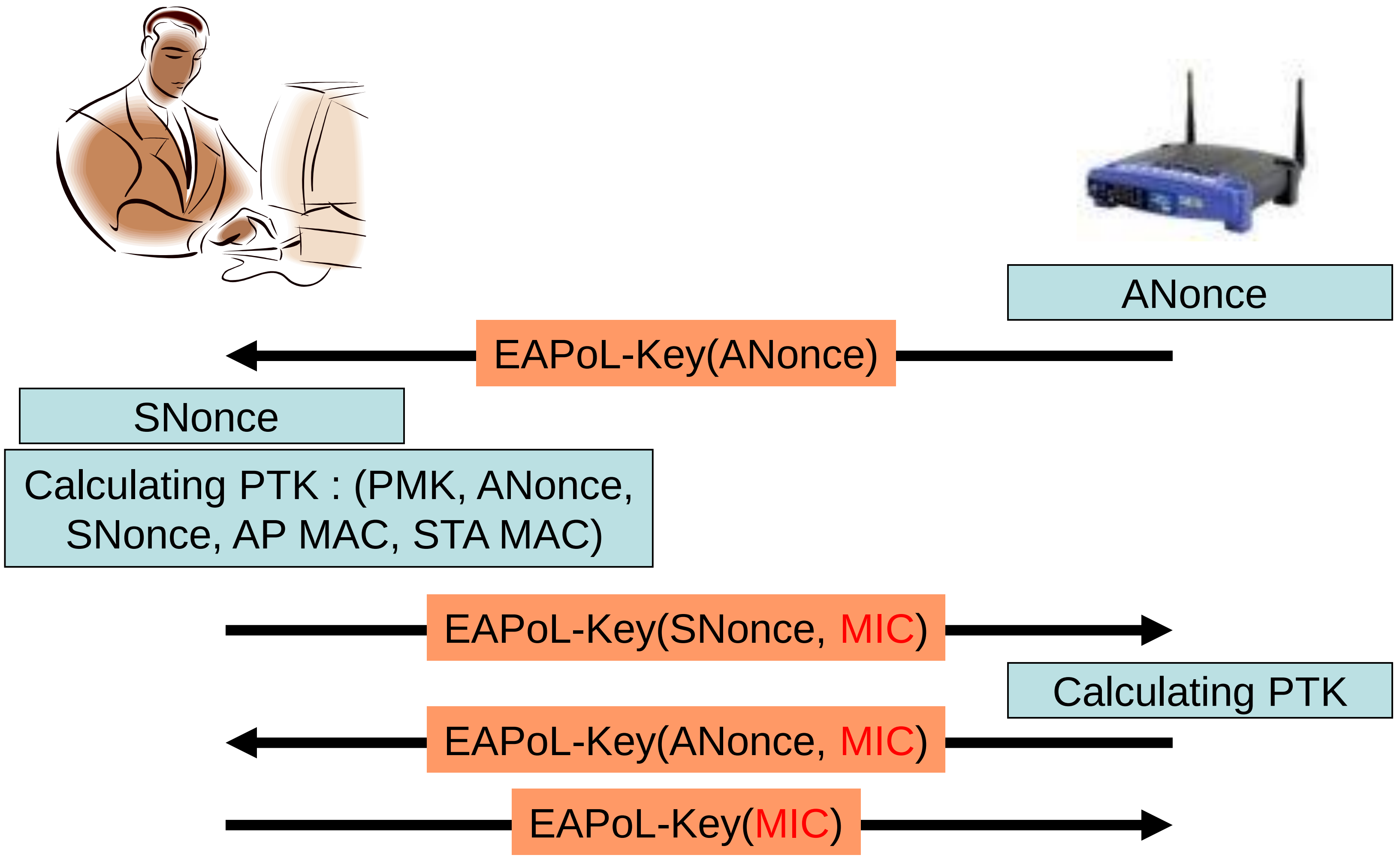
802.1X work phases (cont.)

- Key transport
  - Moving the Pairwise Master Key (PMK) to the Access Point
- 802.1X key management
  - Check the validity of the PMKs
  - Generating fresh keys (PTK)

802.1X key management

- Using the Pairwise Master Key (PMK) the user (STA) and the Access Point (AP) generates the Pairwise Transient Key (PTK)
  - Only they know the PMK (Trust in the AS who generates the PMK)
  - The PTK is derived from PMK and nonces. If they have the same PTK then it was the same PMK as well
    - 4-way handshake
  - The rest of the keys are coming from the PTK, using the appropriate bits or created individually and transported using the KEK (just like Group TK)

4-way handshake



4-way handshake

- MIC: Protect the integrity of the message (using PTK)
- In order to avoid man-in-the-middle attacks
  - Message no. 2 proves
    - The user (STA) knows the correct PMK
    - And he or she got the right ANonce value
  - Message no. 3 proves
    - The Access Point (AP) knows the correct PMK
    - And he or she got the right SNonce value
- Message 4 is just there to finish a request/reply sequence

EAP

- Extensible Authentication Protocol
- Possible authentication methods
  - EAP-TLS
  - EAP-TTLS
  - EAP-MSCHAPv2
  - EAP-MD5
  - EAP-OTP
  - EAP-SIM
  - …

EAP-TLS

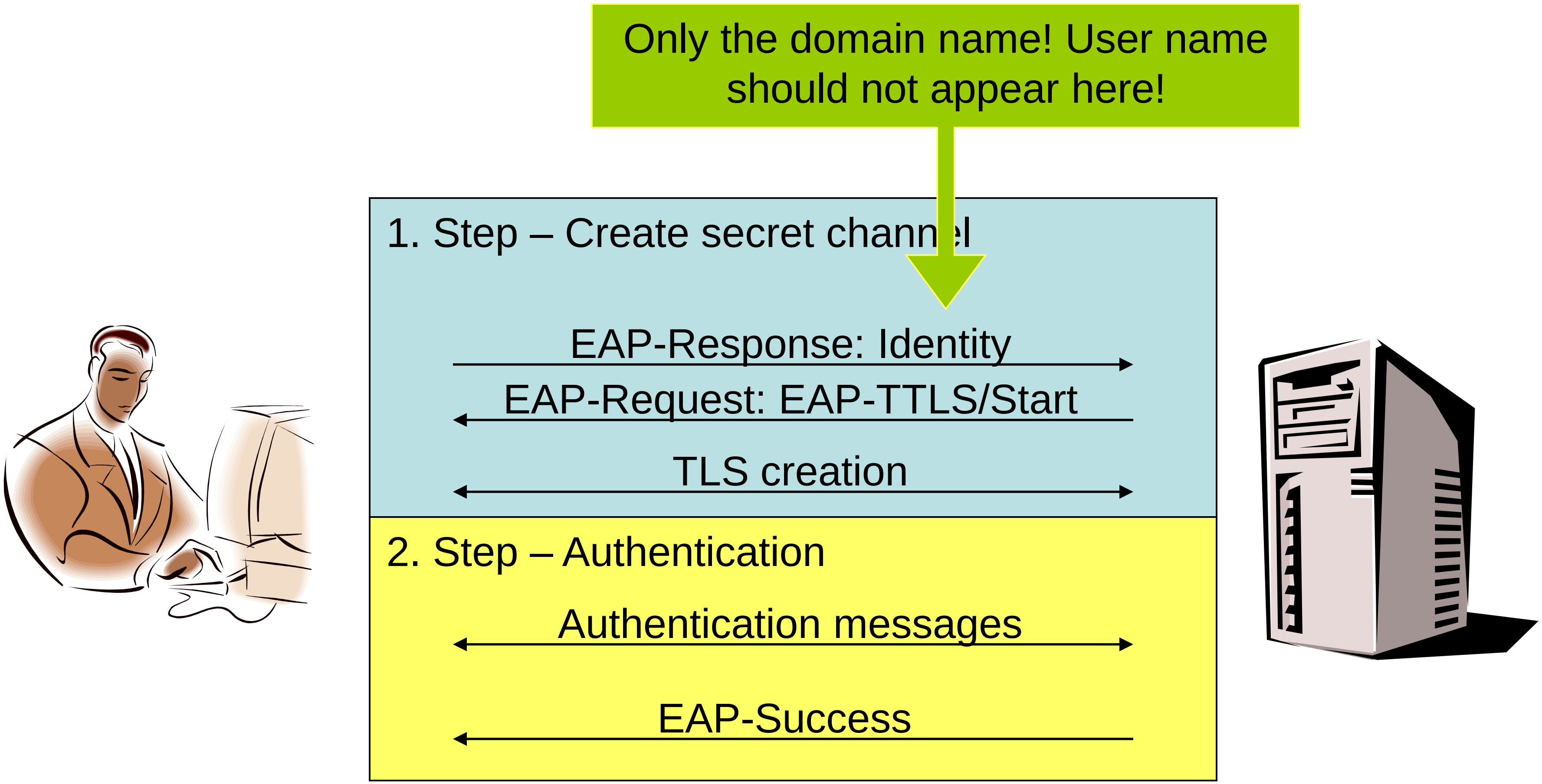
- TLS – Transport Layer Security
  - Mutual authentication
    - Certificate, using PKI
    - Certificates for both client and server
  - Integrity protection
  - Key exchange
- EAP-TLS
  - IETF RFC 2716
  - TLS functions for authentication
  - Just the handshake phase, no data confidentiality!

EAP-TTLS

- EAP-TTLS
  - Tunneled Transport Layer Security
  - IETF draft: Funk, Meetinghouse

- Authentication
  - 1. step: Create a secure channel (TLS)
    - Only the server authenticates itself
  - 2. step: Authentication
    - AVP messages, just like RADIUS
  - Supported authentication methods:
    - EAP methods, PAP, CHAP, MS-CHAP, MS-CHAPv2

EAP-TTLS messages



PEAP

- PEAP
  - Protected EAP
  - IETF draft: Microsoft (+ Cisco and RSA)

- Authentication

  (Similar tot EAP-TTLS)
  - 1. Step: Create secret channel (TLS)
    - Only the server authenticates itself
  - 2. Step: Authentication
  - Supported authentication methods:
    - Only EAP methods

Protocol layers

- EAP-TTLS / PEAP layers

EAP method (MD5, OTP, …)
EAP (or other protocols in the case of EAP-TTLS)
TLS
EAP-TTLS
EAP
Transport protocol (PPP, EAPoL, RADIUS, …)

EAP comparison

- EAP methods comparison

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Authentication	MD5	Certificates	Any authentication	EAP methods
Certificates	-	Client & server	Server	Server
Authentication type	Client only	Mutual	Mutual	Mutual
Protecting the user identity	No	No	TLS	TLS

- The PEAP and EAP-TTLS are similar in the aspect of the functionality. EAP-TTLS has free clients on many platforms. The PEAP is Microsoft specific

WLAN layer 2 protection

	WEP	***TKIP***	***CCMP***
Cipher	RC4, 40 or 104 bit keys	RC4, 128 and 64 bit keys	AES, 128 bit key
Key validity	24 bit IV	48 bit IV	48 bit IV
Packet key	Concatenation	TKIP key mixing	Not needed
Header integrity	No protection	Michael: Src and dest MAC	CCM
Data integrity	CRC-32	Michael	CCM
Replay protection	No protection	IV rules	IV rules
Key management	No key management	IEEE 802.1X	IEEE 802.1X