IEEE 802.11i / 802.1X

Lars Strand - 15 Feb. 2005, Linpro

Goals

* briefly cover all TG – “the alfabetic soup”

* How WEP works

* Why WEP don't work

* 802.11i

* real-life numbers

* Misc

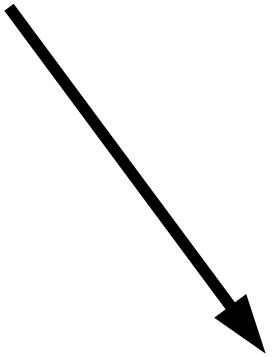
IEEE 802 LAN/MAN Standards Committee

"LAN/MAN for 2 lowest layer in OSI ref. mod.":

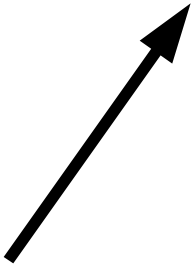
* Ethernet family
* Token ring
* Wireless

Task Group (TG)

Enhance portions of the standard



IEEE 802.11x



Institute of Electrical
and Electronics Engineers

Working Group (WG)

"Setting the standards for wireless LANs"

IEEE COMPUTER SOCIETY

TGs within WG 11 of 802

802.11-1997: The IEEE standard for wireless networks

- often called “802.11 legacy”

- 1-2Mb/s

- physical layer (PHY):
  i) infrared (obsolete)
  ii) requence-hopping spread spectrum (FSSS)
  iii) direct-sequence spread spectrum (DSSS)

- 2.4GHz is crowded

- today: “802.11 uses three different PHY:”
  i) 802.11a
  ii) 802.11b
  iii) 802.11g

TGs within WG 11 of 802

802.11a-1999: Also called 'Wi-Fi5'

- PHY: orthogonal frequency division multiplexing (OFDM)
- not so crowded 5GHz band
- 6 to 54Mb/s

802.11b-1999: Also called '802.11 High Rate' or 'Wi-Fi'

- most used today
- ratified version of 802.11
- PHY: high rate DSSS in the crowded 2.4GHz band
- 1, 2, 5.5, 11 Mb/s
- 802.11b+ (non-standard) up to 22Mb/s

802.11c – does not exists

- Task group C exists however, but has not created their own standard. Instead they have added standard from LAN-bridging (802.1D) to wireless AP operations

TGs within WG 11 of 802

802.11d-2001: New countries
- modified PHY to met regulatory requirements

802.11e-2003: Enhance MAC layer to improve QoS
- extension: Wi-Fi Multimedia (WMM) specification
- a, b, g

802.11f-2003: Inter-Access Point Protocol (IAPP)

802.11g-2003: Higher rate extension to 2.4GHz band
- up to 54Mb/s
- full backwards compatible with 802.11b
- vendor pre-shipped g before standard was completed
- Super G = channel bonding up to 108Mb/s

TGs within WG 11 of 802

802.11h - 2003: 5GHz i Europe

- in Europe, strong potensial for 802.11a interfering with satelite communications
- modified 802.11a (sucessor?)

802.11i – 2004: New standard for wireless security

802.11j - work in progress: add 4.9-5GHz in Japan

802.11k - work in progress: aims to provide measuerment information to make wireless networks more efficient

- roaming decisions
- RF channel knowledge
- hidden nodes
- client statistics
- 2005?

TGs within WG 11 of 802

802.11l – skipped because it look like 802.11i

802.11m – work in progress: for maintenance

802.11n – work in progress: new WLAN standard

- build from ground up (no “turbo-mode” chips)
- 100Mb/s real speed (250Mb/s at teoretical PHY level)
- better operating distance
- not until several years! Fighting within group..

802.11o - work in progress: Voice over WLAN (faster handoff, prioritce voice traffic over data)

TGs within WG 11 of 802

802.11p – 2004: Dedicated Short Range Communications (DSRC)

- ~300m, 6Mb/s
- Wireless Access in Vehicular Environments (WAVE)
- 2007-2008?

802.11q- work in progress: support for VLAN

802.11r – work in progress:

- r for “roaming”
- handling “fast handoff” when roaming between AP

802.11s – work in progress: self-healing/self-configuring mesh networks

802.11x – if often uses to summarize all standards within the WG. NOT a standard

802.15 og 802.16??

IEEE 802.15 Working Group:

- “Personal Areal Network” (PAN)

IEEE 802.16 Working group:

- **standard 2002**
- “WiMAX”
- longer distance, high bandwith (up to 134Mb/s)
- several different PHY
- new mobilephone network?
- “WiMax Forum” - (WfiFi Alliance equivalent)

Wi-Fi Alliance

*** industriforum 1999**
- mange deltakere!

*** markedsfører 802.11 som "WiFi"**

*** sørger for kompatibilitetstester**

Wired Equivalent Privacy (WEP)

* Relies on a secret key *k* shared between the nodes

*** Checksumming**

- Integrity checksum c(M) on the message *M*
- called Integrity Check Value (ICV) based on CRC-32
- Plaintext **P = <M, c(M)>**

*** Encryption**

- chosen initial vector (IV) *v* and a given secret key *k*
- RC4 produces a keystream as a function of *v* and *k*
- **XOR the plaintext with the keystream to obtain ciphertext: C = P ⊕ RC4(v, k)**

WEP 2

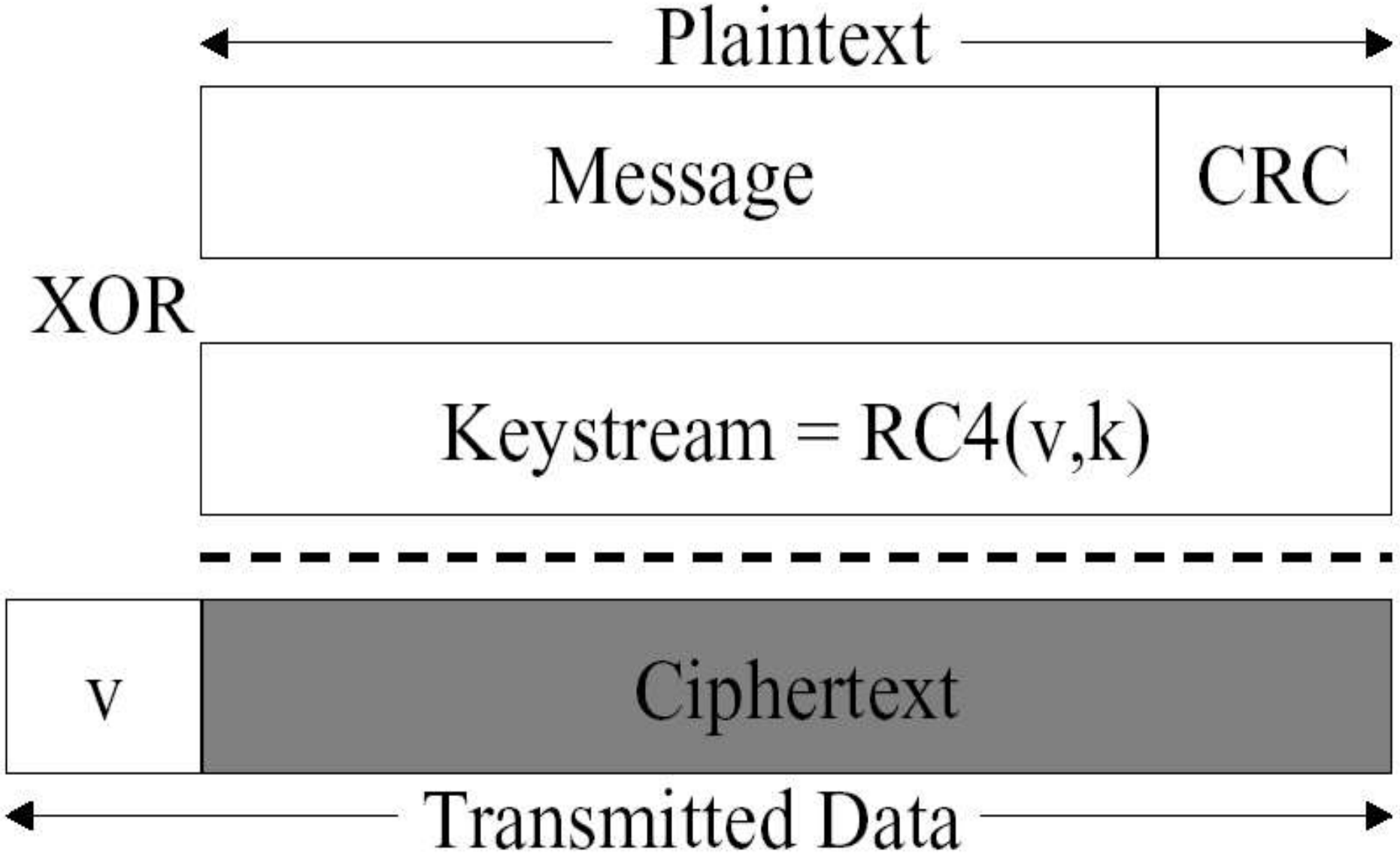


Figure borrowed from Borisov, Goldberg, Wagner 2001

WEP goal

WEP protocol enforce three main security goals:

1. **Confidentiality**
   - **prevent eavesdropping**

2. **Access Control**
   - **must know the secret key**
   - **accept only encrypted packets**

3. **Data Integrity**
   - **prevent tampering with messages**

All which has been broken

WEP attacks

*** Brute-force:**

- 40bits key in standard
- 104bits (128) extended (non-standard!)
- brute force impossible at 104 keys
- other “short-cut” attacks

*** Bit flipping:**

- flip one bit in ciphertext
- corresponding bit is descrypted
- CRC-32 is linear! (CRC ≠ hash)

*** No key managment!**

- static manual stored keys

*** No access point authentication!**

WEP attack

*** Keystream reuse (both 40 and 104 bits)**

- streamcipher pitfall:
- encrypt two messages with same IV and key reveals information about both messages:

If $C1 = P1 \oplus RC4(v,k)$

and $C2 = P2 \oplus RC4(v,k)$

then $C1 \oplus C2 =$

$(P1 \oplus RC4(v,k)) \oplus (P2 \oplus RC4(v,k)) =$

$P1 \oplus P2$

- XOR'ing the two ciphertext causes the keystream to cancel out
- know P1 --> you will get P2
- **per-packet IV should prevent this! But:**
  - i) IV to small (24 bit)
  - ii) IV is NOT encrypted! (common)
  - iii) IV is reused to frequent in various implementations

WEP attack

* **Fluhrer-Mantin-Shamir (FMS) attack (2001)**
  - most know attack on WEP (and WEP2)
  - statistical attack using “interesting” and “weak” IVs
  - complexity of the attack is linear (long keys)
  - some vendors responded by filtering out these IVs
  - Airsnort, kismet ....

"WEP is not only insecure, it is robustly insecure."
-- Bruce Schneier

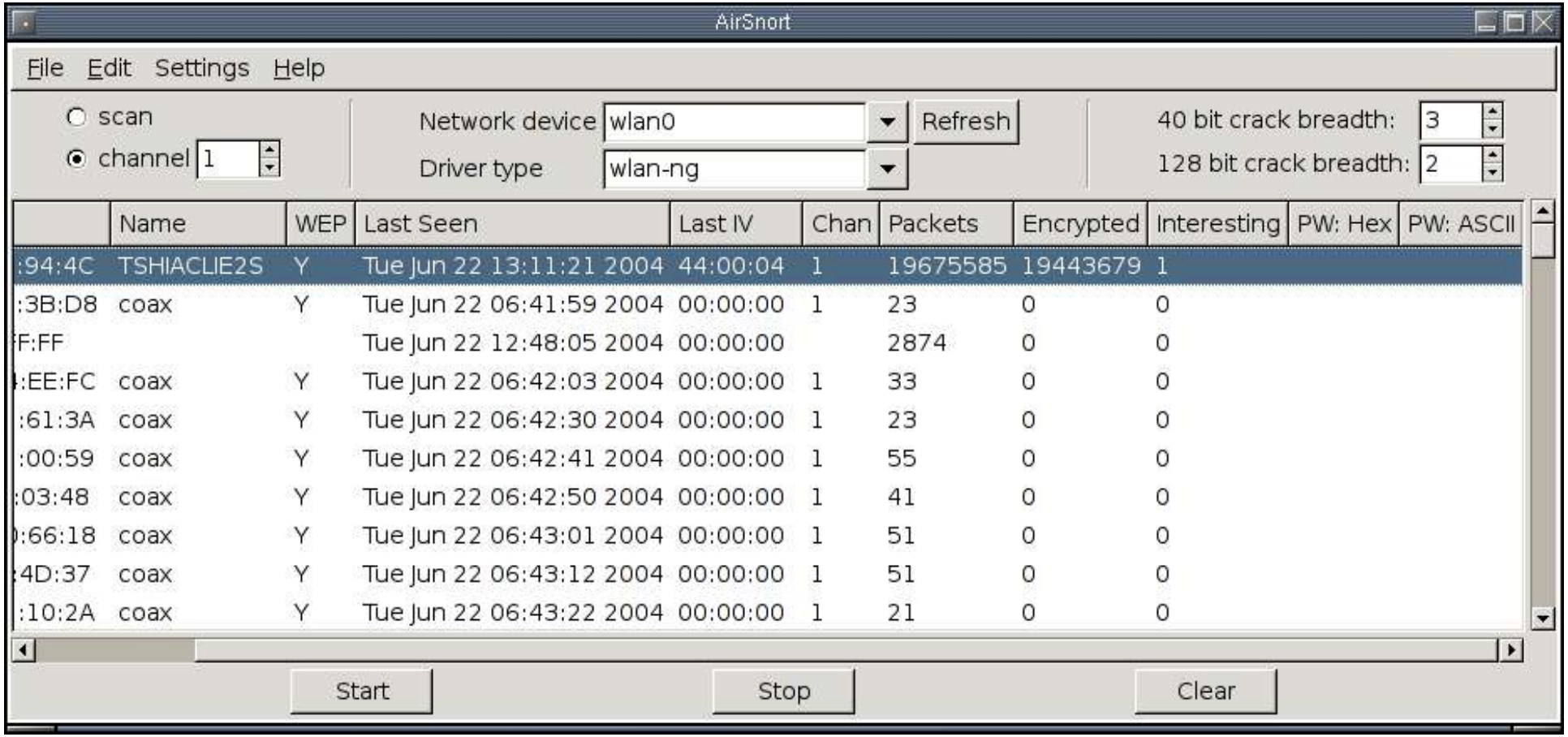
*** Conclusion: Wired Equivalent Privacy (WEP) isn't!**

*** Vendor specific "fixes": longer keys, dynamic keys, longer IV (WEP2) ,VPN**

*** Crack-tool: Airsnort, kismet, aircrack, dwepcrack, WepAttack, WEPCrack, WepLab**

Airsnort

* not all drivers support capturing all 802.11 frames



802.11i

* **802.11i to the rescue!**

Goal: new standard for wireless security!

Consist of three major parts:

1) Temporary Key Integrity Protocol (TKIP)
2) Counter Mode with CBC-MAC Protocol (CCMP)
3) Port-based authentication protocol (802.1X)

\+ key management

Other features: secure IBSS, secure fast handoff, secure deauthentication, disassociation and roaming support

Ratified June 2004

TKIP

*** Industry: *”DO SOMETHING!”***

*** Wi-Fi Alliance felt the pressure**

*** Wi-Fi had not the time to wait for 802.11i to be finished**
- took a snapshot of the draft (draft 3)
- called it Wi-Fi Protected Access (WPA)

*** Temporary Key Integrity Protocol (TKIP)**
- goal: fix WEP using the same hardware
- TKIP fixes all WEPs weaknesses
- uses RC4 --> need only software/firmware upgrade
- degrade performance: TKIP use more CPU (AP)
- Not an long term solution!
- TKIP = ”stepping stone”

TKIP

1. Initial Vector (IV)

- 48bits counter: when “tipping over” --> new TK!

2. Temporal Key

- all host generates a unique RC4 key stream
- per-user, per-packet, per-session encryption
- 128bit (key + IV) generated in two phases using:
  - i) transmitter address (48bits)
  - ii) 48bits IV
  - iii) Temporal Key (128bit)

3. Michael: Crypthographic Message Integrity Code (MIC)

- 64 bits MIC designed by Niels Ferguson
- SHA-1/MD5 to CPU expensive
- MAC = Media Access Controll (MAC = Message Authentication Code). MIC used as MAC in 802.11

CCMP-AES

*** The new flagship of wireless security!**

*** Counter Mode with Cipher-Block-Chaining Message Authentication Code Protocol (CCMP)**

- 128bit keys, 48bits IV
- uses AES encryption
- require new hardware (but not always)
- public domain
- designed by: N. Ferguson, R. Housley and D. Whiting

*** CCMP designed from ground-up**

- not withstood the test of time
- but based on well know technology
- critized for beeing to complex

*** What about WRAPS?**

- based upon Offset Codebook (OCB) mode of AES
- plagued by intellectual property rights (patents)
- RSN: CCMP is mandatory, WRAPS optional

802.1X

* Port based authentication protocol (802.1X)

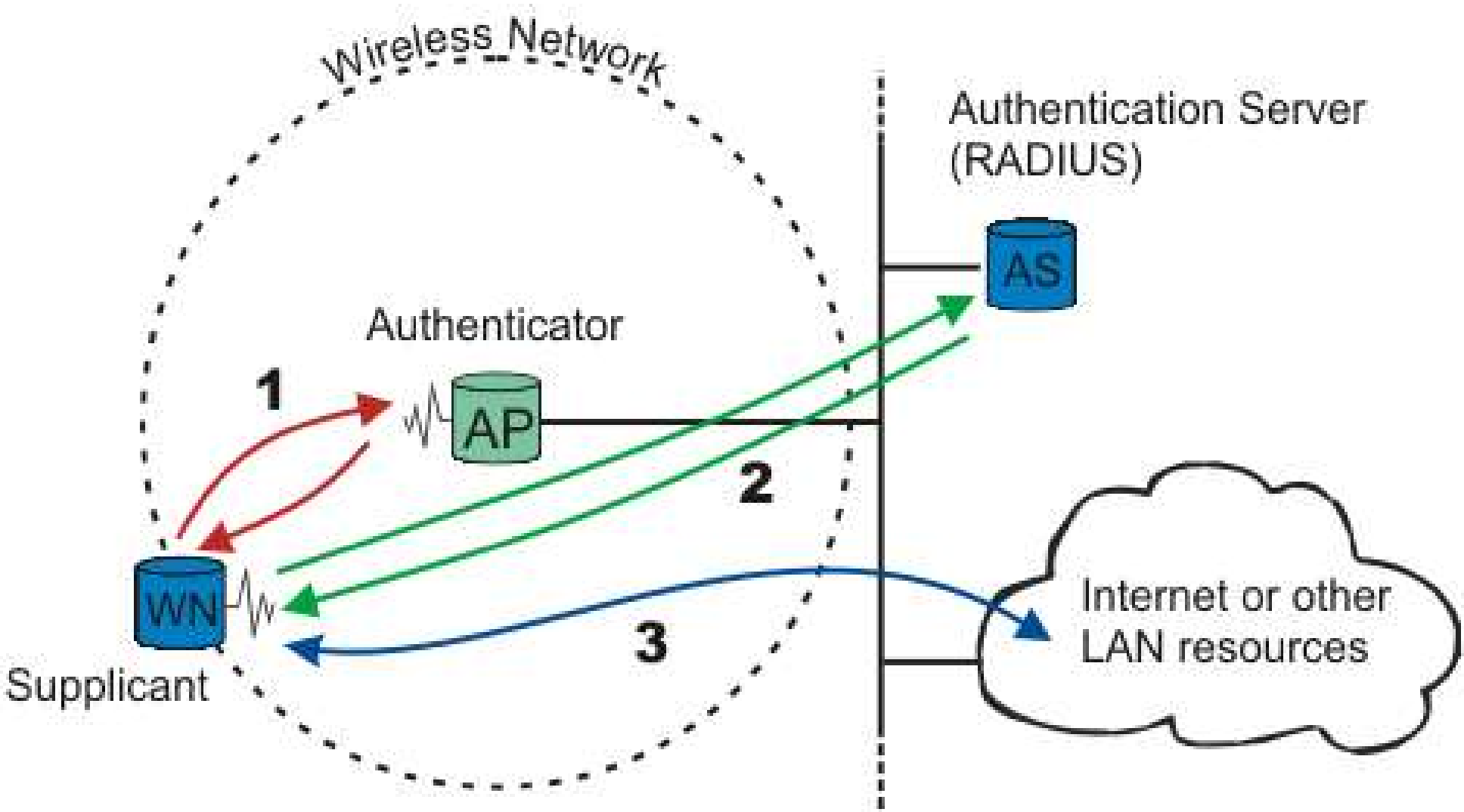
* Uses Extensible Authentication Protocol (EAP)

* June 2004: RFC3748 Extensible Authentication Protocol (EAP)
  (Obsoletes RFC2284)

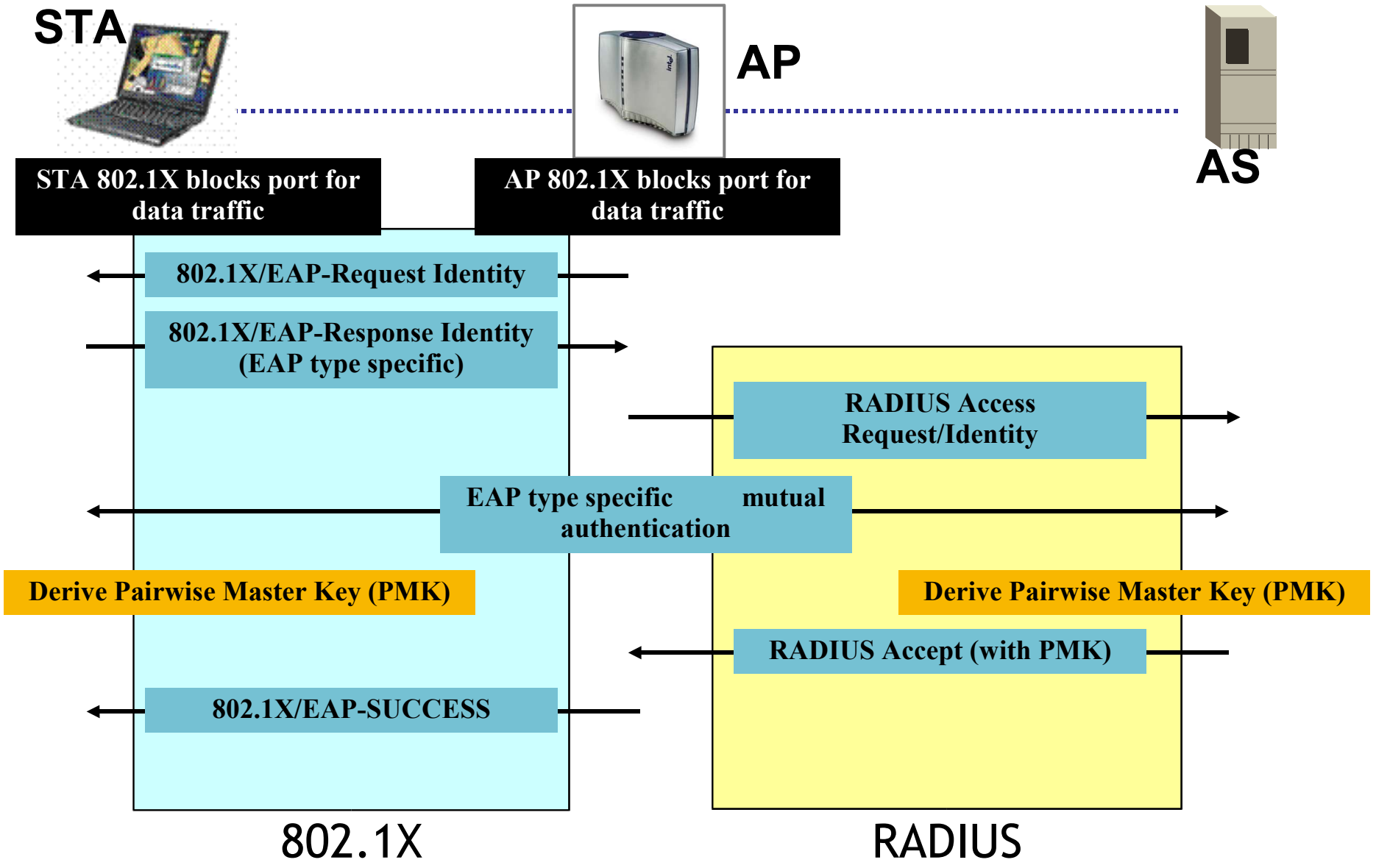
"This document defines the Extensible Authentication Protocol (EAP), an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP."

"EAP is used to select a specific authentication mechanism, typically after the authenticator requests more information in order to determine the specific authentication method to be used." --RFC3748, page 3

802.1X

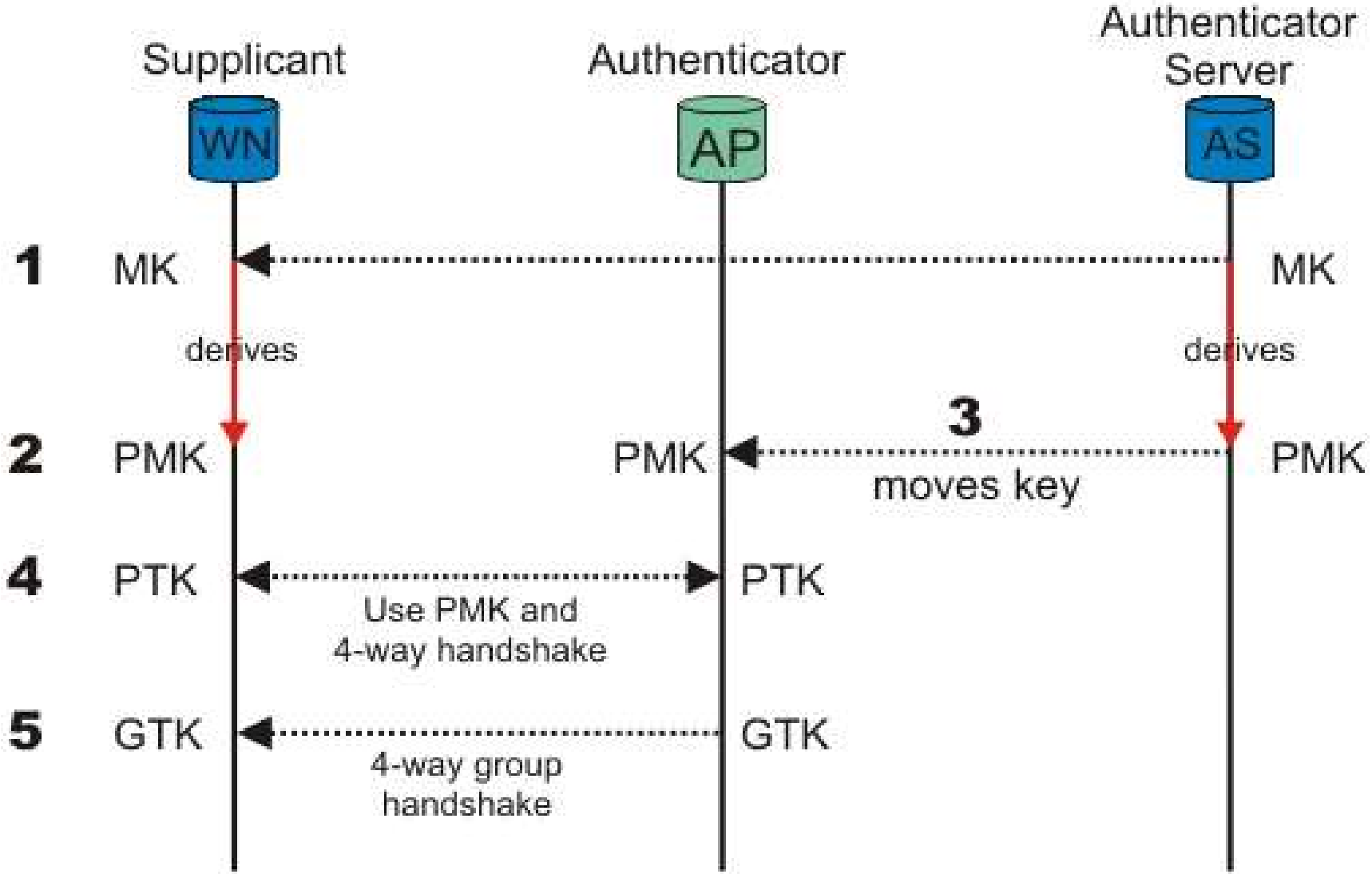

Wireless Network
Authentication Server
(RADIUS)
AS
Authenticator
1
AP
2
WN
3
Supplicant
Internet or other
LAN resources

802.1X-EAP authentication overview



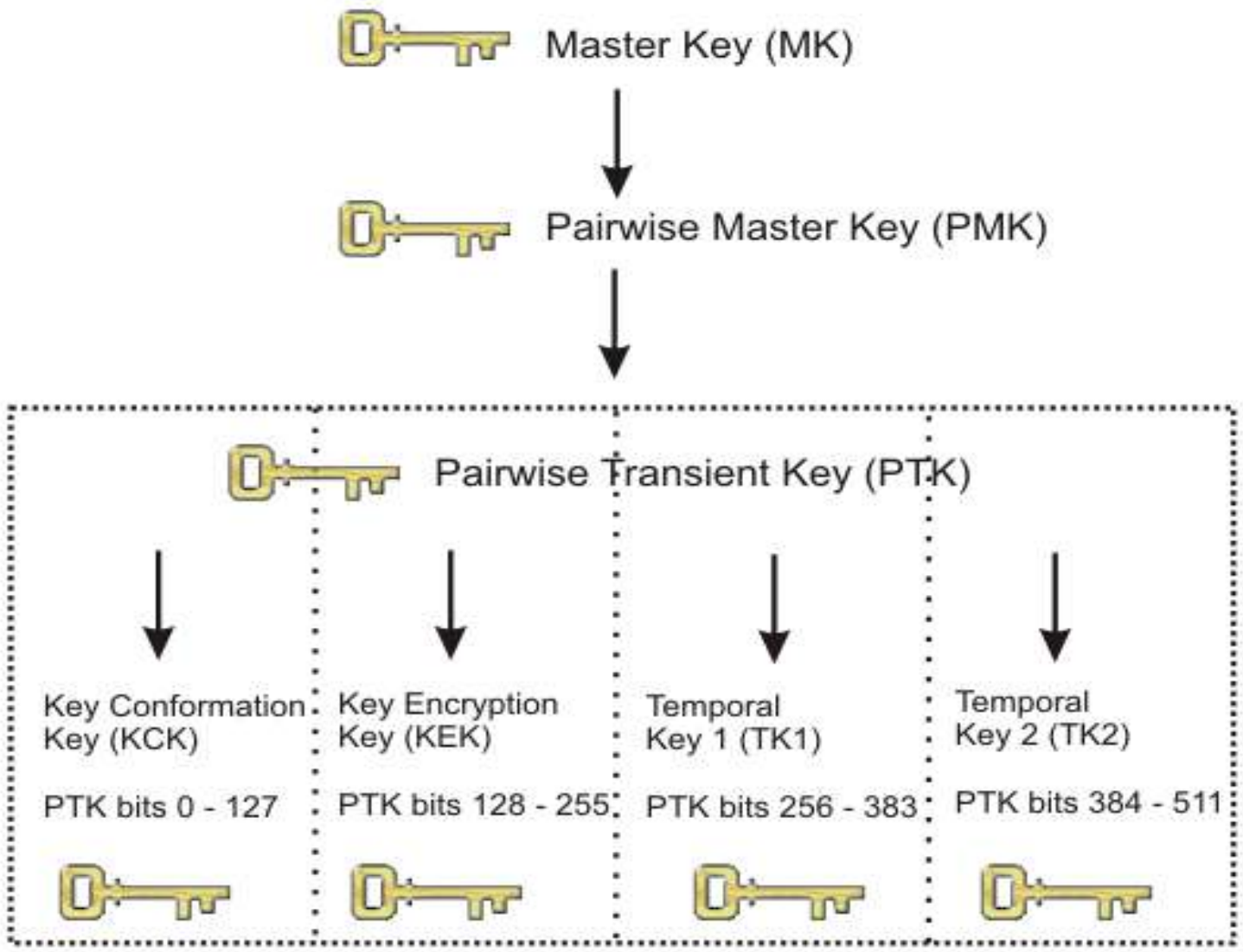
Slide borrowed from Jesse Walker

key managment

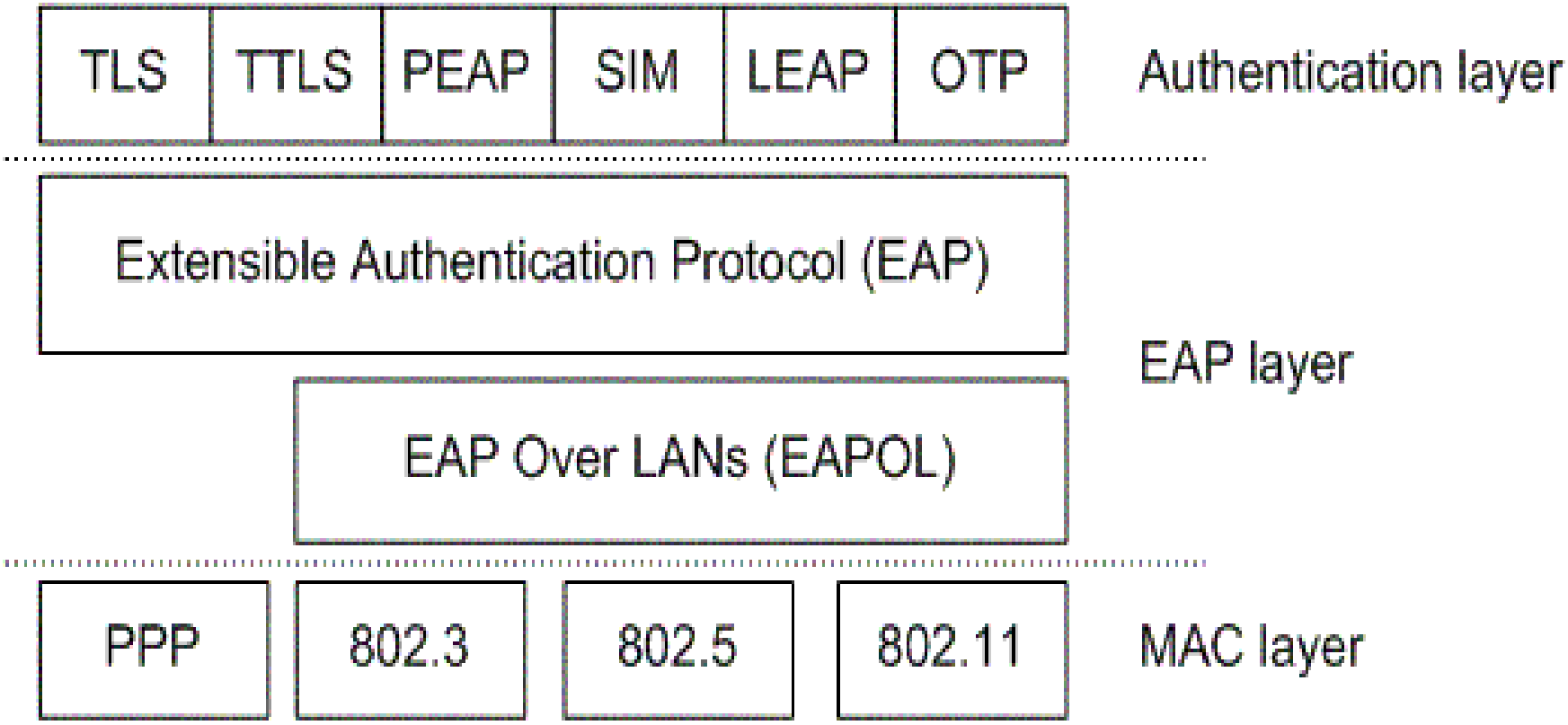


Key hierarchy

* **Used by both TKIP and CCMP**



802.1X - EAP



TLS - Transport Layer Security. Certificate based
TTLS - Tunneled TLS. Hybrid: certificate/password
PEAP - Protected EAP. Hybrid: certificate/password
SIM - SIM card based
LEAP - Cisco EAP variant. Password based
OTP - One Time Password. Password based

802.1X-EAP

* EAP provides a framework for authentication

* RADIUS is NOT part of 802.11i, but a 'back-end' protocol!
(but is the *de-facto* back-end protocol!)

* May support several different authentication mechanism (not part of 801.11i):
  - EAP-MD5: Username/password (IETF draft)
  - EAP-TLS: Creates a TLS session within the EAP authentication process. Needs certificates and therefore PKI. (RFC2716)
  - LEAP: Cisco propertiary
  - MS-CHAPv2: Microsoft username/password. (RFC2759)
  - EAP-TTLS vs. PEAP: tunnel mode for safe transport of authentication data

Linux support?

Supplicant:

- xsupplicant, wpa_supplicant

Authentication Server:

- FreeRADIUS

Note: problem with older drivers!

* Windows XP SP1: WPA

Okay - now what?

*** WorldWide WarDrive 4**

- covered 4 continents
- dicovered 228537 wireless networks
- **only 38% was using WEP!**
- WEP not the whole picture

*** WEP = insert a password and you're up**

*** 802.11i slightly more stuff!**

- **but: WPA-PSK**

Joachim Mæland

*** Who?**

- one of OLUG founding members
- likes wireless networks
- has a laptop running kismet
- uses GPS
- taxi driver

--> dangerous combination!

*** "At work":**

- laptop in front seat
- covered 68000km, 4000hours
- found 45000 wireless networks (50km radius Oslo)
- 55% don't use WEP/ WPA
- many AP don't change admin password
- DNS spoofing + phising anyone?
- *"where did my bank account go?"*

*** Impressive database: search for MAC-adress, vendors, ++**

- www.wlanhacker.net (online soon!)

802.11i summary

* **802.11i consist of three main part:**
  1. TKIP
  2. CCMP
  3. 802.1X
  + key managment

* **Wi-Fi Protected Access (WPA)**
  - TKIP + 802.1X
  - not a long term solution!
  - WPA-Personal (WPA-PSK) vs. WPA-Enterprise (WPA)

* **Robust Secure Networks (RSN)**
  - CCMP + 802.1X
  - likly to be called WPA2 so the marked not get confused

* **Transition Security Network (TSN)**
  - RSN which used TKIP instead of CCMP