Wireless Security - 802.11i

Lars Strand
lars (at) unik no
June 2004

THALES

Working Group 11 of IEEE 802

'Task Groups' within the WG enhance portions of the standard:

802.11 – 1997: The IEEE standard for wireless networks

- often called '802.11legacy'
- transfer using infrared or the 2.4GHz band
- radio uses frequence-hopping spread spectrum (FSSS) or direct-sequence spread spectrum (DSSS)
- 1 to 2 Mbps
- ratified in 1999, resulted in 802.11b
- today: '802.11 uses three different physical layers (PHY): 802.11a, 802.11b and 802.11g'

802.11a – 1999: Also called 'Wi-Fi5'

- uses orthogonal frequency division multiplexing (OFDM)
- not so crowded 5GHz with data rates from 6 to 54Mbps

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

- most used today
- ratified version of 802.11 (and the 802.11 groups was born)
- theoretical 11Mbps speed (average is 4-6Mbps)
- high rate DSSS in the (crowded) 2.4GHz band
- uses only DSSS
- 802.11b+ (non-standard) up to 22Mbps

802.11 Task Groups

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

802.11d – 2001: New countries

- modify physical layer to meet regulatory requirements

802.11e – 2002: Enhance MAC layer to improve QoS

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

802.11g – 2003: Higher rate extension to 2.4GHz band

- rate up to 54Mbps
- full backwards compatible with 802.11b (g's slow down to b)
- Super G = channel bonding up to 108Mbps

802.11h – 2003: Modified 802.11a

- in Europe, strong potensial for 802.11a interfering with satelite communications
- uses the 5GHz band
- will become the sucessor of 802.11a?

802.11i – 2004: new standard for wireless security

802.11j – work in progress: add 4.9 GHz and 5 GHz 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
- Transmit Power Control (TPC)

802.11 Task Groups

802.11l – skipped because it looks like 802.11i

802.11m – work in progress: for maintaince

802.11n – work in progress: new WLAN standard

- build from ground up (no “turbo-mode” chips)
- 100Mbps real speed (250Mbps at PHY level)
- better operating distance
- standard by the end of 2005?

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

802.11p – work in progress: using 5.9GHz band for ITS (long range)

802.11p – work in progress: using 5.9GHz band for ITS (long range)

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 – is often used to summarize all standards within the Working Group, but it is NOT a standard!

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 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)**

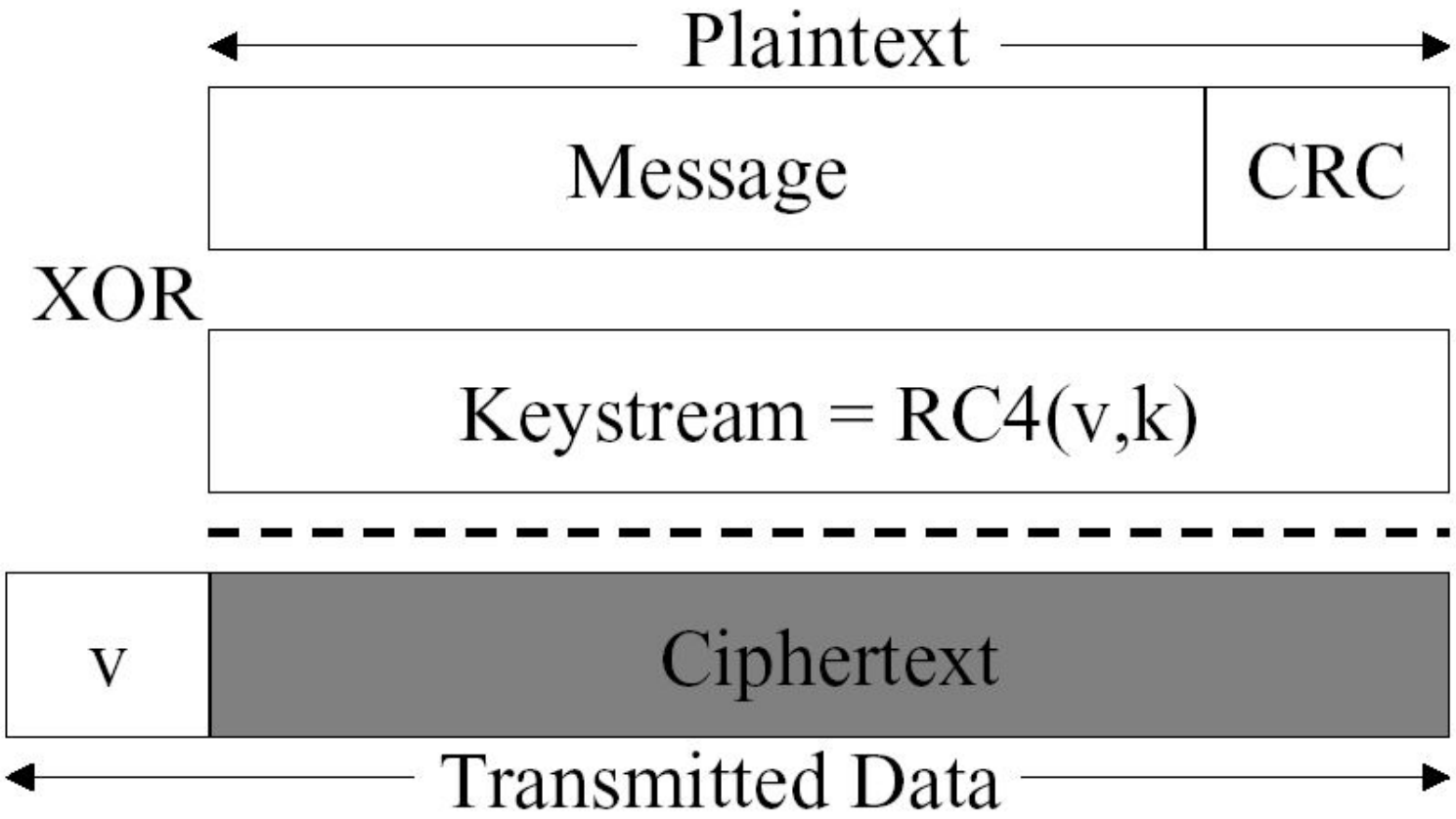


Figure borrowed from Borisov, Goldberg, Wagner 2001

Vulnerability of WEP

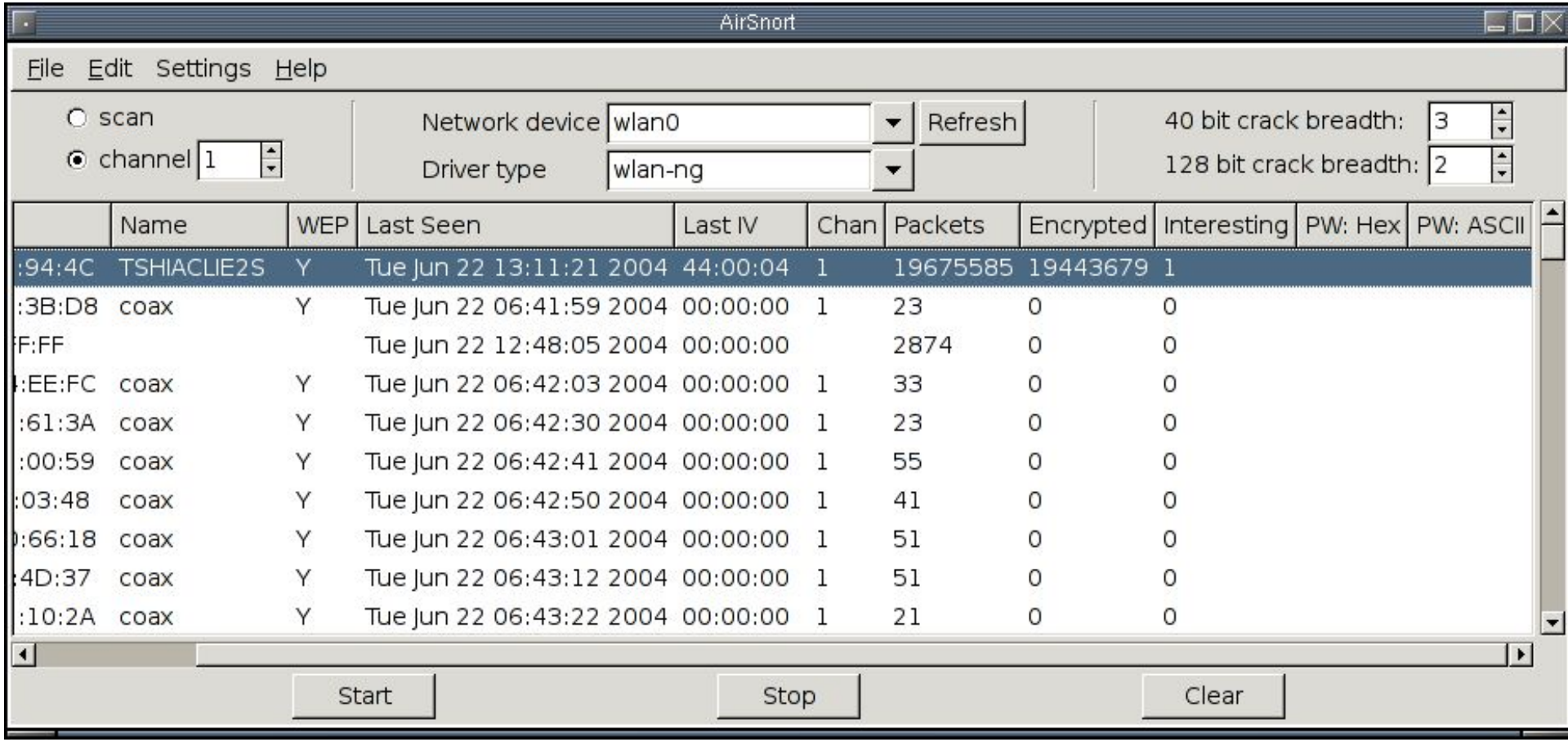
- WEP key recovery – limited IV range (0 to 16777215). Same IV used over and over again: information to crack WEP key (data confidentiality, access control)
- Violation of data integrity – modify the ciphertext and forward changed message even without knowing the encryption key (data integrity)
- Key management – static manual stored keys
- No access point autentication (authentication, access control)

Crypto experts: "WEP is a broken protocol!"

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

Vendor specific "fixes": longer keys, dynamic keys, VPN

Crack-tool: Airsnort


AirSnort
File Edit Settings Help
scan
channel 1
Network device wlan0
Refresh
Driver type wlan-ng
40 bit crack breadth: 3
128 bit crack breadth: 2
Name WEP Last Seen Last IV Chan Packets Encrypted Interesting PW: Hex PW: ASCII
:94:4C TSHIACLIE2S Y Tue Jun 22 13:11:21 2004 44:00:04 1 19675585 19443679 1
:3B:D8 coax Y Tue Jun 22 06:41:59 2004 00:00:00 1 23 0 0
F:FF Tue Jun 22 12:48:05 2004 00:00:00 2874 0 0
:EE:FC coax Y Tue Jun 22 06:42:03 2004 00:00:00 1 33 0 0
:61:3A coax Y Tue Jun 22 06:42:30 2004 00:00:00 1 23 0 0
:00:59 coax Y Tue Jun 22 06:42:41 2004 00:00:00 1 55 0 0
:03:48 coax Y Tue Jun 22 06:42:50 2004 00:00:00 1 41 0 0
:66:18 coax Y Tue Jun 22 06:43:01 2004 00:00:00 1 51 0 0
4D:37 coax Y Tue Jun 22 06:43:12 2004 00:00:00 1 51 0 0
:10:2A coax Y Tue Jun 22 06:43:22 2004 00:00:00 1 21 0 0
Start
Stop
Clear

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

Temporary Key Integrity Protocol (TKIP)

802.11's response to do something – anything – to improve security
Wi-Fi Alliance did not have time to wait for 802.11i --> WPA

- Enhancment of WEP – fixes all know WEP flaws
- Software/firmware upgrade 802.11b equipment
- Will degrade performance: uses more CPU in 802.11b devices!
- Not ideal design – more 'hacks' to make it work
- **NB! Not a long term solution!**

1. Michael: Crypthographic Message Integrity Code (MIC)

- SHA-1/MD5 are to CPU-expensive
- 64bit MIC designed by Niels Ferguson
- 'weak' integrity protection (2^29 attack exists) – limited CPU!
- TKIP countermeasure: MIC is encrypted + key discarded if attacked (more than 2 failed MIC pr. second)
- only 'secure' when used with a secure encryption system (RC4 with rapid re-keying and per-packet mixing)
- defeating forgeries

2. IV sequence enforment

- IV extended from 24 to 48 bits
- careful sequencing rules to prevent reuse
- defeating replays

3. Key mixing: per-packet keying – defeating weak keys

* phase 1:

  temporary key (TK) 128bit, client's MAC address (TA), IV32 (most significant 32 bits of IV) = P1K 80bits

* phase 2:

  P1K, IV16, TK = per-packet key (RC4KEY) 128bit

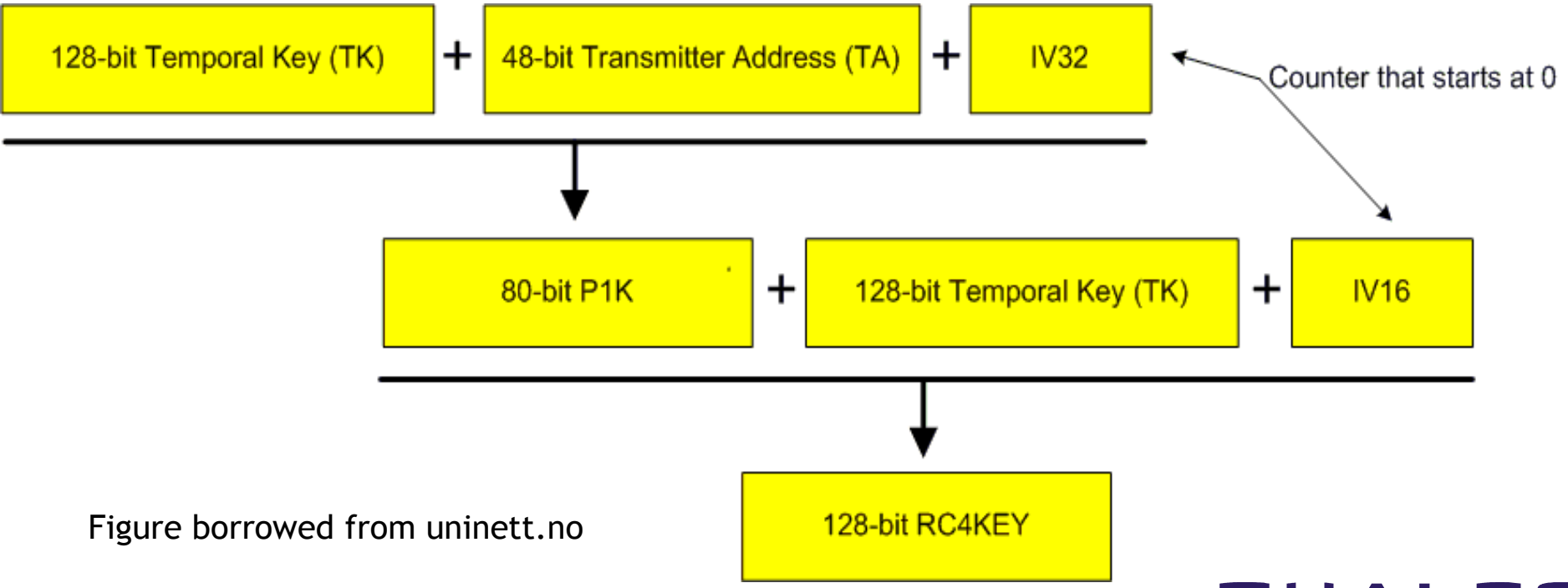
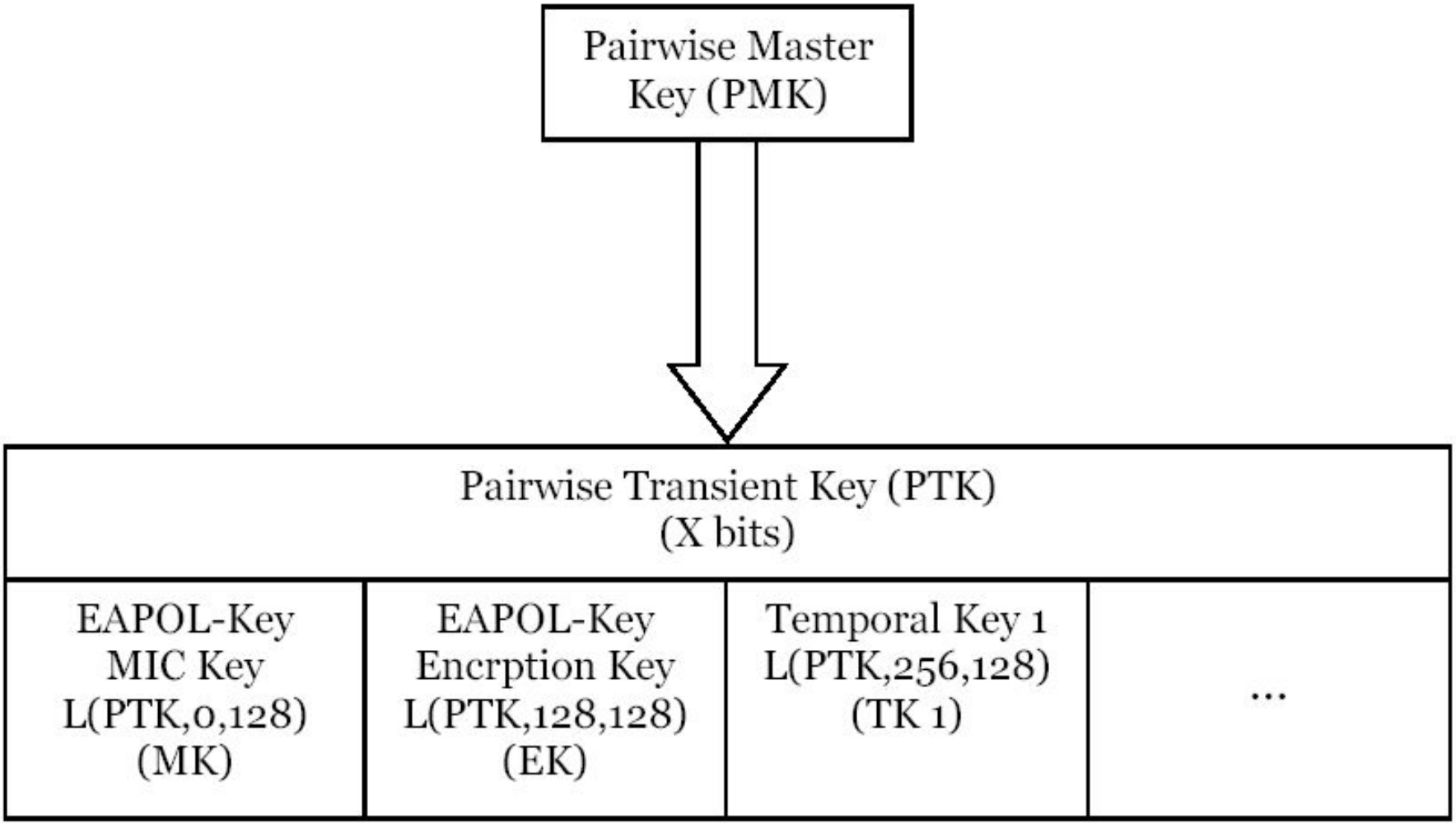


Figure borrowed from uninett.no

4. Rekeying – delivers fresh keys to various TKIP algorithms

- Master Key normally generated by authentication
- PMK is derived from the master key



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

The new flagship of wireless security!

* designed by N. Ferguson, R. Housley and D. Whiting

* public domain

* protocol designed from ground-up
  - not withstood the test of time...
  - but based on well known technology
  - critized for beeing to complex

* block ciphers provides privacy but not authenticy
* combined modes (authenticated-encryption modes)
    - privacy AND authentication

* CCMP = combined mode:
    - Counter Mode (CTR) encryption mode = privacy
    - CBC- MAC = integrity and authentication

Uses flashy new AES with 128bit keys, 48bit IV

What about Wireless Robust Authentication Protocol (WRAP)??
    - based upon Offset Codebook (OCB) mode of AES
    - plagued by intellectual property rights (patents)
    - RSN: CCMP is mandatory, WRAPS optional

Port based authentication protocol for Ethernet (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

General EAP authentication with RADIUS as AAA protocol

AAA = Authentication, Authorization, Accounting

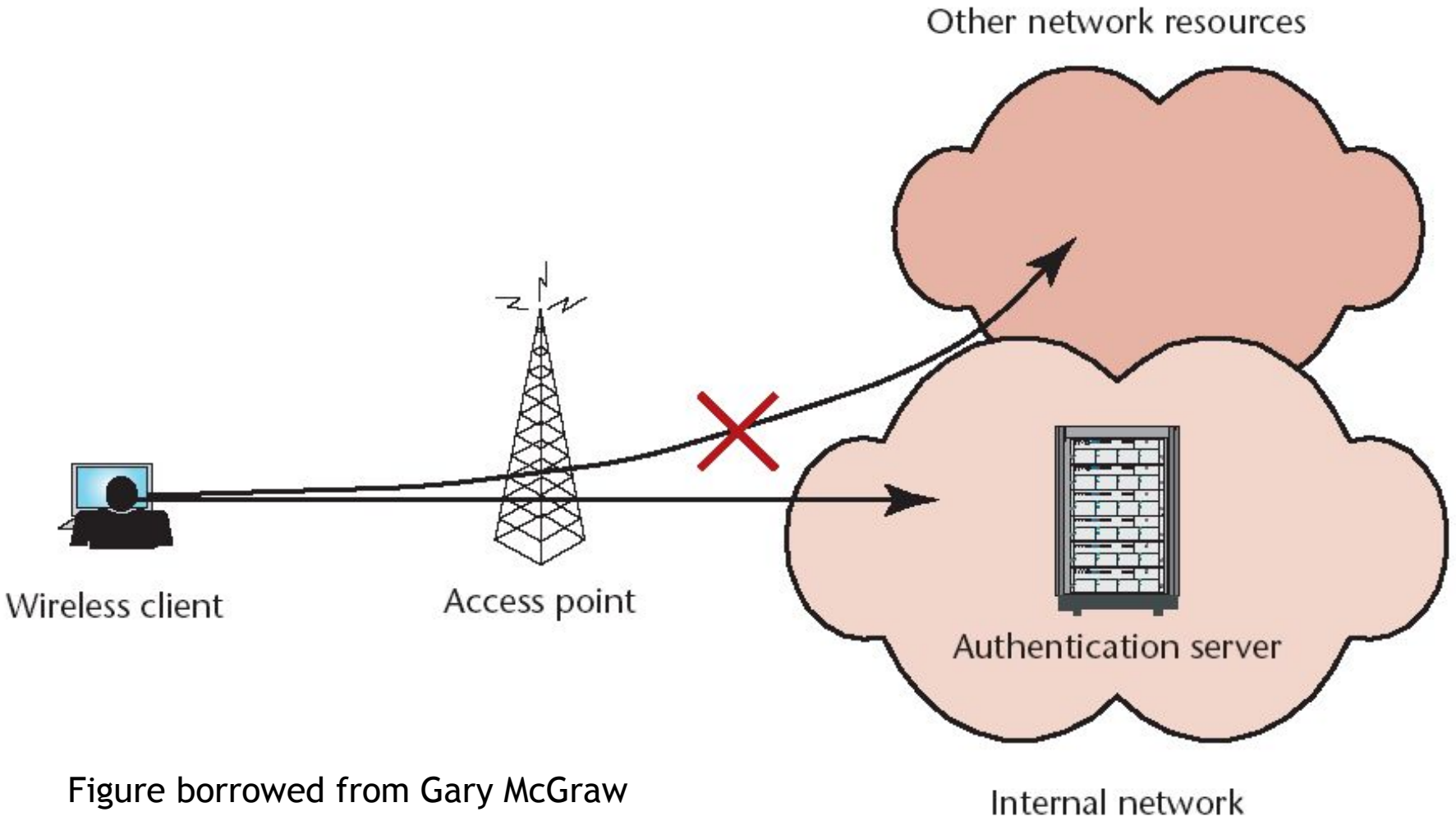
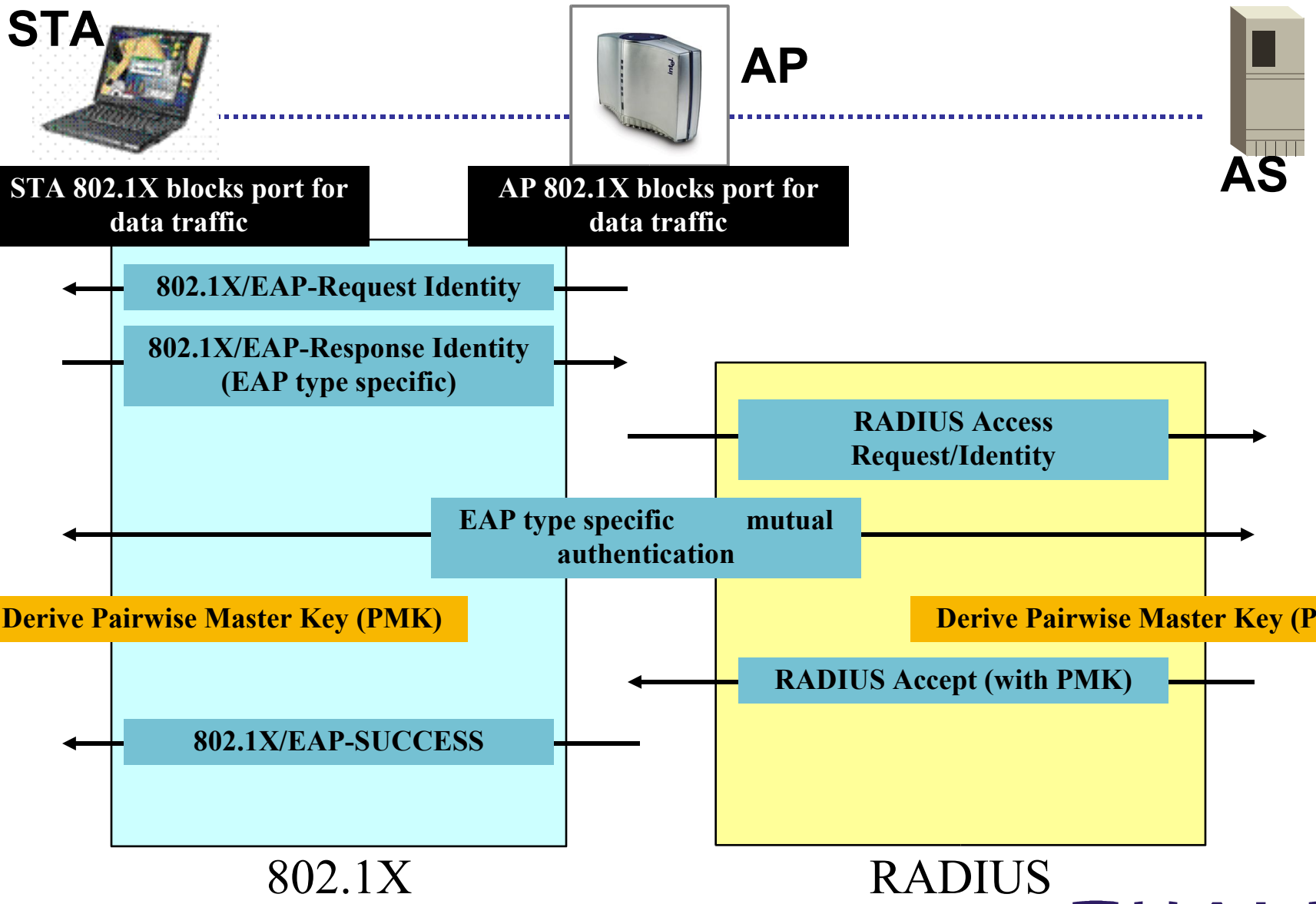


Figure borrowed from Gary McGraw

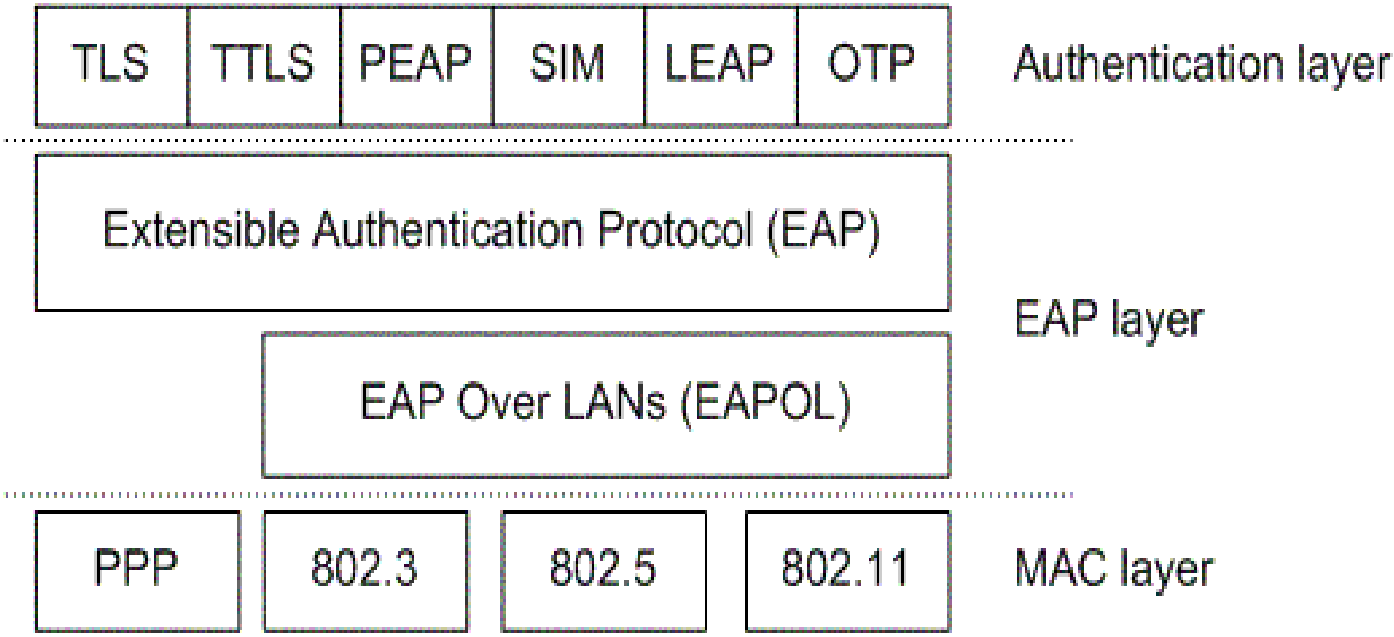
802.1X- EAP authentication overview



Slide borrowed from Jesse Walker

THALES

Security layers



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

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

EAP provides a framework for authentication

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

802.11i consist of three main part:

1) TKIP

2) CCMP

3) 802.1X

+ key management!

Wi-Fi Protected Access (WPA)

- TKIP + 802.1X
- Wi-Fi Alliance tok 'snapshot' of unfinished 802.11i = WPA

Robust Secure Networks (RSN)

- CCMP + 802.1X
- may also be called WPA2

Transition Security Network (TSN)

- RSN which uses TKIP instead of CCMP

* how to support roaming between access points?
  - update all other AP?

* how to make key-architecture support ad-hoc networks?
  - today:
    i) session oriented to syncronize master key
    ii) assume 802.1x authentication server
    --> Oakly, Diffie-Hellman, El-Gamal? - must share a secret!

Does NOT exists in ad-hoc networks!
  - add these security mechanism
  - alter the security architecture
  --> else: security not possible

Eurofighter: authenticate and make devices talk

Distributed RADIUS server?

- Group keys: Who issues master keys? Vote for master?
- what if two manet merges? --> issue new master group key?

Existing solution: change to EAP

Two level authentication