SECURE WIRELESS LAN

Keamanan Jaringan

Program Studi Teknik Telekomunikasi

Fakultas Teknik Elektro

Telkom University

2017

KERANGKA

- What's Wireless LAN
- Security History
- Main WEP Vulnerabilities
- WLAN Security Enhancement
- Summary

WIRELESS LAN

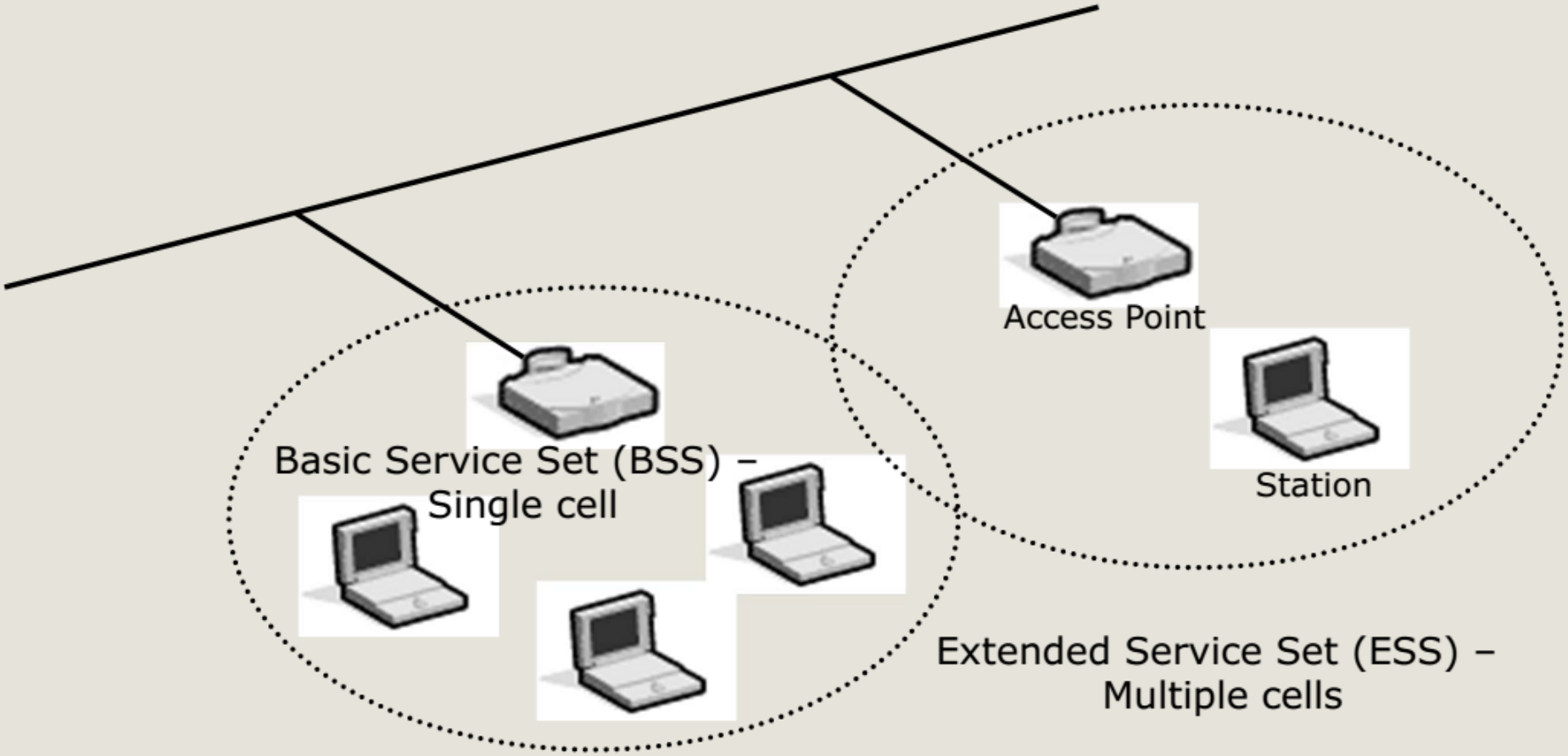
- IEEE ratified 802.11 in 1997.
  - Also known as Wi-Fi
  - Last ratified version in 2007
- Wireless LAN at 1 Mbps & 2 Mbps
- WECA (Wireless Ethernet Compatibility Alliance) promoted Interoperability
  - Now Wi-Fi Alliance
- 802.11 focuses on Layer 1 & Layer 2 of OSI model.
  - Physical layer
  - Data link layer

WIRELESS LAN (MODE)

- Infrastructure mode
  - Basic Service Set
    - One access point
  - Extended Service Set
    - Two or more BSSs forming a single subnet.
  - Most corporate LANs in this mode.
- Ad-hoc mode
  - Independent Basic Service Set
  - Set of 802.11 wireless stations that communicate directly without an access point.
    - Useful for quick & easy wireless networks.

WIRELESS LAN (MODE)

Infrastructure mode

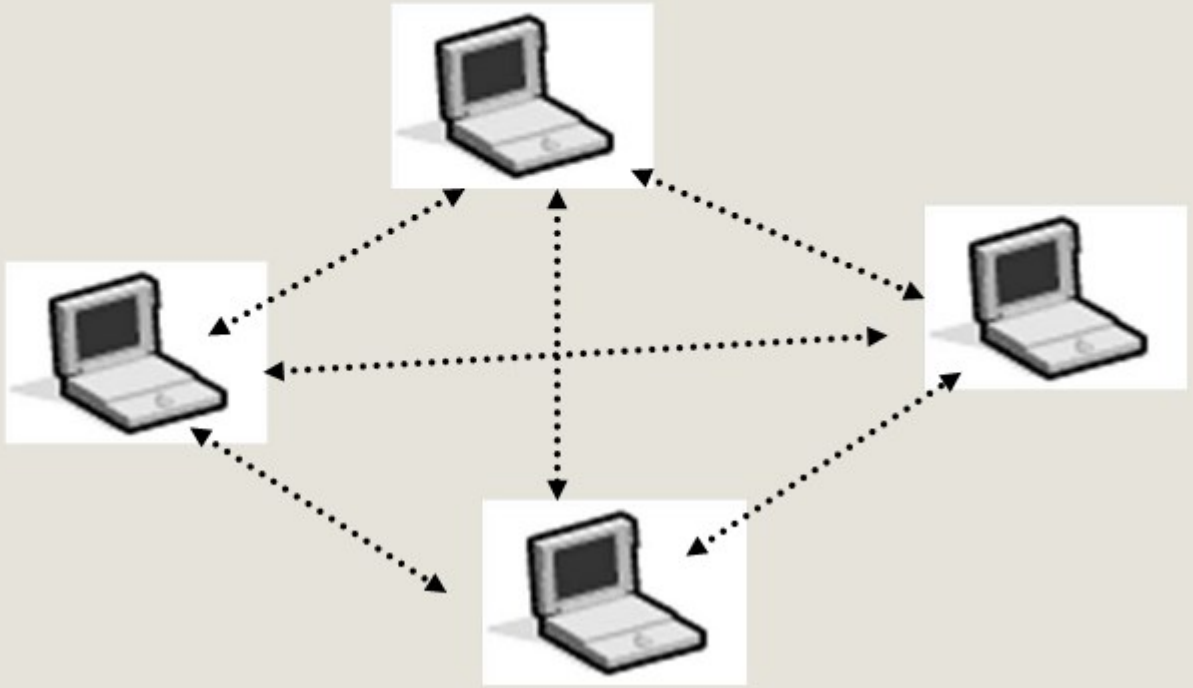


SSID (Service Set Identifier) attached to all packets belonging to a BSS

multiple APs with same SSID form Extended Service Set.

WIRELESS LAN (MODE)

Ad-hoc mode



WLAN SECURITY

SEJARAH KEAMANAN WLAN

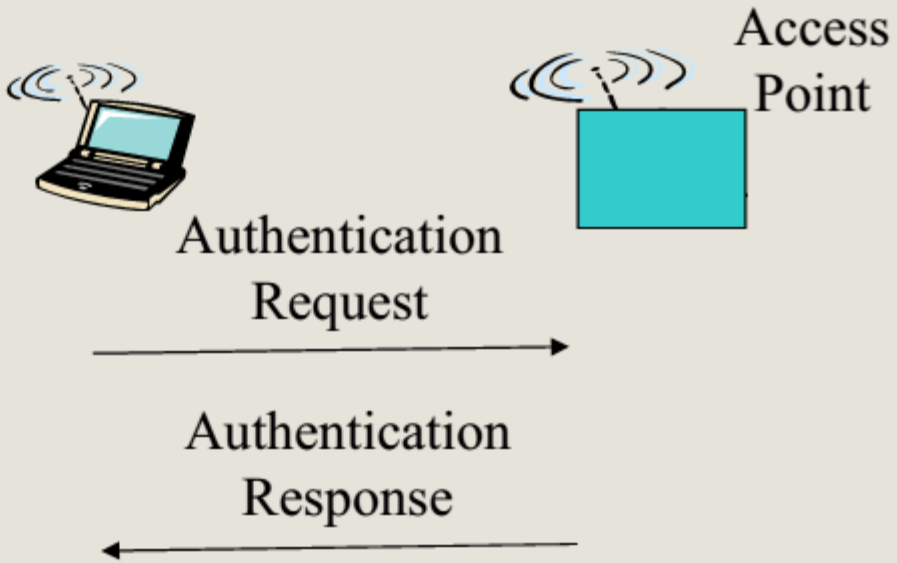
- Wireless LAN uses radio signal
- Attacker needs equipment capable of:
  - monitoring (passive attacks) and transmitting (active attacks) encrypted traffic
    - passive attacks can be carried out using off-the-shelf equipment by modifying driver settings
    - active attacks are more difficult but not beyond reach and easy when firmware (e.g., Orinocco) of PCMCIA cards can be upgraded
- Prudent to assume that motivated attackers have full access to link layer for passive and active attacks

SEJARAH KEAMANAN WLAN (LAYANAN KEAMANAN 802.11B)

- Authentication
  - Open System Authentication
  - Shared Key Authentication
- Confidentiality, Access Control, Data integrity
  - Wired Equivalent Privacy (WEP)

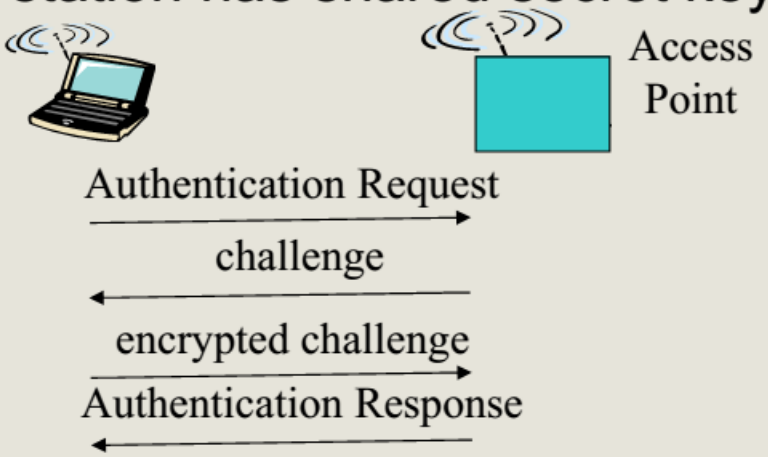
SEJARAH KEAMANAN WLAN (OTENTIKASI SISTEM TERBUKA)

- Authentication Request = Station ID
- Authentication Response = success or failure
- On success: both stations mutually authenticated



SEJARAH KEAMANAN WLAN (OTENTIKASI SHARED KEY)

- When station requests association with Access Point
  - AP sends random number to station (challenge)
  - Station encrypts random number
    - Uses RC4
    - Encrypted random number (encrypted challenge) sent to AP
  - AP decrypts received message
    - Uses RC4
  - AP compares decrypted random number to transmitted random number
- If numbers match, station has shared secret key.



SEJARAH KEAMANAN WLAN (WIRED EQUIVALENT PRIVACY)

- Shared key, usually, between all:
  - Stations.
  - An Access Point.
- Extended Service Set
  - All Access Points will have, usually, same shared key.
- Usually, no key management
  - Shared key entered usually manually into:
    - Stations
    - Access points
    - Key management nightmare in large wireless LANs

KEAMANAN WLAN (KODE RON NOMOR 4)

- Ron's Code number 4 (RC4)
  - Symmetric key encryption
  - RSA Security Inc.
  - Designed in 1987 by Ronald Rivest
  - Trade secret until leak in 1994.
- RC4 can use key sizes from 1 byte to 256 bytes
- Supports:
  - RC4-KSA (Key Scheduling Algorithm): translates key of length 1 byte to 256 bytes to initial permutations of numbers 0 to 255
  - RC4-PRNG: generates stream of pseudo random using initial permutation numbers
    - XORed with plaintext to create ciphertext.

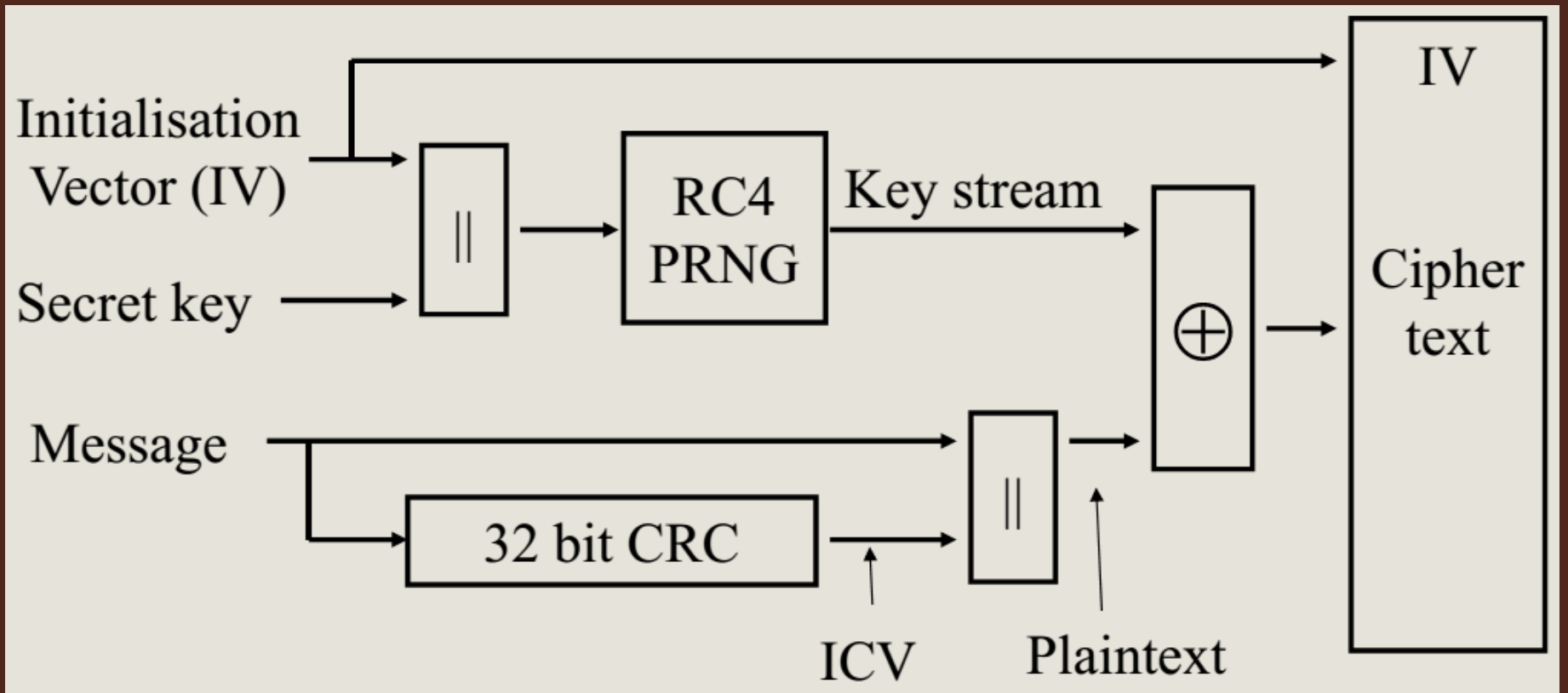
KEAMANAN WLAN (KODE RON NOMOR 4)

- Pseudocode algoritma RC4
  - i, j = 0;
  - while (true) {
    - i = (i + 1) mod 8;
    - j = (j + S[i]) mod 8;
    - Swap (S[i], S[j]);
    - t = (S[i] + S[j]) mod 8;
    - k = S[t]; }

KEAMANAN WLAN (PENGIRIMAN WEP)

- Compute Integrity Check Vector (ICV)
  - 32 bit Cyclic Redundancy Check.
  - Appended to message to create plaintext.
  - Provides integrity
- Plaintext encrypted via RC4
  - Provides confidentiality.
  - Plaintext XORed with long key stream of pseudo random bits.
  - Key stream is function of
    - 40-bit secret key (vendors extended this to 104-bits)
    - 24 bit Initialisation Vector (IV)
- Ciphertext is transmitted.

KEAMANAN WLAN (ENKRIPSI WEP)

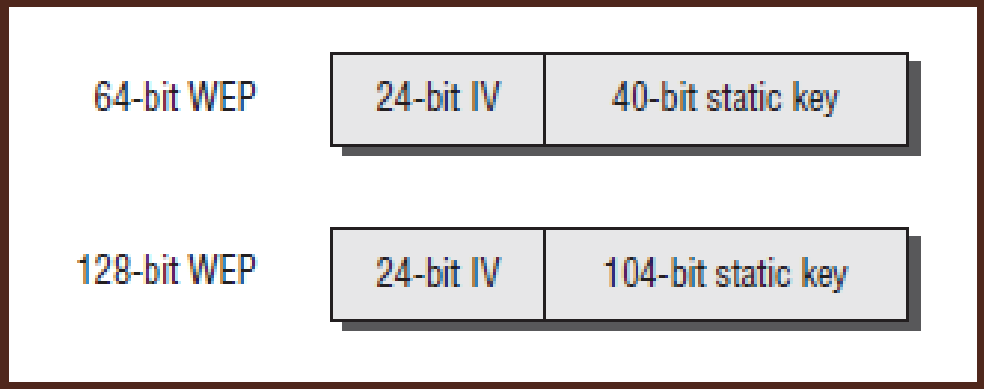


PRNG = Pseudo Random Number Generation
(note: RC4-KSA also part of RC4 PRNG block)

KEAMANAN WLAN (PENERIMAAN WEP)

- Ciphertext is received.
- Ciphertext decrypted via RC4
  - Ciphertext XORed with long key stream of pseudo random bits.
  - Key stream is function of
    - 40-bit secret key (or 104-bit secret key)
    - 24 bit initialisation vector (IV)
- Check ICV
  - Use plaintext and separate ICV from message.
  - Compute ICV for message
  - Compare with received ICV

Static WEP Encryption Key and Initialization Vector (1)



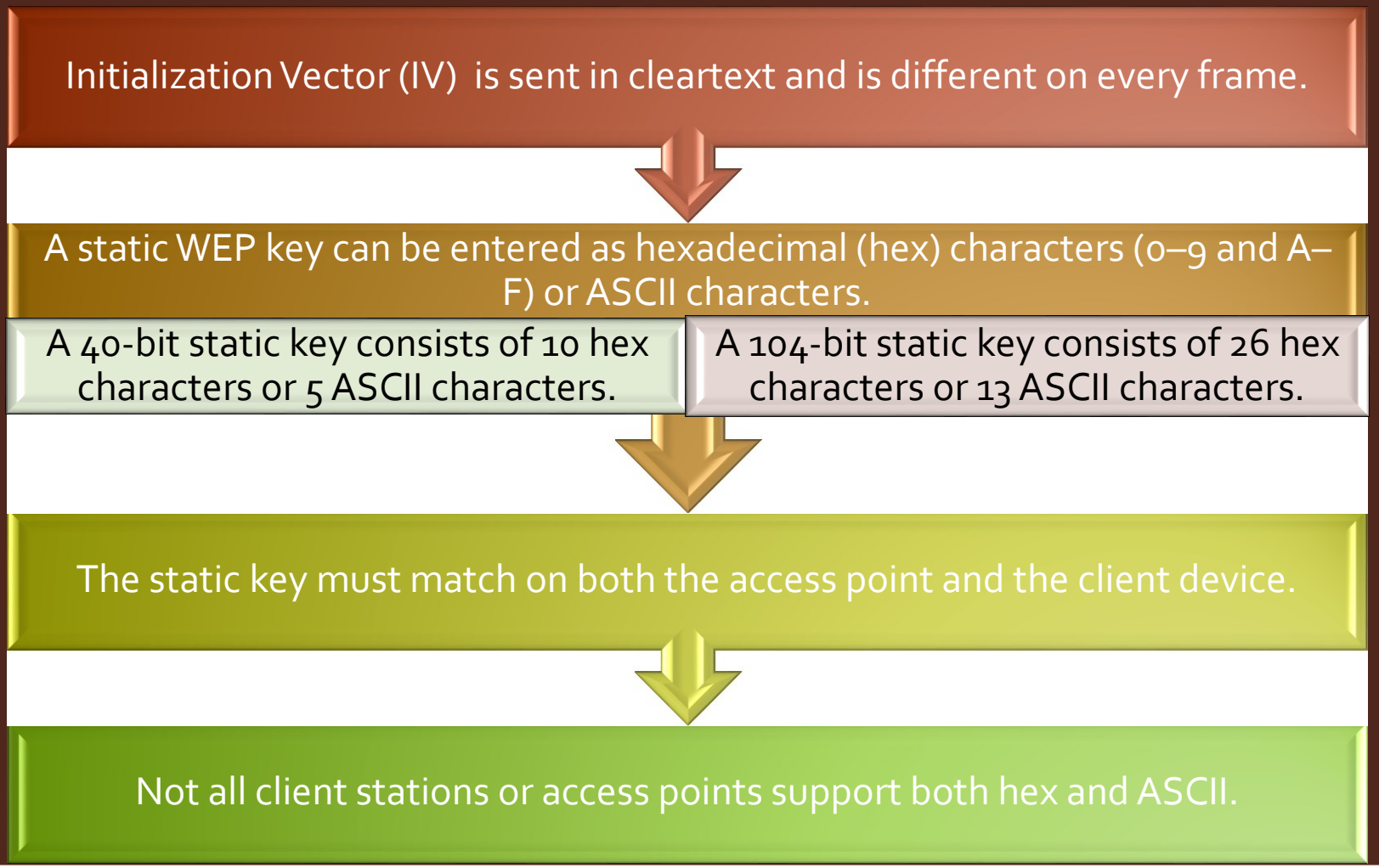
64-bit WEP

- a secret 40-bit static key
- a 24-bit number Initialization Vector (IV)

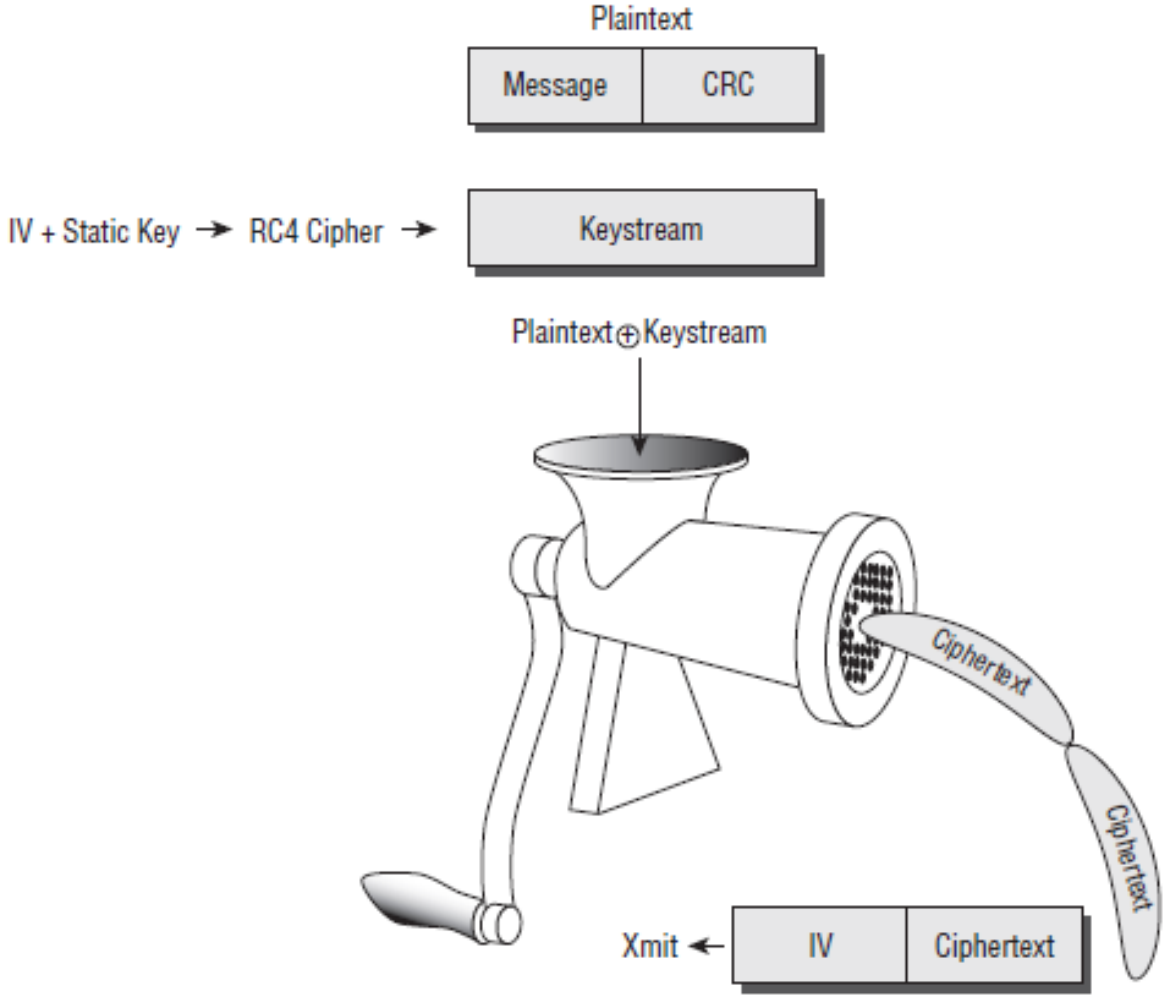
128-bit WEP

- a secret 104-bit static key
- a 24-bit number Initialization Vector (IV)

Static WEP Encryption Key and Initialization Vector (2)

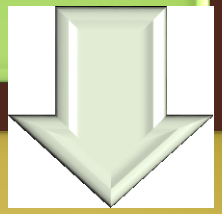


How does WEP work? (1)

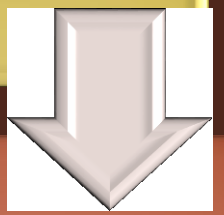


How does WEP work? (2)

WEP runs a cyclic redundancy check (CRC) on the plaintext data that is to be encrypted and then appends the Integrity Check Value (ICV) to the end of the plaintext data.



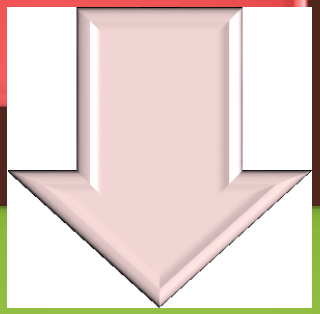
A 24-bit cleartext Initialization Vector (IV) is then generated and combined with the static secret key.



WEP then uses both the static key and the IV as seeding material through a pseudo-random algorithm that generates random bits of data known as a keystream.

How does WEP work? (3)

The pseudo-random bits in the keystream are then combined with the plaintext data bits using a Boolean XOR process.



The end result is the WEP ciphertext, which is the encrypted data. The encrypted data is then prefixed with the cleartext IV.

KELEMAHAN WEP (SERANGAN WEP PASIF)

- If 24 bit IV is an ascending counter,
  - If Access Point transmits at 11 Mbps and packet length approx. 1500 bytes
  - All IVs are exhausted in roughly 5 hours.

Buktikan!

- If 24 bit IV uses a random generator:
  - due to birthday paradox, and assuming that probability of sequnce number match is 50% then a number of collisions occur after transmitting approx. 5000 packets, recovered within a transmission of few minutes
  - Birthday paradox equation, see also Appendix B in:

http://betterexplained.com/articles/understanding-the-birthday-paradox/

$$n \approx \sqrt{-2 * \ln(1-m)} * \sqrt{T}$$

Where:

n = number of packets before a collision occurs

m = probability of match (that two packets use the same sequence number)

T = Maximum number of packets with different sequence number

SERANGAN WEP PASIF

- Passive attack:
  - Attacker collects all traffic
  - Attacker could collect two messages:
    - Encrypted with same key and same IV
    - Xoring two ciphertexts causes keystream to cancel out and result is the XOR of two plaintexts
    - each of the XORed plaintexts can be calculated when there is partial knowledge of some part of the plaintexts:
      - statistical attacks to reveal plaintext

KELEMAHAN IV

- Paper from Fluhrer, Mantin, Shamir (FMS), 2001:
  http://wiki-files.aircrack-ng.org/doc/rc4_ksaproc.pdf
- Passive attack on WEP able to retrieve entire secret key in relatively small amount of time (4.000.000 packets)
- get information about all key bytes when PRNG input is known:
  - Capture packets with weak IV
    (specific IV values that easy calculation of a key byte when previous key bytes are known)
  - First output byte ciphertext per IV is known:
    Every wireless frame has reliable and known first byte
    - Sub-network Access Protocol header (SNAP) used in logical link control layer, upper sub-layer of data link layer.
    - First byte is 0xAA

SERANGAN WEP AKTIF

- If attacker knows plaintext and ciphertext pair
  - Keystream for IV values are known.
    - Plaintext XOR Ciphertext = Keystream
    - Build decryption dictionaries as tables of
      - Keystream value ⇔ IV value
  - Attacker can create correctly encrypted messages.
      - keystream XOR plaintext = cyphertext
      - cyphertext sent together with known IV
  - Access Point is deceived into accepting messages.
- Message authentication using CRC checksum not secure enough, e.g. Bitflipping, for integrity check:
  - Flip a bit in ciphertext
  - Bit difference in CRC-32 can be computed due to linear property:
    - checksum(M XOR Diff) = checksum(M) XOR checksum(Diff)

Mengapa?

PENGUATAN KEAMANAN WLAN

WI-FI PROTECTED ACCESS

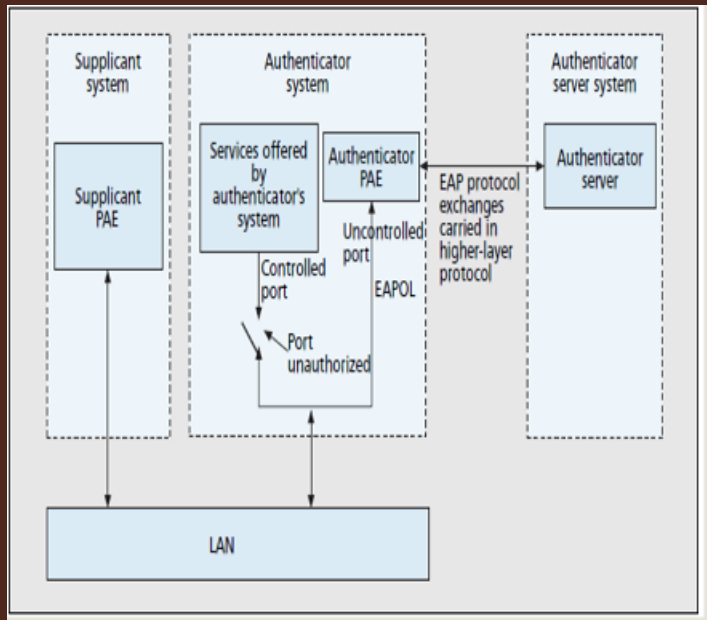
PENGUATAN KEAMANAN WLAN

- defines security framework in upper OSI layers to provide compatible authentication & authorization for IEEE 802 LAN
- distributes keys for 802.11 and enabling authentication and encryption between APs and wireless stations

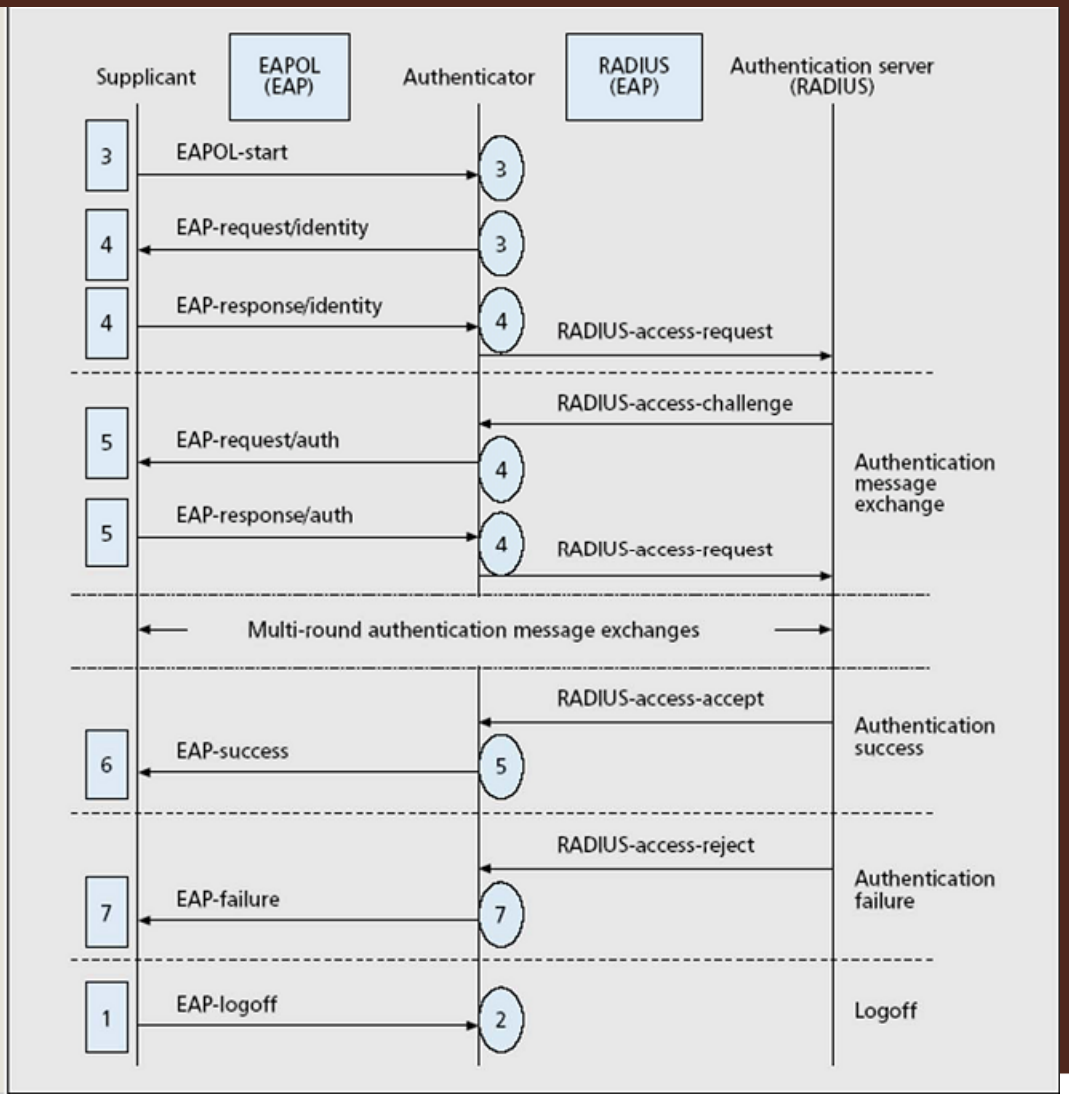
Main components:

- Supplicant (*wireless station*)
- Authenticator (*access point*)
- Authentication server (RADIUS or DIAMETER)
- EAP (RFC2284):
  - MD5, TLS, Tunelled TLS (TTLS), Protected EAP (PEAP), EAP SIMs
  - only supplicant & authentication server need understand authentication mechanisms
- EAP over LANs (EAPOL): encapsulates EAP messages between Supplicant & Authenticator

PENGUATAN KEAMANAN WLAN (IEEE 802.1X)



- IEEE 802.1x : port-based network access control



PENGUATAN KEAMANAN WLAN (IEEE 802.1X)

Supplicant Roaming

- supplicant should re-authenticate with Authenticator or Authentication Server when roaming to another 802.1X-enabled network
- Intra-subnet roaming:
  - moves from one Authenticator to another within the same IP subnet
- Intersubnet roaming:
  - Moves from one Authenticator to another Authenticator located in another IP subnet (Supplicant has to change its IP address)
  - Use IETF Mobile IP to support mobility management in the IP layer
- More info on IEEE 802.1X:
  - http://www.ieee802.org/1/files/public/docs2000/8021xSecurity.PDF

PENGUATAN KEAMANAN WLAN (WPA)

Wi-Fi Protected Access (WPA)

- Pre-shared mode: home environment, use Pre-shared keys (PSK)
- Enterprise mode: use
  - 802.1X authentication & key management
  - EAP & (RADIUS or DIAMETER)

Encryption:

- TKIP (Temporal Key Integrity Protocol) or WEP2
  - 128-bit secret key
  - RC4 session-based dynamic encryption keys, with 32 CRC as ICV
  - 48b TKIP sequence counter (TSC) is used to generate IV and
    - avoid replay attack (verify sequence order of MPDU); reset to 0 on new key and incremented.
    - IV reuse is prevented by changing WEP key on IV recycling
  - Michael 8 byte key: a non-linear message integrity code (MIC) in addition to 32 CRC
  - Longer IV + Per-Packet Key mixing => Per-Packet WEP Key + MIC

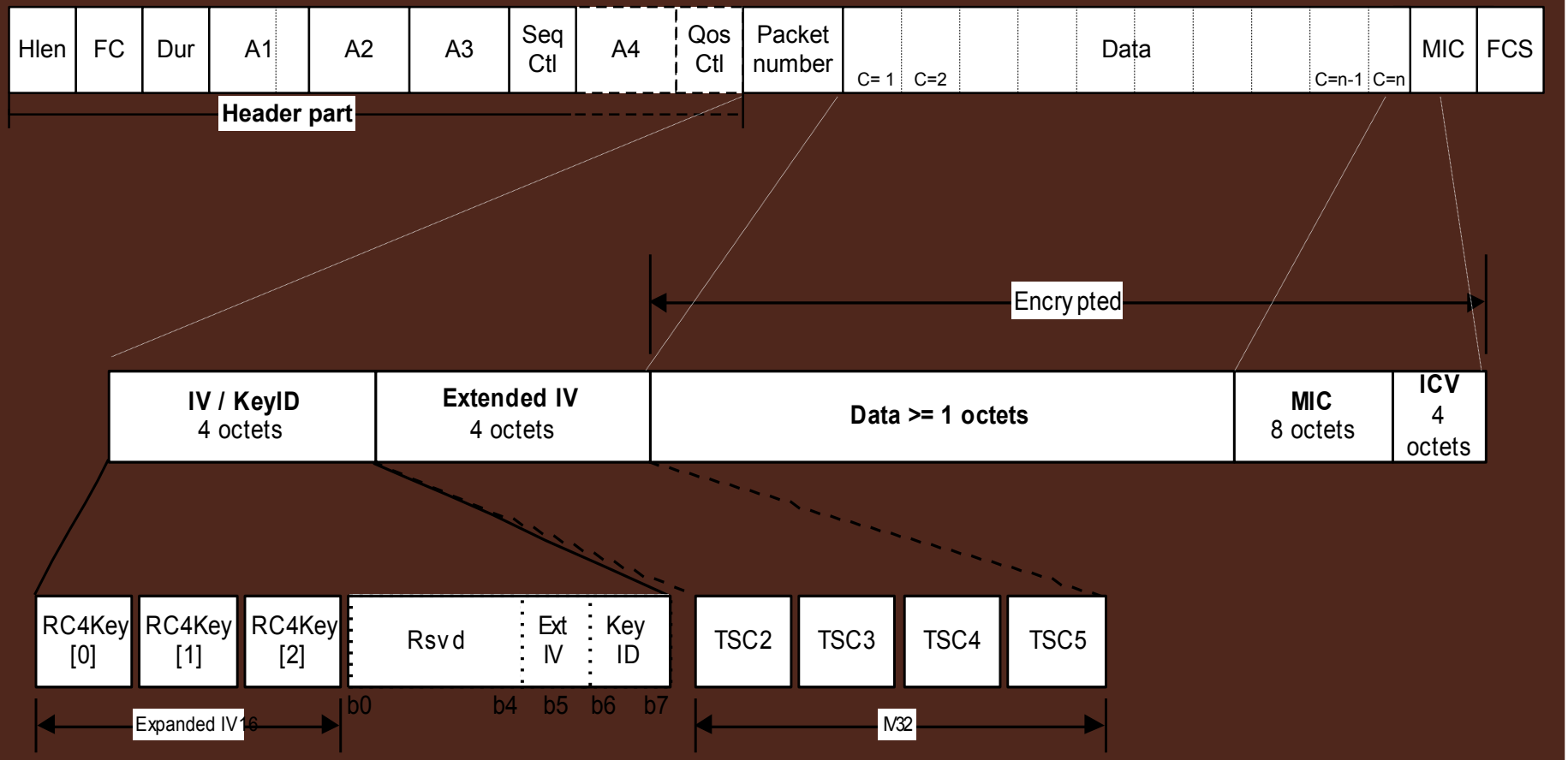
TKIP

- TKIP: *T*emporal *K*ey *I*ntegrity *P*rotocol
- Designed as a wrapper around WEP
  - Can be implemented in software
  - Reuses existing WEP hardware
  - Runs WEP as a sub-component
- Meets criteria for a good standard: everyone unhappy with it

TKIP design challenges

- Mask WEP's weaknesses…
  - Prevent data forgery
  - Prevent replay attacks
  - Prevent encryption misuse
  - Prevent key reuse
- … On existing AP hardware
  - 33 or 25 MHz ARM7 or i486 already running at 90% CPU utilization before TKIP
  - Utilize existing WEP off-load hardware
  - Software/firmware upgrade only
  - Don't unduly degrade performance

TKIP MPDU Format



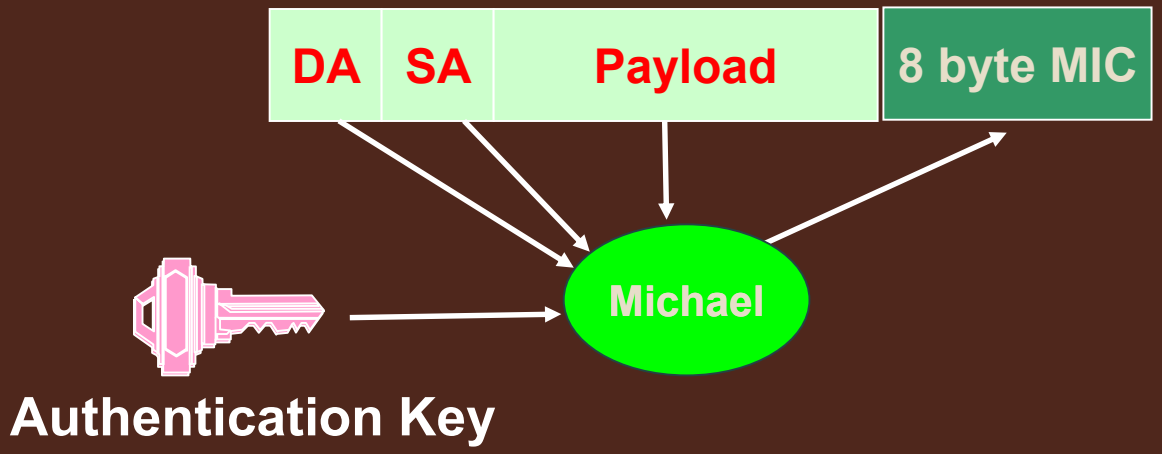
TKIP Keys

- TKIP Keys
  - 1 128-bit encryption key
    - AP and STA use the same key
    - TKIP's per-packet key construction makes this kosher
  - 2 64-bit data integrity keys
    - AP, STA use different keys for transmit

TKIP Design (1) -- Michael

Protect against forgeries

- Must be cheap: CPU budget ≤ 5 instructions/byte
- Unfortunately is weak: a 2^{29} message attack exists
- Computed over MSDUs, while WEP is over MPDUs
- Uses two 64-bit keys, one in each link direction
- Requires countermeasures: rekey on active attack, rate limit rekeying



TKIP Countermeasures

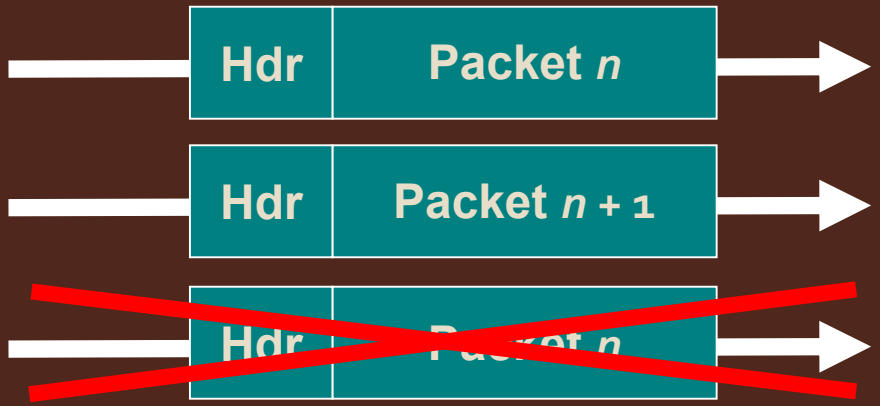
- Check CRC, ICV, and IV before verifying MIC
  - Minimizes chances of false positives
  - If MIC failure, almost certain active attack underway
- If an active attack is detected:
  - Stop using keys
  - Rate limit key generation to 1 per minute

TKIP Design (3)

Protect against replay

- reset packet sequence # to 0 on rekey
- increment sequence # by 1 on each packet
- drop any packet received out of sequence

Wireless Station

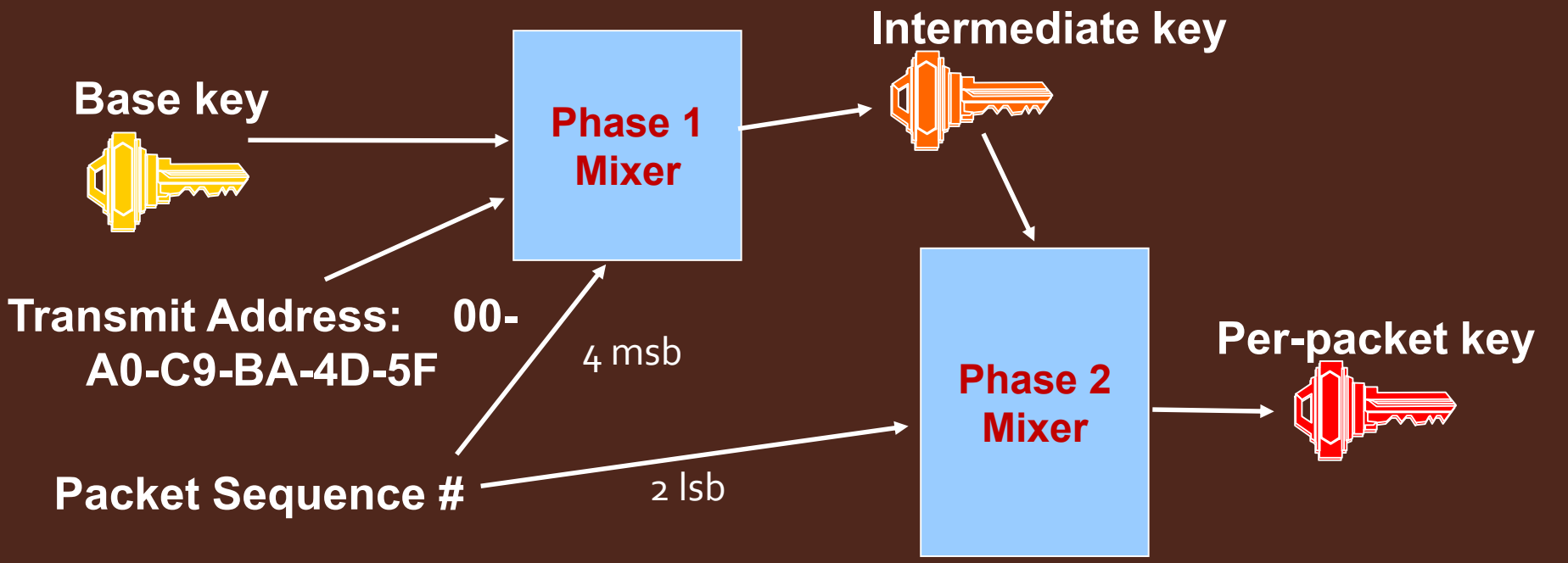


Access Point

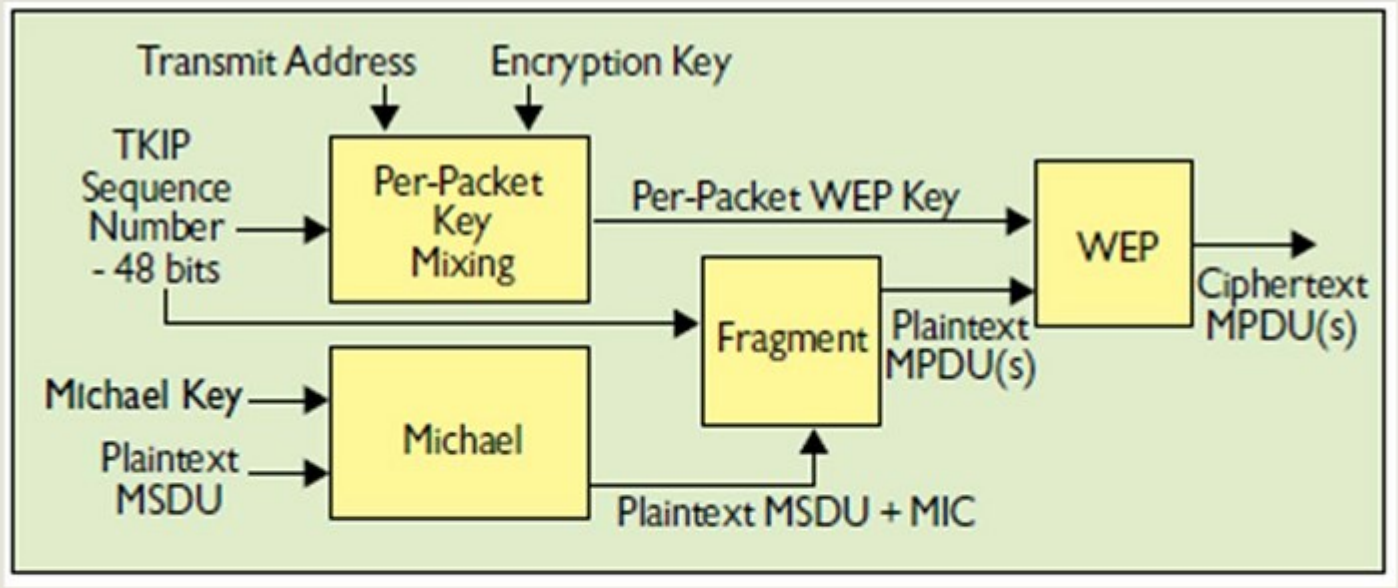
TKIP Design (4)

Stop WEP's encryption abuse

- Build a better per-packet encryption key…
- … by preventing weak-key attacks and decorrelating WEP IV and per-packet key
- must be efficient on existing hardware



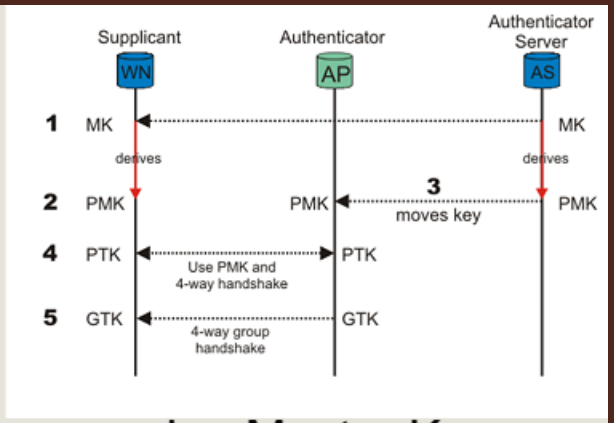
PENGUATAN KEAMANAN WLAN (WPA)



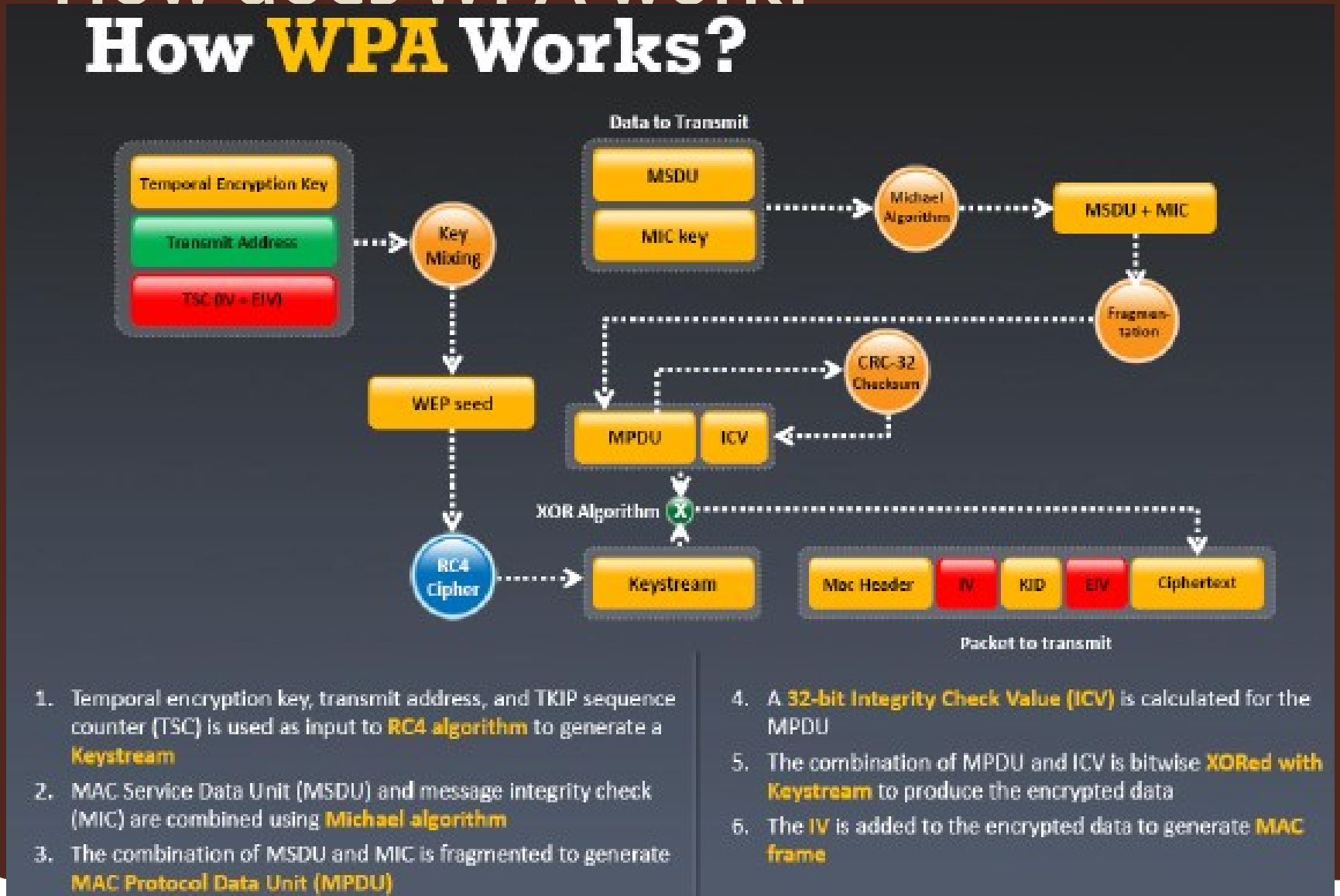
- Taken from: http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf

PENGUATAN KEAMANAN WLAN (WPA)

- Key management and establishment
  - Manual
  - Automatic: 802.1X used for support key management:
    - After 802.1X Supplicant & Authentication server using Master Key (MK) obtain independently the Pairwise Master Key (PMK)
    - Authentication Server sends PMK to Authenticator
    - Supplicant & Authenticator use PMK & more.., to generate each:
      - Pairwise Transient Key (PTK) using four way handshake, consists of:
        - » EAPOL-Key Confirmation Key (KCK)
        - » EAPOL-Key Encryption Key (KEK)
        - » Temporal Key (TK 1 & 2) used for encrypting wireless traffic; TK is further computed using MAC address and IV to produce unique security key per wireless station and per packet
      - Group Transient Key (GTK) for encrypting broadcast message



How does WPA work?



How WPA Addresses The WEP Vulnerability

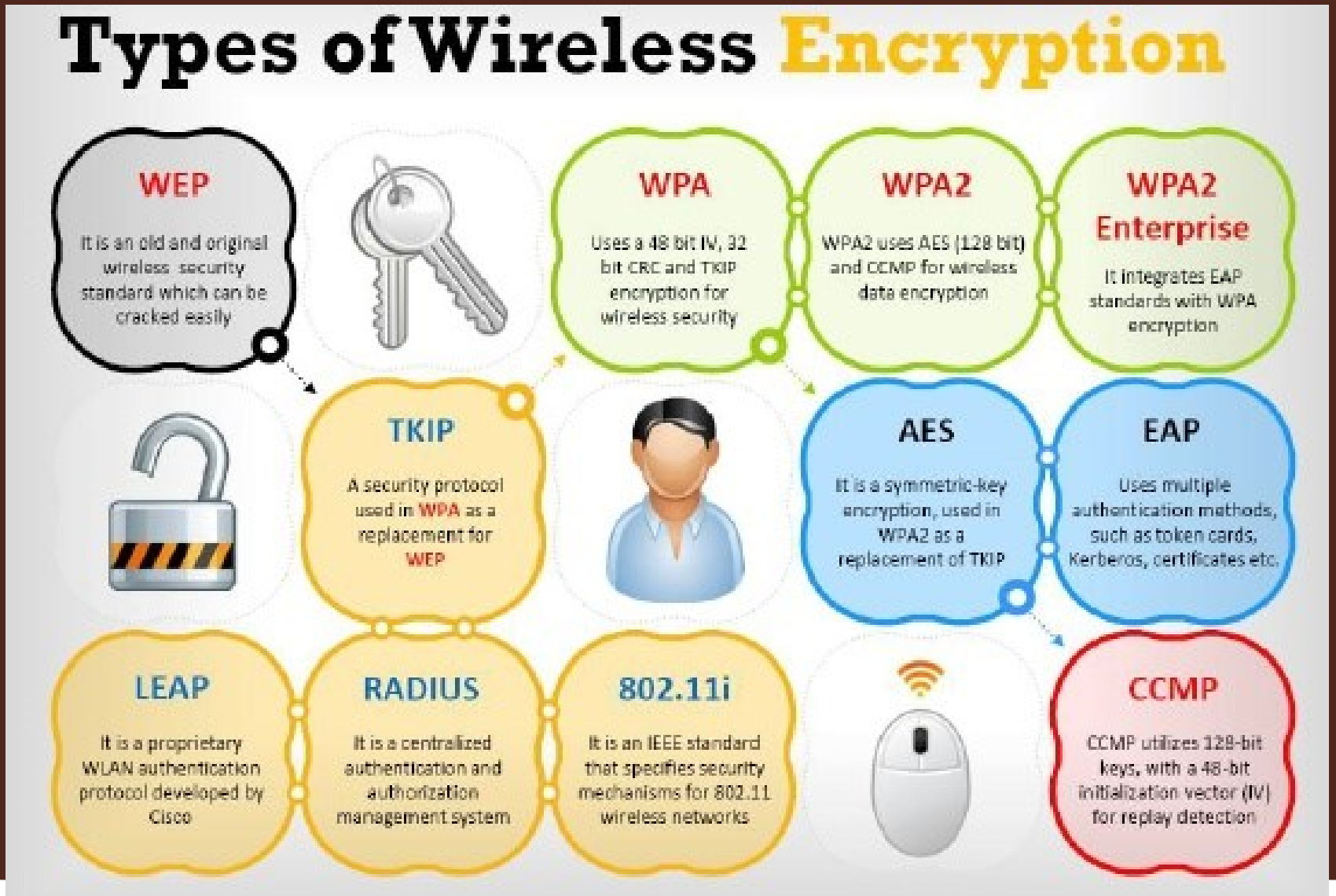
- WPA wraps RC4 cipher engine in four new algorithms
  1. Extended 48-bit IV and IV Sequencing Rules
     - ✓ 2^48 is a large number! More than 500 trillion
     - ✓ Sequencing rules specify how IVs are selected and verified
  2. A Message Integrity Code (MIC) called Michael
     - ✓ Designed for deployed hardware
     - ✓ Requires use of active countermeasures
  3. Key Derivation and Distribution
     - ✓ Initial random number exchanges defeat man-in-the-middle attacks
  4. Temporal Key Integrity Protocol generates per- packet keys

PENGUATAN KEAMANAN WLAN (SERANGAN WPA PRAKTIS)

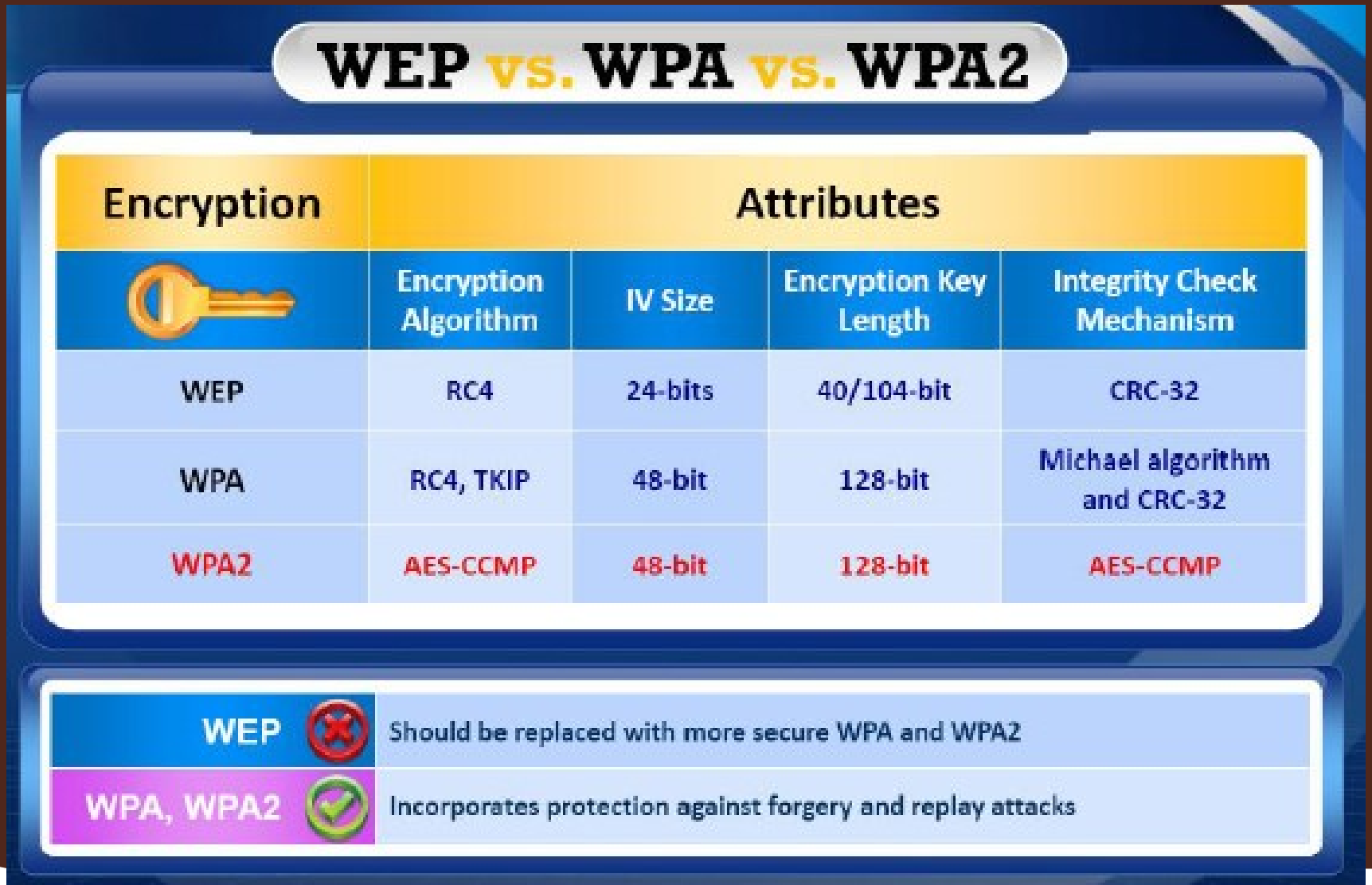
- Dictionary attack on pre-shared key mode
  - CoWPAtty, Joshua Wright

    http://www.securiteam.com/tools/6L00F0ABPC.html
- Denial of service attack
  - If WPA equipment sees two packets with good ICV check and invalid MICs check in 1 minute:
    - All clients are disassociated
    - All activity stopped for one minute
    - Access Point rekeys TKIP session key

Resume (1)


Types of Wireless Encryption
WEP
It is an old and original wireless security standard which can be cracked easily
WPA
Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security
WPA2
WPA2 uses AES (128 bit) and CCMP for wireless data encryption
WPA2 Enterprise
It integrates EAP standards with WPA encryption
TKIP
A security protocol used in WPA as a replacement for WEP
AES
It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP
EAP
Uses multiple authentication methods, such as token cards, Kerberos, certificates etc.
LEAP
It is a proprietary WLAN authentication protocol developed by Cisco
RADIUS
It is a centralized authentication and authorization management system
802.11i
It is an IEEE standard that specifies security mechanisms for 802.11 wireless networks
CCMP
CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection

Resume (2)


WEP vs. WPA vs. WPA2
Encryption
Attributes
Encryption Algorithm
IV Size
Encryption Key Length
Integrity Check Mechanism
WEP
RC4
24-bits
40/104-bit
CRC-32
WPA
RC4, TKIP
48-bit
128-bit
Michael algorithm and CRC-32
WPA2
AES-CCMP
48-bit
128-bit
AES-CCMP
WEP
Should be replaced with more secure WPA and WPA2
WPA, WPA2
Incorporates protection against forgery and replay attacks

LAYERED SECURITY

OVERVIEW

Example security protocols

- Application layer: PGP
- Transport layer: SSL/TLS
- Network layer: IPsec
- Data link layer: IEEE 802.11
- Security at the physical layer?

Security in what layer?

- Depends on the purpose…
  - What information needs to be protected?
  - What is the attack model?
  - Who shares keys in advance?
  - Should the user be involved?
- E.g., a network-layer protocol cannot authenticate two end-users to each other
- An application-layer protocol cannot protect IP header information
- Also affects efficiency, ease of deployment, etc.

Generally…

- When security is placed as lower levels, it can provide automatic, "blanket" coverage…
  - …but it can take a long time before it is widely adopted
- When security is placed at higher levels, individual users can choose when to use it…
  - …but users who are not security-conscious may not take advantage of it

Note…

- The “best” solution is *not* necessarily to use PGP over IPsec!
  - Would have been better to design the Internet with security in mind from the beginning…

Example: PGP vs. SSL vs. IPsec

- PGP is an application-level protocol for "secure email"
  - Can provide security on "insecure" systems
  - Users choose when to use PGP; user must be involved
  - Alice's signature on an email proves that Alice actually generated the message, and it was received unaltered; also non-repudiation
  - In contrast, SSL would secure "the connection" from Alice's computer; would need an additional mechanism to authenticate the user
  - Communication with off-line party (i.e., email)

Example: PGP vs. SSL vs. IPsec

- SSL sits at the transport layer, "above" TCP
  - Packet stream authenticated/encrypted
  - End-to-end security, best for connection-oriented sessions (e.g., http traffic)
  - User does not need to be involved
  - The OS does not have to change, but applications do if they want to communicate securely
  - If TCP accepts a packet which is rejected by SSL, then TCP will reject the "correct" packet (detecting a replay) when it arrives!
    - SSL must then close the connection…

Example: PGP vs. SSL vs. IPsec

- IPsec sits at the network layer
  - Individual packets authenticated/encrypted
  - End-to-end or hop-by-hop security
    - Best for connectionless channels
  - Need to modify OS
  - All applications are "protected" by default, without requiring any change to applications or actions on behalf of users
  - Only authenticates hosts, not users
  - User completely unaware that IPsec is running

IPSec Overview

- IPsec can provide security between any two network-layer entities
  - host-host, host-router, router-router
- Used widely to establish *VPNs*
- IPsec encrypts and/or authenticates network-layer traffic, and encapsulates it within a standard IP packet for routing over the Internet

IPSec Overview

- IPsec consists of two components
  - IKE --- Can be used to establish a key
  - AH/ESP --- Used to send data once a key is established (whether using IKE or out-of-band)
- AH
  - Data integrity, but no confidentiality
- ESP
  - Data integrity + confidentiality
  - (Other differences as well)

REFERENCES

- A. Pras, P.T. Boer, A. Sperotto, R. Sadre, "Secure Wireless LAN", University of Twente, 2012
- J. Katz, "Computer and Network Security", University of Maryland, Spring 2012
- W. Stallings, "Cryptography and Network Security", 6th ed., Prentice Hall, 2014

THANK YOU