# Understanding Wireless Security

# Outline

- What you will learn
  - General overview of 802.11
  - Authentication Methods
    - WEP
      - Overview
      - Key Hierarchy
      - Encryption/Decryption
    - WPA
      - Overview
      - Key Hierarchy
      - Encryption/Decryption
    - WPA2
      - Overview
      - Encryption/Decryption
  - Defense Strategies
  - Monitoring
- Summary
- Question and Answer

# What you should know

In order to cover the largest amount of information we are going to have make some assumptions:

- You have a general understanding of the TCP/IP protocol suite
  - Primarily layers 2 – 3
- You have a general understanding of protocol basics
- You have a general understanding of how Radio Frequency (RF) works

# 802.11 Primer

- Borne out of the IEEE 802 LAN/MAN Standards Committee (LMSC)
- Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications standard
- Drop in replacement for Ethernet (802.3)
  - Upper layer protocols should be none the wiser
  - This seamless integration comes at a stiff price – under the hood complexity

# 802.11 Primer: Physical Interface

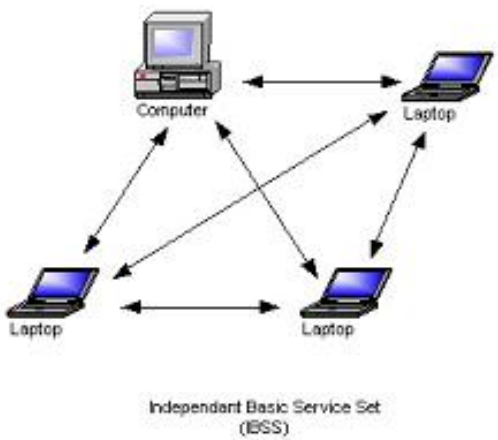
- DSSS
  - Direct Sequence Spread Spectrum
  - 2.4GHz ISM Band
    - Industrial / Instrumentation, Scientific, Medical (ISM)
    - 2.400GHz – 2.4835GHz
    - 14 channels or frequency divisions
      - 1 – 11 used in the United States
  - 1000mW power maximum
    - Most devices are 30mW – 100mW

# 802.11 Primer: MAC Sublayer Tidbits

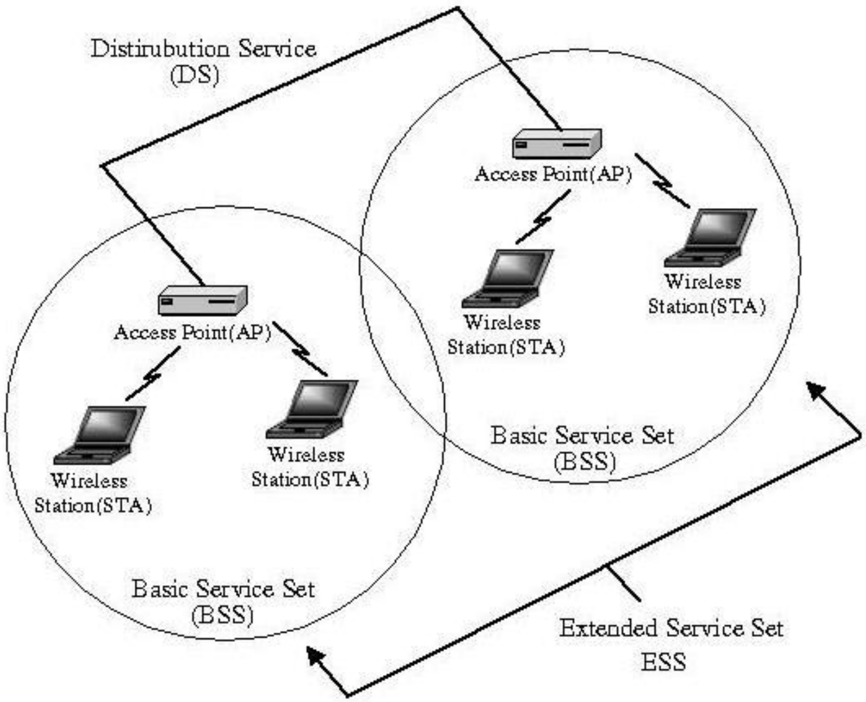
- CSMA/CA
  - LBT (Listen Before Talk)
  - Exponential back off and retry
  - Collision avoidance via physical carrier sense and Network Allocation Vector
    - Network Allocation Vector (NAV)
      - Virtual Carrier Sense
      - Limits the need for physical carrier sensing of the air interface in order to save power.

# Configuration Options

AD Hoc




Infrastructure



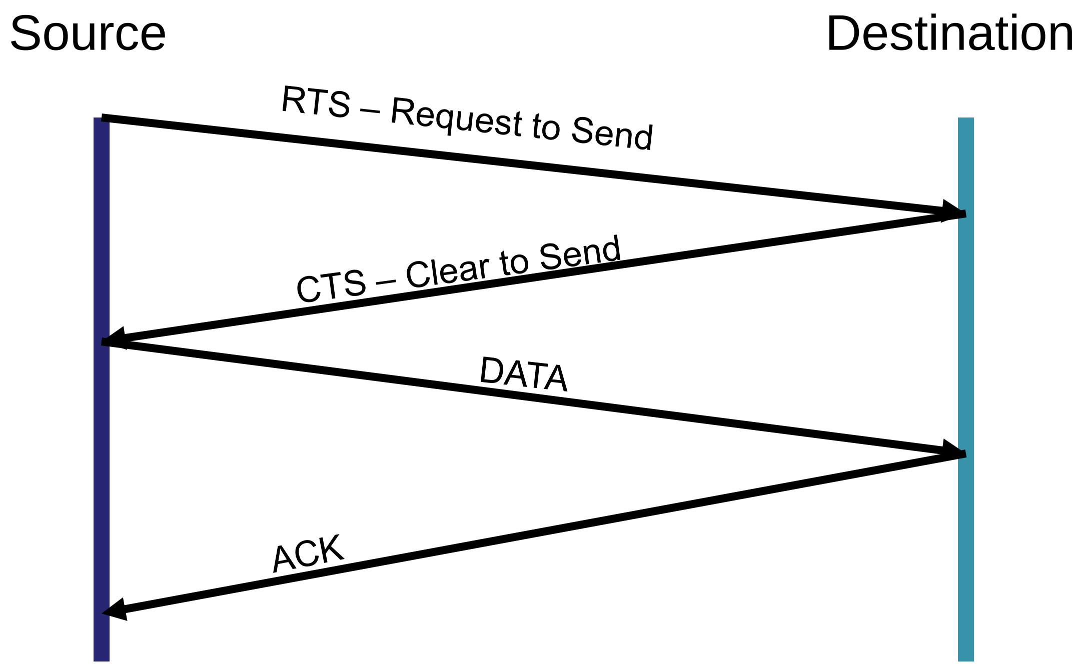
# Management Frame Subtypes

- Beacon
  - Transmitted frequently announcing availability and capabilities of BSS
- Probe Request and Response
  - Client initiated request for a WLAN
  - Response is essentially the same as a beacon
- Associate Request and Response
  - "I'd like to be a part of your BSS"
- Disassociate
  - "Get a stepping!"

# Control Frame Subtypes

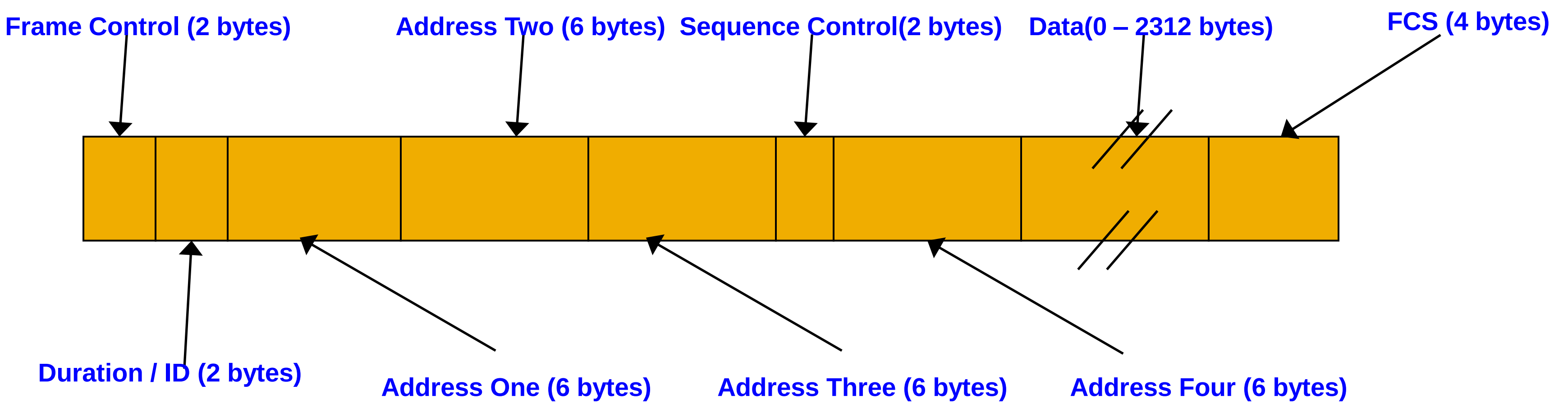
- Request to Send (RTS)
  - "I'd like to send a frame or two"
  - Updates NAV values for neighboring stations (transmitter)
- Clear to Send (CTS)
  - "Sounds good"
  - Updates NAV values for neighboring stations (receiver)
- Acknowledge (ACK)
  - "Got your data"
  - Also updates NAV as per CTS

# Four-Way Handshake

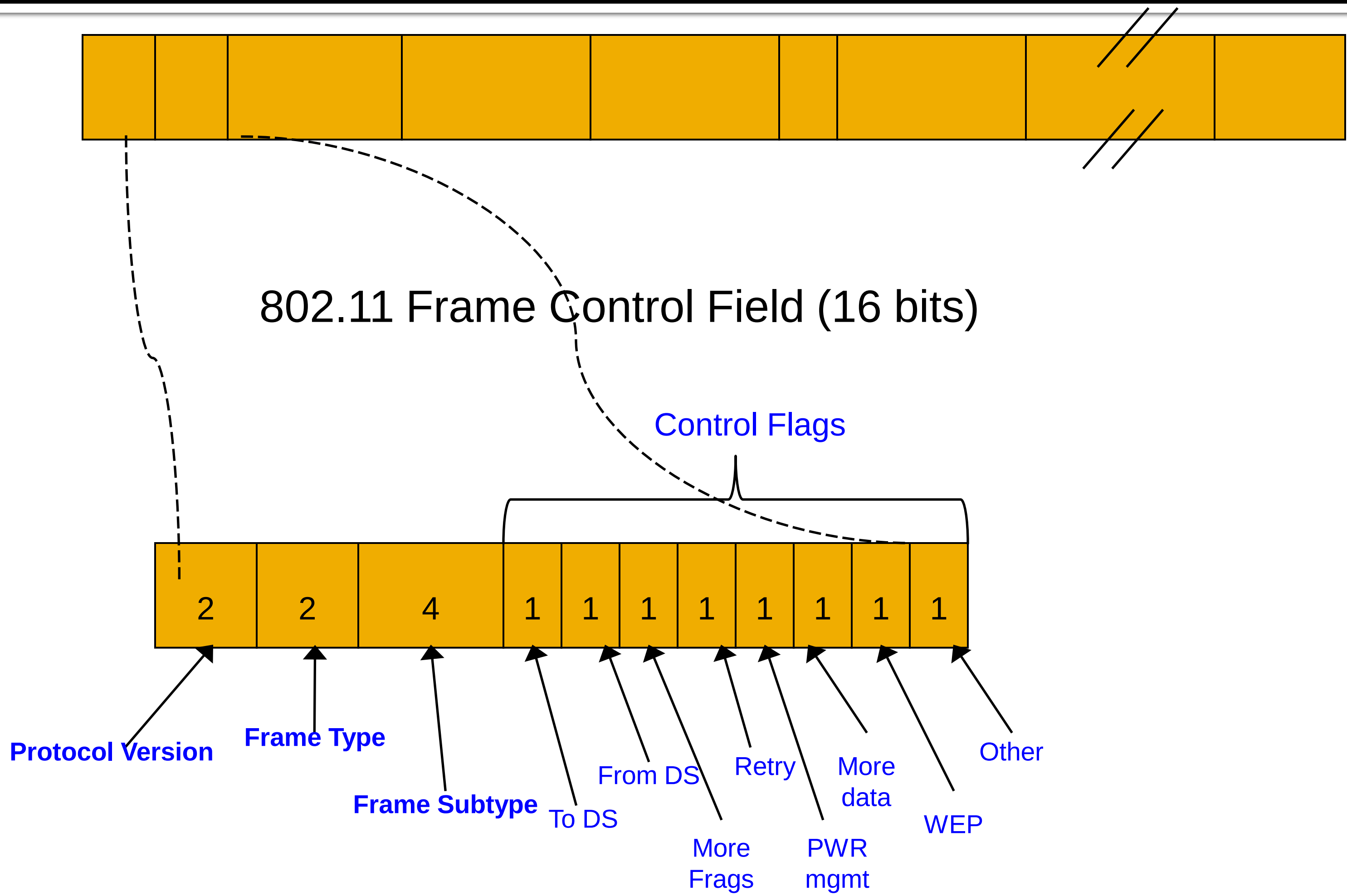


# 802.11 Frame Layout

802.11 Frame Format [34 – 2344 bytes]

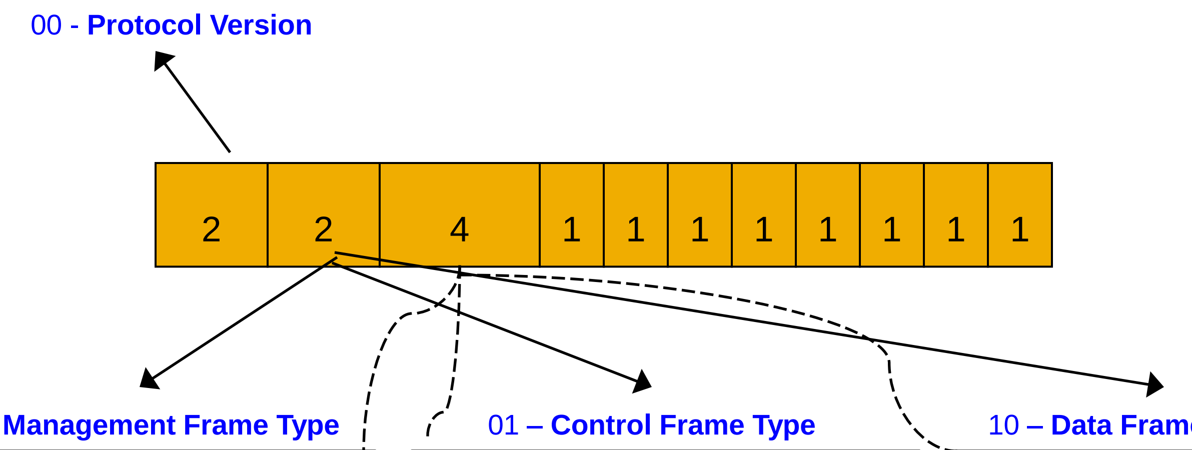


# 802.11 Control Field



# 802.11 Types and Subtypes

## 802.11 Type and Subtypes




**00 – Management Frame Type**

- 0000 – **association request**
- 0001 – **association response**
- 0010 – **reassociation request**
- 0011– **reassociation response**
- 0100 – **probe request**
- 0101 – **probe request**
- 1000 – **beacon**
- 1010 – **disassociation**
- 1011 – **authentication**
- 0111 – de**authentication**

**01 – Control Frame Type**

- 1010 – **power save poll**
- 1011 – **RTS**
- 1100 – **CTS**
- 1101 – **ACK**
- 1110 – **CF-end**
- 1111 – **CF-end + CF-ACK**
- 0110 – **CF-poll (no data)**
- 0111 – **CF-ACK + CF-poll (no data)**

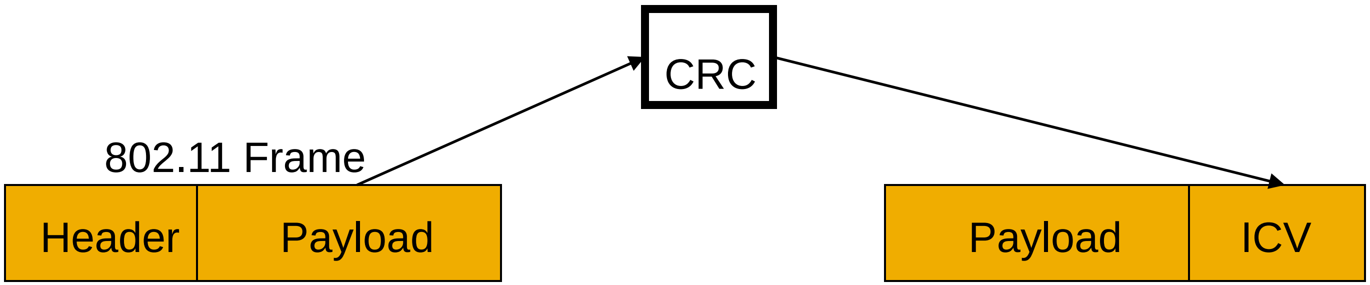
**10 – Data Frame Type**

- 0000 – **data**
- 0001 – **data + CF-ACK**
- 0010 – **data + CF-poll**
- 0011 – **data + CF-ACK + CF-poll**
- 0100 – **NULL (no data)**
- 0101 – **CF-ACK (no data)**
- 0110 – **CF-poll (no data)**
- 0111 – **CF-ACK + CF-poll (no data)**

# Wired Equivalent Privacy (WEP)

- Purpose – bring the security of wired networks to 802.11
- Provides Authentication and Encryption
- Uses RC4 for encryption
- 64-bit RC4 keys
  - Non-standard extension uses 128-bit keys
- Authentication built using encryption primitive – Challenge/Response

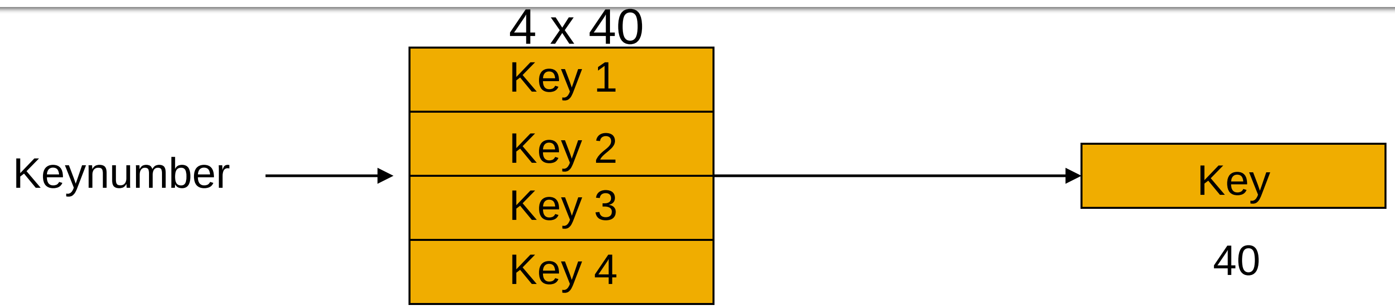
# WEP Encryption




ICV computed – 32-bit CRC of payload

* 4-byte Integrity Check Value (ICV)

# WEP Encryption (cont)




- Integrity Check Value (ICV) computed – 32-bit CRC of payload
- One of four keys selected – 40-bits (10 Hex character)

| WEP Key | ASCII | Hex |
|---|---|---|
| 1 | too complicated | 746f6f2063 |
| 2 | too simple | 746f6f2073 |
| 3 | norfolk southern | 6e6f72666f |
| 4 | locomotive | 6c6f636f6d |

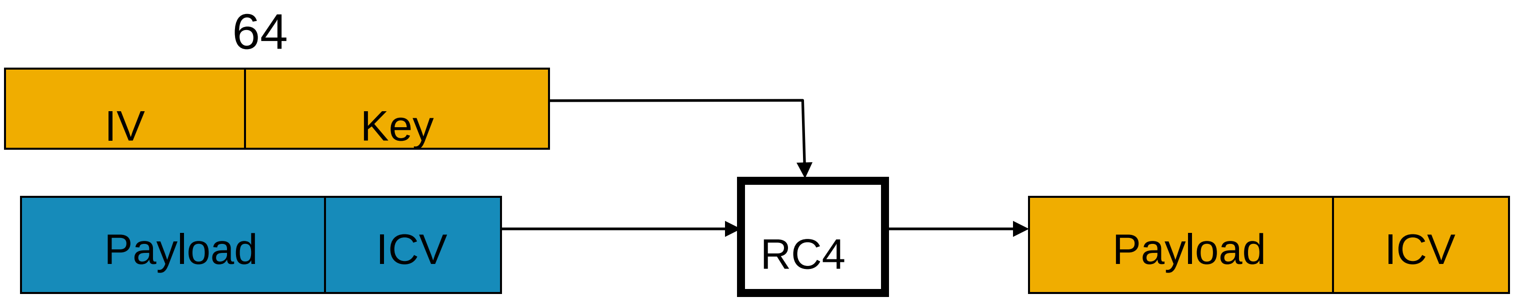
InfoSec DAILY

# WEP Encryption (cont)

| IV | keynumber |
|---|---|
| 24 | 8 |

- Integrity Check Value (ICV) computed – 32-bit CRC of payload
- One of four keys selected – 40-bits
- Initialization Vector (IV) selected – 24-bits, prepended to keynumber

# WEP Encryption (cont)




- Integrity Check Value (ICV) computed – 32-bit CRC of payload
- One of four keys selected – 40-bits
- Initialization Vector (IV) – 24-bits, prepended to keynumber
- IV+key used to encrypt payload+ICV

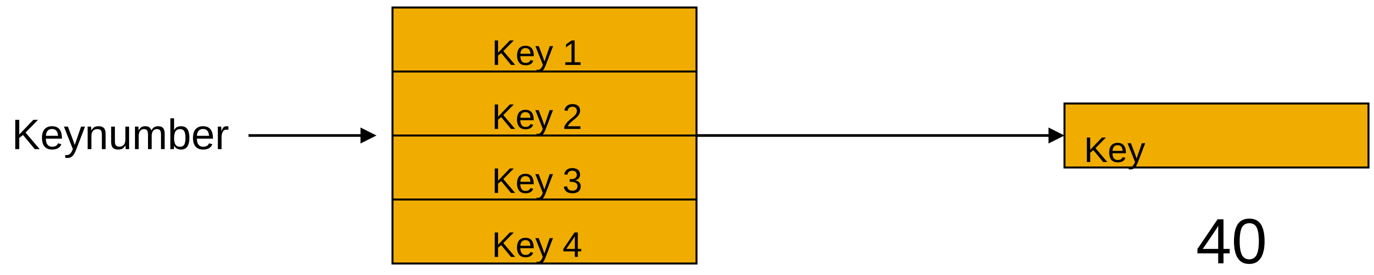
# WEP Encryption (cont)

WEP Frame

| | | | | |
|---|---|---|---|---|
| Header | IV | keynumber | Payload | ICV |

- Integrity Check Value (ICV) computed – 32-bit CRC of payload
- One of four keys selected – 40-bits
- Initialization Vector (IV)  selected – 24-bits, prepended to keynumber
- IV+key used to encrypt payload+ICV
- IV+keynumber prepended to encrypted payload+ICV

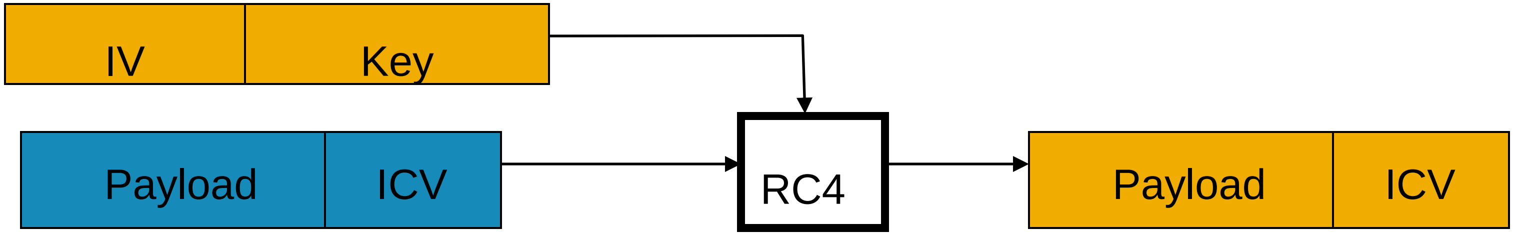
# WEP Decryption




- Keynumber is used to select key

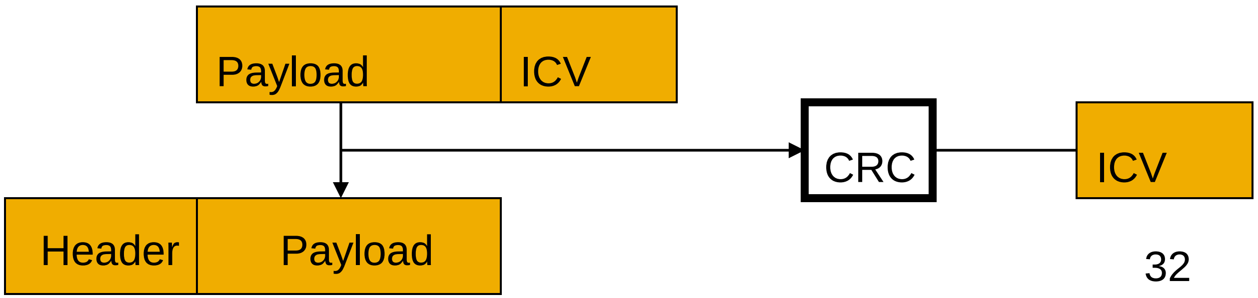
| WEP Key | ASCII | Hex |
|---|---|---|
| 1 | too complicated | 746f6f2063 |
| 2 | too simple | 746f6f2073 |
| 3 | norfolk southern | 6e6f72666f |
| 4 | locomotive | 6c6f636f6d |

# WEP Decryption (cont)




- Keynumber is used to select key
- ICV+key used to decrypt payload+ICV

# WEP Decryption (cont)



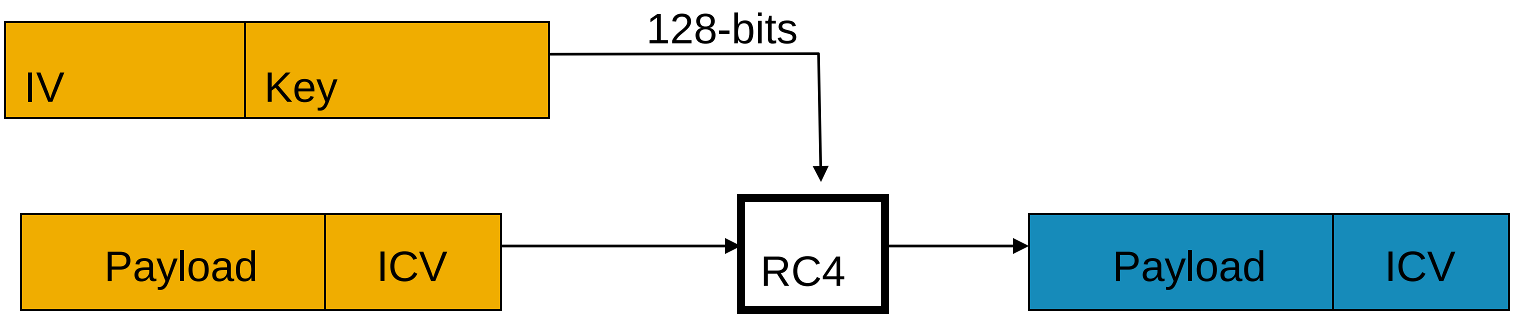

- Keynumber is used to select key
- ICV+key used to decrypt payload+ICV
- Integrity Check Value (ICV) recomputed and compared  against original

# WEP Authentication

- Uses WEP encryption primitives
  - Nonce[1] is generated and sent to client
  - Client encrypts nonce and sends it back
  - Server decrypts response and verifies that it is the same nonce.
- Authentication is optional

[1] *Number used Once*

# 128-bit Variant




- Purpose – increase the encryption key size
- Non-standard, but in wide use
- IV and ICV set as before
- 104-bit key selected
- IV+key concatenated to form 128-bit RC4 key

# WEP Keying

- Keys are manually distributed
- Keys are statically configured
  - Implications: often infrequently changed and easy to remember!
- Four 40-bit keys (or one 104-bit key)
- Key values can be directly set as hex data
- Key generators provided for convenience
  - ASCII string is converted into keying material
  - Non-standard but in wide use
  - Different key generators for 64- and 128-bit

# WEP Vulnerability

- WEP and 802.11 standards recommends (not requires) the IV be changed after every packet.
- No standard to generate IVs
- IV field is 24 bits, forcing a busy connection to exhaust all IVs in less than a half a day
- Random 24 bit IV will be expected to have a collision after transmitting 5000 packets (Birthday Problem)
- 24GB to construct a full table, which would enable the attacker to immediately decrypt each subsequent ciphertext

# Dynamic WEP

- Dynamic WEP changes WEP keys dynamically
  - Different key on a per-user, per-session basis
  - Key changes based upon a timer or number of packets
- Theory: Prevent attacker from being able to collect enough data to crack the current encryption keys
- Reality: Can be cracked given current technologies
  - Though Key only good until a timer or number of packets threshold is reached

# WEP Attacks (1)

- The FMS Attack (2001)
  - Named for Fluhrer, Mantin, and Shamir
  - First key recovery attack
  - Based on predictable headers
    - Attack can compromise the first few bytes of the keystream
    - Leads to correlations in other bytes
  - 4-6 million packets needed to succeed with probability greater or equal to 50%

# WEP Attacks (2)

- Korek[1] Attack (2004)
  - Based on the FMS Attack, but extended with 16 more correlations between the first few bytes of an RC4 key, keystream, and the next key byte.
  - Reduced the number of packets needed to 700,00 to succeed with probability greater or equal to 50%

1 Korek was a forums username where the majority of wireless cracking mathematical efforts were postulated.

# WEP Attacks (3)

- PTW Attack (2007)
  - Named for Pyshkin, Tews and Weinmann
  - Extends both FMS and KoreK
  - Process every packet and cast votes for likelihood of key
  - The key is generally close to having the most votes
    - Test each key for correctness
  - Reduced the number of packets needed to 35,000-40,000 to succeed with probability greater or equal to 50%

# WEP Attacks (4)

- Chopchop Attack
  - Allows an attacker to decrypt the last *m* bytes by sending *m* * 128 packets to the network.
  - Does not reveal the root key
    - Only plaintext
  - Some access points are not vulnerable to this attack
    - Some may seem vulnerable at first but actually drop data packets shorter that 60 bytes

# Wi-Fi Protected Access (WPA)

- Security standard developed after WEP's vulnerabilities had been exposed and successfully attacked
- Development was a collaborative effort between the Wi-Fi Alliance and the Institute of Electrical and Electronics Engineers (IEEE)
- Purpose was to be an immediate solution while the long-term solution (802.11i/WPA2) was being finished

# Wi-Fi Protected Access (WPA) (cont)

- WPA strengthened WEP by:
  - Including authentication using 802.1X framework (commercial systems) or a passphrase (home systems)
  - Creating a key hierarchy out of the master key
  - Doubling the size of the initialization vector (IV) used during encryption
  - Including a more robust data integrity algorithm (Michael)

# Wi-Fi Protected Access (WPA) (cont)

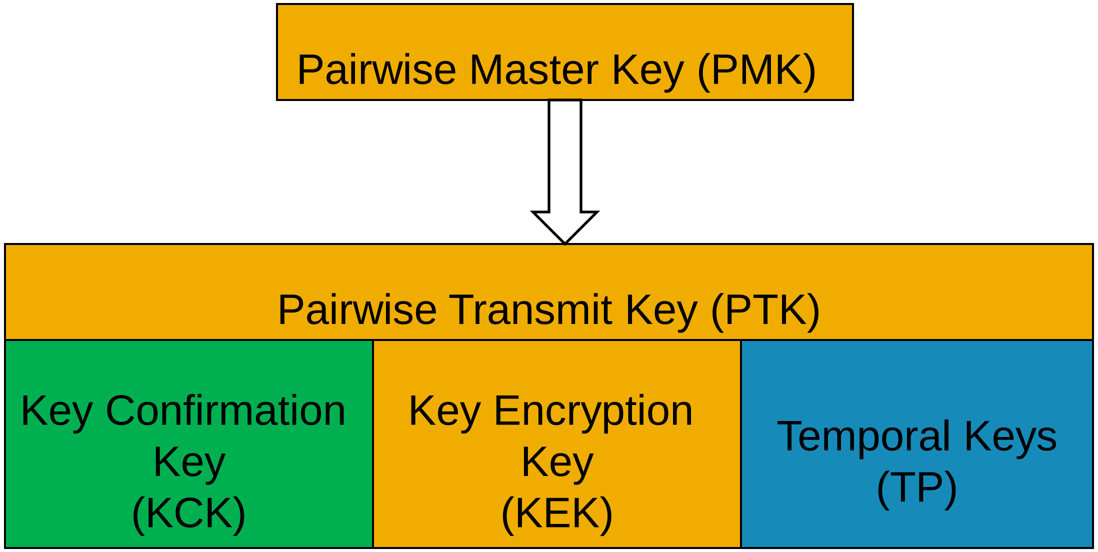
- A session consists of:
  - Authentication of the client to the access point (802.1X/passphrase)
  - 4-way handshake to exchange key values and generate the key hierarchy
  - Data session to send encrypted information using the Temporal Key Integrity Protocol (TKIP)
    - RC4 for encryption
    - Michael for integrity checking (MIC)

# WPA Key Hierarchy

- Key Hierarchy consists of a master key and session keys
  - Master key, called the Pair-wise Master Key, is derived from either an 802.1X key or from the passphrase
  - Session keys, collectively called the Pair-wise Transient Key, are derived from the master key

# WPA Key Hierarchy (cont)

- Pair-wise Transient Key is segmented into:
  - Key Confirmation Key and Key Encryption Key used during the 4-way handshake
  - Temporal Keys (2) used during the data session



# Beck-Tews Attack

- Martin Beck from the Technical University of Dresden discovered a flaw in the TKIP protocol
  - Assisted by Erik Tews[1] from the Technical University of Darmstadt
- Allows an attacker to decrypt data to a wireless client, slowly
- Once a packet is decrypted, opportunity to transmit up to 7 forged packets of any content
- No authorization needed for success

[1] Erik Tews of PTW fame

# Beck-Tews Attack (cont)

- Not a key recovery attack
  - Attacker can only decrypt one packet at a time; does not allow earlier/later frame decryption
- Does not affect AES-CCMP[1] networks (required for FIPS 140-2)
- Workarounds will mitigate this flaw
  - Not perfect, but will buy some time
- Some APs can be configured to mitigate this flaw

[1] **C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol

# Who Is Affected?

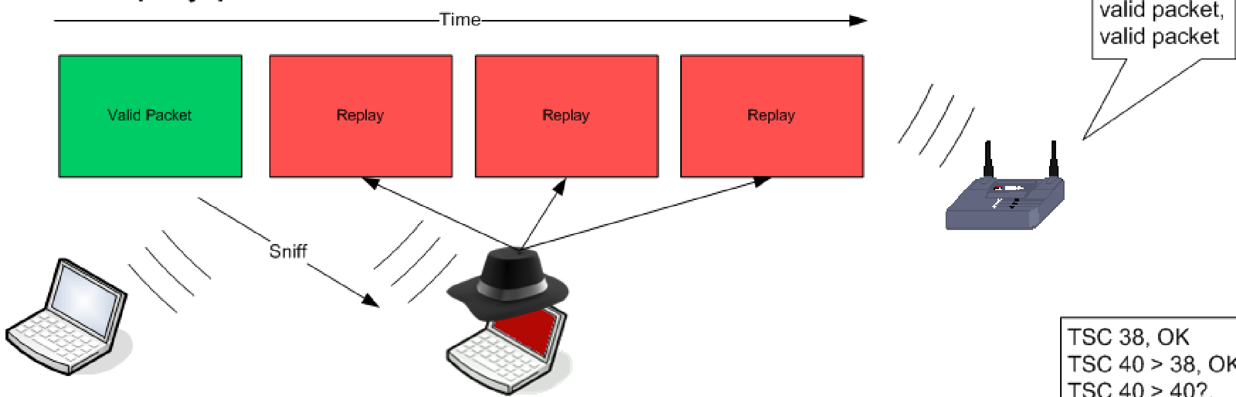
- All deployments of TKIP
  - Regardless of WPA or WPA2
  - Regardless of PSK or 802.1X/EAP authentication
- Current exploits target TKIP networks with QoS enabled
  - QoS is required for much of 802.11n

# Attacker Opportunity

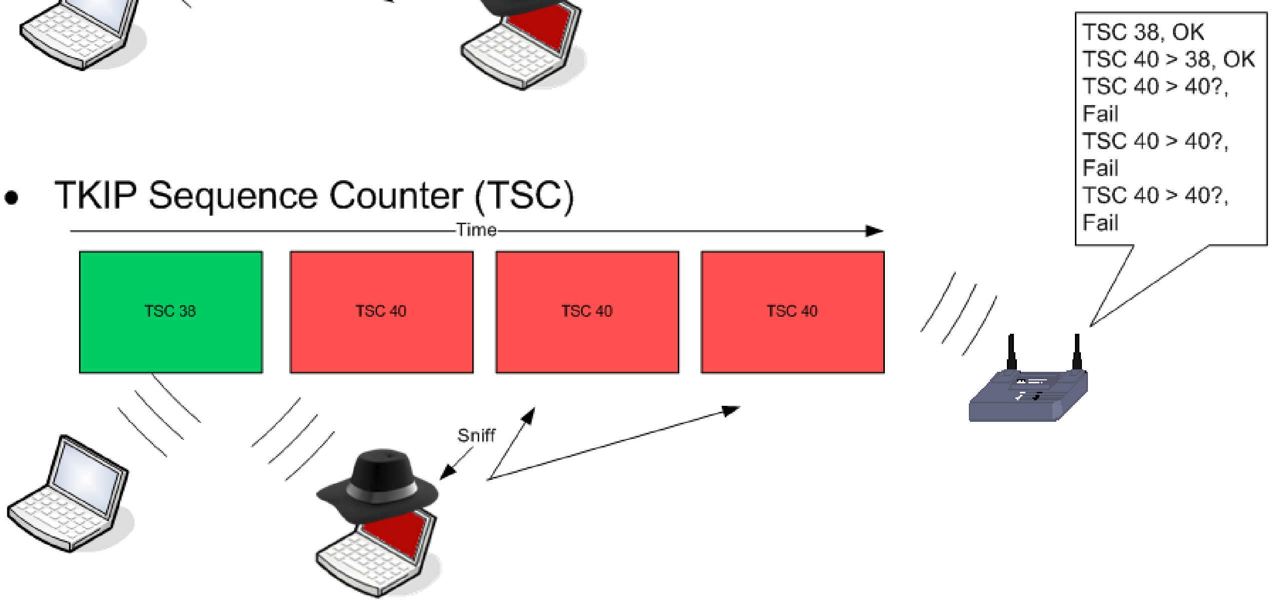
- Attacker can decrypt a plaintext packet from AP to station (not station to AP)
  - Not more than 1 unknown byte per minute
  - Any packet can be selected for partial data
- Targeting an ARP packet (68 bytes), between 14 and 17 bytes are unknown
  - 8 MIC, 4 ICV, 2-5 IP source and destination
- Once plaintext is known, attacker can inject not more than 15 arbitrary packets
  - ARP poisoning, DNS manipulation, TCP/SYN request

# April 2003: TKIP Fixes WEP Flaw

- No replay protection with WEP

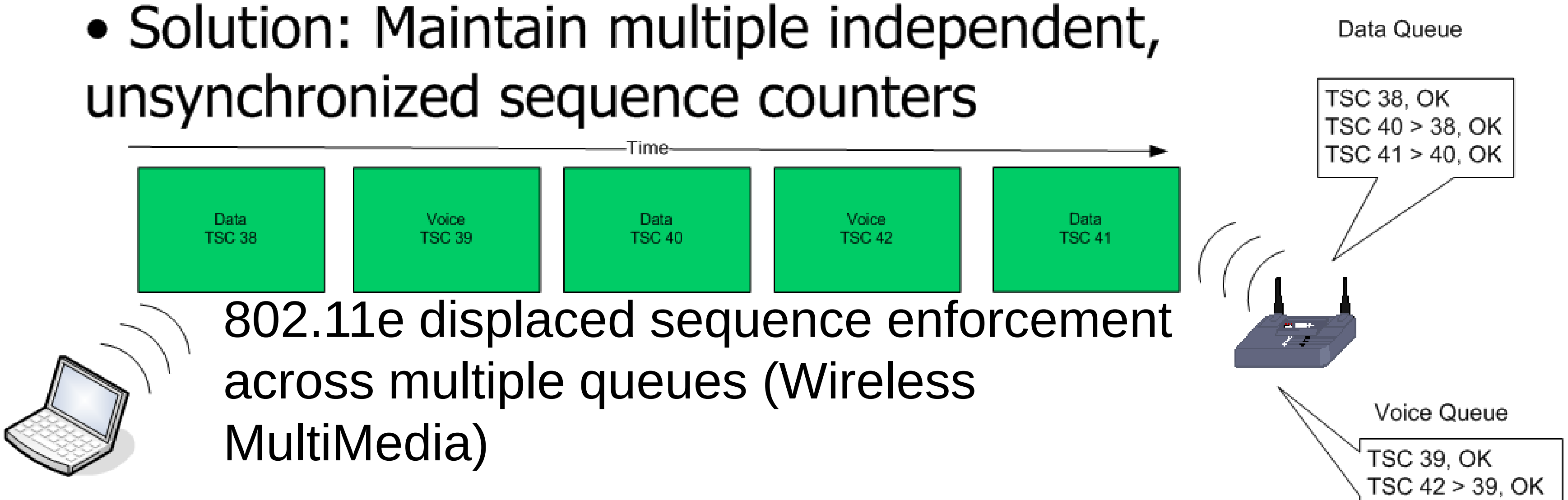



- TKIP Sequence Counter (TSC)



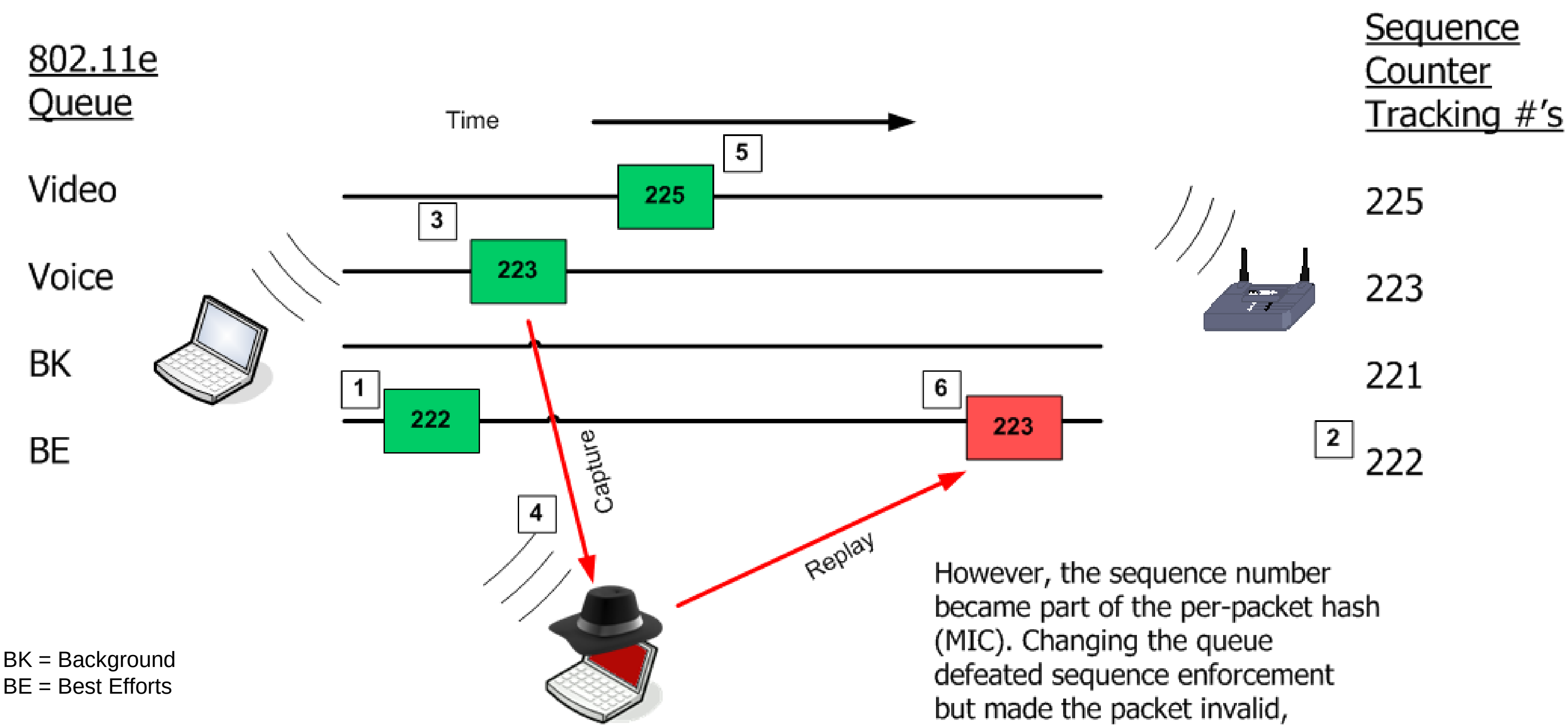
# July 2005: QoS Complicates Matters

- QoS relies on the ability to reorder packets for delivery
- This requirement conflicts with TKIP sequence delivery
- Solution: Maintain multiple independent, unsynchronized sequence counters




802.11e displaced sequence enforcement across multiple queues (Wireless MultiMedia)

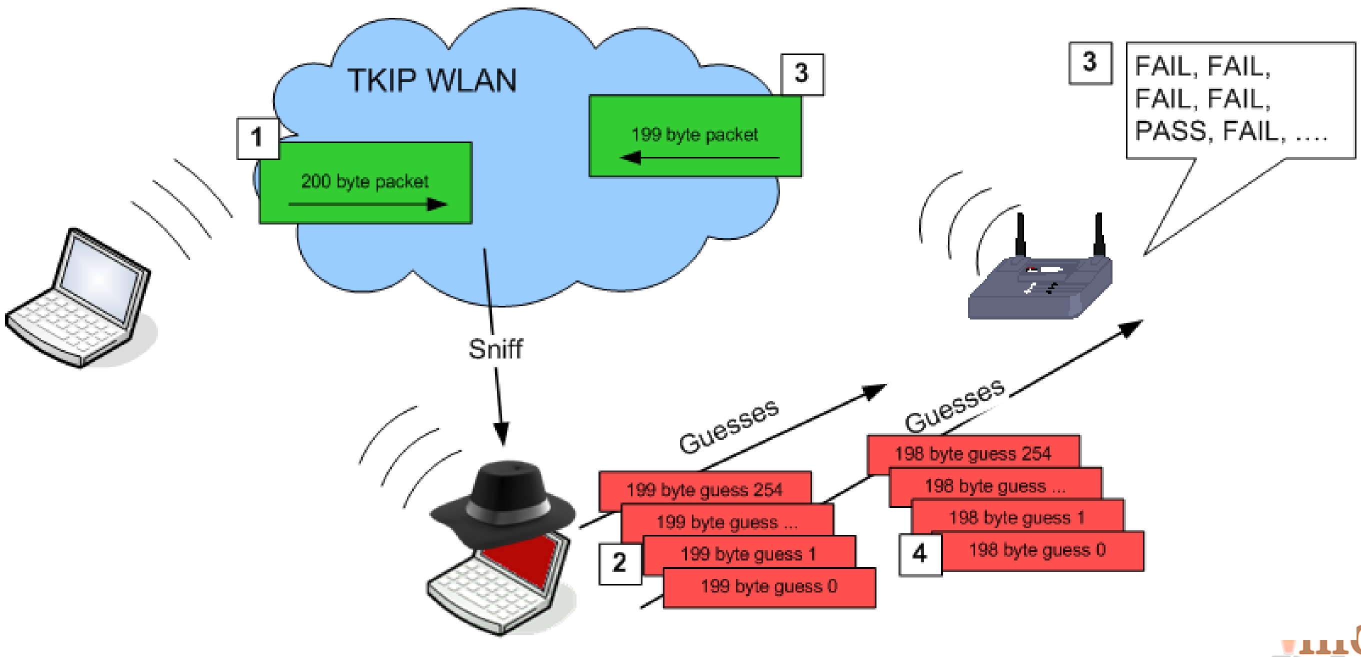
# 802.11e Replay Attack




However, the sequence number became part of the per-packet hash (MIC). Changing the queue defeated sequence enforcement but made the packet invalid, DoS'ing all stations on a target AP.

# WEP ICV Attack - ChopChop

- Integrity Check Value (ICV) – WEP 32-bit CRC
- Vulnerable to modification and repeated guess until positive response observed (chopchop attack)
- Repeated to recover entire plaintext packet contents

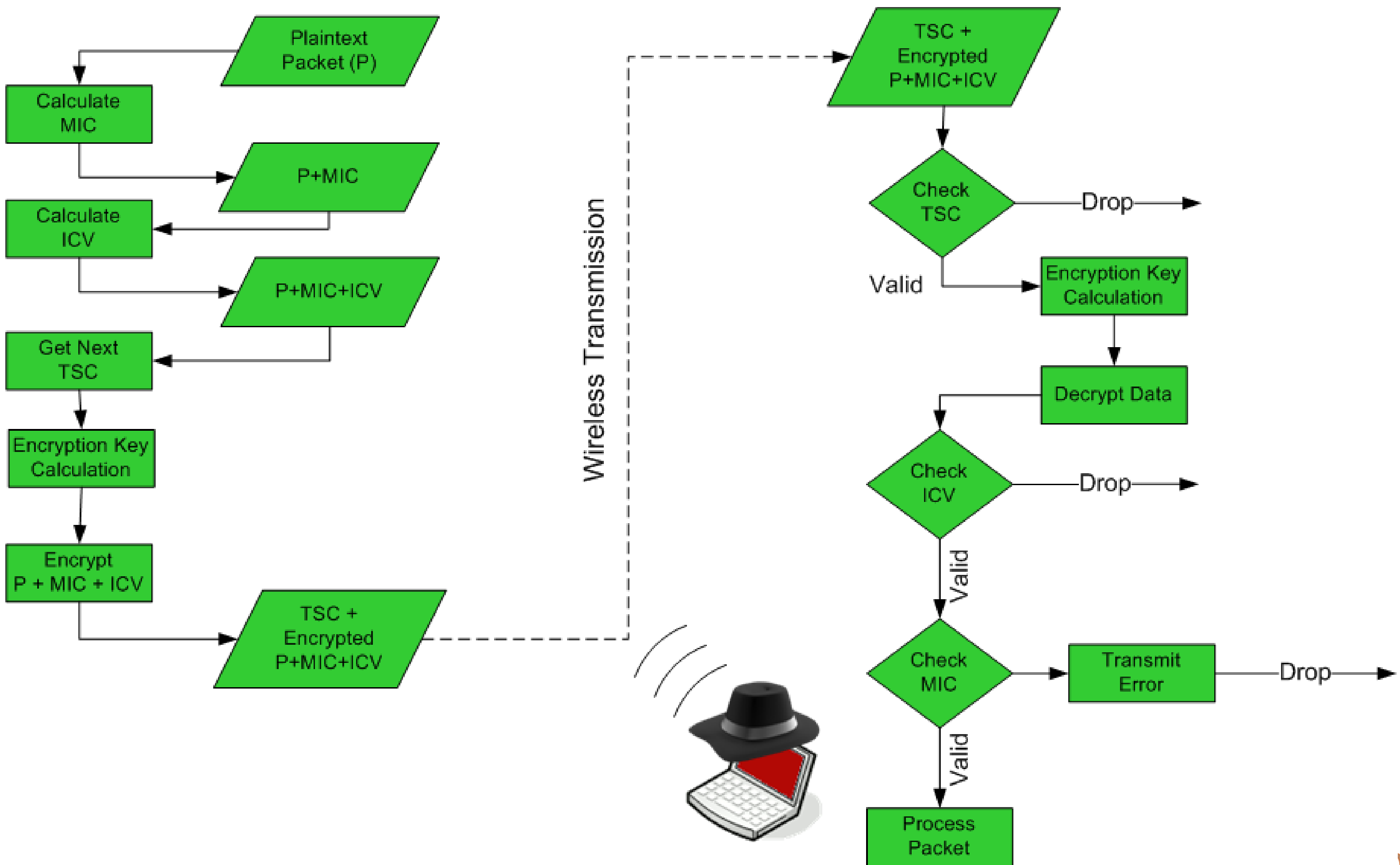



InfoSec DAILY

# Fixed in TKIP

- TKIP adds a new per-packet hashing algorithm (MIC) known as Michael
- Weak algorithm, but best that could be accommodated on legacy WEP hardware
- Includes provision for countermeasures
  - Two invalid MIC's within 60 seconds shuts down AP and STA's for 60 seconds
  - Must pass ICV and TSC check first
  - Called MIC countermeasures

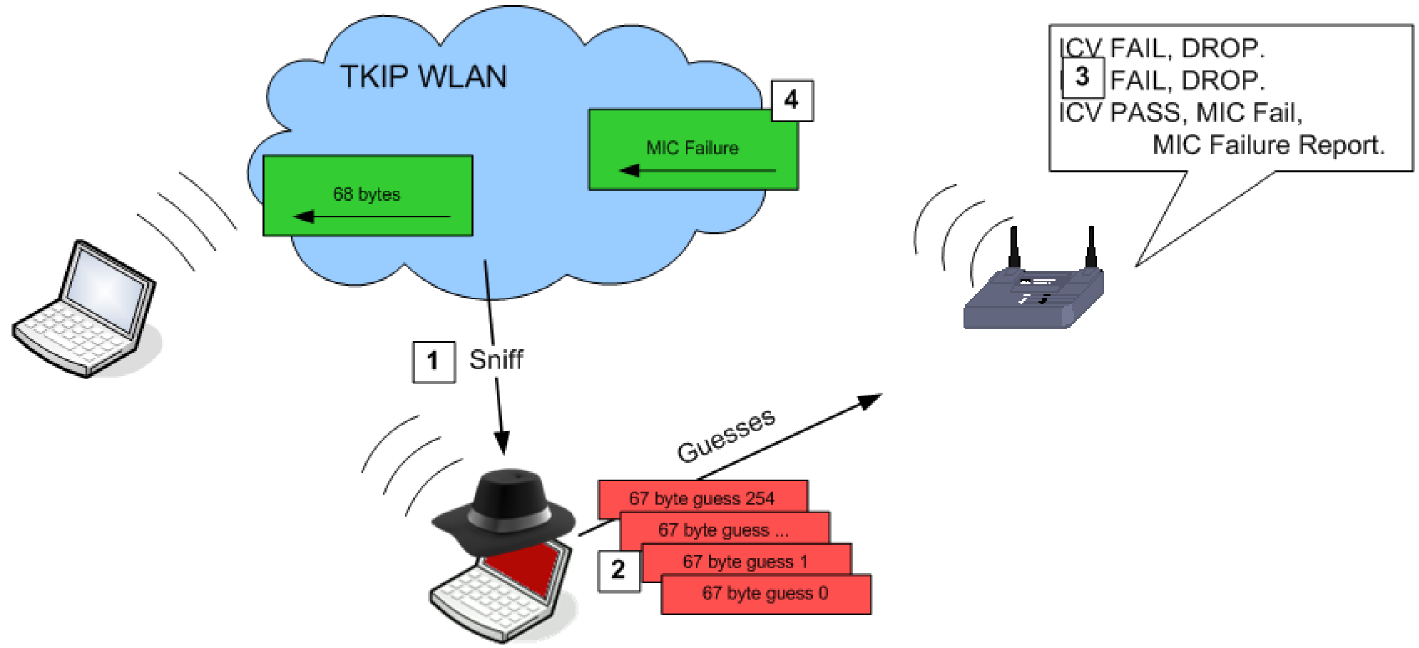
# TKIP Encryption/Decryption



# So How Is This Exploited?

- ICV failure generates no network activity
  - MIC failure causes the client to generate a notice the attacker can observe
- If MIC failure observed, ICV passed!
- Take a packet, chop last byte, guess and TX until MIC failure observed
- Wait 60 seconds to not trigger countermeasures
- Repeat for next-to-last byte

# TKIP Chopchop ICV Attack




| | | | | |
|---|---|---|---|---|
| **1. Attacker captures TKIP encrypted packet that looks like ARP** | **2. Attacker removes last payload byte, invalidating ICV and MIC. Attempts to fix ICV with guess 0 and sends to station.** | **3. Client receives frame, most have ICV failures and are dropped. One passes ICV, but fails MIC.** | **4. A MIC failure message is sent to AP to coordinate Michael countermeasures. Though encrypted, attacker can observe this frame to identify valid ICV, revealing one byte of plaintext.** | **Attacker waits 60 seconds to avoid MIC countermeasures, then repeats process with 66 byte packet. Continues until all packet plaintext is known.** |

# Attack Result

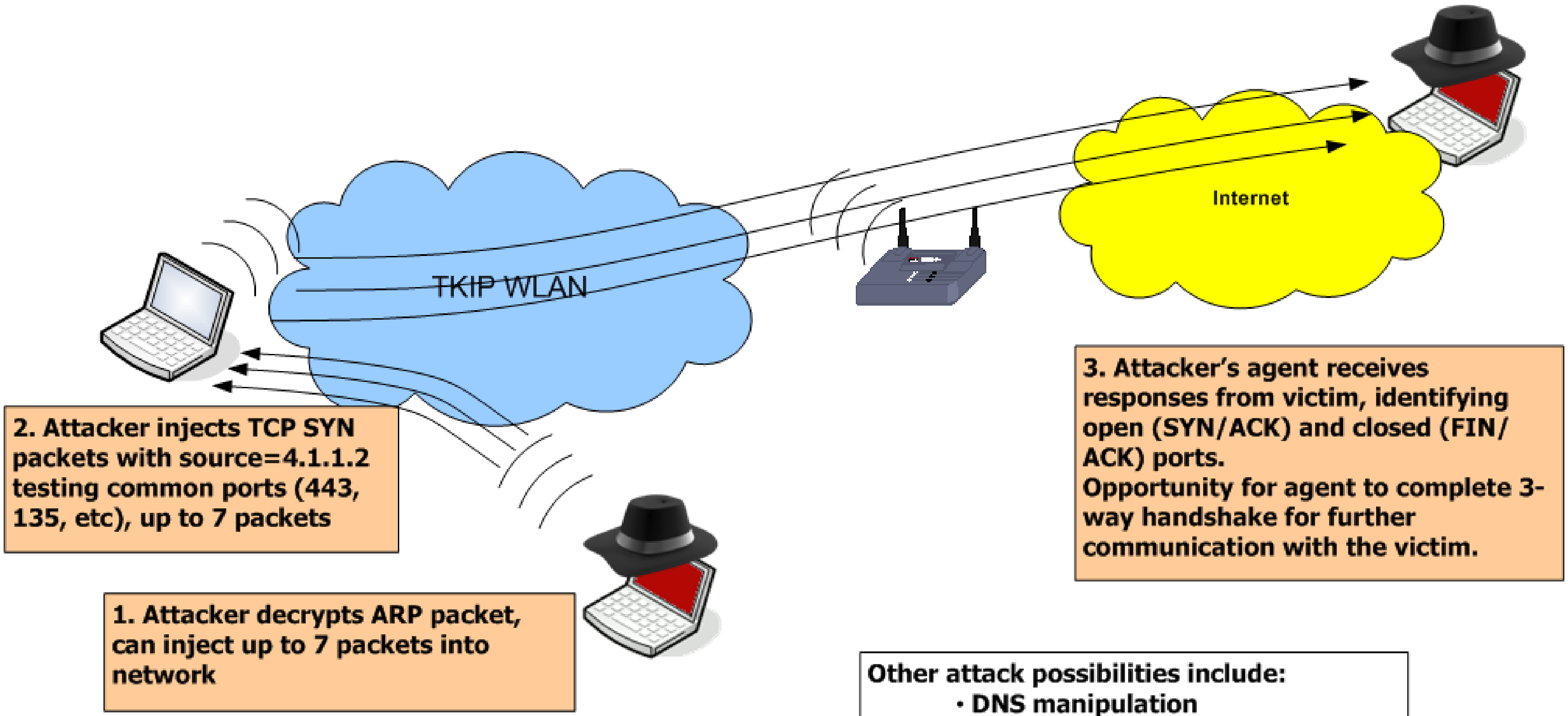
- Not more than 1 byte per minute decrypted
- ARP is mostly known plaintext
  - Five bytes unknown assuming /24 (A.B.C.Y and A.B.C.Z)
- Also need to determine ICV and MIC values (12 bytes)
- Only 17 bytes to recover, 14 if network is known (RFC1918 guess?)

Result: 68 bytes ARP, 8 bytes MIC, 4 bytes ICV known plaintext to the attacker in 14-17 minutes

# Another Michael Weakness

- Michael is invertible; you can determine the key from plaintext + MIC
- Attacker decrypts ARP, knows Michael key and can craft any packet up to 68 bytes
- Attacker can use other QoS queues where attacked
- TSC is lower to inject arbitrary packets into network (can target any destination or protocol)
- Injection is blind, attacker cannot decrypt responses
- Attacker can only inject up to 7 packets (3 other standard 802.11e queues and 4 non-standard)
  - Potential for 15 injected packets, depending upon driver
  - One Linux implementation can potentially inject 31 packets

# Practical TKIP Attack Example




**Other attack possibilities include:**

- **DNS manipulation**
- **Delivering UDP-based exploits**
- **ARP manipulation on LAN**

# MIC DoS Attacks Easy Now

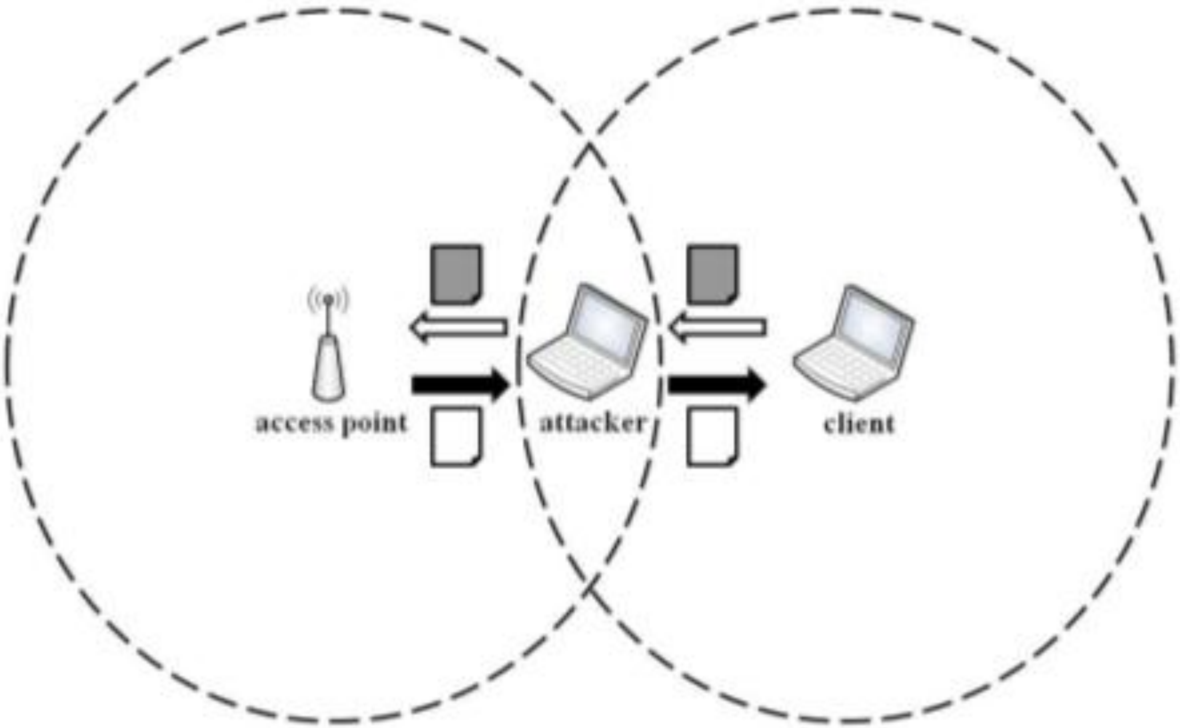
- Michael algorithm countermeasures
  - AP must disconnect all stations and shutdown the network following two MIC failures within 60 seconds
- Very easy for an attacker to trigger, shutting down AP for 60 seconds

DOT11-TKIP_MIC_FAILURE: TKIP Michael MIC failure was detected on a packet (TSC=0x0) received from [mac-address]

# Message Falsification Attack on WPA

- Developed by Toshihiro Ohigashi and Masakatu Morii
- Applies Beck-Tews attack to the MITM attack in order to work any WPA implementation.
  - Three modes required for attack:
    - Repeater mode: Attacker relays to the receiver all packets that include SSID beacon with no modification
    - MIC key recovery mode: The purpose of this mode is to obtain a MIC key. A MIC and a checksum are recovered by the chopchop attack based on the MIM attack, and the MIC key is recovered. The execution time is about 12-15 minutes.
    - Message falsification mode: The purpose of this mode is to falsify an encrypted packet using a MIC key. When a target is an ARP packet, the execution time of the method is about 4 minutes.

# Message Falsification Attack on WPA (cont)



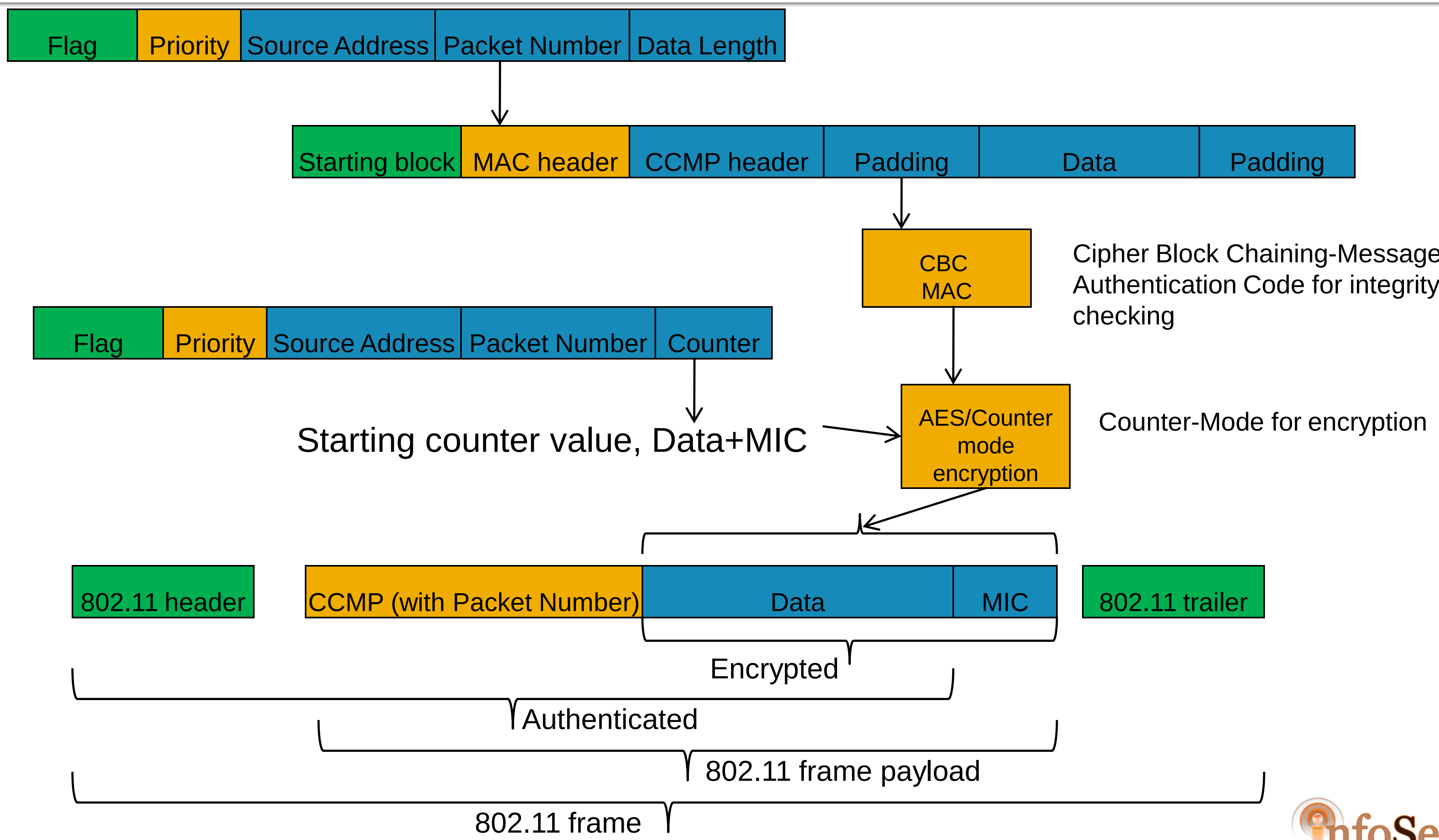
# Message Falsification Attack on WPA (cont)

- Reducing the Execution Time of the Attack
  - Beck-Tews attack recovers all the 4 bytes of the checksum
  - Checksum is compared with the checksum calculated from candidates of the ARP packet.
  - Comparison of 4 bytes checksum is effective
    - Requires at least 3 minutes for the wait time for MIC error.
  - Ohigashi and Morii compare only parts of checksum (last byte)
  - Reduce the time of the wait time for MIC error.
  - Attack reduces the Beck-Tews attack by three minutes
  - Execution time is about one minute.

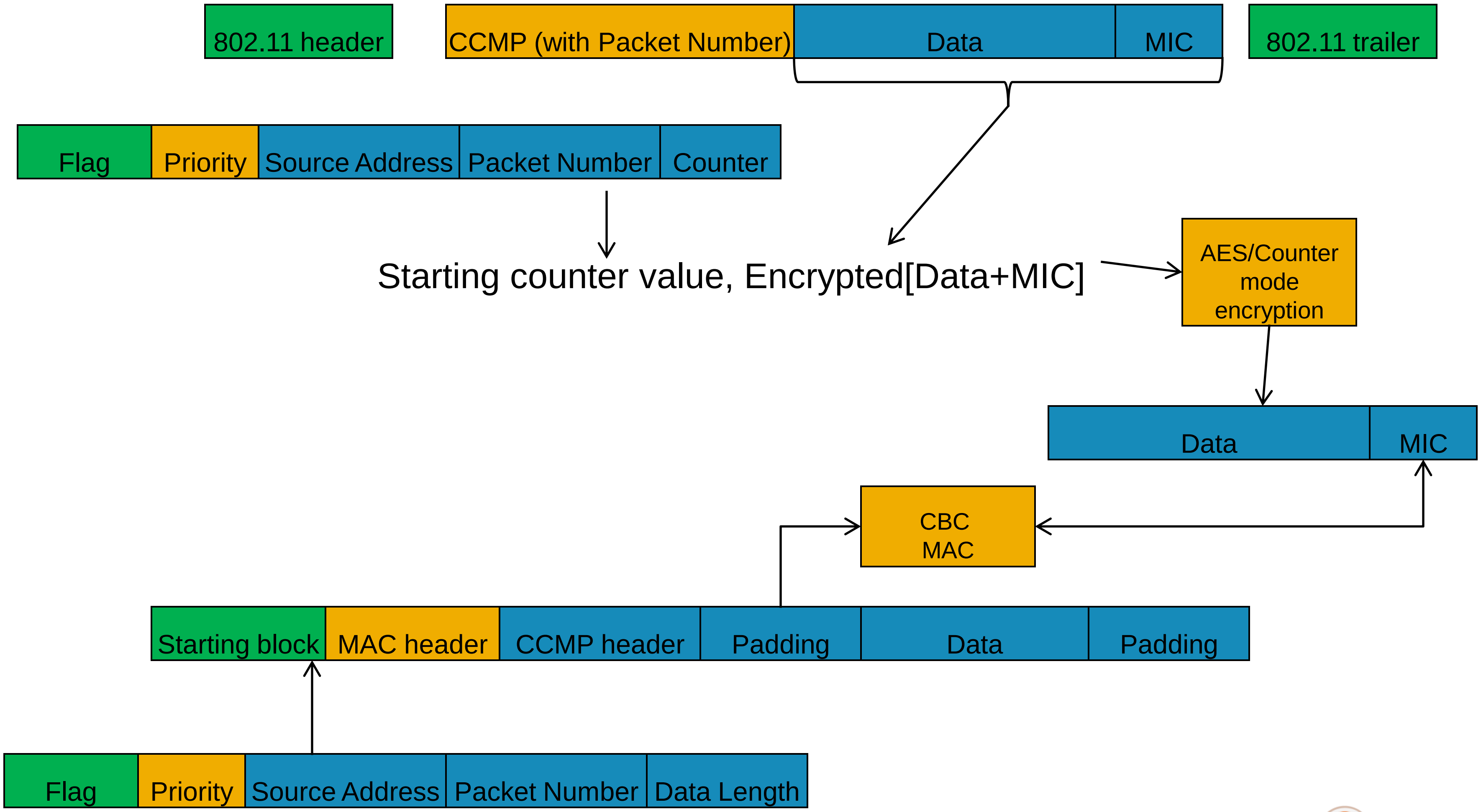
# Wi-Fi Protected Access 2 (WPA2)

- Security standard developed by the Wi-Fi Alliance and is an implementation of IEEE's 802.11i
- Uses the same authentication process, 4-way handshake, and key hierarchy as WPA
- Replaces TKIP with the Advance Encryption Standard (AES) CCMP protocol
  - AES in Counter-Mode for encryption
  - AES in Cipher Block Chaining-Message Authentication Code (CBC-MAC) for integrity checking

# WPA2 Encryption



# WPA2 Decryption



# So are we recommending?

- WEP
  - Dynamic WEP
  - Current key rotation is set to
    - Remember our recommendation is reduce key to 2 minutes
    - This comes a cost to performance
  - Cisco Aironet changes the initialization vector (IV) on a per-packet basis
- WPA
  - Not currently using QoS
  - Start planning transition to AES-CCMP
  - Investigate and apply TKIP key rotation every 2 minutes
  - Capture and analyze logging data on AP's

# Defense Strategies

- Best approach: migrate away from TKIP to AES-CCMP
  - Will likely require moving to WPA2
- Difficult to implement if you need to support any legacy devices
  - Laptops and embedded devices (handhelds, etc)
- Client re-configuration will be necessary, making this resource-intensive
  - Active Directory simplifies deployment

# Defense Strategies (cont)

- Forcing more frequent key rotation will limit how much plaintext can be derived
  - Each minute of key life can be used to determine a byte of plaintext
  - 4 minute key rotation = 4 bytes plaintext
- Consensus is to reduce key lifetime to 2 minutes

This defense is the best immediate-term option, but requires testing to understand the impact to all devices.

# Product-Specific Steps

```
configure terminal
aaa authentication dot1x <profilename>
multicast-keyrotation
unicast-keyrotation
timer mkey-rotation-period 120
timer ukey-rotation-period 120
```

Cisco Autonomous – 802.1X reauthenticate
Warning: Significant negative impact

```
conf t
dot1x timeout reauth-period 120
broadcast-key change 120
```

# Defense Strategies (cont)

- Disabling QoS support on an AP will defeat tools, does not solve issue
  - Not an option for 802.11n High-Throughput (HT) networks
- Vendors may choose to fix TKIP with implementation hacks
  - Keep an eye on AP and client vendor software update pages

# Monitoring

- WIDS technology can identify this attack
  - You may need a software update to get new signature support
  - Action: look for WIDS that can detect the "TKIP ICV attack"
  - No signature in Kismet … yet
- Log monitoring on AP's

Cisco Autonomous APs

```
DOT11-TKIP_MIC_FAILURE_REPORT:
Received TKIP Michael MIC failure
report from the station [mac-address]
on the packet (TSC=0x0) encrypted and
protected by [key] key
```

Aruba Networks

```
Received TKIP Micheal MIC
Failure Report from the
Station [mac addr] [bssid]
[apnames]
```

# Q & A

- Questions and Answers

# Resources

- IEEE Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
  - http://standards.ieee.org/getieee802/download/802.11-2007.pdf
- Tews/Beck paper on TKIP and WEP
  - http://dl.aircrack-ng.org/breakingwepandwpa.pdf
- Raul Siles attack analysis information
  - http://radajo.blogspot.com/2008/11/wpatkipchopchop-attack.html
- Toshihiro Ohigashi and Masakatu Morii
  - http://jwis2009.nsysu.edu.tw/location/paper/A Practical Message Falsification Attack on WPA.pdf