CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Classes

- Security in Networks
  - Threats in Networks
    - Threats in Layer 1 & Layer 2
    - Threats in Network (IP) Layer
    - Threats in Transport layer

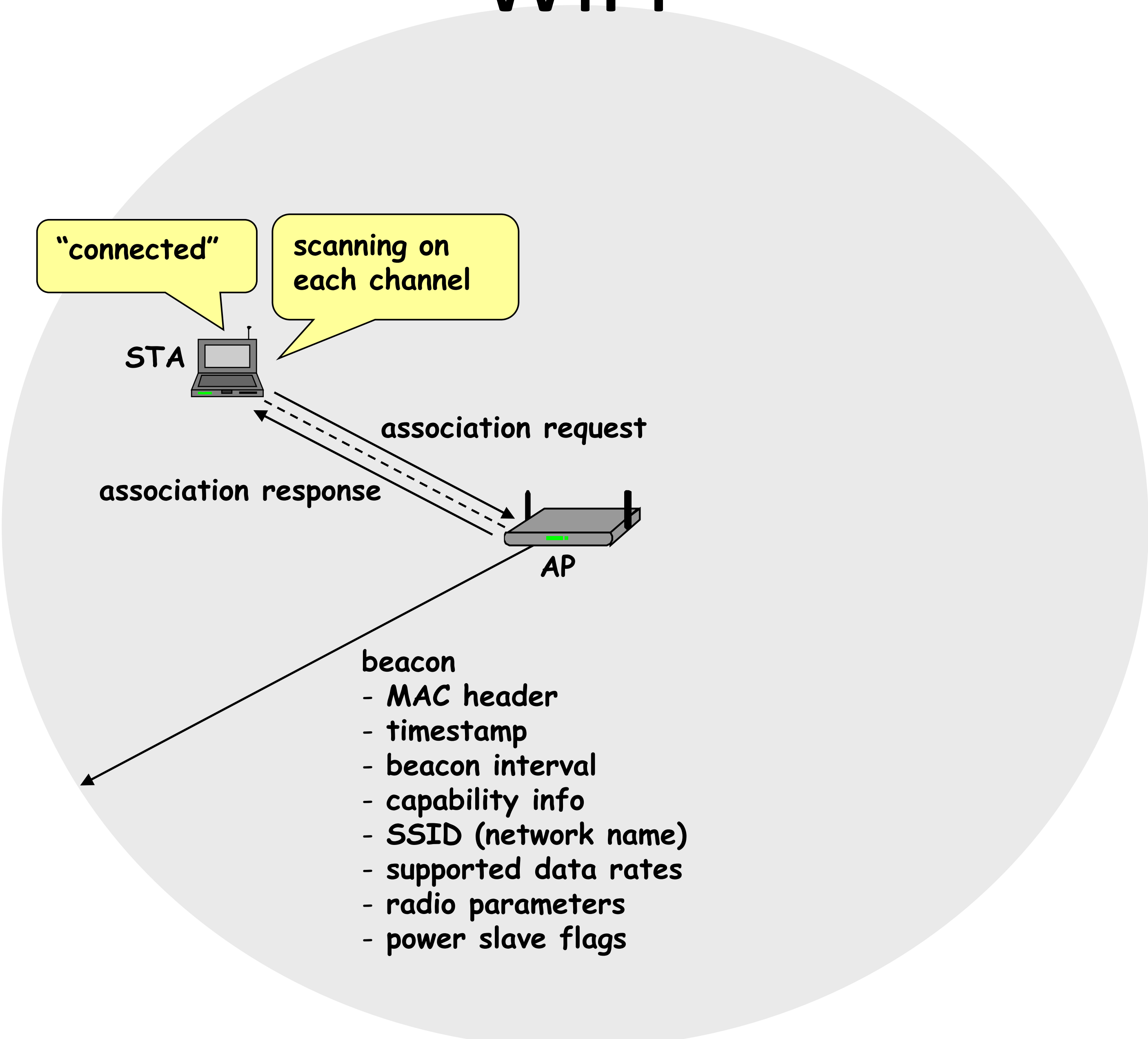
Present class

- Security in Networks
  - Network Security Controls
    - Link
      - WEP, WPA, WPA2
    - Network
      - VPN, IPSec
    - Transport
      - TLS / SSL,
    - Application
      - PGP

Attacks discussed

- Layer1:
  - Attacks on Copper cable
  - Attacks on Optical fiber
  - Attacks on Wireless Microwave \satellite
- Layer2:
  - CAM table poisoning\ overflow
  - VLAN hopping
  - ARP Spoofing (ARP Poisoning)
  - DHCP starvation
- IPayer3
  - IP Spoofing: Route Redirecting (MIM attack)
  - Teardrop attack
  - ICMP attacks: Ping Flood
  - Smurf attack
- TCP Layer
  - Syn Flooding, Session hijacking, Session poisoning etc..

WiFi


"connected"
scanning on each channel
STA
association request
association response
AP
beacon
- MAC header
- timestamp
- beacon interval
- capability info
- SSID (network name)
- supported data rates
- radio parameters
- power slave flags

What an Attacker Might Do?

- Read communication
- Modify communication
- Forge communication
- Inhibit communication

Link-layer security controls

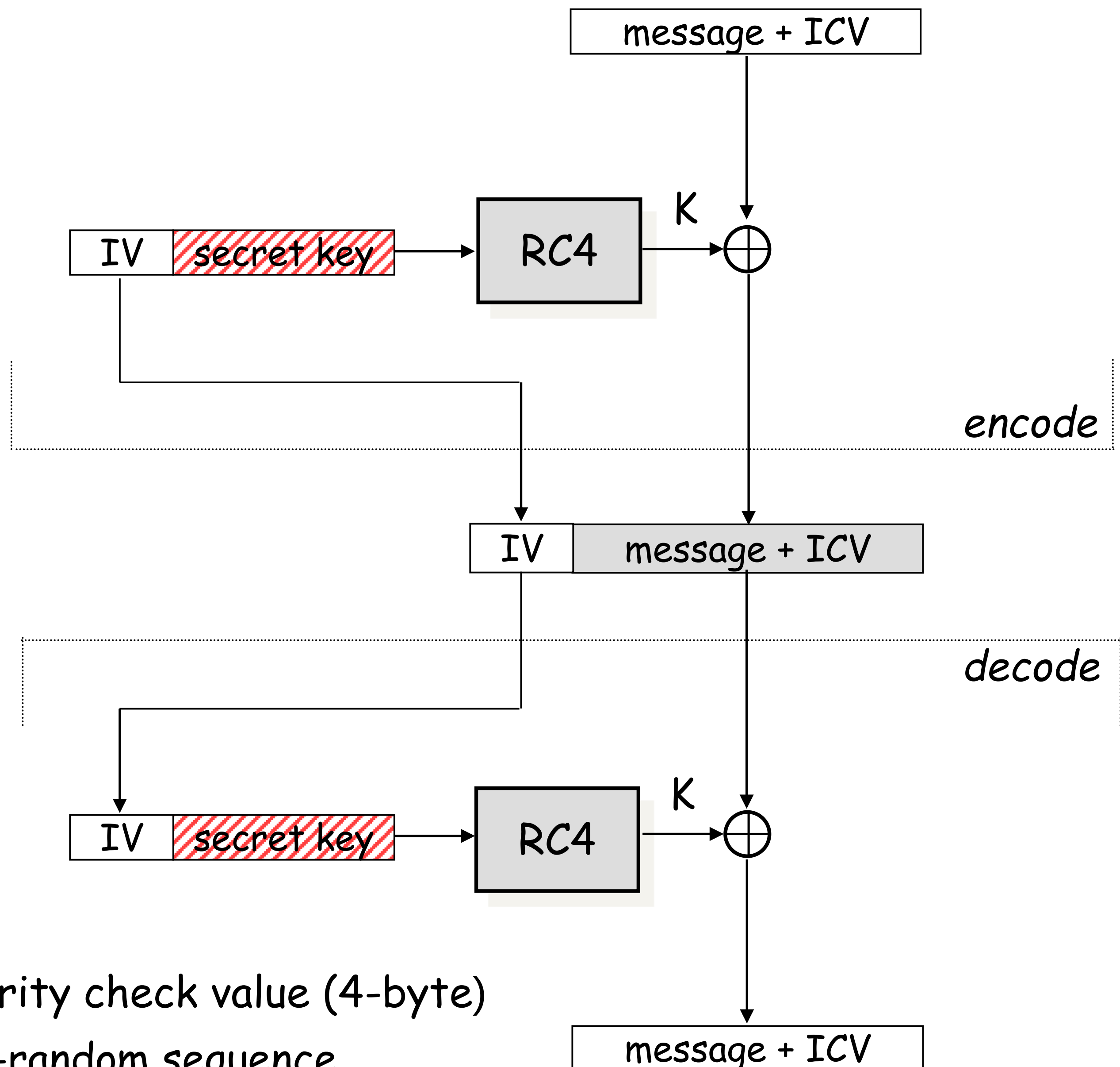
- Intended to protect local area networks
- Most common example today:
  - WEP (Wired Equivalent Privacy)
- WEP was intended to enforce three security goals:
  - Confidentiality
    - Prevent an adversary from learning the contents of your wireless traffic
  - Access Control
    - Prevent an adversary from using your wireless infrastructure
  - Data Integrity
- Unfortunately, none of these is actually enforced!

WEP description

Brief description:

- The sender and receiver share a secret *k*
  - *The secret k is either 40 or 104 bits long*
- In order to transmit a message *M*:
  - Compute a checksum *c(M)*
    - this does not depend on *k*
  - Pick an IV (a random number) *v* and generate a keystream *RC4(v,k)*
  - XOR <*M,c(M)*> with the keystream to get the ciphertext
  - Transmit *v* and the ciphertext over the radio link

WEP – Message confidentiality and integrity



ICV: integrity check value (4-byte)

K: pseudo-random sequence

WEP description

- Upon receipt of *v and the ciphertext*:
  - Use the received v and the shared *k* to generate the keystream *RC4(v,k)*
  - XOR the ciphertext with *RC4(v,k)* to get *<M',c'>*
  - Check to see if *c'* = *c(M')*
  - If it is, accept *M'* as the message transmitted

- Issue: *v is 24 bits long*
  - *Why is this a problem?*

WEP data integrity

- Issue : the checksum used in WEP is CRC-32
  - Quite a poor choice; there's already a CRC in the protocol to detect random errors, and a CRC can't help you protect against malicious errors.

- The CRC has two important properties:
  - It is independent of *k* and *v*
  - It is linear: $c(M \text{ XOR } D) = c(M) \text{ XOR } c(D)$

WEP Authentication

Algorithm Num	Transaction Seq.	Status Code	Challenge Text

Authentication Message format

Algo No: 0 Open Authentication and 1 for WEP authentication

- Issue : the adversary has seen both the plaintext and the ciphertext of the challenge
- this is enough not only to inject packets (as in the previous attack), but also to execute the authentication protocol himself!

Recovering a WEP key

- Note that none of these attacks :
  - Use the fact that the stream cipher was RC4 specifically recovered *k*
- Since 2002, there have been a series of analyses of RC4 in particular
  - Issue : it turns out that when RC4 is used with similar keys, the output keystream has a subtle weakness

Wi-Fi Protected Access (WPA)

- Flaws in WEP known since January 2001 - flaws include weak encryption (keys no longer than 40 bits), static encryption keys, lack of key distribution method.
  - These observations have led to programs that can recover either a 104-bit or 40-bit WEP key in under 60 seconds, most of the time

- In April 2003,
  - the Wi-Fi Alliance introduced an interoperable security protocol known as WiFi Protected Access (WPA).
  - WPA was designed to be a replacement for WEP networks without requiring hardware replacements.
  - WPA provides stronger data encryption (weak in WEP) and user authentication (largely missing in WEP).

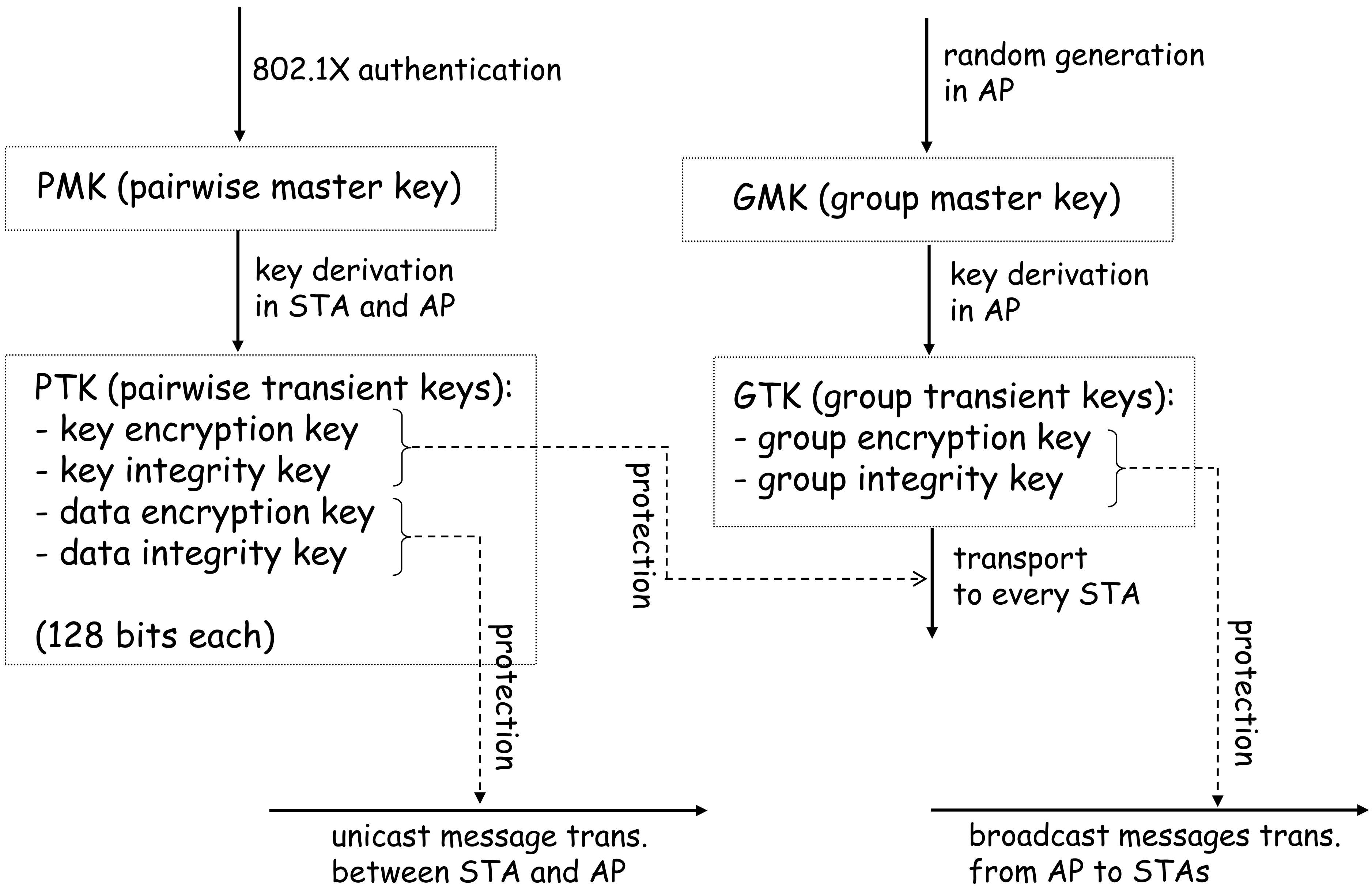
Replacing WEP

- Wi-fi Protected Access (WPA) was rolled out as a short-term patch to WEP while formal standards for a replacement protocol (IEEE 802.11i, later called WPA2) were being developed
- WPA:
  - Replaces CRC-32 with a real MAC (here called a Message Authentication code)
  - IV is 48 bits
  - Key is changed frequently (TKIP)
  - Ability to use 802.11x authentication server
    - But maintains less-secure PSK (Pre-Shared Key) mode for home users
  - Able to run on most older WEP hardware

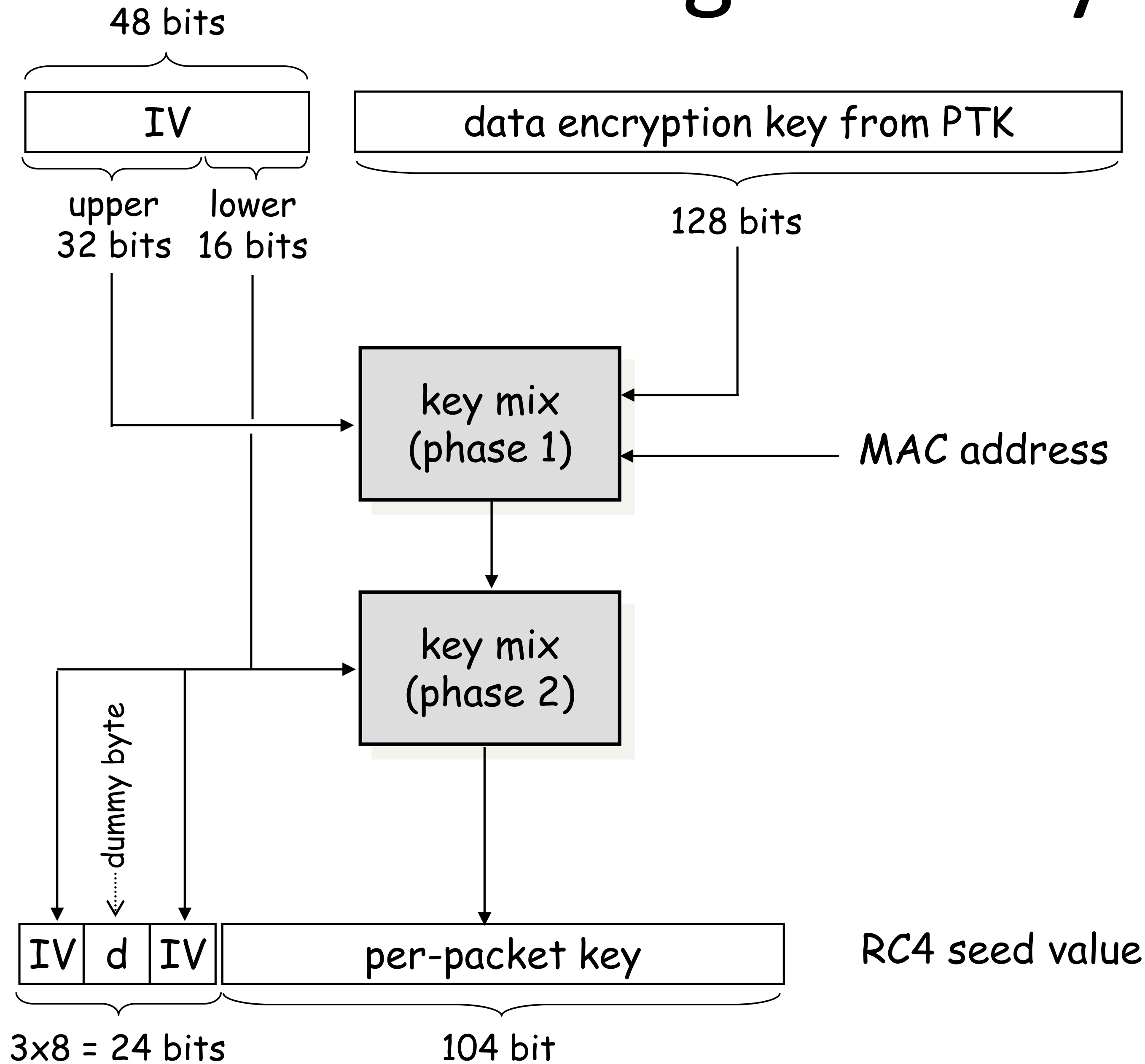
Replacing WEP

- The 802.11i standard was finalized in 2004, and the result (called WPA2) has been required for products calling themselves "Wi-fi" since 2006
- WPA2:
  - Replaces the RC4 and MIC algorithms in WPA with the CCMP algorithm, which uses AES
  - Considered strong, except in PSK mode
    - Dictionary attacks still possible

Key hierarchies



TKIP – Generating RC4 keys



AES-CCMP

- CCMP means CTR mode and CBC-MAC
  - integrity protection is based on CBC-MAC (using AES)
  - encryption is based on CTR mode (using AES)
- CBC-MAC
  - CBC-MAC is computed over the MAC header, CCMP header, and the MPDU (fragmented data)
  - mutable fields are set to zero
  - input is padded with zeros if length is not multiple of 128 (bits)
  - CBC-MAC initial block:
    - flag (8)
    - priority (8)
    - source address (48)
    - packet number (48)
    - data length (16)
  - final 128-bit block of CBC encryption is truncated to (upper) 64 bits to get the CBC-MAC value
- CTR mode encryption
  - MPDU and CBC-MAC value is encrypted, MAC and CCMP headers are not
  - format of the counter is similar to the CBC-MAC initial block
    - "data length" is replaced by "counter"
    - counter is initialized with 1 and incremented after each encrypted block

- Thanks