CT437
COMPUTER SECURITY AND FORENSIC COMPUTING

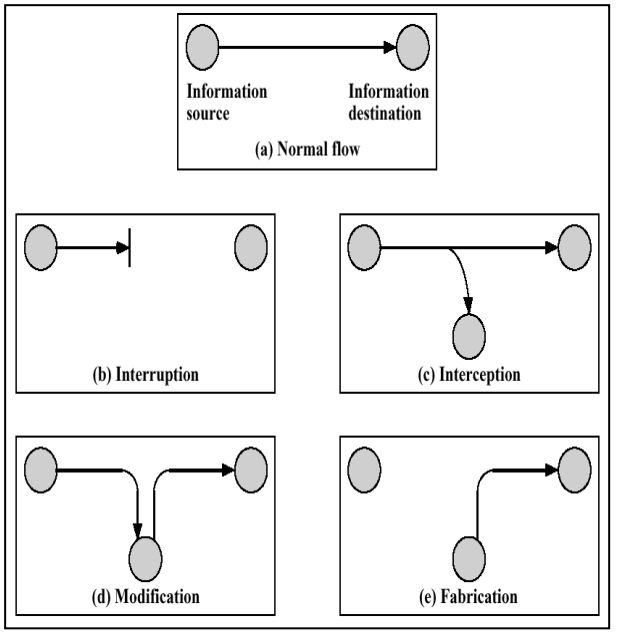
SECURE NETWORK COMMUNICATION PRINCIPALS

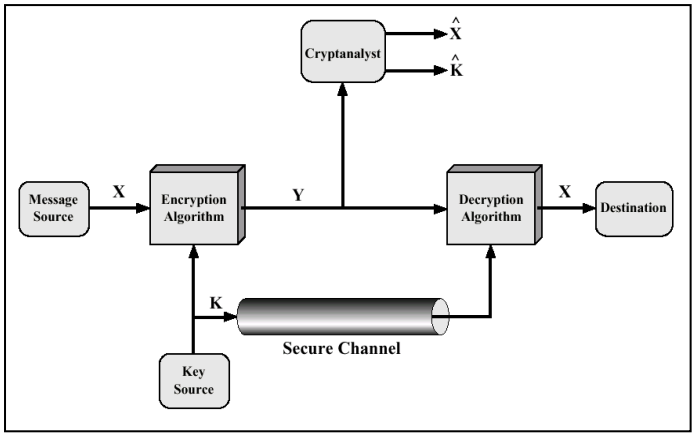
Dr. Michael Schukat

Ollscoil na Gaillimhe
University of Galway

Lecture Overview

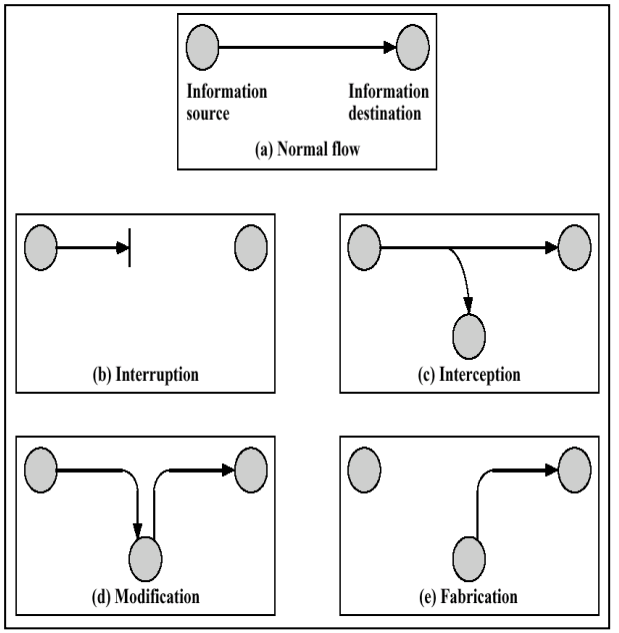
- This lecture will look in more detail into how data encryption and hashing mechanisms can be applied to provide secure peer-to-peer data communication over an (unsecure) network

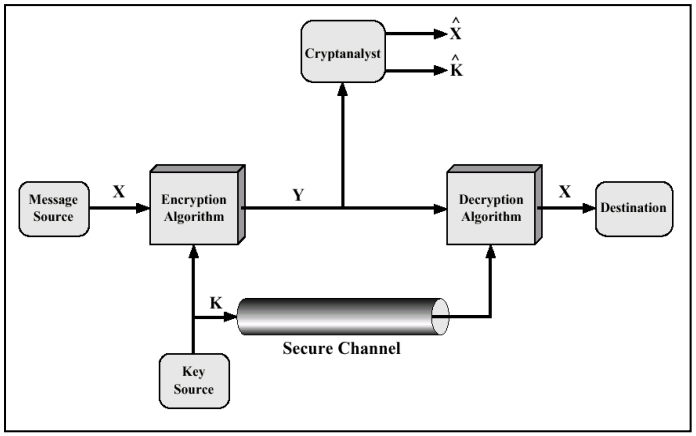




Lecture Overview

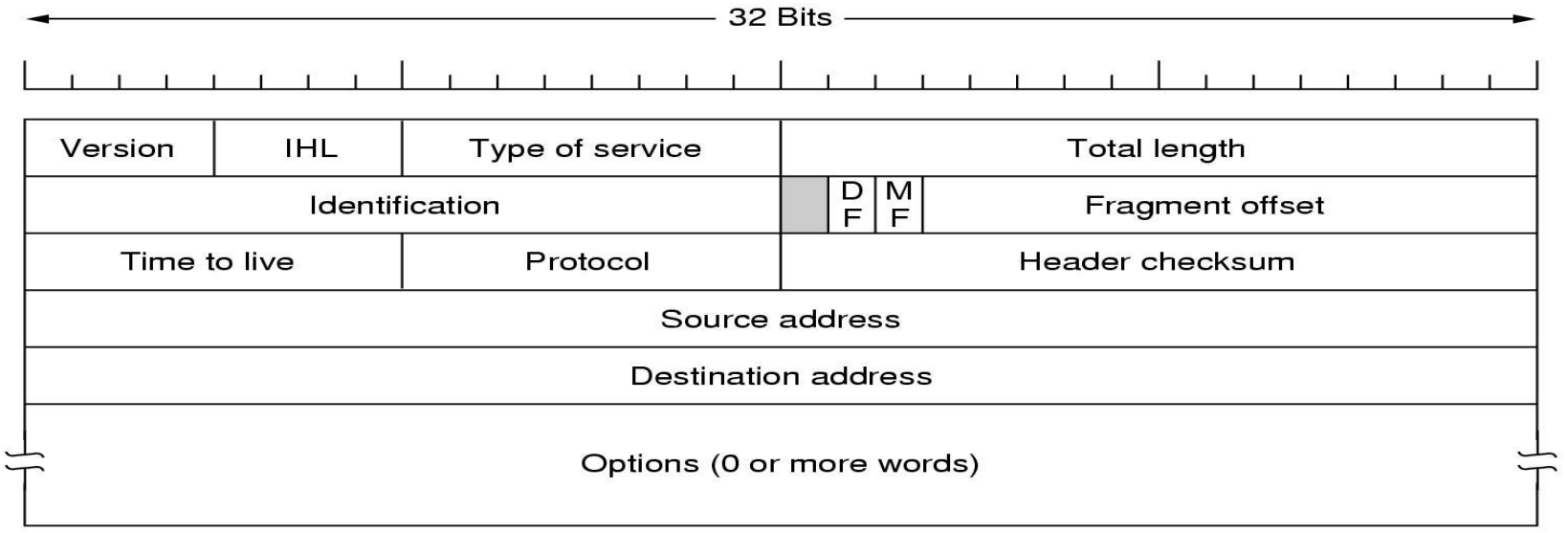
- Symmetric block and stream ciphers allow the encryption of data in transit
  - Needs robust key management and distribution
- Hash functions / MACs allow authentication of data in transit
- Digital certificates allow end-point authentication
- Hashing and encryption provide mechanisms to address some of security attack types on information in transit
  - Example Wireshark
- This lecture will look in more detail into how these mechanisms can be applied to provide secure peer-to-peer data communication over a network





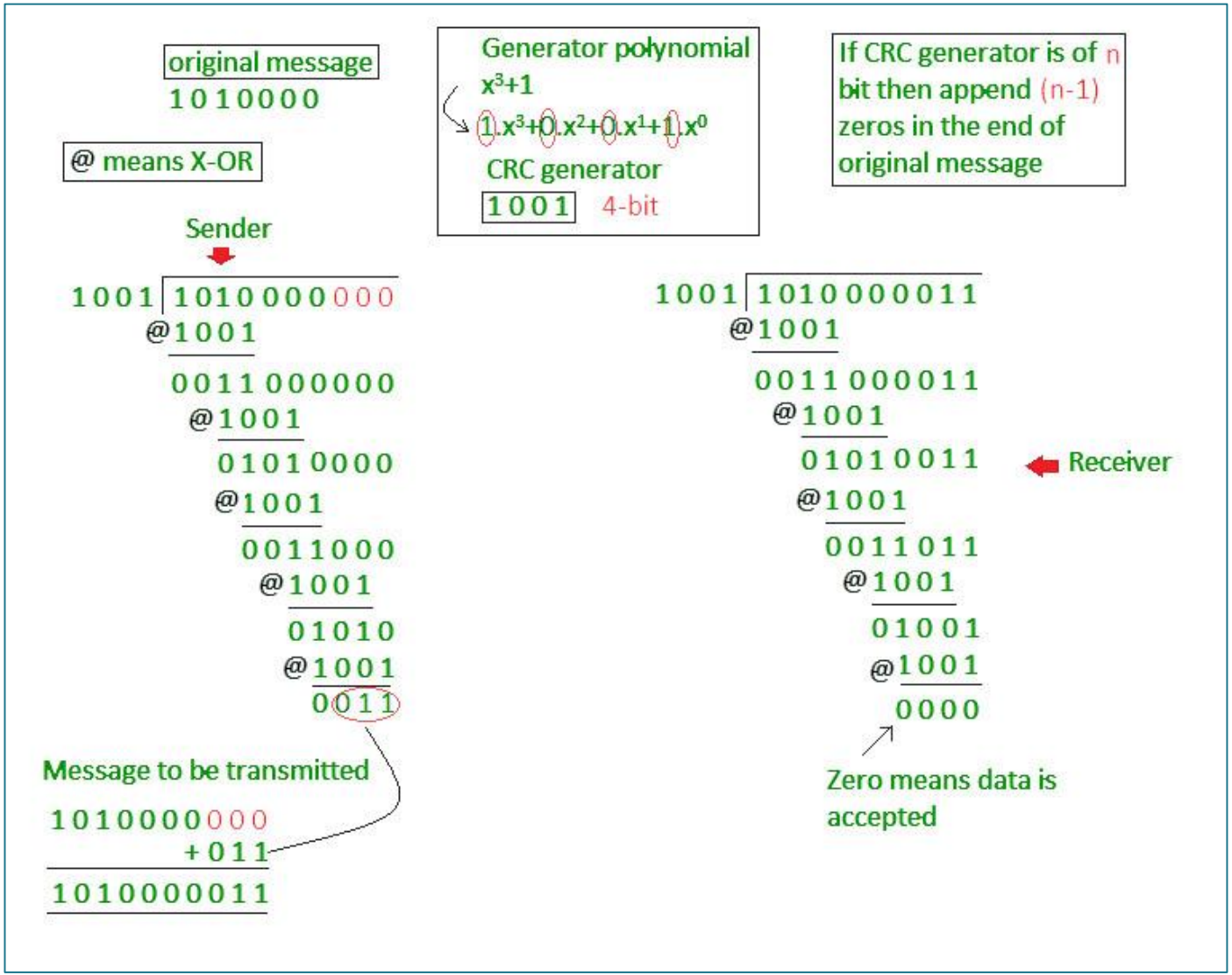
Issues with the IP Protocol

- IP payload is not encrypted (no confidentiality) and can be manipulated in transit
- IP header fields can be manipulated in transit (CRC can be adjusted on-the-fly → next slide)
  - IP addresses can be spoofed (no authentication)
- IP header has mutable fields that can change during datagram transport



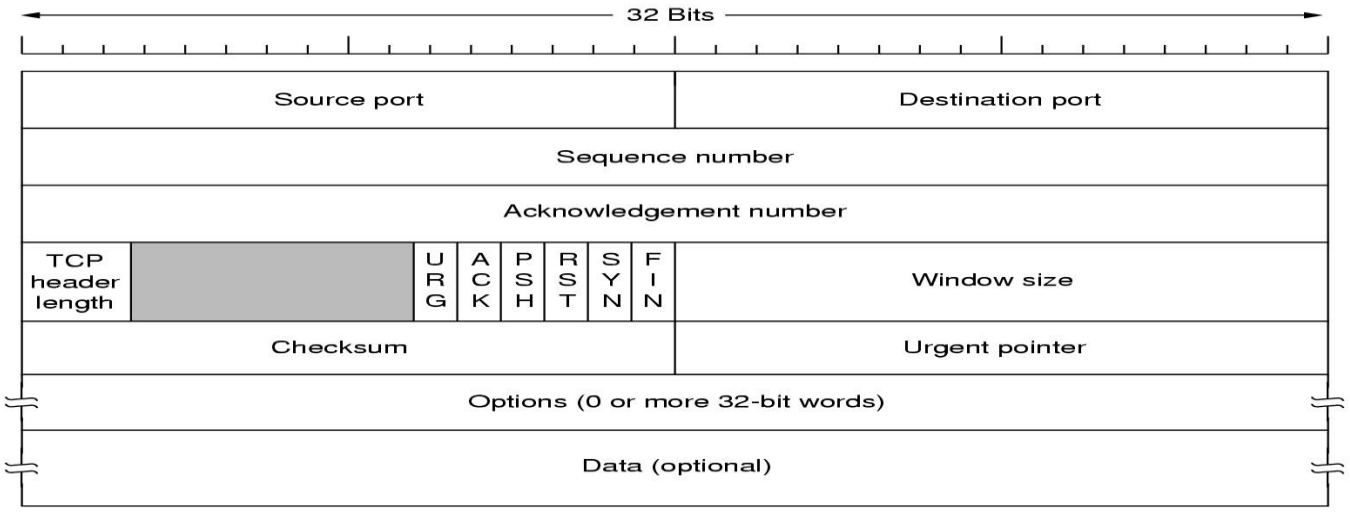
Mx2

Recap: Cyclic Redundancy Check (CRC)



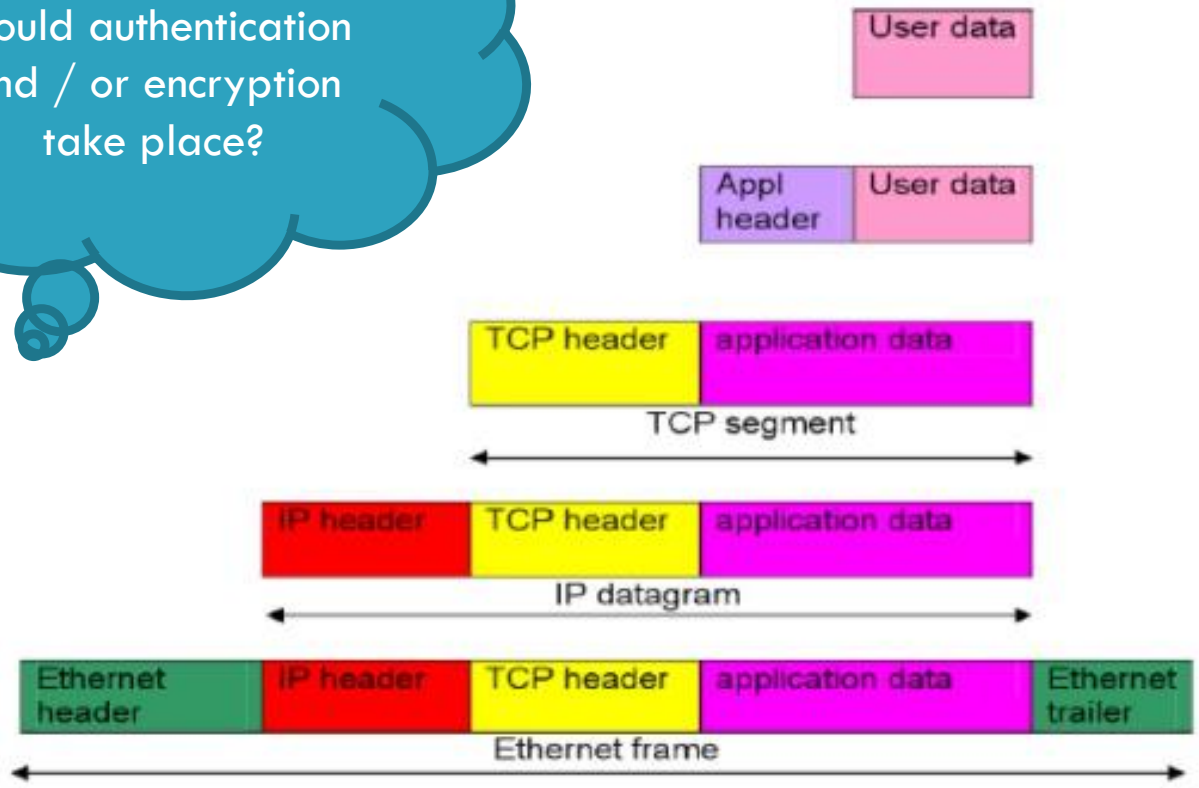
Issues with the Transport Layer Protocol (Example TCP)

- TCP payload is not encrypted (no confidentiality) and can be manipulated in transit
- TCP header fields can be manipulated in transit (CRC can be adjusted)
  - TPDUs can be rearranged in transit via manipulating sequence and acknowledgement numbers



TCP/ IP Header Hierarchy

On what level(s) should authentication and / or encryption take place?



L5/6

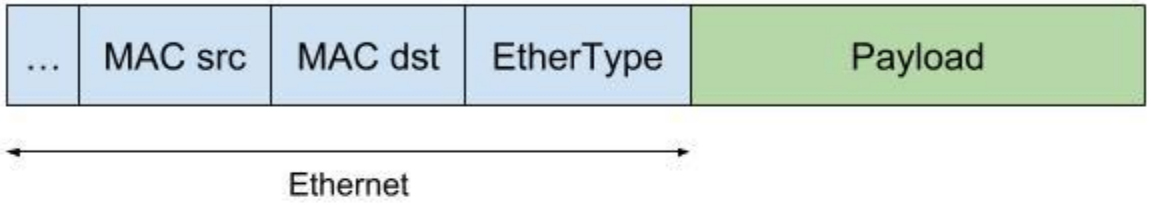
L4

L3

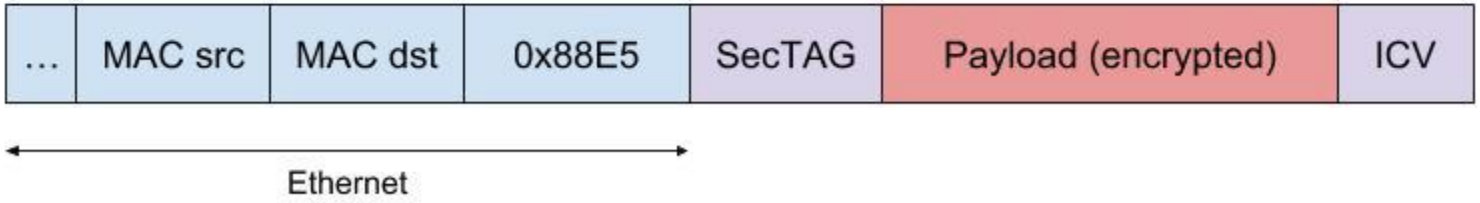
L2

Example MACsec

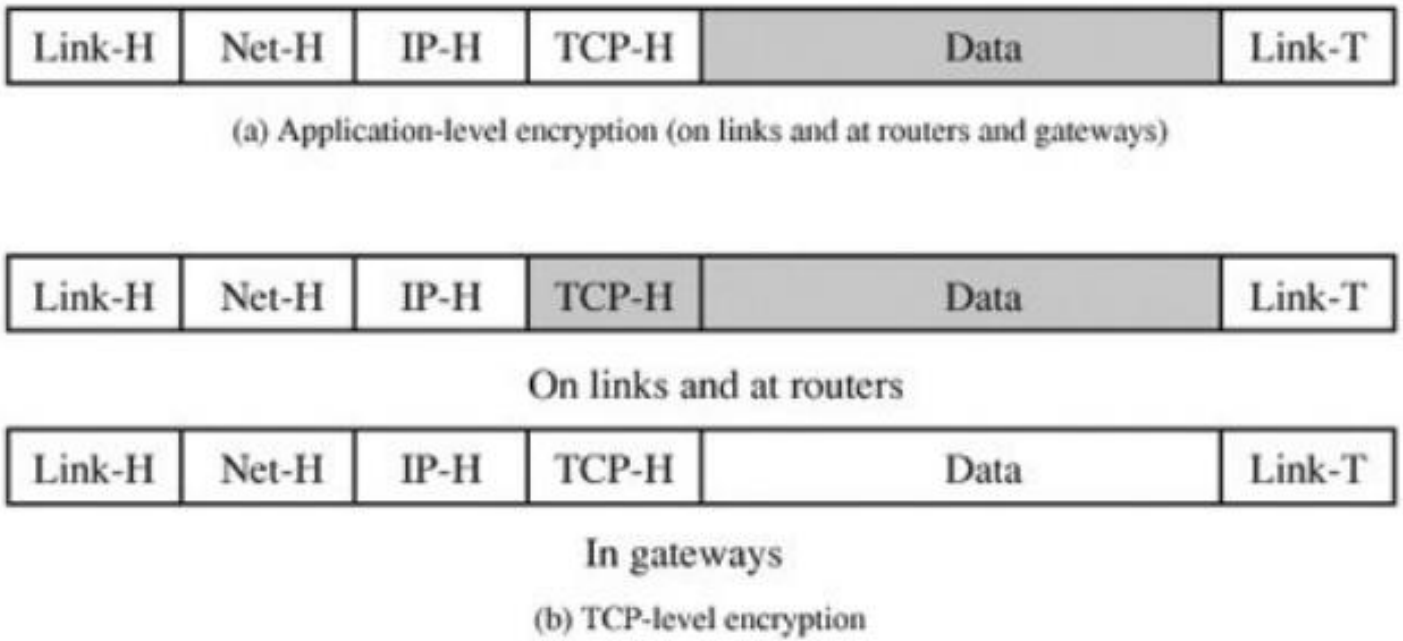
Ethernet frame and its payload



Ethernet frame and its payload,
using MACsec (encryption enabled)

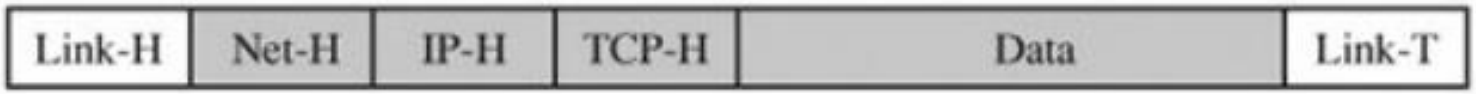


Encryption Coverage Implications

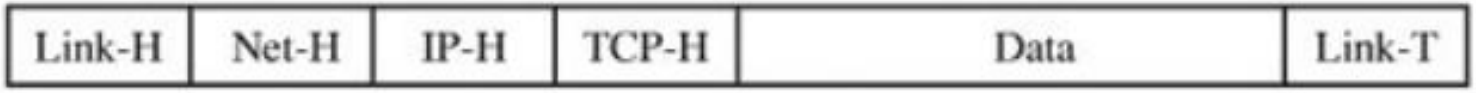


TCP-H – TCP header
IP-H – IP header
Net-H – Network-level header (e.g., X.25 packet header, LLC header)
Link-H – Data link control protocol header
Link-T – Data link control protocol trailer

Encryption Coverage Implications



On links



In routers and gateways

(c) Link-level encryption

Shading indicates encryption.

TCP-H	=	TCP header
IP-H	=	IP header
Net-H	=	Network-level header (e.g., X.25 packet header, LLC header)
Link-H	=	Data link control protocol header
Link-T	=	Data link control protocol trailer

WEP

Example for an unsecure network security protocol

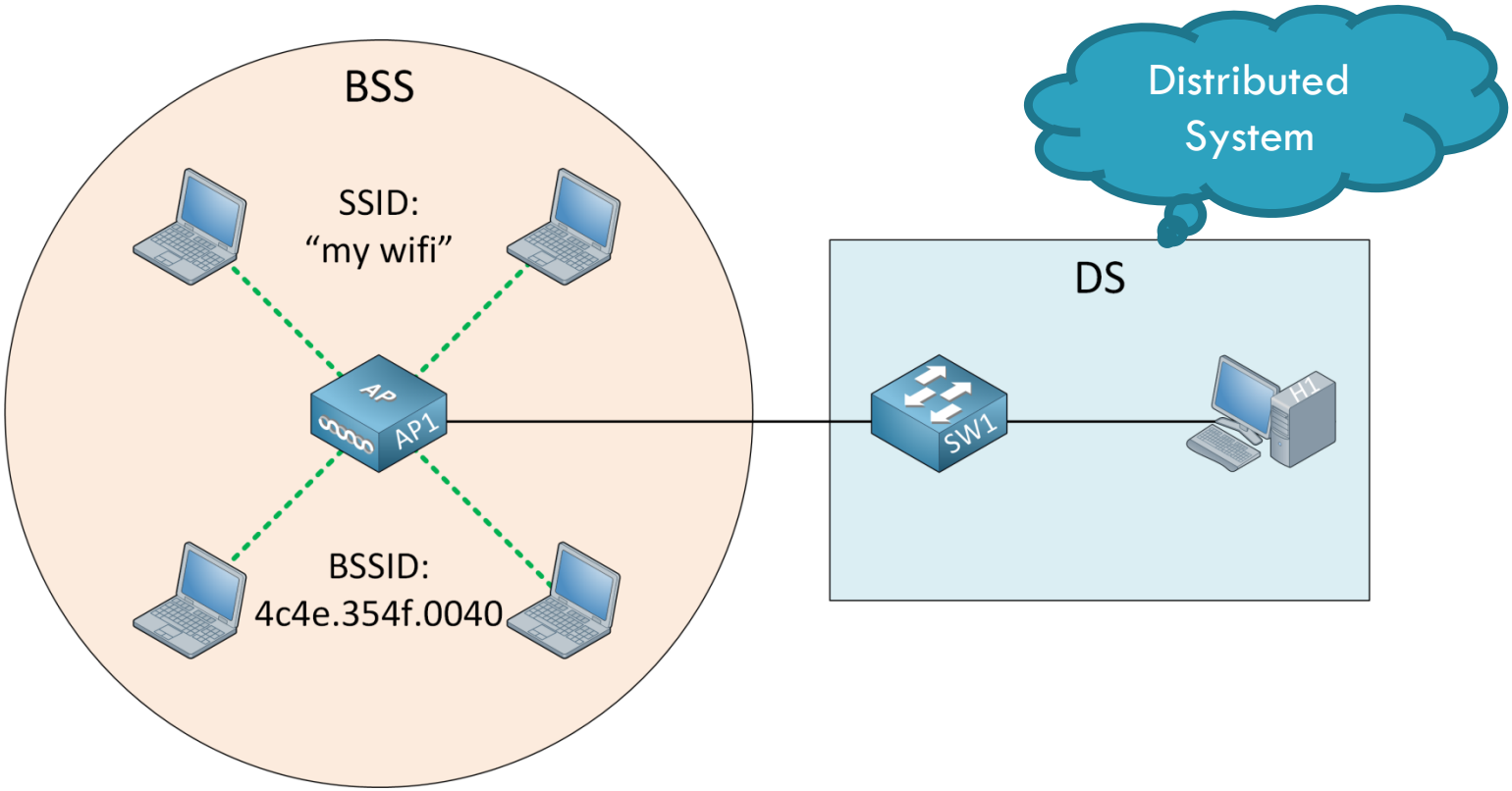
Wire Equivalent Privacy (WEP)

- The first attempt of encrypting 802.11 (Wi-Fi) communication
- It was the de-facto 802.11 security protocol for a couple of years, implemented in all Wi-Fi routers at the time
- However, it has a flawed design and has been broken in the early 2000s
  - It is completely obsolete by now – Don't use it!
- Nonetheless it makes a good case study…

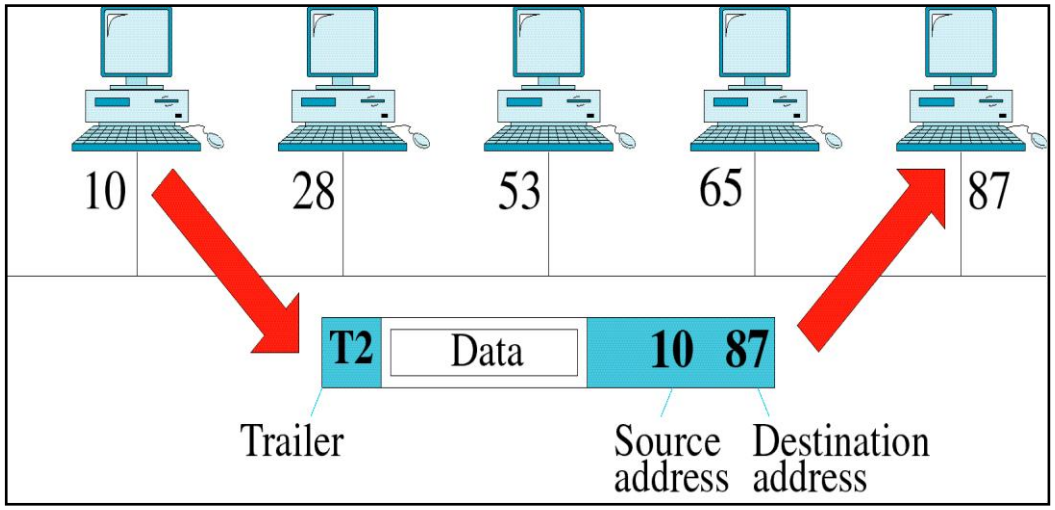
802.11 Summary

- Wireless network protocol, operates on 2.4 GHz or 5 GHz carrier frequency
- The base version of this IEEE standard was released in 1997, with various amendments since
- In the common *infrastructure mode* networks are organise as wireless network basic service set (BSS)
- A BSS consists of one redistribution point (i.e., an access point) together with one or more client stations that are associated with it
- Each BSS has a
  - unique id (BSSID), like a 48 medium access sublayer (MAC) address
  - Customisable name, the Service Set ID (SSID)
- 802.11 is based on the exchange of plaintext messages and as such prone to Wi-Fi eavesdropping too (→ Wireshark)

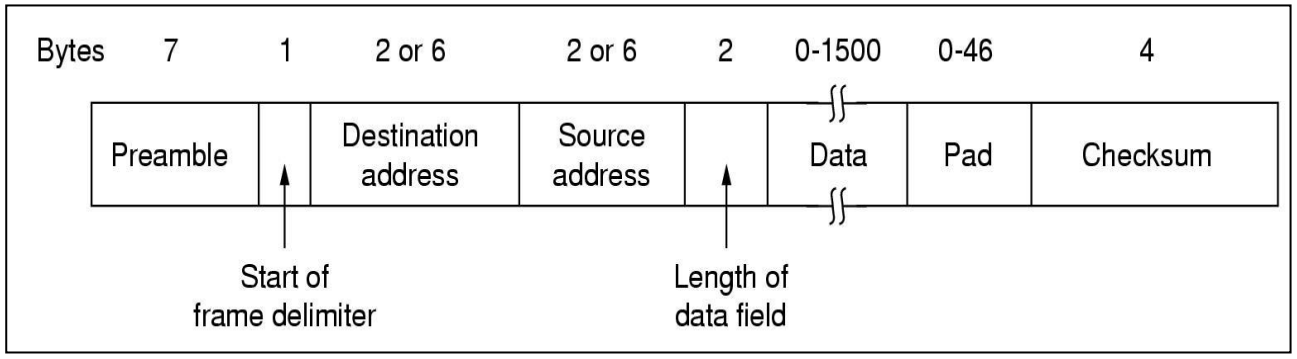
BSS, BSSID and SSID



Recall: The 802.3 MAC Sublayer Protocol

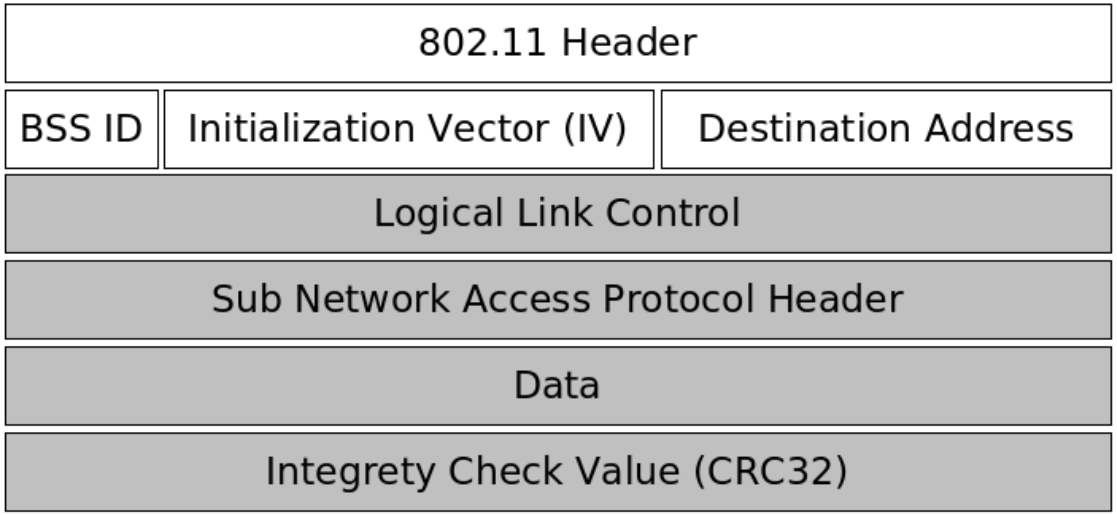


- Simpler than 802.3 packet structure:



WEP Overview

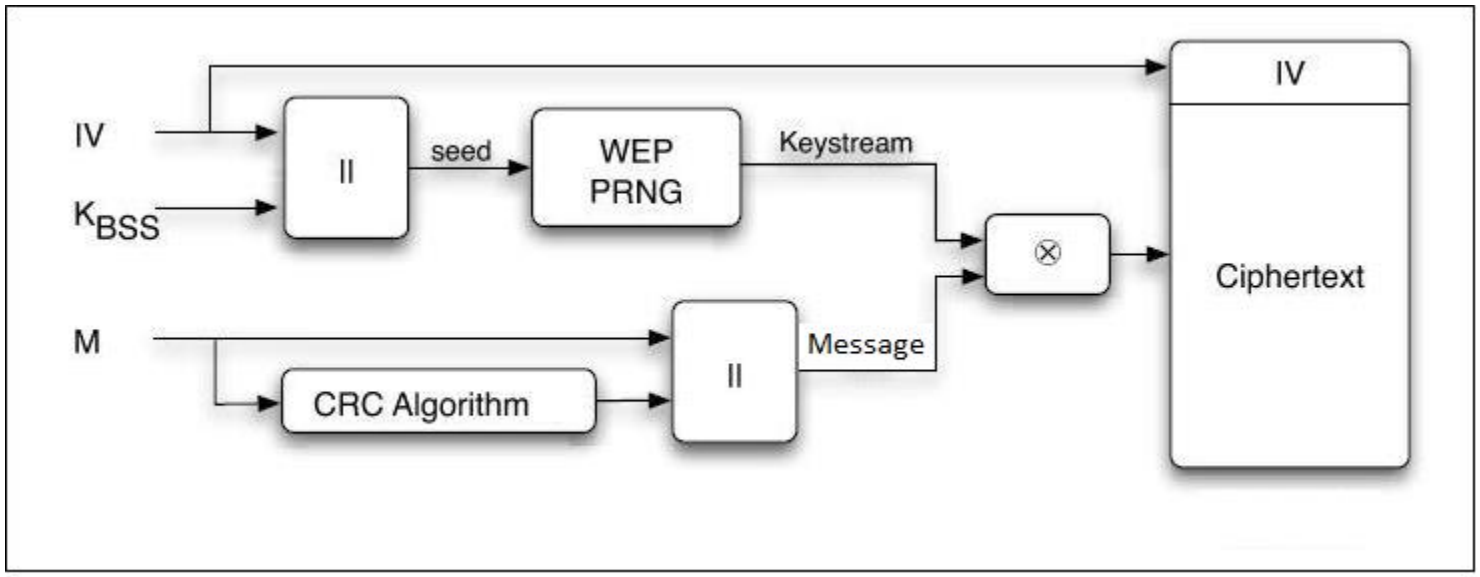
- WEP was ratified as a Wi-Fi security standard in 1999
- Two main flavours,
  - WEP-40 (40-bit secret key plus 24-bit shared initialisation vector), i.e., 64-bit WEP
  - WEP-104 (104-bit secret key plus 24-bit shared initialisation vector), i.e., 128-bit WEP
- WEP uses
  - the stream cipher RC4 for confidentiality
  - the CRC-32 checksum for integrity
- Both flavours were deprecated in 2004 (!)
- The WEP header is shown on the right with encrypted sections highlighted in dark
  - Note the (24-bit) plaintext initialisation vector is incremented with every packet



WEP Encoding

- A secret BSS key K_{BSS} (40 bit or 104 bit) is shared between the AP and all clients
- Every Wi-Fi packet contains a random 24-bit initialisation vector IV chosen by the sender
- IV ¦¦ K_{BSS} is the seed for an RC4 stream cipher (WEP PRNG)
- The payload M is complemented by a 32-bit CRC (cyclic-redundancy-checksum) and bitwise EXORed with the key stream
- The resulting encrypted message is complemented with the IV and transmitted

WEP Encoding



802.11 Header		
BSS ID	Initialization Vector (IV)	Destination Address
Logical Link Control		
Sub Network Access Protocol Header		
Data		
Integrety Check Value (CRC32)		

Encrypted / authenticated

Recap: RC4 as used in WEP

- RC4 is a stream cipher
- It consists of a
  - key-scheduling algorithm (KSA) and a
  - pseudo-random generation algorithm (PRGA)
- The KSA uses IV ¦¦ K_{BSS} as a key to initialise the algorithm
- Subsequently the PRGA returns pseudo-random byte at a time

WEP Weaknesses

- Because RC4 is a stream cipher, the same traffic key must never be used twice
- The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network
  - 16,777,216 different RC4 cipher streams when the IV is just incremented
  - Even worse, when a new IV is randomly picked for each packet, there is a 50% probability the same IV will repeat after 5,000 packets (Birthday paradox)
- There's a range of WEP attacks that takes advantage of that

Summary

- Network security (i.e., data encryption and / or authentication) is important for obvious reasons
- The layered structure of the TCP/IP stack allows positioning the extra security layer in different levels
- Each of these options has its advantages and disadvantages / limitations, for example with regard to
  - the portions of a packet that can be secured
  - compatibility with network routing, NAT, etc.
- WEP as a much weaker and depreciated option shows how encryption / authentication may take place on data-link layer