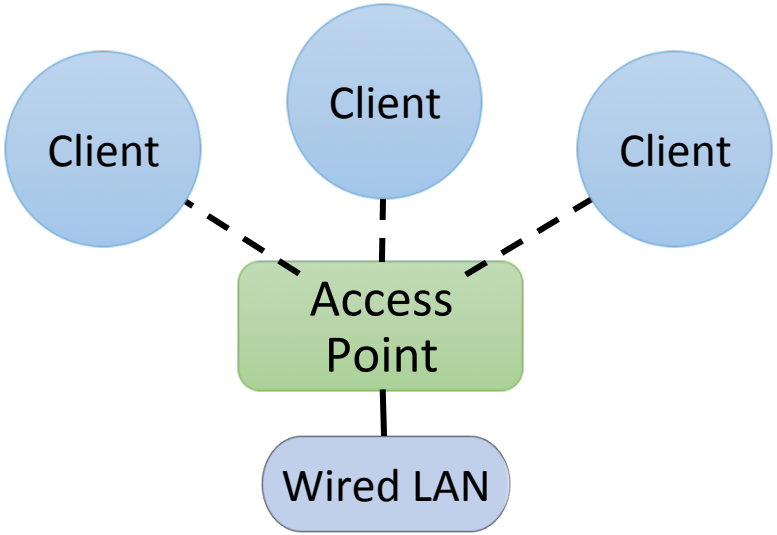
Module 3
Network Security

Submodule 4: Wireless Security

Wireless Technologies

- In wireless networking, parties connecting to a network are referred to as clients.
- A wireless router or other network interface that a client connects to is Access Point (AP)
- Client establishes a wired network, which provides a gateway to the Internet



Wireless Security Concerns

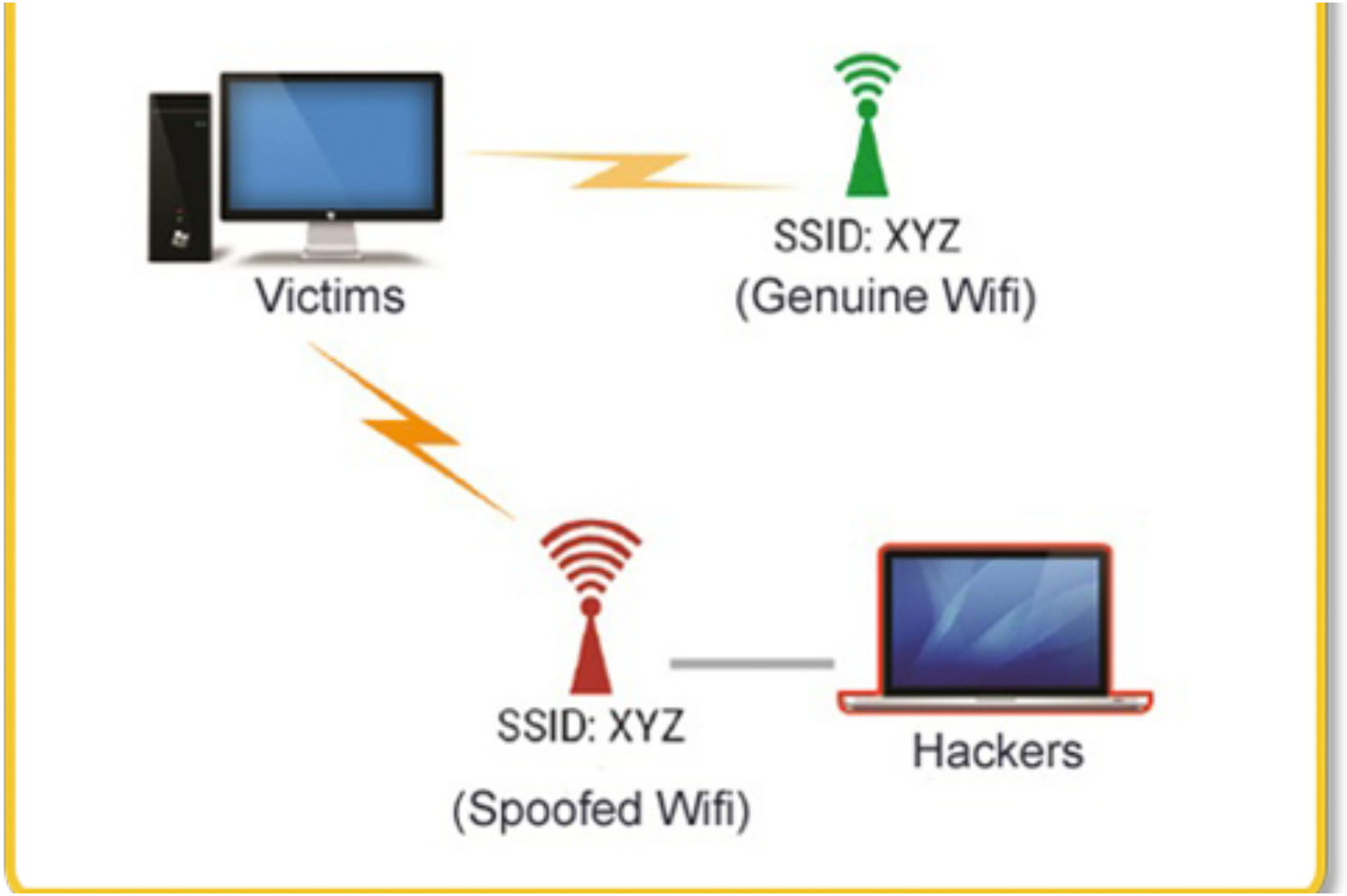
- Radio signals may leak outside buildings
- Wireless network is susceptible to sniffing
- Wireless communication can easily be intercepted
- Unauthorized user can use someone else's wireless access point
- Authorization and authentication are more challenging in wireless networking

Wireless Protocols

- Most wireless networks use protocols defined by the IEEE 802.11 family of standards.
  - Methods for transmitting data via radio waves over predefined radio frequency ranges
  - 802.11 defines the structure of wireless frames that encapsulate the higher layers of the IP stack
  - Most TCP/IP implementations perform reframing of packets depending on their intended recipient.
    - Wireless traffic received in the form of 802.11 frames is converted into Ethernet frames that are passed to higher layers of the TCP/IP stack
    - Ethernet frames to be routed to wireless clients are converted into 802.11 frames

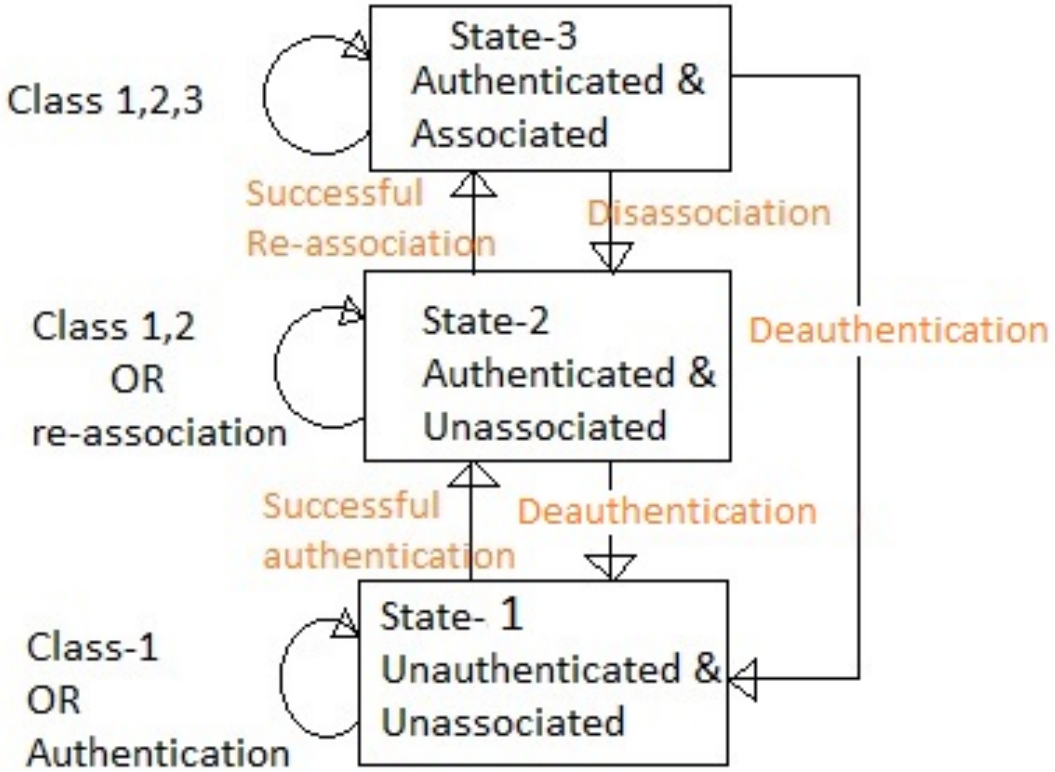
Service Set ID (SSID)

- Multiple wireless network can coexist
  - Each network is identified by a 32-character SSID
  - Typical default SSID of access point is manufacturer's name
  - SSIDs often broadcasted to enable discovery of the network by prospective clients
- SSIDs are not signed, thus enabling a simple spoofing attack
  - Place a rogue AP in a public location and use the SSID of an ISP
  - Set up a login page similar to the one of the ISP
  - Wait for clients to connect to rogue AP and authenticate


Victims
SSID: XYZ
(Genuine Wifi)
SSID: XYZ
(Spoofed Wifi)
Hackers

Wireless Networking Frames

- 802.11 standards defines:
  - Authentication frame: client use it or present its identity to an AP
  - Association request frame: client sends it to ask AP to allocate resources
  - Association response frame
  - Disassociation frame: sent by an AP to terminate a wireless connection
  - Deauthentication frame: an AP can send it to cut off communications altogether
  - Reassociation request frame
  - Reassociation response frame



802.11 State Diagram

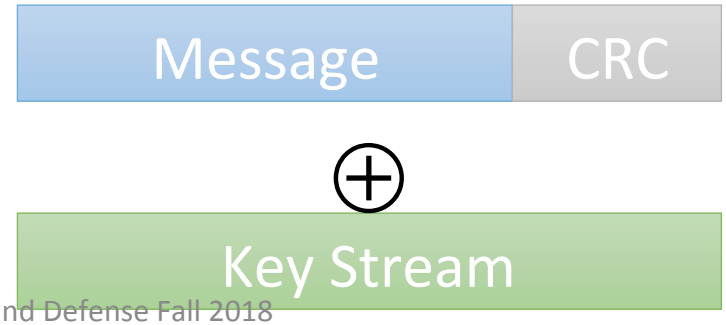
[WLAN Class 1, 2, 3 frames]

Wired Equivalent Privacy (WEP)

- WEP protocol was incorporated into the original 802.11 standard to provide:
  - Confidentiality: eavesdropping is prevented
  - Data integrity: packets cannot be tampered with
  - Access control: only properly encrypted packets are routed
- Design constraints of WEP:
  - Inexpensive hardware implementation with 90's technology
  - Compliance with early U.S. export control regulations on encryption (40-bit keys)

WEP Protocol

- Setup
  - Access point and client share 40-bit key K
  - The key never changes during a WEP session
- Encryption
  - Compute CRC-32 checksum of message M (payload of frame)
  - Pick 24-bit initialization vector V
  - Using the RC4 stream cipher, generate key stream S(K,V)
  - Create ciphertext C = (M || crc(M)) ⊕ S(K,V)



WEP Protocol (cont.)

- Client authentication:
  - Open system: client doesn't need any credentials
  - Shared key authentication:
    - Access point sends unencrypted random challenge to client
    - Client responds with encrypted challenge
- Transmission
  - Send V|| C

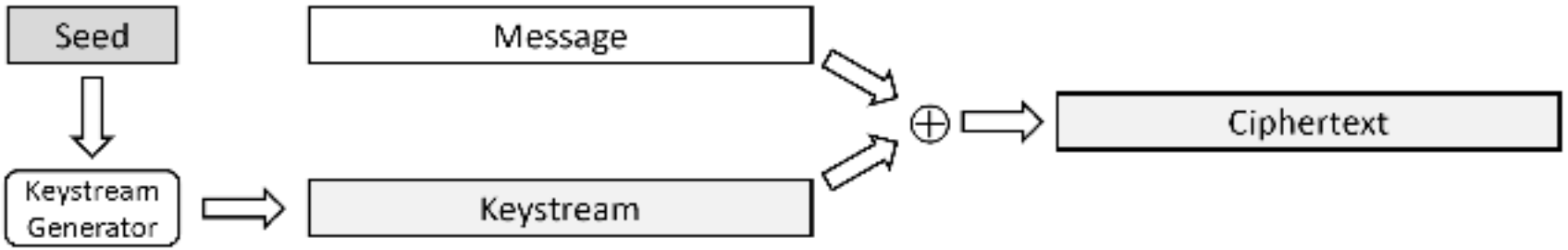
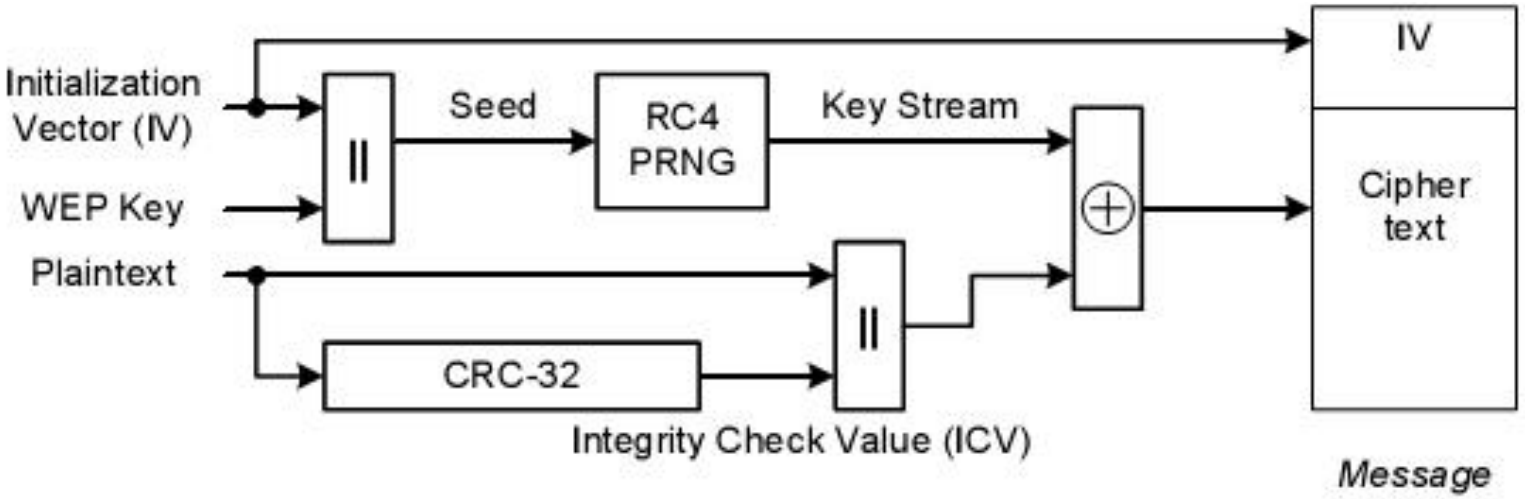


Figure 6.24: Encryption with a stream cipher.

Authentication Spoofing

- Attacker wants to spoof a legitimate client
  - Does not know the secret key K
  - Can eavesdrop authentication messages
- Attack
  - Obtain challenge R and encrypted challenge C = (R || crc(R)) ⊕ S(K,V)
  - Compute key stream S(K,V) = (R || crc(R)) ⊕ C
  - Reuse key stream S(K,V) when challenged from access point


Initialization Vector (IV)
WEP Key
Plaintext
||
Seed
RC4 PRNG
Key Stream
CRC-32
||
Integrity Check Value (ICV)
IV
Cipher text
Message

Reused Initialization Vectors

- Repeated IV implies reused key stream
  - Attacker obtains XOR of two messages
  - Attacker can recover both message and key stream
  - Recovered key stream can be used by attacker to inject traffic
- Default IV
  - Several flawed implementations of IV generation
  - E.g., start at zero when device turned on and then repeatedly increment by one
- Random IV
  - Small length (24 bits) leads to repetition in a short amount of time even randomly generated
  - E.g., collision expected with high probability after $2^{12} \approx 4{,}000$ transmissions

Wi-Fi Protected Access (WPA)

- WEP became widely known as insecure
  - In 2005, FBI publically cracked a WEP key in only 3 minutes!
- Wi-Fi Protected Access (WPA) proposed in 2003
- Improves on WEP in several ways:
  - Larger secret key (128 bits) and initialization data (48 bits)
  - Supports various types of authentication besides a shared secret, such as username/password
  - Dynamically changes keys as session continues
  - Cryptographic method to check integrity
  - Frame counter to prevent replay attacks

WPA2

- WPA was an intermediate stepping-stone
  - Final version: IEEE 802.11i, aka WPA2
- Improvements over WPA are incremental rather than changes in philosophy:
  - Uses AES instead of RC4
  - Handles encryption, key management, and integrity
  - MAC provided by Counter Mode with Cipher Block Chaining (CCMP) used in conjunction with AES
- WPA2 needs recent hardware to operate properly, but this will get better over time

Alternatives and Add-Ons

- WEP, WPA, and WPA2 all protect your traffic only up to the access point
  - No security provided beyond access point
- Other methods can encrypt end-to-end:
  - SSL, SSH, VPN, PGP, and so on
- End-to-end encryption is often simpler than setting up network-level encryption
- Most of these solutions require per-application configuration

- WPA2 Has Been Broken. What Now?

Acknowledgement

- Part of the content in this document is adopted from the recommended textbook:

Michael Goodrich, Roberto Tamassia, “Introduction to Computer Security”, 1st Edition. Pearson. ISBN-13: 978-0321512949, ISBN-10: 9780321512949