CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

WiFi Authentication and Encryption

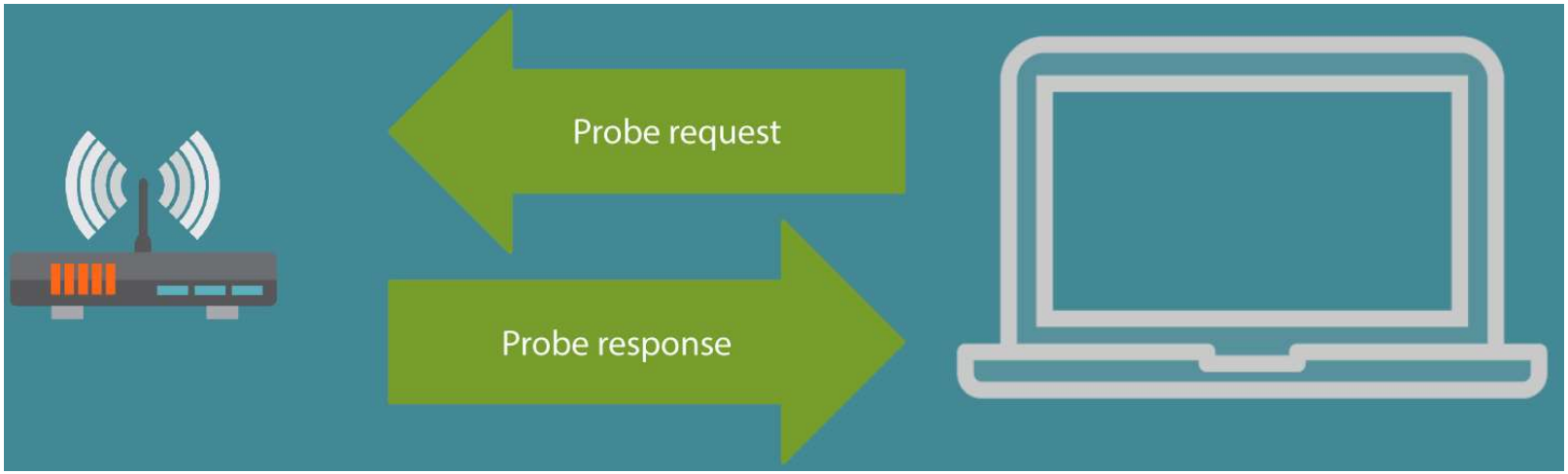
Video summary

- WiFi Authentication Modes
- WiFi Encryption
- WEP, WPA, and WPA2
- Procedures to Improve Wireless Security

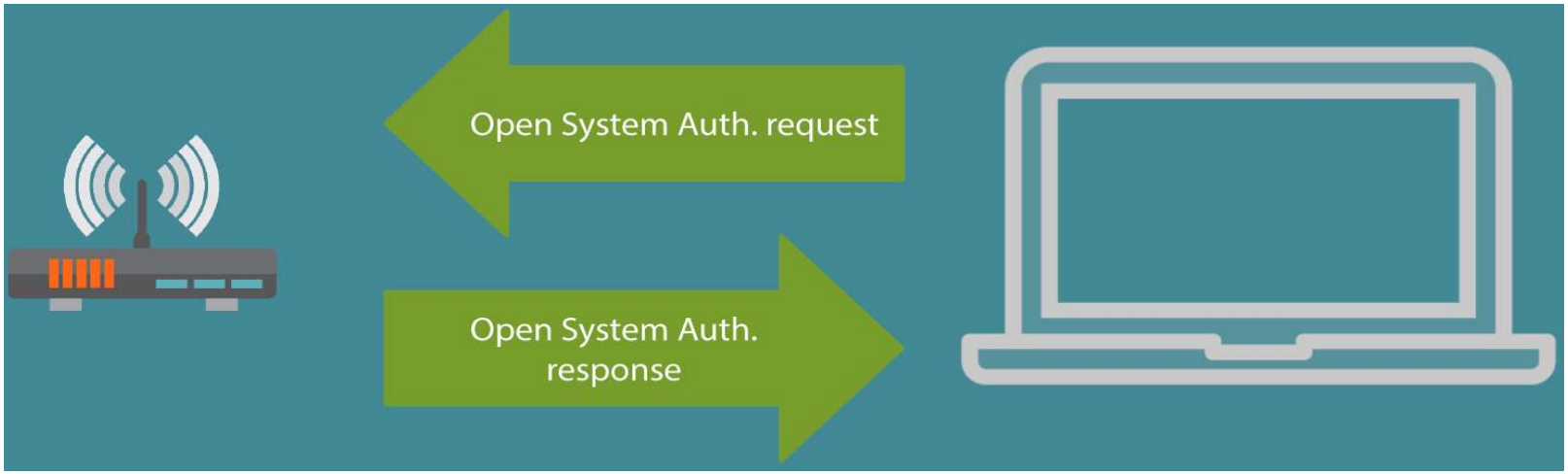
WiFi Authentication

- Open System Authentication
- Shared Key Authentication
- IEEE 802.1X

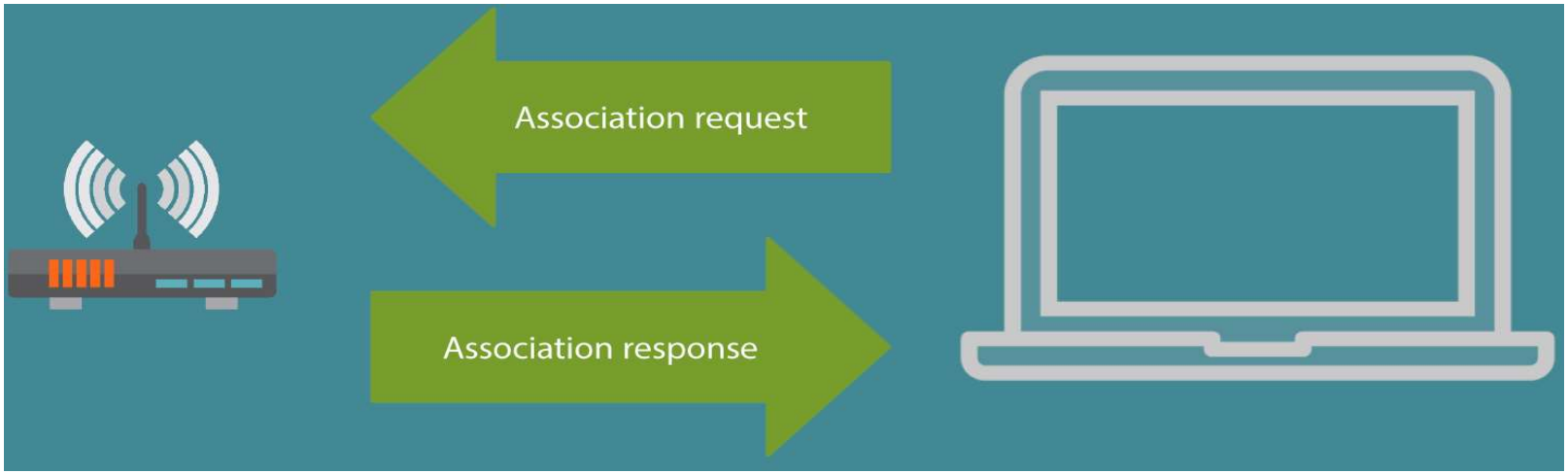
Open System Authentication



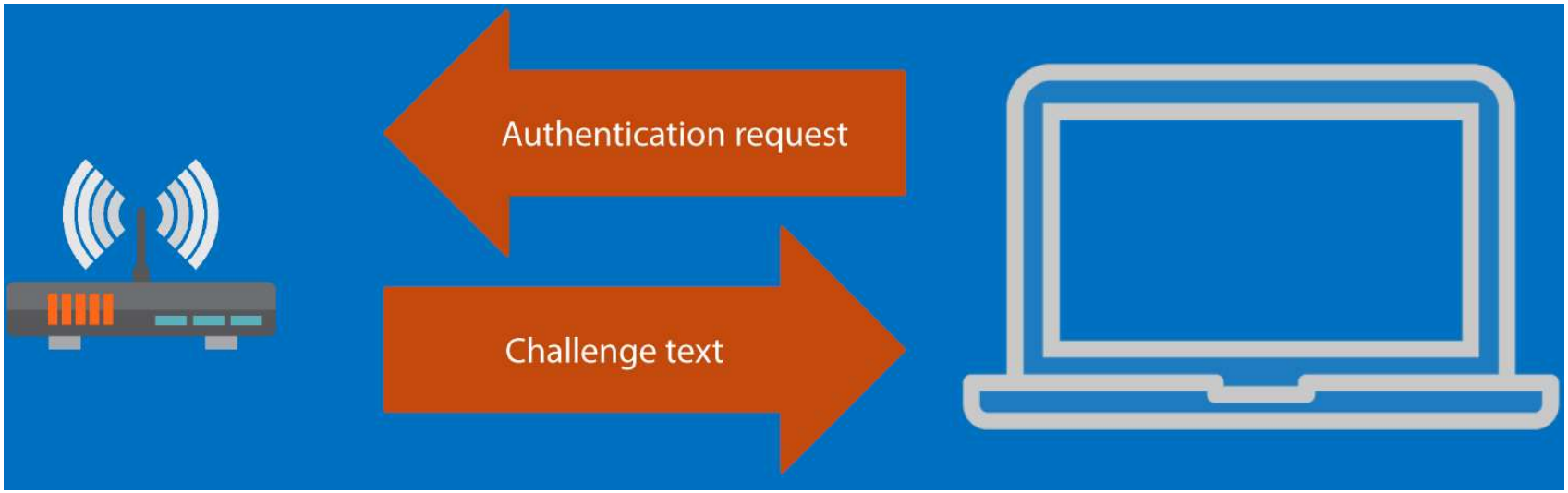
Open System Authentication



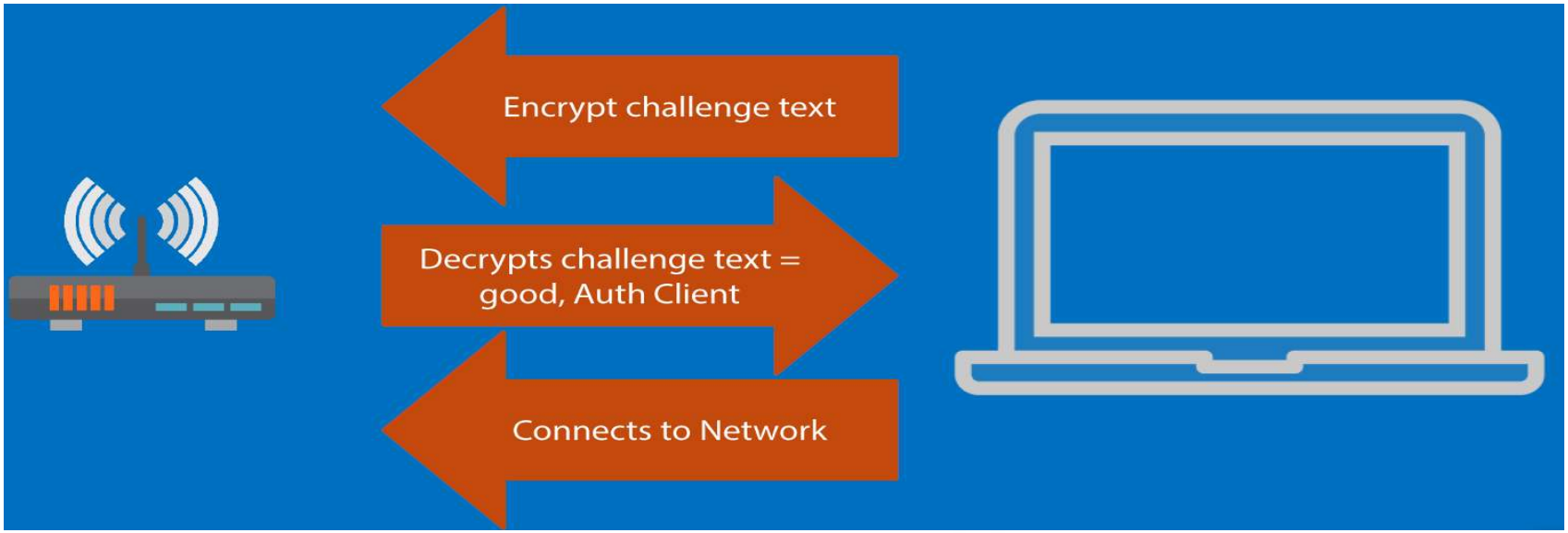
Open System Authentication



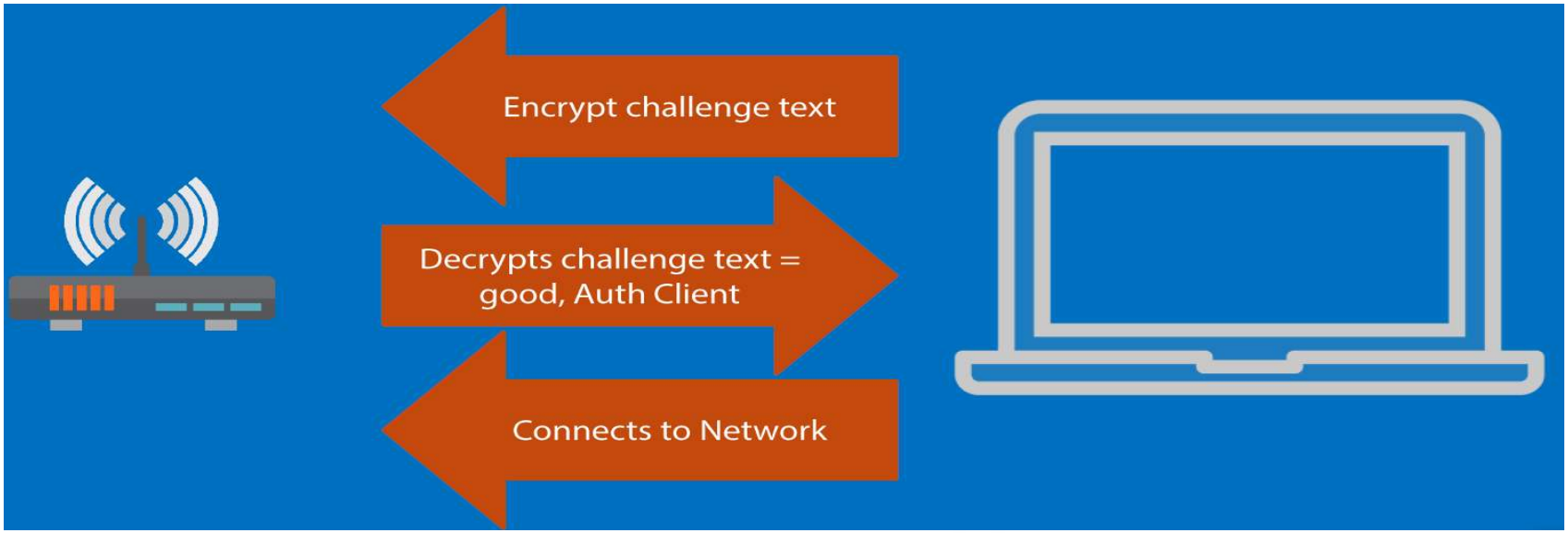
Shared Key Authentication



Shared Key Authentication



Shared Key Authentication



WiFi Encryption

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)

Wired Equivalency Protocol (WEP)

- The original native security mechanism for WLAN
  - Uses an RC4 stream cipher.
    - Pseudo-random bytes.
  - Two versions: 64-bit and 128-bit versions.

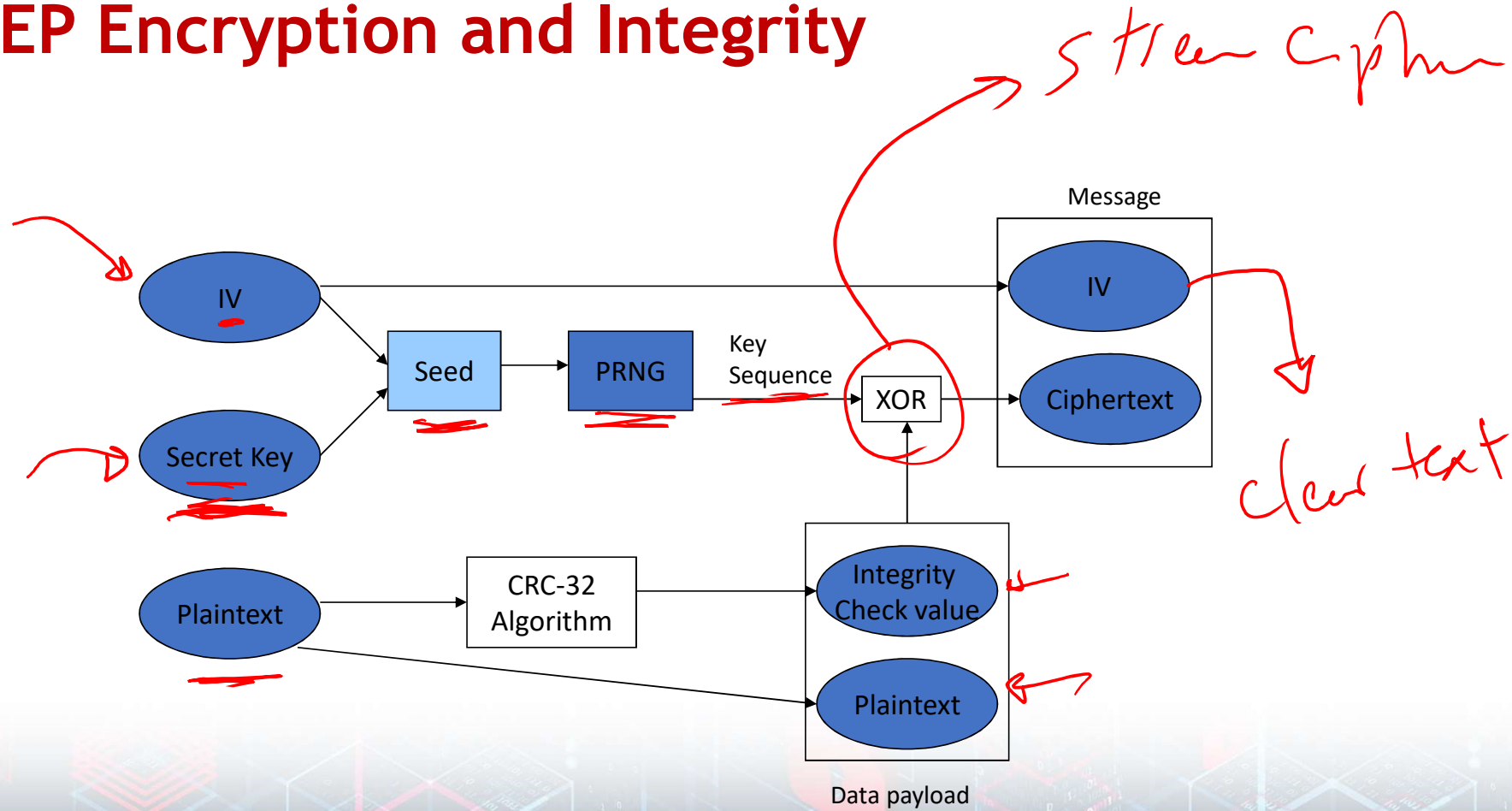
Block
stream

- Used to protect wireless communication from eavesdropping (confidentiality)

- Prevent unauthorized access to a wireless network (access control)

- Uses static encryption keys.
  - Easy to crack (short IV and static key)

WEP Encryption and Integrity



PRNG – RC4 Pseudorandom number generation algorithm

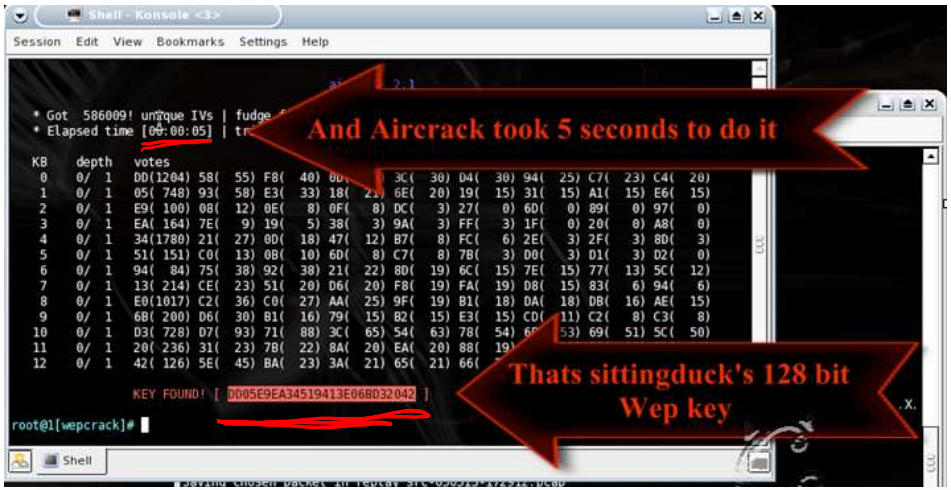
WEP Flaws and Vulnerabilities

- Weak keys:
  - ✓ It allows an attacker to discover the default key being used by the Access Point and client stations
  - ✓ This enables an attacker to decrypt all messages being sent over the encrypted channel.

- IV (initialization vector) reuse and small size:
  - ✓ There are 2^{24} different IVs
  - ✓ On a busy network, the IV will surely be reused, if the default key has not been changed and the original message can be retrieved relatively easily.

Attacks on WEP

- WEP encrypted networks can be cracked in seconds
- Goal is to collect enough IVs to be able to crack the key



Wi-Fi Protected Access (WPA)

- This is a new standard from the Wi-Fi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet.
  - Firmware update to replace WEP.
  - 128-bit Temporal Key Integrity Protocol (TKIP) encryption.
    - Uses a master key that is regularly changed.
  - Improved data encryption (48 bit IV)
  - Strong user authentication

WEP vs. WPA

	WEP	WPA
Encryption	Flawed	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static-same keys used by everyone on network	Dynamic session keys. Per-user, per-session, per-packet keys
	Manual distribution	Automatic Distribution
Authentication	Flawed, uses WEP key itself	Strong user authentication using 802.1X and EAP

Wi-Fi Protected Access 2 (WPA2)

- Designed to replace WEP.
  - 128-bit Advanced Encryption Standard (AES).
- The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- Based on the IEEE 802.11i standard.
- Uses PSK (256 bit key) and 8-63 ASCII Characters

WPA2

- WPA2 has immunity against many types of hacker attacks
  - ✓Man-in-the middle
  - ✓Authentication forging
  - ✓Replay
  - ✓Key collision
  - ✓Weak keys
  - ✓Packet forging
  - ✓Dictionary attacks

WEP vs WPA vs WPA2

	WEP	WPA	WPA2
ENCRYPTION	RC4	RC4	AES
KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys
KEY DISTRIBUTION	Manually typed into each device	Automatic distribution available	Automatic distribution available
AUTHENTICATION	Uses WEP key as Authentication	Can use 802.1x & EAP	Can use 802.1x & EAP

Procedures to Improve Wireless Security

- Use wireless intrusion prevention system (WIPS)
- Use WPA2 where possible
- Use a good + long passphrase
- AES is more secure, use TKIP for better performance
- Change your SSID every so often
- Wireless network users should use or upgrade their network to the latest security standard released

Video summary

- WiFi Authentication Modes
- WiFi Encryption
- WEP, WPA, and WPA2
- Procedures to Improve Wireless Security