ECE590
Computer and Information Security

Fall 2018

Wireless and Mobile Security

Tyler Bletsch

Duke University

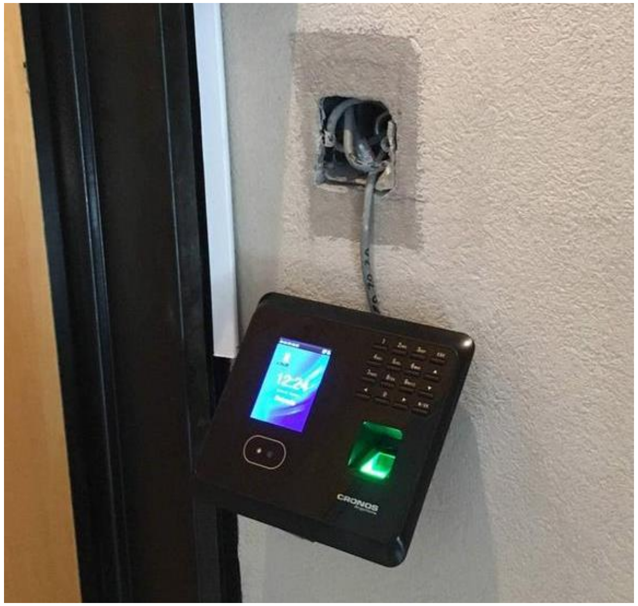
Adapted from “Chapter 24: Wireless Network Security” by Dr. Hossein Saiedian at Univ. Kansas, which in turn was adapted from Chapter 24 of our textbook

Wireless Security

Wireless Security Overview

It’s like regular security, but the communications medium is more accessible.

Like if your wired network was like this:



Wireless Network Modes

- WiFi is specified in IEEE 802.11 with various lettered suffixes
- 802.11 wireless networks operate in two basic modes:
  - **Infrastructure mode**
    - Each wireless client connects directly to a central device called Access Point (AP)
    - No direct connection between wireless clients
    - AP acts as a wireless hub that performs the connections and handles them between wireless clients
  - **Ad-hoc mode**
    - Each wireless client connects directly with each other
    - No central device managing the connections
    - Rapid deployment of a temporary network where no infrastructure exists
    - Being deprecated by OS vendors (Windows 10 doesn’t support it 😢)

Wireless Networking Components

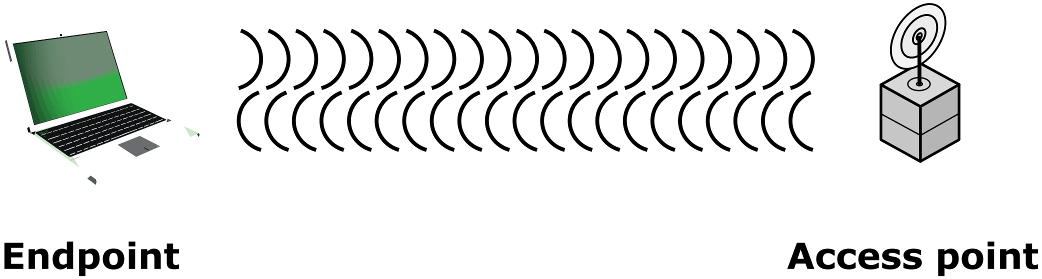


Figure 24.1 Wireless Networking Components

Wireless client: WIFI-enabled laptop/tablet, cell phone, Bluetooth device, …
Access point: Cell towers, WIFI hotspots, wireless routers
Transmission medium: carries signals

For WiFi, APs are identified by SSID:

- A client must set the same SSID as the one in that particular AP to join the network
- Without SSID, the client won't be able to select and join a wireless network

Wireless Network Threats

- Inappropriate association (either accidental or malicious)
- Identity theft (MAC spoofing)
- Man-in-the middle attacks
- Denial of service (DoS)
- Network injection
  - Bogus reconfiguration commands to routers/switches that degrade performance
- Unique attacks on non-traditional networks
  - Bluetooth, proprietary wireless

Proposed advice on securing wireless networks (some good, some okay, some bad)

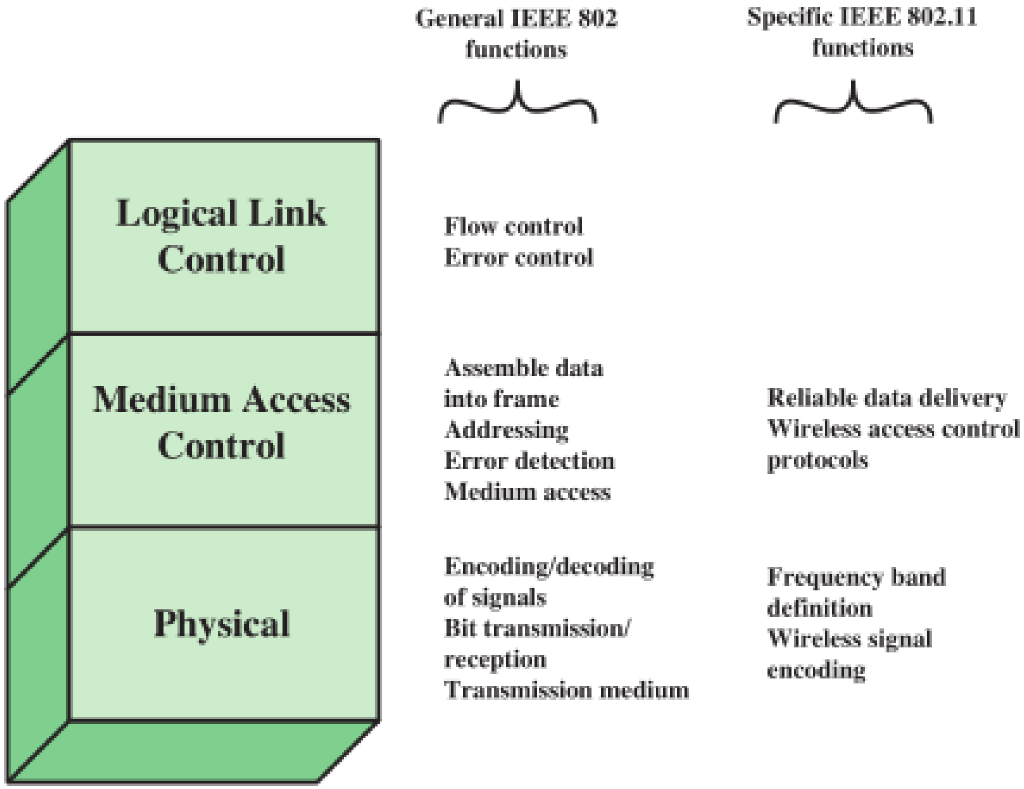
- Use encryption
  - Yes, especially strong modern algorithms (WPA2)
- Change router's preset password
  - Yes. Not having a publically known key usually helps with encryption...
- Use and enable anti-virus, anti-spyware, firewall
  - True, but unrelated to wireless.
- Change default identifier on router
  - Good idea so you know what's-what, but does nothing for security.
- Reduce signal strength
  - Place away from windows and external walls, use directional antennas
  - Problem: attackers can boost power, get directional antennas, etc...
- Turn off SSID broadcasting
  - Waste of time.
- Apply MAC-filtering
  - Almost entirely useless due to MAC spoofing.

IEEE 802.11 Wireless LAN

- IEEE 802: a committee responsible for LANs
- IEEE 802.11: responsible for developing wireless protocols
  - Key standards:
    - 802.11b: Uses 2.4GHz spectrum, up to 11Mbps
    - 802.11g: Uses 2.4GHz spectrum, up to 54Mbps
    - 802.11n: Uses 2.4 and 5GHz spectrum, up to 288Mbps or 600Mbps
    - 802.11ac: Uses 5GHz spectrium, up to ~3Gbps
      - A variant can use the frequencies formerly used in analog TV
    - 802.11ax: Uses 2.4GHz and 5GHz spectrum, up to 10Gbps
      - *Upcoming* – not commonly deployed yet!

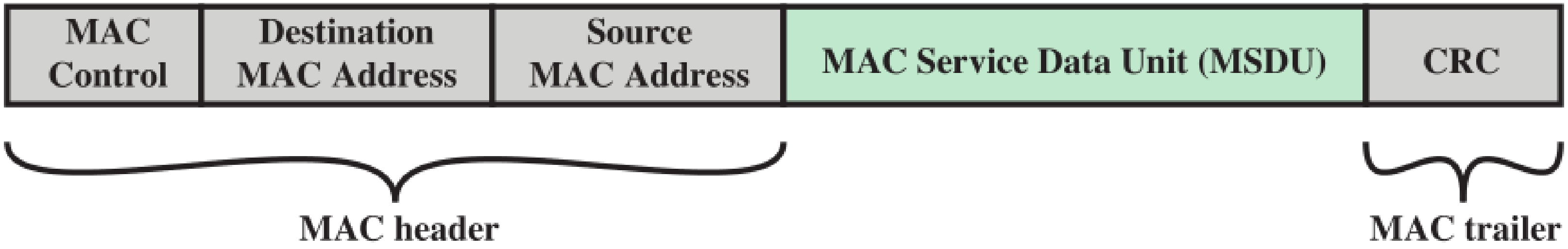
IEEE 802.11 Protocol Stack

- **Physical layer** (encode/decode signals)
- **MAC layer**: assembles MAC frame, disassembles frames and performs address recognition
- **LLC**: keeps track of frame transmission



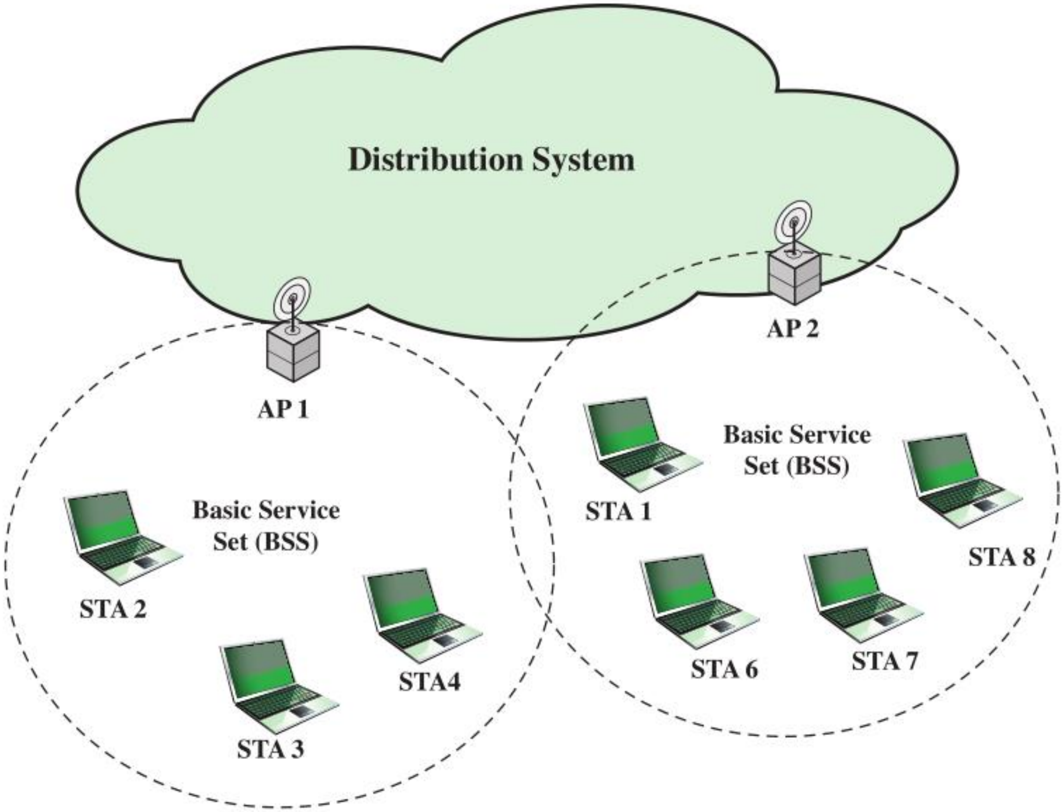
A MAC Frame (MPUD)

- MAC protocol data unit (MPUD)

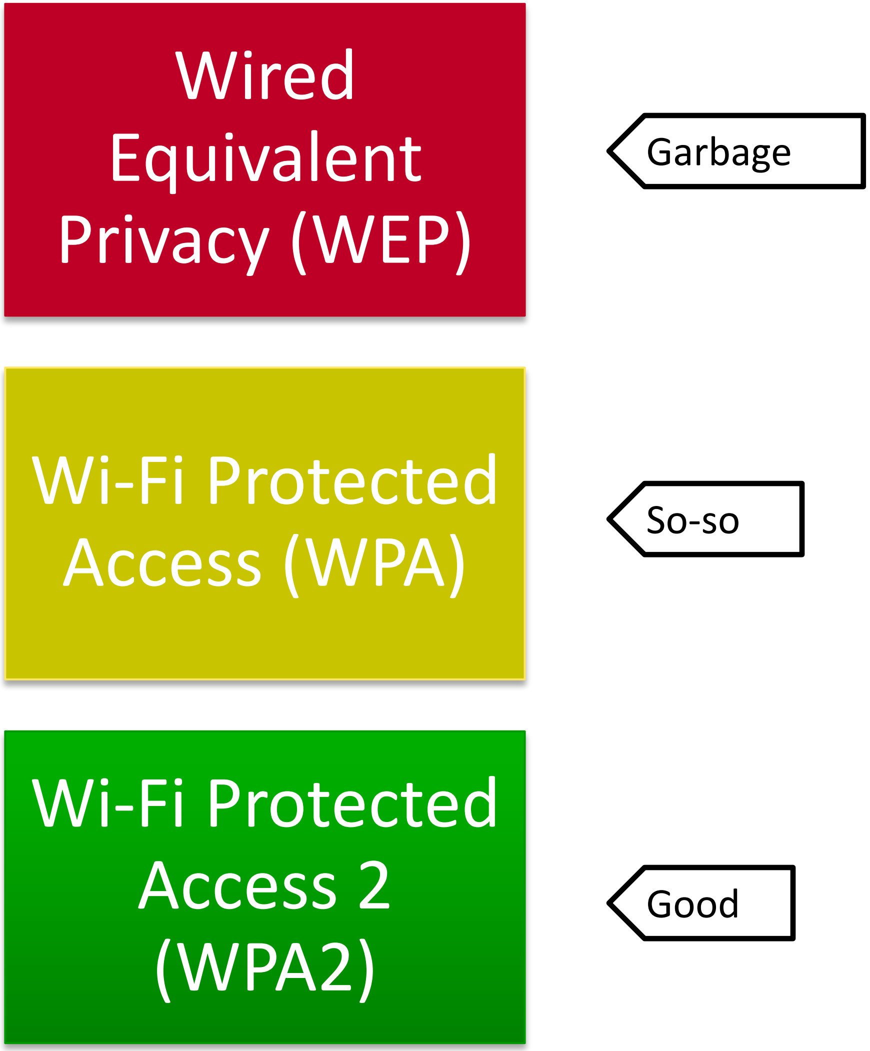


IEEE 802.11 Extended Service Set

- **BSS**: the smallest building block
- BSSs connected via **A**
  - Aps functions as bridg
- **ESS**: two or more BSS



IEEE 802.11# Wireless Security



Wired Equivalent Privacy (WEP)

Garbage

Wi-Fi Protected Access (WPA)

So-so

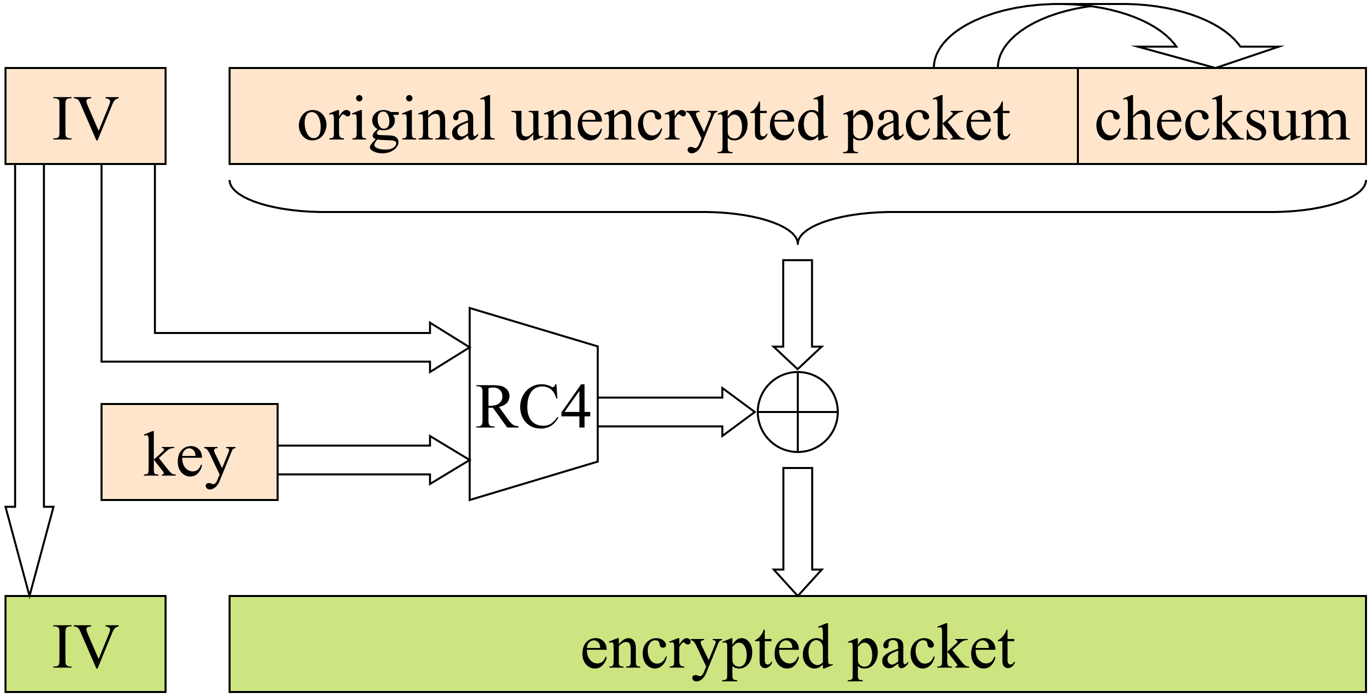
Wi-Fi Protected Access 2 (WPA2)

Good

WEP - Wired Equivalent Privacy

- The original native security mechanism for WLAN
- provide security through a 802.11 network
- Used to protect wireless communication from eavesdropping (confidentiality)
- Prevent unauthorized access to a wireless network (access control)
- Prevent tampering with transmitted messages
- Provide users with the equivalent level of privacy inbuilt in wireless networks.

How WEP works

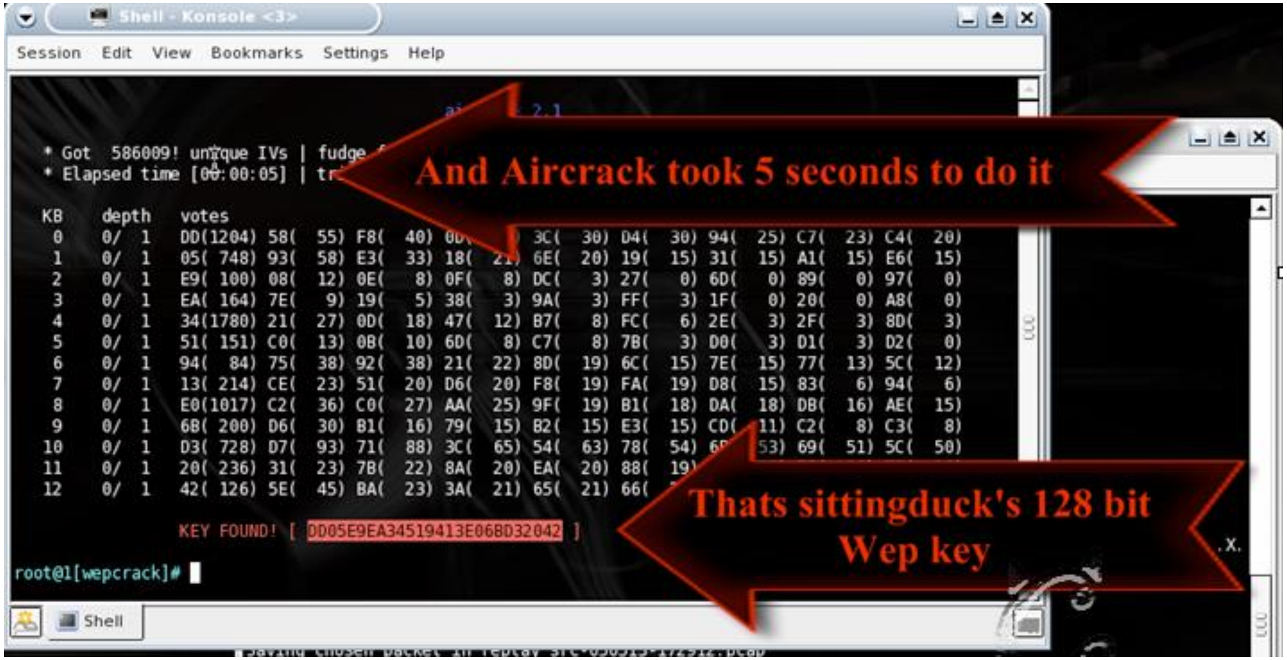


WEP Flaws and Vulnerabilities

- 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 224 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 10 minutes
- Goal is to collect enough IVs to be able to crack the key
- IV = Initialization Vector, plaintext appended to the key to avoid Repetition
- Injecting packets generates IVs



```
 * Got  586009! unique IVs | fudge f
 * Elapsed time [00:00:05] | tr

 KB    depth   votes
  0    0/  1   DD(1204) 58(  55) F8(  40) 0D(        3C(  30) D4(  30) 94(  25) C7(  23) C4(  20)
  1    0/  1   05( 748) 93(  58) E3(  33) 18(  21) 6E(  20) 19(  15) 31(  15) A1(  15) E6(  15)
  2    0/  1   E9( 100) 08(  12) 0E(   8) 0F(   8) DC(   3) 27(   0) 6D(   0) 89(   0) 97(   0)
  3    0/  1   EA( 164) 7E(   9) 19(   5) 38(   3) 9A(   3) FF(   3) 1F(   0) 20(   0) A8(   0)
  4    0/  1   34(1780) 21(  27) 0D(  18) 47(  12) B7(   8) FC(   6) 2E(   3) 2F(   3) 8D(   3)
  5    0/  1   51( 151) C0(  13) 0B(  10) 6D(   8) C7(   8) 7B(   3) D0(   3) D1(   3) D2(   0)
  6    0/  1   94(  84) 75(  38) 92(  38) 21(  22) 8D(  19) 6C(  15) 7E(  15) 77(  13) 5C(  12)
  7    0/  1   13( 214) CE(  23) 51(  20) D6(  20) F8(  19) FA(  19) D8(  15) 83(   6) 94(   6)
  8    0/  1   E0(1017) C2(  36) C0(  27) AA(  25) 9F(  19) B1(  18) DA(  18) DB(  16) AE(  15)
  9    0/  1   6B( 200) D6(  30) B1(  16) 79(  15) B2(  15) E3(  15) CD(  11) C2(   8) C3(   8)
 10    0/  1   D3( 728) D7(  93) 71(  88) 3C(  65) 54(  63) 78(  54) 6    53) 69(  51) 5C(  50)
 11    0/  1   20( 236) 31(  23) 7B(  22) 8A(  20) EA(  20) 88(  19
 12    0/  1   42( 126) 5E(  45) BA(  23) 3A(  21) 65(  21) 66(

                   KEY FOUND! [ DD05E9EA34519413E06BD32042 ]

root@1[wepcrack]#
```

And Aircrack took 5 seconds to do it

Thats sittingduck's 128 bit Wep key

WPA - WI-FI Protected Access

- New technique in 2002
- Replacement of security flaws of WEP
- Improved data encryption
- Strong user authentication
- Because of many attacks related to static key, WPA minimize shared secret key in accordance with the frame transmission
- Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data.

WPA2 - WI-FI Protected Access 2

- Based on the IEEE 802.i standard
- The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- The encryption in WPA2 is done by utilizing either AES or TKIP
- Two modes:
  - **Personal mode** uses a PSK (Pre-shared key) & does not require a separate authentication of users
  - **Enterprise mode** requires the users to be separately authenticated by using the EAP protocol

- *DukeBlue is WPA2-EAP!*

WPA2

- WPA2 has immunity against many types of 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

- Enable **WPA2-PSK** (personal) or **WPA2-EAP** (enterprise)
  - AES is more secure, use TKIP for better performance
- Use a good passphrase
- Upgrade network to the latest security standard released

- “Change your SSID every so often”
  - ^ This was in the original slides and is totally nuts.

Wireless Network Tools

- MAC Spoofing
  - http://aspoof.sourceforge.net/
  - http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp
  - http://www.klcconsulting.net/smac/
- WEP Cracking tools
  - http://www.backtrack-linux.org/
  - http://www.remote-exploit.org/articles/backtrack/index.html
  - http://wepattack.sourceforge.net/
  - http://wepcrack.sourceforge.net/
- Wireless Analysers
  - http://www.kismetwireless.net/
  - http://www.netstumbler.com/

Mobile Security

Two ways to think about mobile security

- Security *against* mobile devices: mindset of the sysadmin
  - Our focus

- Security *for* mobile devices: mindset of vendors...sometimes?
  - We'll leave this aside unless we have extra time.
  - Short version:
    - Encryption
    - Per-app permissions and isolation
    - Sandboxing

Mobile Device Security Challenges

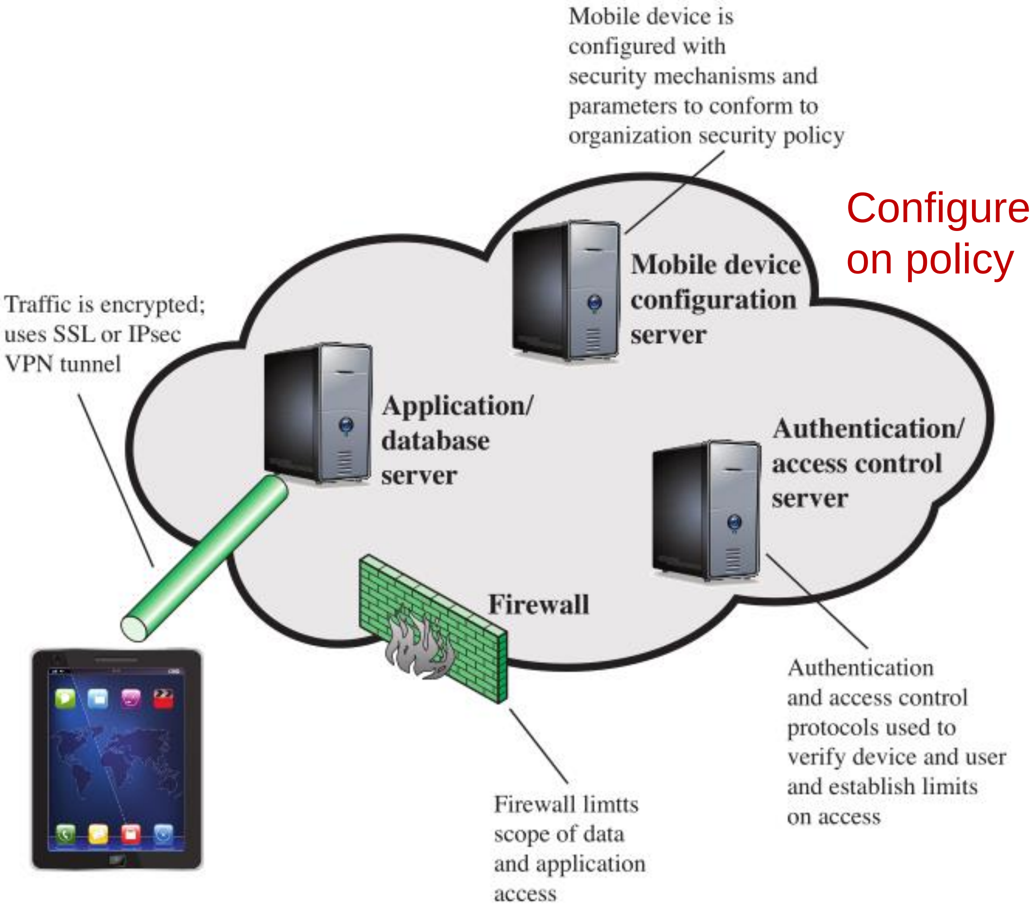
- Trends:
  - Bring Your Own Device (BYOD)
    - No more tight control over computing devices
  - De-perimeterization: static network perimeter is gone
    - Mobile network allows Internet gateways you don’t control
  - External business requirements (guests, third-party contractors, …) keep the above true
- Resulting threats:
  - Lack of physical security control
  - Use of untrusted mobile devices
  - Use of untrusted networks
  - Use of apps created by unknown parties
  - Interaction with other systems (e.g., cloud-based data sync)
  - Use of untrusted content

Mobile Device Security

- User training
- Mobile device configuration:
  - Enable auto-lock
  - Enable password/PIN/thumbprint protection
  - Disable/discourage auto-completion for passwords
  - Enable remote wipe
  - Up-to-date OS/software
  - Encrypt sensitive data
  - Prohibit installation of third-party apps
  - Most of the above can be enforced by policy via e.g. Microsoft Exchange
- Network/service configuration:
  - User devices disallowed on trusted networks
  - User devices must be registered (tied to human) to get on a network (e.g. Dukeblue)
  - Remote access via VPN only
  - Configure/enable SSL to prevent MITM attacks on infected endpoints

Mobile Device Security Elements

Encrypt



Mobile device is configured with security mechanisms and parameters to conform to organization security policy

Traffic is encrypted; uses SSL or IPsec VPN tunnel

Mobile device configuration server
Application/ database server
Authentication/ access control server
Firewall

Authentication and access control protocols used to verify device and user and establish limits on access

Firewall limtts scope of data and application access

Configure based on policy

Authenticate/ access control