* 03/15/18
* 4 Top mobile security concerns
  + Physical security
    - Unattended device
    - Multiple layers
  + Application
    - Too many privileges
  + Data leakage
    - ~hacking~
  + Malware
    - Trojans
    - Worms
    - RATs
    - Bots
    - Spyware
    - Adware
    - Ransomware
* Evolution of Data Networks
  + First data communication
    - Morse Code
    - 1844
  + Telegraphy << Telephony (advent of public switched telephone network (PSTN)) << early data network << modem << circuit switching << packet switching
    - Alexander Grand Bell
  + IBM accomplished first successful interface between digital devices over analog PSTN
    - 300 bits per second
  + Network Effect
    - A single device becomes more useful as new devices enter the network
  + First fax sent in 1962 over standard PSTN
    - Modulation of data into sound by modems (modulator/demodulator)
      * Modem convert digital data into an analog signal for transport
  + Digital over analog
    - More efficient use of bandwidth
    - Greater utilization
    - Improved error rates
    - Less susceptibility to noise/interference
    - Increased throughput
    - Support of additional services
  + Packet switching vs circuit switching
    - Circuit: needs personal physical connection to connect
    - Packet: each packet holds the source and destination along with the data
      * Digitized voice before wrapping in a packet
      * More efficient
      * More resilient
        + Multiple paths
      * Lost/dropped packets don't degrade too much due to size
        + Need many lost before noticeable
* Internet Revolution
  + TCP/IP - Transmission control protocol/internet protocol
    - Developed form the ARPANET project, predecessor to modern internet
    - Prompted creation of ISDN (Integrated Services for digital network)
      * Supported simultaneous voice, video, data
    - By 1980 PCs were becoming prevalent so LAN allowed them to connect to a mainframe
* 03/12/18
* Mobile phones and creation of new network
  + First analog mobile phone system was developed in the 1980s,
    - Known as Advanced mobile phone system (AMPS). 1st gen wireless network (1G) - 2.4 kbps
    - Successful, but major vulnerabilities
      * Unencrypted
      * Vulnerable to eavesdropping
  + 2nd Generation (2G) - 64 kbps
    - Digital instead of analog
    - 2 versions
      * US: Code Division Multiple Access (CDMA)
      * Europe: Global System for Mobile (GSM)
    - Encrypted
  + As technology advanced
    - Phone size shrank
    - Electronics and batteries improved (Moore’s Law)
    - Denser cells (coverage areas)
    - More cell towers
      * Less battery power
  + Introduction to Short Message Service (SMS) in late 90s
    - Initially designed for network engineers to communicate over a back channel
    - 120 characters format
* Wireless Local Area Networks (WLAN) became modern data network
  + Highlighted wireless mobility
  + WLAN and WiFi often used interchangeably
  + A WiFi device is a device based on IEEE 802.11 standard
    - IEEE 802 standard pertains to LAN
    - .11 is standards for WLAN
* Computers go Mobile
  + Outside of workplace mobile communication was becoming commonplace
    - Affordable, easy-to-configure WLAN routers conditioned users to expect wireless connectivity
      * Hotspots in must public places
      * WLAN access points and routers to connect multiple devices
        + Issues of security rouge routers to ethernet are unsecured
        + Convenience vs necessity
* Convergence of mobile and data networks
  + Expansions on CDMA and GSM standards to allow low-bandwidth voice-over-circuit switched paths
  + Allowed data transfers
  + Barely sufficient for access to low-resolution web pages using wireless access protocol (WAP) sites
  + Advancements in for of General Packet Radio Service (GPRS) or 2G+
    - Packet-based data service for mobile networks
  + This led to the development of 3G mobile IP broadband - 2000 kbps
    - Ability of mobile networks to handle high-speed packet-switched internet access
    - New “Smartphones” were able to maximize 3G capability
    - Laptops became mobile thanks to use of 3G subscriber identification modules (SIMs)
      * Made lightweight notebooks specifically for internet access over 3G
  + After 3G came Long Term Evolution(LTE) and 4G - 100,000 kbps
    - Current version
    - Offers all-IP mobile network
    - Ushered in WiMAX (Worldwide interoperability for Microwave Access) and satellite
* IP Movility
  + The goal is to provide the ability to roam while maintaining network access anywhere on the premise and on any WLAN enabled device
    - Seamless transfer of an IP address from one network to another without losing IP sessions
* Basic Tenets of Network Security
  + Core principles of network and data security is the C-I-A triad
    - Confidentiality - Maintaining privacy of information so only those who are authorized to access information are able to do so
      * Achieved through encryption and cryptography
        + HTTPS - hypertext tansfer prtocol secure

Encrypts data between secure browsers and secure websites

* + - * + SSL - Secure Sockets Layer

Uses 128 bit encryption between a safe HTTPS website and safe browser

* + - Integrity - Ensure accuracy of data
      * Ensuring data remains unchanged
      * Includes techniques like hashing algorithms to verify data integrity
        + If message-digest is same before and after transmission then data hasn’t been tampered with
    - Availability - Data is available to only authorized viewers
      * Related to services, like email, that will be available when required
      * Provided through security measures such as firewalls or high-availability network designs for redundancy and fault tolerance
        + Attacks on availability would be DoS (Denial of Service) and brute-force password hack attempts
* Cybercrime refers to a wide range of illegal activities performed on a network
  + First hackers emerged in 1960s
    - Researched the PSTN telephone network by re-engineering the audible signals used by systems to switch calls
    - Would re-create the exact tone and send through handset, which gave them free access to the international exchange
  + Cybercrime legally recognized as a federal criminal offense in 1986
    - US Govt formed Computer Emergency Readiness Team (CERT) to counter cybercrime
* 03/14/18
* Networking and the Open System Interconnection Reference Model (OSI)
  + Defines 7 layers
  + Standards for physical wire all the way up to the application interfaces on computers
  + Each layer has specific function
  + Can only communicate with layer above and below current
    - Use headers to communicate inter-stack
* The 7 layers - APSTNDP
  + Layer 1 - Physical
    - Signal path over which data is transmitted
    - Wires, radio signals
    - Units at this layer are bytes and bits
      * Specifications
        + Transmission - bit-by-bit procedures
        + Electrical - signal level, amplification, attenuation
        + Mechanical - specifications for cable (type, length) connectors
        + Procedural - modulation schemes, synchronization, signaling, and multiplexing
        + Wireless transmission - frequencies, signal strength, and bandwidth
        + Throughput - bit rates
        + Topologies - bus, ring, mesh, point-to-point, point-to-multipoint
  + Layer 2 - Data Link
    - Helps establish communication path by specifying the media access control(MAC) address of each device
    - Viewed as “switching” layer - where switching paths are determined in LANs
    - Ethernet is the dominant protocol, especially for data centers and large area networks
    - Unit of information is the data frame
  + Layer 3 - Network Layer
    - Routing or IP layer
    - Handles communication paths between LANs
    - IP exists at this layer
    - Unit of information is the packet
  + Layer 4 - Transport layer
    - Bridge between network and the application processing software
    - Data from applications is broken down into packets
    - Packets are suitable for transport and then reassembled on receiving device
  + Layer 5 - Session Layer
    - Define and manages communication between applications on separate devices
  + Layer 6 - Presentation Layer
    - Formats information sent to and from the applications
  + Layer 7 - Application Layer
    - Top of the stack; connects software applications to the network
* Communicating over a network
  + Important to understand aspects that may impact wireless security
    - 2 main keys to communication
      * Conditioning the data for transport
        + Performed on “application layers”(5-7)
        + Dont care
      * Ensuring the data reaches the correct destination
        + Performed on layers 3 and 4

Primarily through TCP/IP

* + Communication on network layer is achieved through a logical addressing scheme that enables routers to move packets across the network to the correct destination
    - Scheme is called IP addressing
      * Allows data communication between LANs via routed WANs
      * Enables network to correctly route packets across a network
    - IPv4
      * 32 bit address
      * Four octets
      * First octets defines network segment; remaining octets define the hosts on the network
      * Each octet from 0 to 255
    - IPv6
      * 128 bit address
      * Eight fields of four-digit hex numbers
        + Leading zeroes are stripped for shorthand
      * Advantages over IPv4
        + Auto-configuration
        + Improved address management
        + Built-in security/encryption capability
        + Optimized routing
      * Most machines still use IPv4 due to massive upgrade costs
  + Security of wireless networks primarily revolve around securing the most common wireless network technology: WiFi
* What is WiFi
  + Wireless network technology providing high-speed internet and network connections
    - Can refer to any wireless local area network(WLAN) product based on 802.11 standards
    - Devices can connect to an access point or directly to each other
      * Ad hoc network
      * AP usually allow connection to a wired network
  + Difference between wireless router and an AP
    - AP does not have a firewall
  + Difference between AP and hotspot
    - Hotspot is the physical space where wireless service is provided
  + What does WiFi stand for
    - Some say Wireless Fidelity
    - Actually trademarked phrase that means IEEE 802.11x
      * Originally used for only 2.4 GHz 802.11b standard
      * Now other standards are used, but still referred to as WiFi
  + How does it work
    - Broadcast wireless signal via Radio Frequency(RF)
      * Typically 2.4GHz, but 5GHz is newer standard
      * Wireless router provides access to internet or computer network
  + Different Standards:
    - 802.11b
      * First widely used tech
    - 802.11g
      * 2003
      * Developed greater performance
      * Higher bandwidth (54Mbps)
      * Backwards compatible with b
    - 802.11n
      * Improved performance by utilizing multiple wireless signals and antennae (MIMO)
      * 300 Mbps bandwidth
      * Backwards compatible with both b/g
    - 802.11ac
      * Dual band wireless tech, supports connections on both 2.4 and 5GHz bands
      * Up to 450 Mbps on 2.4GHz
  + Dynamic rate scaling allows WiFi to maintain a reliable connection over longer distances by transferring data slower, thus avoiding flooding the wireless connections with data and subsequent retry requests
    - WiFI protocols additionally test the quality of the signal between two devices and adjust the connection’s data rate down if needed to increase reliability
  + Security methods of a wireless network
    - Data encryption (WEP, WPA, WPA2)
    - User authentication
    - Control systems that protect the devices that connect to the network
    - Firewall
      * Controls incoming and outgoing network traffic based on predetermined security rules
    - Limit broadcast range of wireless network
  + IEEE set out to develop a security standard as part of 802.11
    - Goal was for WLAN to be considered as secure as their wired equivalent
      * Allow confidentiality, integrity, and availability
      * Beginning iterations(WEP,WAP) proved to be very flawed
* Economic impact of wireless network
  + Health care - use RFID and other wireless tech
    - Information portals
    - Tagging inventory to reduce loss
    - Monitoring patient outside of hospital
    - Mobility within hopital
* Warehousing and logistics
  + Asset tracking
  + Picking efficiency
  + Loss control
* Retail
  + Inventory counts
  + Customer satisfaction
* IoT
* 03/16/18
* What to protect
* Information Security
  + Processes and practices that must be implemented to secure the digital assets you wish to protect from various threats
* Security Plans
  + Security plans involve the following
    - What are you trying to protect?
      * Corporate data, intellectual property, customer data, or financial assets
    - Why are you trying to protect
      * Protection mandated by a government or industry agency, or is it internal best practice
    - What is the value of the asset
      * Have the assets been quantified
      * Has the cost of the breach been estimated
    - What are you protecting it from?
      * Threats internal or external
      * Data theft, device control, or system access
      * Environmental or human in origin
    - What constraints prevent you from protecting the asset
      * Is broad access required
      * Does the data change or move around
* Security must be cost effective
  + Should spend enough to meet the risk-reduction and no more
* Securing network is complex
  + Requires standards and best practices that fit need
* General threat categories
  + Confidentiality - preventing unauthorized disclosure of information
    - Privacy of information - protecting data from being seen
    - Secrecy of information - hiding knowledge of data’s existence or whereabouts
  + Integrity - preventing unauthorized modification of information
    - Using hashes can mitigate man-in-the-middle attacks
  + Availability - preventing unauthorized withholding or resources or services
    - A measure of reliability
    - Preventing DoS attacks
      * Attackers launch DoS attacks through synchronization (SYN) flooding of TCP/IP to disrupt the 3 way handshake
        + SYN, SYN-ACK, ACK
  + Accountability - make users accountable for their actions
    - Must be mechanisms in place for authorized internal users
    - Key point is authentication
      * login/password
      * Keycard
      * Biometrics
  + Nonrepudiation - preventing the denial that an action has been taken
    - Addresses when someone denies they took a certain action
      * Undeniable evidence that an action was taken, and by whom
        + Application might be a digital signature upon delivery
* Threats to wireless and mobile devices
  + 3 categories
    - Data theft
    - Device control
    - System access
  + Wireless networks are vulnerable due to many entry points
    - Attacker only needs 1 way in vs defender who has to account for all entry points
    - Attackers will try to gain access to a wireless network for many reasons
      * Main reason to steal, snoop, or alter data coming across the network
      * Typically try to hide identity, will often use TOR and other tools
* Data Theft
  + Typical data theft revolves around targeting personally identifiable information
    - Information that can ID, contact, or locate a single person
    - ID an individual in context
  + Areas of interest include:
    - Credentials for personal or business accounts
    - Credentials for personal or business information
    - Credentials for remote access software for business networks
    - Access to data and phone services
  + Attacks include
    - Sniffing/snooping
      * Intercepting data during transmission
      * How: man-in-the-middle
      * Fix: Encryption
    - Malware
      * Any malicious software
      * How:
        + Virus,worms,trojans, botnets, rootkits, …
      * Fix
        + Anti-malware software, intrusion detection Systems (IDS)
    - Browser exploits
      * Take advantage of vulnerabilities of mobile web browsers
      * Change settings, internet options, and changing URL prefixes
      * Fix:
        + Update browsers, firewall, safe sites
    - Wireless phishing
      * Fake emails or SMS to get victim to link that takes them to a fraudulent website
      * Fix:
        + Don’t be an idiot
    - War driving
      * Searching for WiFi networks by a person in a vehicle using a portable device
      * Can also use special software to view all AP around
    - Social Engineering
    - Lost/Stolen devices
      * While neither are true “attacks”, both can lead to data theft
* Device Control
  + Use a device to launch other attacks
  + Leverage permissions on device to gain access to higher valued targets
    - Can do so by lily padding-hops from one device to next, until target is reached
  + Attacks include
    - Replay attacks
      * Valid data transmission is maliciously repeated or delayed
      * How:
        + Steak ID key from communication between 2 parties, use key to talk to one of them
    - Bluejacking
      * Send unsolicited messages to another device via bluetooth
    - BlueSnarfing
      * Gain access to contacts and data stored on the phone an redirects incoming calls
    - Unauthorized and modified clients
      * User-created vulnerabilities that circumvented policies or device configurations
        + Jailbreaking
        + Rooting
    - Endpoint attacks
      * Attack wireless client directly with tools
        + Metasploit
* System attacks
  + Attacks Include
    - DOS
  + Jamming/interference
    - Disruption of network
    - Can be caused by degradation of service
    - Often due to multiple wireless signals being transmitted across multiple platforms
    - Fix
      * Spectrum analyzer can narrow down what is causing the problem
      * Boost power of existing access points to overpower jamming device
  + Rouge Access point
    - An acces point added to network without one’s knowledge
    - Can create backdoor
    - Fix
      * Network control access to authenticate to network
  + Evil Twin
    - Replicate another AP
    - Scrape data
    - Fix:
      * Don’t connect to bad networks
      * Encrypt your data
  + Initialization vector (IV) attacks
    - Causes modification to the IV
    - Get key from device, decrypt their shit
  + WEP/WPA attacks
    - Exploits vulnerabilities in the protocol
  + Script Kiddies
    - Steal someone else’s exploit and run it without knowing how it works
* 03/19/18
  + Skipped class
* 03/21/18
* Tonight SFS - pay for college and get job
* Midterm only - no final(possibly)
* SKIPPED A FEW DAYS
* 03/26/18
* Soon going to be application, instead of lecture
* Needs assignments
* SKIPPED MORE DAYS
* 04/09/18
* Midterm 18th
* WLAN topologies
  + Components
    - Radio card
      * Called a Station by 802.11 standards
        + Can be any 802.11 device (laptop, smartphone, tablet, …)
      * If device is endpoint, referred to as a Client station
      * Access Point(AP) (Also a station) serves as a central hub
        + May also act as a bridge to connect another AP
    - Antenna
* Wireless client device
  + For radio ability, no difference between smartphone, tablet, laptop…
    - Client station is configured to associate with an AP by creating a layer 2(data link) connection. If mobile, must also have ability to switch to stronger signal when appropriate
    - Every AP is IDd by a Service Set Identifier (SSID)
      * If AP have been configured with same SSID, then client will be handed over to the strongest signal (we call this overlay)
    - To detect an AP, a client does one of two methods
      * Passive scanning
        + Client listens for a beacon, which an AP continually emits
        + When client “hears” a beacon advertising an SSID for which it has been preconfigured, it will select that access point
      * Active scanning
        + Client scans network by sending out probe pulse requests
        + Requests can contain SSID or preconfigured network (Direct Probe) OR it can “discover networks by leaving SSID field blank (Null Probe Request)

Directed probe - all AP configured with configured SSID will respond

Null Probe Request ALL available access points will respond with a probe request

* + - Advantages of active scanning
      * Client can find and connect to AP with best signal
      * Client can build map of available APs with signal strengths
        + Can assist in handover speed and efficiency
      * Client can go off network to check for stronger signals
    - Disadvantages of active scanning
      * Security risk
        + Could fall prey to rogue AP
* 802.11 Service Sets
  + Standards define 4 topologies called service sets for how devices connect with each other
    - Basic Service Set (BSS)
      * Single AP connects with several clients
      * AP is usually connected to distribution network
      * Client stations cannot communicate directly with each other(all communication goes through AP)
      * Typically used in small office/home (SOHO)
      * Size and shape depend on factors:
        + Radio power
        + Antenna gain
        + Surrounding environment
    - Extended service set(ESS)
      * Used in larger networks to connect several AP to ethernet LAN
      * Connection of 2 or more BSS connected
        + Seamless roaming - client can roam from one AP to another without disruption
        + Nomadic roaming - no overlap, client will lose connection until enters area of another AP
        + Collocation model - 100% overlap between 2 AP areas, used to address client capacity issues for many clients
    - Independent Basic Service Set (IBSS)
      * No AP used
        + Client stations form peer-to-peer relationships with other client stations
    - Mesh Basic Service Set(MBSS)
      * Clients, AP, gateways all meshed together, enabling client-to-client and AP-to-AP communication
* 802.11 radio communication is half-duplex - both devices can receive and transmit, but 1 at a time
* Ethernet is Full-duplex - can transmit/receive simultanious
* Client station can operate in 1 of 2 configurable modes
  + Infrastructure Mode - most common WLAN topology. Uses AP as a central connection point and portal to distribution center
    - Enables clients to communicate via BSS or ESS
  + Ad hoc Mode - enables wireless clients to communicate directly
    - IBSS set up in ad hoc mode as a as-needed basis
* Narrowband and spread spectrum
  + Narrowband - uses very little bandwidth by transmitting over narrow beam
    - Uses greater power to transmit over narrow range of frequencies
      * Possibility of interference of 2 narrowband stations in same proximity
  + Spread spectrum - transmission is spread across entire frequency space available
    - Wide band makes it harder to block
    - 10x the size, 1/100 the power
* Multipath
  + Bouncing causes multiple versions of same waves
  + Causes delayed or out of phase signals
* Frequency hopping spread spectrum (FHSS)
  + Continuously change frequency during transmission
    - Length of time on given requency is called dwell time
      * Predetermined
    - Specific pattern
      * Once complete, begins again
    - 802.11 standard limits steps to 1MHz
      * Typically 75-79 hoops per squence
    - Transmitter and receiver must be on same frequency, so need same sequence
    - Issues
      * Can only communicate durring dwell time
        + Shorter dwell time = Lower throughput, greater protection from jamming
    - Rarely used for Wi-Fi, but most BT use
* Direct Sequence Spread Spectrum (DSSS)
  + Uses hopping, but stays on fixed channel, hoping within frequency space in that channel
    - Uses Data encoding
      * Encodes Each bit and then transmits as multiple bits
        + Each bit is converted into series of bits called chips
        + data converted to binary sequence(looks like noise)
      * Receiving device converts back to data bit
        + 9 out of 11 chips can be lost without degrading communication
* Wireless Access Points (WAP)
  + Half-duplex switch with a radio card that can be turned to one or more unlicensed radio frequencies
    - Can transmit only if no other station is already doing so
    - Does more than a hub
      * Works at the control and data-functional layers
      * Has some “switch-like” intelligence
    - Must make connection and maintain connection over the air
  + Works by acting as portal for another network
    - Usually connect loal wireless devices and to act as a portal to another physical network (called distribution network)
    - WAP raido cards work on 1 of 2 bands over several channels
      * Channels MUST be 5 channels apart to prevent overlap
    - Continuously transmit beacons on selected RF bands and channel to advertise presence and configuration
      * Includes:
        + Timestamp for synchronization
        + Channel
        + Data rate
        + Spread spectrum parameters
        + SSID
        + Quality of service parameters
* Association for WAP
  + NOT authentication
  + WPA2 uses 4-way handshake
    - 1: WAP sends nonce(single-use random number), called ANonce; client uses this value to create key
    - 2: client sends own nonce, called SNonce….
    - …
    - 4: Client sends confirmation to WAP, which completes Association
* WAP vs Router
  + Not same thing
  + AP have evolved over years to mean something different than they did in the early years of Wi-Fi
  + Used to AP was added for wireless device
  + Most routers have Wi-FI and play many roles including AP
  + **Router can be access point, but an access point can’t be a router**
* WAP architecture
  + 2 types of WAPs
    - Autonomous
      * Operate at control and data layer
      * Switch like intelligence
    - Thin access points
      * Switch like intelligence stripped out and put in controller device
      * Controller acts as a central admin for several AP
      * Easy to manage many WAPs on a WLAN
* Switch like intelligence
  + Able to recognize, reframe, address, deliver packets between networks or another WAP
  + Intelligence is referred to as Integration service and Distribution service
    - Integration service(IS)
      * Frame translation method between 802.11 frames and other mediums
    - Distribution Service(DS)