- Rogue access points
    - An unauthorized wireless access point
        - May be added by an employee or an attacker
        - Not necessarily malicious
        - A significant potential backdoor access point
    - Very easy to plug in a wireless AP
    - Or enable wireless sharing in your OS.
- Schedule a periodic survey
- Walk around your building/campus
- Use third party tools
- Consider using 802.1X (network access control)
    - You must authenticate
- Wireless evil twins
    - Looks legitimate, but actually malicious
    - The wireless version of phishing
- Configure an access point to look like an existing network
    - Same (or similar) SSID and security settings/captive portal
- Overpower the existing access points
    - May not require the same physical location
- Wifi hotspots (and users) are easy to fool
    - And they're wide open
- You encrypt your communication
    - Use HTTPS and a VPN

- Bluejacking
    - Sending of unsolicited messages to another device via Bluetooth
        - No mobile carrier required
    - Typical functional distance is about 10 meters
        - More or less, depending on antenna and interference
    - Bluejack with an address book object
        - Instead of contact name, write a message
        - Third party software may also be used Bluesniff
- Bluesnarfing
    - Access a bluetooth enabled device and transfer data
    - Contact list, calender, email, pictures, videos etc
- First major security weakness in Bluetooth
    - Patched
- Serious security issue
    - If you know the file, you can download it without authentication

---

- Wireless network
    - Surfing along on your wireless network and then the wifi disappears
    - Wifi stops working and theres nothing you can do
    - Wireless deauthentication attack

        - A significant wireless DoS attack
- 802.11 management frames
    - Wireless includes a number of management frames
    - Frames that make everything
    - How to find access points, manage QoS, associate/disassociate with an access point
    - Original wireless standards did not add protection for management frames
- Protecting against deauth attacks IEEE addresses the problem
- Some of the important management frames are encrypted
    - Disassociate, deauthenticate, channel switch announcements
- Not everything is encrypted
    - Beacons, probes, auth, and association

- Radio frequency jamming (RF)
    - Denial of Service
        - Prevent wireless communication
    - Transmit interfering wireless signals
        - Decrease the signal to noise at the receiving device
        - The receiving device cant hear the good signal
    - Sometimes its not intentional
        - Interference, not jamming
        - Microwave oven, fluorescent lights
        - Jamming is intentional
            - Someone wants your network to not work
    - Wireless Jamming
        - Constant, random bits / Constant, legitimate frames
        - Data sent at random times - random data and legitimate frames
        - Reactive jamming - only when someone tries to communicate
        - Needs to be somewhere close
            - Difficult to be effective from a distance
        - Time to go fox hunting
            - You'll need the right equipment to hunt down the jam
            - Directional antenna, attenuator

- RFID (radio frequency identification)
    - It's everywhere, access badges, inventory/assembly line tracking/pet animal identification
    - Radar technology
        - Radio energy transmitted to the tag
        - RF powers the tag, ID is transmitted back
        - Bidirectional communication
        - Some tag formats can be active/powered
    - Data Capture
        - View communication

        - Replay attack
    - Spoof the reader
        - Write your own data to the tag
    - Denial of Service
        - Signal jamming
    - Decrypt communication
        - Many default keys are on Google
- NFC (Near field communication)
    - Two way wireless communication
        - Builds on RFID, mostly one way
    - Payment systems
        - Many options available
    - Bootstrap for other wireless
        - NFC helps with Bluetooth pairing
    - Access token, identity “card”
        - Short range with encryption support
- NFC security concerns
    - Remote capture
        - Its a wireless network
        - 10 meters for active devices
    - Frequency jamming
        - Denial of service
    - Replay/ Relay attack
        - On path attack
    - Loss of RFC device control
        - Stolen/Lost device

- Randomizing Cryptography
    - Cryptography without randomization
    - Photo of Dog and a Photo of encrypted 128 bit dog and color is off but for the most part you can see the dog because the keys are not randomized
- Cryptographic nonce
    - Arbitrary number
        - Used once
        - “For the none” - for the time being
    - A random or pseudo random number
        - Something that can't be reasonably guessed
        - Can also be a counter
    - Use a nonce during the login process
        - Server gives you a nonce
        - Calculate your password hash using the nonce
        - Each password hash sent to the host will be different, so a replay attack wont work.
    - Common Nonce: Initialization Vector (IV)

- A type of nonce
- Used for randomizing an encryption scheme
- The more random the better
- Used in encryption ciphers, WEP, and some SSL implementations
- Salt
  - A nonce most commonly associated with password randomization
    - Make the password hash unpredictable
  - Password storage should always be salted
    - Each user gets a different salt

- On-path network attack
  - How can an attacker watch without you knowing
    - Also known as man-in-the-middle attack
  - Redirects your traffic
    - Then passes it on to the destination
    - You never know your traffic was redirected.
  - ARP poisoning
    - On-path attack on the local IP subnet
    - ARP has no security
  - Computer will ask who is the router and the router will respond with that it is the router with assigned ip and mac address
  - Computer then stores the information in an ARP cache
  - On path attacks and pretends to be the router and doesn't have to be requested by the computer due to ARP security not being presented (unprompted request but still takes it in) Replaces old info in the ARP cache with new info. To complete poisons the router uses the same process and will then become a relay.
- On path browser attack
  - What if the middleman was on the same computer as the victim?
    - Malware/Trojan does all the proxy work
    - Formerly known as man-in-the-browser attack
  - Huge advantages for the attackers
    - Relatively easy to proxy encrypted traffic
    - Everything looks normal to the victim
    - The malware in your browser waits for you to login to your bank

---

- Mac Flooding and Cloning
  - Ethernet Media Access Control address of a network
    - The physical address of a network adapter
    - Unique to a device
    - 48 bits / 6 bytes long
      - Displayed in hexadecimal
      - First 3 bytes are Organizationally Unique Identifier (OUI) manufacturer portion of the mac address

            - Last 3 bytes - Network interface controller specific (the serial number)
- Lan Switching
    - Forward or drop frames
        - Based on the destination MAC address
    - Gather a constantly updating list of MAC addresses
        - Builds the list based on the source MAC address of incoming traffic
        - These age out periodically, often in 5 minutes
    - Maintain a loop free environment
        - Using Spanning Tree Protocol (STP)
- LEarning the Macs
    - Switches examine incoming traffic
        - Make a note of the source MAC address
    - Adds unknown MAC addresses to the MAC address table
        - Sets the output interface to the received interface
        - Frame Switching
- MAC flooding
    - The MAC is only so big
    - Attacker starts sending traffic with different source MAC addresses
        - Force out the legitimate MAC addresses
    - The table fills up
        - Switch begins flooding traffic to all interfaces
        - All traffic is transmitted to all interfaces
        - No interruption in traffic flows
    - Attacker can easily capture all network traffic
    - Flooding can be restricted in the switch's port security settings
- MAc cloning / MAC spoofing
    - An attacker changes their MAC address to match the MAC address of an existing device
        - A clone / a spoof
    - Circumvent filters
        - Wireless or wired MAC filters
        - Identify a valid MAc address and copy it
    - Create a DoS
        - Disrupt communication to the legitimate MAC
    - Easily manipulated through software
        - Usually a device driver option

- DNS Poisoning
    - Modify the DNS server
        - Requires some crafty network
    - Modify the client host file
        - The host file takes precedence over DNS queries
    - Send a fake response to a valid DNS request

    - Requires a redirection of the original request or the resulting response.
- Domain Hijacking
  - Get access to the domain registration, and you have control where the traffic flows.
    - You don't need to touch the actual servers
    - Determines the DNS names and DNS Ip addresses
  - Many ways to get into the account
    - Brute force
    - Social Engineer the password
    - Gain access to the email address that manages the account
    - The usual things
  - Domain Hijacking
    - Saturday Oct 22 2016
    - Domain name registrations of 36 domains are changed
    - Under hacker control for 6 hours
    - The attacker became the bank
  - URL hijacking
    - Make money from your mistakes
    - Theres a lot of advertising on the net
    - Sell the badly spelled domain to the actual owner
      - Sell a mistake
    - Redirect to a competitor
      - Not as common, legal issues
    - Phishing site
      - Looks like the real site, please login
    - Infect with a drive by download
      - You’ve got malware.
- Types of URL hijacking
  - Typosquatting / brand jacking
    - Take advantage of poor spelling
  - Outright misspelling
    - Professormesser.com vs professormessor.com
  - A typing error
    - professormeser.com
  - A different phase
    - Professormessors.com
  - Different top level domain
    - Professormesser.org
- Domain reputation
  - The internet is tracking your security posture
    - They know when things go sideways
  - Email reputation
    - Suspicious activity
    - Malware originating from the IP address

  - Check with the email or service provider to check the reputation
    - Follow their instructions to remediate
  - Infected systems are noticed by the search engines
    - Your domain can be flagged or removed
    - Users will avoid the site
      - Sales will drop
      - Users will avoid your brand
  - Malware might be removed quickly
    - Recovery takes much longer

- Denial of Service
  - Force a server to fail
    - Overload the service
  - Take advantage of a design failure of vulnerability
    - Keep your systems patched
  - Cause a system to be unavailable
    - Competitive advantage
  - Create a smokescreen for some other exploit
    - Precursor to a DNS spoofing attack
  - Does Not have to be complicated
    - Turn off the power
- A “friendly DoS”
  - Unintentional DoSing
    - It's not always a ne’er-do-well
  - Network DoS
    - Layer 2 loop without STP
  - Bandwidth DoS
    - Downloading multi-gigabyte Linux Distro over a DSL line
  - The waterline breaks
- Distributed Denial of Service (DDoS)
  - Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
- This is why the attackers have botnets
  - Thousands or millions of computers at your command
  - At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- Asymmetric threat
  - The attacker may have fewer resources than the victim
- DDoS amplification
  - Turn your small attack into a big attack
    - Often reflected off another device or service
  - An increasingly common network DDos technique
    - Turn your internet services against
  - Uses protocols with little authentication or checks

    - NTP, DNS, ICMP
    - A common example of protocol abuse
- Application DoS
  - Make the application break or work harder
    - Increase the downtime and costs
  - Fill the disk space
    - A 42 kilobyte .zip compressed file
    - 4.5 petabytes
    - Antivirus will identify there
    - Overwhelm the system
  - Overuse a measured cloud resource
    - More CPU/memory/network is more money
  - Increase the cloud server response time
    - Victim deploys a new application
- Operational Technology (OT) Dos
  - The hardware and software for industrial equipment
  - Electric grids, traffic control, manufacturing plants
- This is more than a web server failing
  - Power grid drops offline
  - All traffic lights are green
  - Manufacturing plants shut down
- Requires a different approach
  - A much more critical security posture

- Scripting and Automation
  - Automate tasks
    - You don't have to be there
    - Solve problems in your sleep
    - Monitor and resolve problems before they happen
  - They need for speed
    - The script is as fast as the computer
    - No typing or delays
    - No human error
  - Automate the attack
    - The hacker is on borrowed time
- Windows Powershell
    - Command line for sys administrators
    - .ps1 file extension
    - Included with windows 8 8.1 and 10
  - Extend command line functions
    - Use cmdlets (command-lets)
    - Powershell scripts and functions
    - Standalone executables
  - Attack windows systems

        - System administration
        - Active domain administration
        - File share access
- Python
    - General purpose scripting language
        - .py file extension
    - Popular in many technologies
        - Broad appeal and support
    - Commonly used for cloud orchestration
        - Create and tear down application instances
    - Attack the infrastructure
        - Routers, servers, switches
    - Shell script
        - Scripting the Unix/Linux shell
            - Automate and extend the command line
            - Bash, Bourne, Korn, C
            - Starts with a shebang or hash-bag #!
                - Often has a .sh file extension
        - Attack the Linux/Unix environment
            - Web Database, visualization servers
            - Control the OS from the command line
                - Malware has a lot of options
- Macros
    - Automate functions within an application
        - Or operating system
    - Designed to make the application easier to use
        - Can often create security vulnerabilities
    - Attackers create automated exploits
        - They just need the user to open the file
        - Prompts to run the macro
- Visual Basic For Applications (VBA)
    - Automates processes within Windows applications
        - Common in Microsoft Office
    - A powerful programming language
        - Interacts with the operating system
    - CVE-2010-0816 / MS10-031
        - VBA does not properly search for ActiveX controls in a document
        - Run arbitrary code embedded in a document