Wireless Security

Wireless Network Attacks

Access control attacks

These attacks attempt to penetrate a network by using wireless or evading WLAN access control measures, like AP MAC filters and 802.1X port access controls.

Type of Attack	Description	Methods and Tools
War Driving	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rogue Access Points	Installing an unsecured AP inside firewall, creating open backdoor into trusted network.	Any hardware or software AP
Ad Hoc Associations	Connecting directly to an unsecured station to circumvent AP security or to attack station.	Any wireless card or USB adapter
MAC Spoofing	Reconfiguring an attacker's MAC address to pose as an authorized AP or station.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS Cracking	Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin AP.	Packet capture tool on LAN or network path between AP and RADIUS server

Confidentiality attacks

These attacks attempt to intercept private information sent over wireless associations, whether sent in the clear or encrypted by 802.11 or higher layer protocols.

Type of Attack	Description	Methods and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ettercap, Kismet, Wireshark, commercial analyzers
WEP Key Cracking	Capturing data to recover a WEP key using passive or active methods.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside
Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD
AP Phishing	Running a phony portal or Web server on an evil twin AP to "phish" for user logins, credit card	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP

	numbers.	
Man in the Middle	Running traditional man-in-the-middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap-NG, sshmitm

Integrity attacks

These attacks send forged control, management or data frames over wireless to mislead the recipient or facilitate another type of attack (e.g., DoS).

Type of Attack	Description	Methods and Tools
802.11 Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + Injection Tools
802.1X EAP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless Capture + Injection Tools between station and AP
802.1X RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay.	Ethernet Capture + Injection Tools between AP and authentication server

Authentication attacks

Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services.

Type of Attack	Description	Methods and Tools
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed, vendor default or cracked WEP keys.	WEP Cracking Tools
PSK Cracking	Recovering a WPA/WPA2 PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Capturing user credentials (e.g., e-mail address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)

802.1X Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture Tools
802.1X Password Guessing	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password Dictionary
802.1X LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker
802.1X EAP Downgrade	Forcing an 802.1X server to offer a weaker type of authentication using forged EAP-Response/Nak packets.	File2air, libradiate

Links

- http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks
- http://en.wikipedia.org/wiki/Wireless_security

Preventive Measures

- Wireless intrusion prevention systems (Definition: A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools; Implementation: Sensors, servers, console, secure link; Prevented threats: Rogue AP – WIPS should understand the difference between Rogue AP and External (neighbor's) AP, Mis-configured AP, Client Mis-association, Unauthorized association, Man in the Middle Attack, Ad-hoc Networks, Mac-Spoofing, Honeypot / Evil Twin Attack, Denial of Service (DoS) Attack)
- Hide SSID (simple but relatively ineffective)
- MAC ID filtering (does not work when attacker sniffs MAC address of authorized client and spoofs it)
- Static IP addressing (does not work when attacker sniffs IP address of authorized client and spoofs it)
- End to end encryption (The solution may be encryption and authorization in the application layer, using technologies like SSL, SSH, GnuPG, PGP and similar.)
- Smart cards, USB tokens, and software tokens (the most effective method known today)
- RF shielding (It's practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility.)
- Wireless IPS
- RADIUS (The idea is to have an inside server act as a gatekeeper through the use of verifying identities through a username and password that is already pre-determined by the user.)
- Stealth wallpaper that blocks wireless signals
- Faraday cages around buildings

- **Links:**
- http://en.wikipedia.org/wiki/Faraday_cage
- http://en.wikipedia.org/wiki/Stealth_wallpaper
- http://en.wikipedia.org/wiki/Wireless_security
- http://en.wikipedia.org/wiki/TEMPEST

Satellite Networks and Security

Introduction:

- Components (Radio Device, Footprint, Ground Station, ISDN/PSTN, Base station/gateway, uplink/downlink, satellite)
- Orbit Characteristics (GEO, LEO, MEO, HEO; inclination angle, velocity, time period, geo-stationary satellites, power, footprint)
- Communication Characteristics (frequency bands; time delay in communication; types of Links: ISL, MUL, GWL)
- Communication Paradigms (Cellular, C band, Ku Ban, BSS, DBS, Marine, Space-bourne Land Mobile, Satellite Messaging for Commercial Jets)
- Data Characteristics (low latency, poor bandwidth, noise)
- Error Correction (FEC, ARR, SW, GBN, SR)
- Hybrid Networks
- Pros/Cons Satellite Networks
- Effect of Weather Conditions
- Path Diversity
- Handoffs
- Introduction to GPS – (triangulation technique, satellite systems, gravitational field correction, PRN, limitations, advantages, common applications)

Links:

- http://www.cs.gsu.edu/~cscyip/csc8221/Chapt-11.pdf
- http://www.cs.wustl.edu/~jain/cis788-97/ftp/satellite_nets.pdf

Security in Satellite Networks

- Signal interception by military organizations, eg: CIA, NSA (Space interception of inter-city networks, SIGINT satellites, COMSAT ILC collection, Submarine cable interception)
- Unintentional Threats to Commercial Satellite Systems (Ground based: natural disasters, acts of god, power outages; Space based: solar flares, radiation, temperature variations, space debris; Interference: cosmic rays, other satellites, frequency conflicts)
- Intentional Threats to Commercial Satellite Systems (Ground based: physical destruction of communication equipment and base stations, sabotage; Space-based: space-to-space missiles, anti-satellite weapons, space mines, lasers, Electro magnetic pulse; Cyber attacks: spoofing, data interception, malicious software, denial of service; Signal jamming)

- Commercial Satellite Systems Security (TTC&M protection and security; Digital encryption; Data base protection; Hardware & traffic redundancy + sparing + ISLs; PKI-GPS-Billing Authentication; IP "Spoofing" Accelerators; 99.98% system availability)
- Military and Gov't Satellite Systems Security (Radiation Hardening; Anti-Jamming; 132 bit encryption or better; Enhanced TTC&M security; Use of special frequencies and laser com; IP Sec; Orbits-super synchronous-ISL; Hardware redundancy; System protection-secure tails)

Links:

- http://www.fas.org/irp/eprint/ic2000/ic2000.htm
- http://www.gao.gov/new.items/d02781.pdf
- http://spacejournal.ohio.edu/issue6/pdf/pelton.pdf
- http://en.wikipedia.org/wiki/Anti-satellite_weapon

Cellular Network Security

Comparison of Security to Wired Networks

- Open Wireless Access Medium: Since the communication is on the wireless channel, there is no physical barrier that can separate an attacker from the network.
- Limited Bandwidth: Although wireless bandwidth is increasing continuously, because of channel contention everyone has to share the medium – leads to increased security risks.
- System Complexity: Wireless systems are more complex due to the need to support mobility and making use of the channel effectively. By adding more complexity to systems, potentially new security vulnerabilities can be introduced.
- Relatively Unreliable Network Connection: The wireless medium is an unreliable medium with a high rate of errors compared to a wired network.

Security Issues

- Authentication: Cellular networks have a large number of subscribers, and each has to be authenticated to ensure the right people are using the network. Since the purpose of 3G is to enable people to communicate from anywhere in the world, the issue of cross region and cross provider authentication becomes an issue.
- Integrity: With services such as SMS, chat and file transfer it is important that the data arrives without any modifications.
- Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.
- Operating Systems In Mobile Devices: Cellular Phones have evolved from low processing power, ad-hoc supervisors to high power processors and full-fledged operating systems. Some phones may use a Java Based system; others use Microsoft Windows CE and have the same capabilities as a desktop computer. Issues may arise in the OS which might open security holes that can be exploited.

- Web Services: A Web Service is a component that provides functionality accessible through the web using the standard HTTP Protocol. This opens the cellular device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc
- Location Detection: The actual location of a cellular device needs to be kept hidden for reasons of privacy of the user.
- With the move to IP based networks, the issue arises that a user may be associated with an access point and therefore their location might be compromised.
- Viruses And Malware: With increased functionality provided in cellular systems, problems prevalent in larger systems such as viruses and malware arise. The first virus that appeared on cellular devices was Liberty. An affected device can also be used to attack the cellular network infrastructure by becoming part of a large scale denial of service attack.
- Downloaded Contents: Spyware or Adware might be downloaded causing security issues. Another problem is that of digital rights management. Users might download unauthorized copies of music, videos, wallpapers and games.
- Device Security: If a device is lost or stolen, it needs to be protected from unauthorized use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.

Types of Attacks

- Channel Jamming: Channel jamming is a technique used by attackers to jam the wireless channel and therefore deny access to any legitimate users in the network.
- Eavesdropping: If the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc.
- Message Forgery: If the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing.
- Message Replay: Even if communication channel is secure, an attacker can intercept an encrypted message and then replay it back at a later time and the user might not know that the packet received is not the right one.
- Man In The Middle Attack: An attacker can sit in between a cell phone and an access station and intercept messages in between them and change them.
- Session Hijacking: A malicious user can highjack an already established session, and can act as a legitimate base station.

Security Systems

- A New Authentication Scheme with Anonymity For Wireless Networks: When a mobile user is roaming, it is necessary to provide anonymity to the users so that malicious parties are unable to associate the user with a particular session. The most basic method to provide anonymity is to have a temporary identity (TID) instead of the real id of the user
- Manual Authentication For Wireless Devices: This is a technique used by devices to authenticate one another by manually transferring data between the devices. Elliptic Curve Cryptography For Wireless Security: Elliptic Curve Cryptography (ECC) is a mechanism which uses points on an elliptic curve to encrypt/decrypt data. It has an advantage over the popular RSA algorithm in that it is much faster.
- KASUMI Block Cipher
- The UMTS Authentication and Key Agreement

Links

- http://www.cs.uakron.edu/~dang/CS655/Spring05/3G.pdf
- http://ccc.inaoep.mx/Reportes/CCC-04-002.pdf
- http://www.cse.fau.edu/%7Eed/Fernandez_ISSADS2005Final.pdf
- http://research.microsoft.com/~klauter/IEEEfinal.pdf
- http://www.cse.wustl.edu/~jain/cse574-06/ftp/cellular_security.pdf
- http://www.winlab.rutgers.edu/~trappe/Papers/WiDoS_Wise04.pdf
- http://paginas.fe.up.pt/~mricardo/doc/journals/crossLayerDesign.pdf
- http://www.isg.rhul.ac.uk/~cjm/mafwd4.pdf
- http://www.csl.mtu.edu/cs6461/www/Reading/Zhu04.pdf