BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Wireless Hacking
Session No: 08

Agenda

innovate achieve lead

- Wireless Technology Basics
- Wireless Networking Standards (802.11)
- Authentication Process & Protocols
  - Point to point
  - Extensible Authentication Protocol
  - Wired Equivalent Privacy
  - Wi-Fi Protected Access
- Wireless Hacking
  - Equipment
  - Wardriving
  - Tools
  - Secure Wireless Network

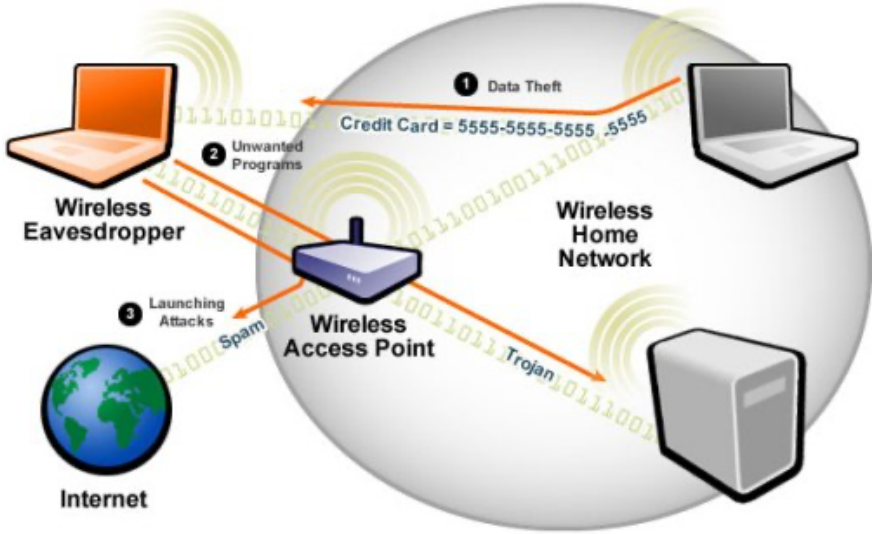
Wireless Technology

Understanding Wireless Technology

- For a wireless network to function
  - hardware
  - Software
- Wireless technology is part of our lives
  - Baby monitors
  - Cell and cordless phones
  - Pagers
  - GPS
  - Remote controls
  - Garage door openers
  - Two-way radios
  - Wireless PDAs

Components of Wireless Technology

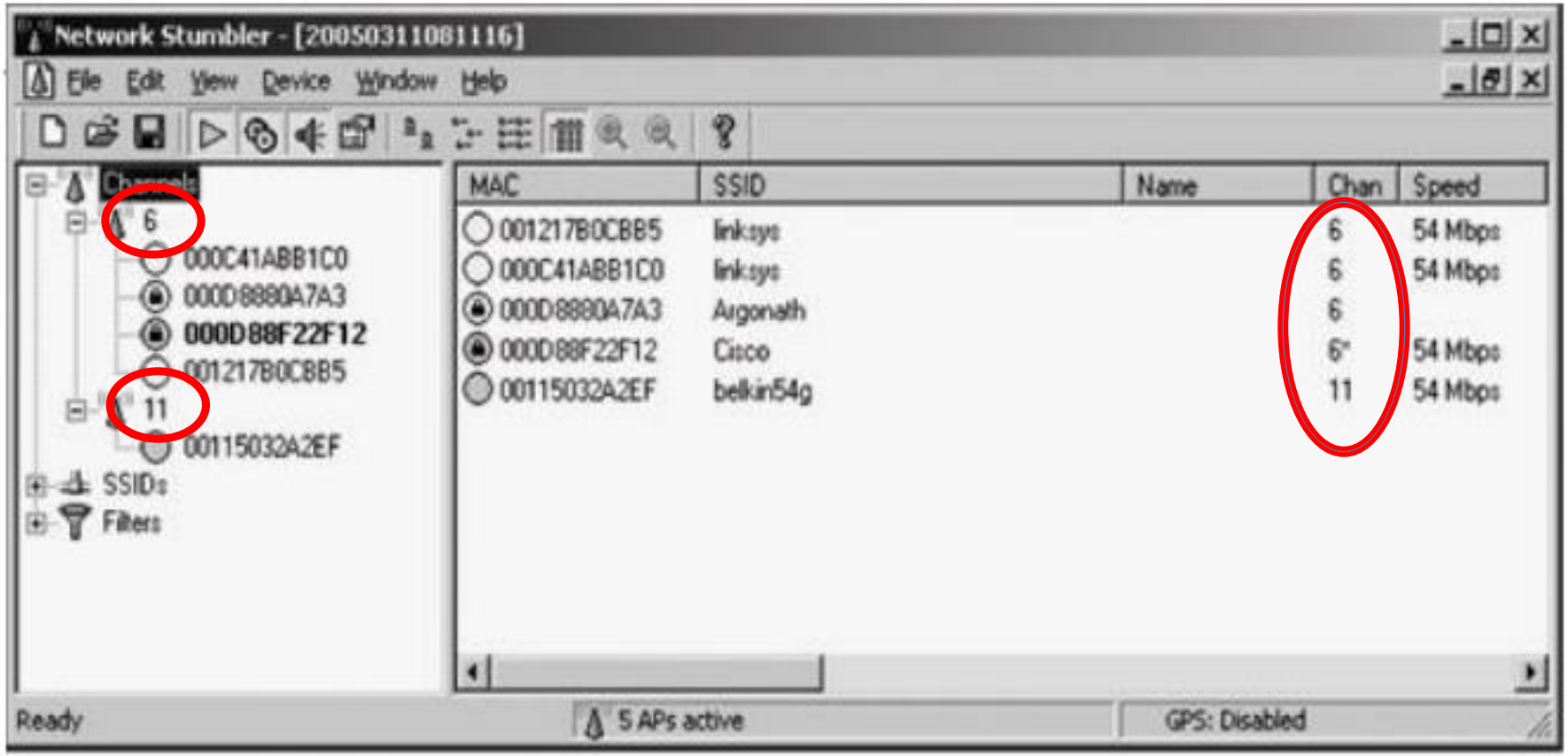
- A wireless network uses radio waves to connect computers and other devices
- There are two frequency bands allocated
  - 2.4 GHz (1 to 14 channels)
  - 5 GHz (36 to 165 channels)
- A wireless network has three basic components
  - Access Point (AP)
  - Wireless network interface card (WNIC)
  - Ethernet cable



Access Point (AP)

- AP is a transceiver that connects to an Ethernet cable
  - Connects the wireless network with the wired network
  - Not all wireless networks connect to a wired network
  - Most companies have WLANs that connect to their wired network topology
- AP is where channels are configured
  - Enables users to connect to a LAN using wireless technology
  - Is available only within a defined area

Access Point (AP) Channels



Service Set Identifier (SSID)

innovate achieve lead

- SSID is the name to identify the wireless local area network (WLAN)
  - Configured on the AP
  - Unique 1- to 32-character case sensitive alphanumeric name
- Wireless computers must configure the SSID before connecting to a wireless network
  - AP usually broadcasts the SSID
    - An AP can be configured to not broadcast its SSID until after authentication
  - SSID is transmitted with each packet
    - Identifies which network the packet belongs

Choose a Wireless Network

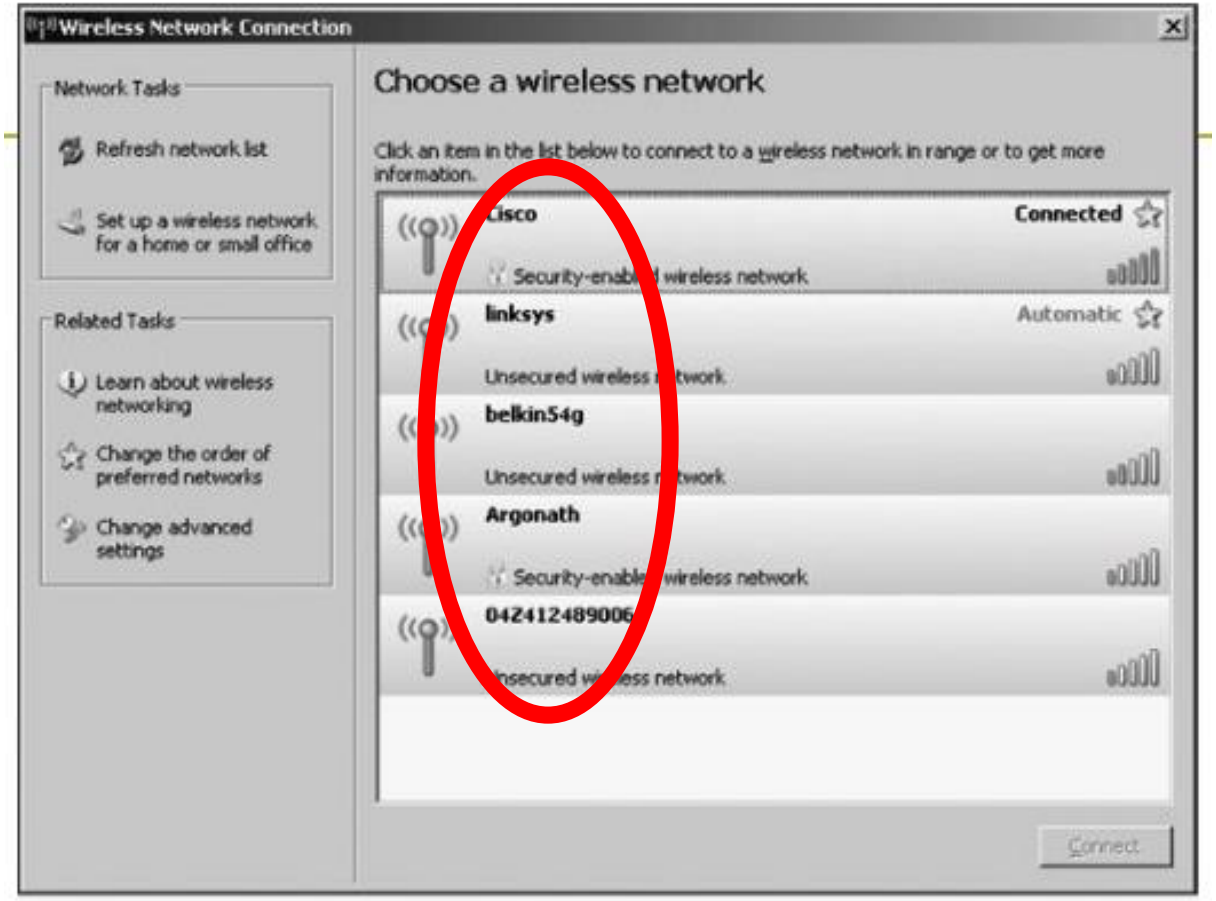


Figure 11-2 SSIDs advertised to a wireless station

Default Service Set Identifier (SSID)

- Many vendors have SSIDs set to a default value
  - Verify that your clients or customers are not using a default SSID

Vendor	Default SSIDs
3Com	3Com
Apple	Airport Network
Belkin (54G)	Belkin54g
Cisco	Tsunami
Compaq	Compaq
D-Link	WLAN, default
Dell	Wireless
Intel	Intel, 101, xlan, 195
Linksys	linksys, Wireless, linksys-g
Microsoft	MSNHOME
Netgear	Wireless, NETGEAR
SMC	WLAN, BRIDGE, SMC
Symantec	101
US Robotics	WLAN, USR9106, USR808054

How to update SSID:

1. Using your computer or mobile device, open a web browser, then log in to the Admin console of your home router.
2. Different router manufacturers have different ways of logging in to the Router Admin Console. Refer your Router Manual for details. The most common is http://192.168.1.1.
3. Go to Wireless menu option.
4. Change the default SSID name in the Wireless Network Name (SSID) field.
5. Click Save or Apply. Some routers need to reboot for the settings to take effect.
6. Reconnect your devices using the new Wi-Fi SSID.

Configuring an Access Point

- Configuring an AP varies depending on the hardware
  - Most devices allow access through any Web browser
- Example: Configuring a D-Link wireless router
  - Enter IP address on your Web browser and provide your user logon name and password
  - After a successful logon you will see the device's main window
  - Click on Wireless button to configure AP options
    - SSID
    - Wired Equivalent Privacy (WEP) keys
- Steps for configuring a D-Link wireless router
  - Turn off SSID broadcast
  - Disabling SSID broadcast is not enough to protect your WLAN
  - Change SSID

Wireless NICs

- For wireless technology to work, each node or computer must have a wireless NIC
  - NIC's main function is converting the radio waves it receives into digital signals the computer understands
- Wireless network standards
  - A standard is a set of rules formulated by an organization
  - Institute of Electrical and Electronics Engineers (IEEE)
    - Defines several standards for wireless networks

802.11 Standard

- First wireless technology standard
  - Defined wireless connectivity at 1 Mbps and 2 Mbps within a LAN
- Applied to layers 1 and 2 of the OSI model
  - Wireless networks cannot detect collisions
  - Carrier sense multiple access/collision avoidance (CSMA/CA) is used instead of CSMA/CD

Architecture of 802.11

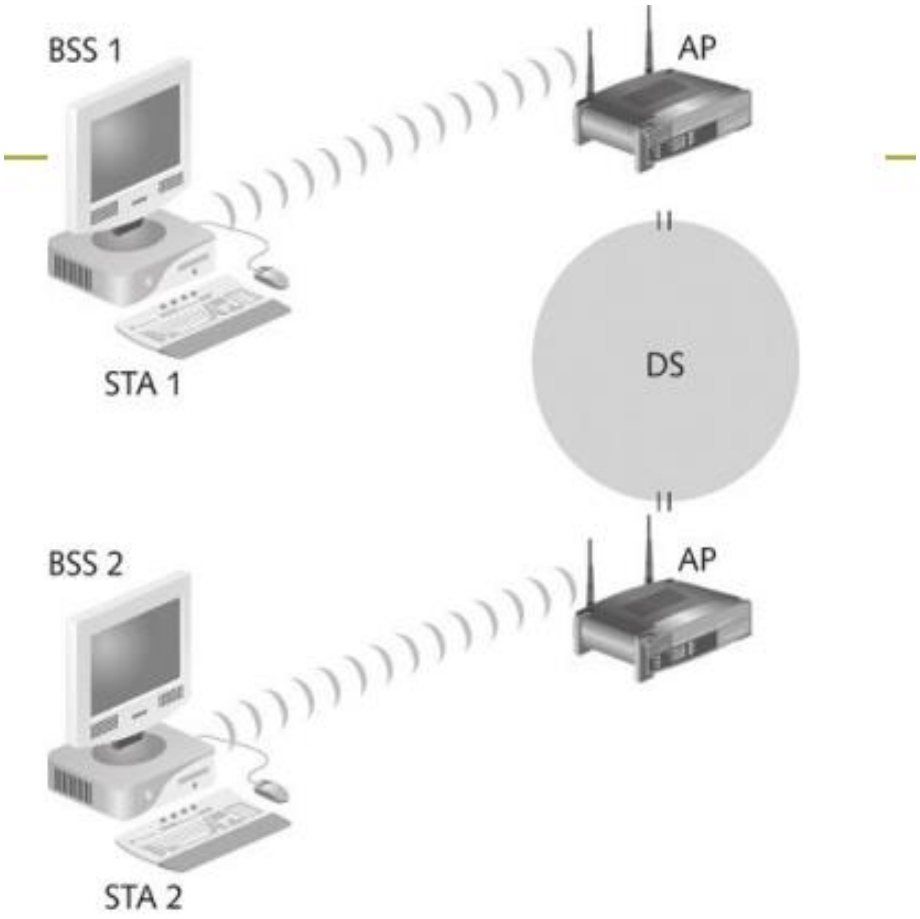


Figure 11-9 Connecting two wireless remote stations

- 802.11 uses a Basic Service Set (BSS) as its building block
  - Computers within a BSS can communicate with each others
- To connect two BSSs, 802.11 requires a distribution system (DS) as an intermediate layer
  - An AP is a station that provides access to the DS
  - Data moves between a BSS and the DS through the AP

Architecture of 802.11: Frequency Bands

Frequency	Range	Wavelength
Extremely low frequency (ELF)	30–300 Hz	10,000–1000 km
Voice frequency (VF) or ultra low frequency (ULF)	300 Hz–3 KHz	1000–100 km
Very low frequency (VLF)	3–30 KHz	100–10 km
Low frequency (LF)	30–300 KHz	10–1 km
Medium frequency (MF)	300 KHz–3 MHz	1 km–100 m
High frequency (HF)	3–30 MHz	100–10 m
Very high frequency (VHF)	30–300 MHz	100 km
Ultra high frequency (UHF)	300 MHz–3 GHz	100 km
Super high frequency (SHF)	3–30 GHz	10–1 cm
Extremely high frequency (EHF)	30–300 GHz	1 cm–1 mm

Architecture of 802.11: Frequency Bands

LOWER FREQUENCY MHZ	UPPER FREQUENCY MHZ	COMMENTS
2400	2500	• 2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi. • Used by 802.11b, g, & n. • It can carry a maximum of three non-overlapping channels. • This band is widely used by many other non-licensed items including microwave ovens, Bluetooth, etc.
5725	5875	• 5 GHz Wi-Fi band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less. • It can be used by 802.11a & n. • It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz. • 5GHz Wi-Fi is preferred because of the higher number of channels and available bandwidth. • There are also fewer other users of this band.

- Each frequency band contains channels
  - A channel is a frequency range
  - 802.11 standard defines 79 channels. If channels overlap, interference could occur

Architecture of 802.11: Frequency Bands

Standard	Frequency	Rate	Modulation
802.11	2.4 GHz	1 or 2 Mbps	FHSS/DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11e	2–6 GHz	22 Mbps	DSSS
802.11i	2.4 GHz	11 Mbps	DSSS
802.15	2.4 GHz	2 Mbps	FHSS
802.16	10–66 GHz	120 Mbps	OFDM
802.20 (Mobile Wire-less Access Working Group)	Below 3.5 GHz	1 Mbps	OFDM proposed (might change)
Bluetooth	2.4 GHz	12 Mbps	Gaussian frequency shift keying (GMSK)
HiperLAN2	5 GHz	54 Mbps	OFDM

Wireless Signal Carriers

- Infrared (IR)
  - Infrared light can't be seen by the human eye
  - IR technology is restricted to a single room or line of sight
  - IR light cannot penetrate walls, ceilings, or floors
- Narrowband
  - Uses microwave radio band frequencies to transmit data
  - Popular uses
    - Cordless phones
    - Garage door openers

Spread Spectrum

- Modulation defines how data is placed on a carrier signal
- Data is spread across a large-frequency bandwidth instead of traveling across just one frequency band
- Methods
  - Frequency-hopping spread spectrum (FHSS)
  - Direct sequence spread spectrum (DSSS)
  - Orthogonal frequency division multiplexing (OFDM)

802.1x Standard

- Wireless technology increases the potential for security problems
- 802.1x defines the process of authenticating and authorizing users on a WLAN
  - Addresses the concerns with authentication
  - Basic concepts
    - Point-to-Point Protocol (PPP)
    - Extensible Authentication Protocol (EAP)
    - Wired Equivalent Privacy (WEP)
    - Wi-Fi Protected Access (WPA)

Point to Point Protocol (PPP)

- Many ISPs use PPP to connect dial-up or DSL users
- PPP handles authentication by requiring a user to enter a valid user name and password
- PPP verifies that users attempting to use the link are indeed who they say they are

Extensible Authentication Protocol (EAP)

- EAP is an enhancement to PPP
- Allows a company to select its authentication method
  - Certificates
  - Kerberos
- Certificate
  - Record that authenticates network entities
  - It contains X.509 information that identifies the owner, the certificate authority (CA), and the owner's public key

Extensible Authentication Protocol (EAP)

- EAP methods to improve security on a wireless networks
  - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
  - Protected EAP (PEAP)
  - Microsoft PEAP
- 802.1X components
  - Supplicant
  - Authenticator
  - Authentication server

Extensible Authentication Protocol (EAP)

Figure 11-11 A supplicant connecting to an AP and a RADIUS server

Wired Equivalent Privacy (WEP)

- Part of the 802.11b standard
- It was implemented specifically to encrypt data that traversed a wireless network
- Works well for home users or small businesses when combined with a Virtual Private Network (VPN)
- WEP has many vulnerabilities

WEP Weaknesses

innovate achieve lead

- **The integrity of the packets is checked using Cyclic Redundancy Check (CRC32).** CRC32 integrity check can be compromised by capturing at least two packets. This leads to unauthorized access to the network.
- **WEP uses RC4 encryption algorithm to create stream ciphers.** The stream cipher input is made up of an initial value (IV) and a secret key. The length of the initial value (IV) is 24 bits long while the secret key can either be 40 bits or 104 bits long. The total length of both the initial value and secret can either be 64 bits or 128 bits long. **The lower possible value of the secret key makes it easy to crack it**.
- Weak Initial values combinations do not encrypt sufficiently. This makes them vulnerable to attacks.
- WEP is based on passwords which makes it vulnerable to dictionary attacks.
- **Keys management is poorly implemented**. Changing keys especially on large networks is challenging. WEP does not provide a centralized key management system.

Wi-Fi Protected Access (WPA)

- Specified as part of 802.11i standard
- Replacement for WEP, developed by Wi-Fi Alliance
- Uses higher Initial Value of 48 bits (as against 24 bits of WEP)
- WPA improves encryption by using Temporal Key Integrity Protocol (TKIP)
- TKIP is composed of four enhancements
  - Message Integrity Check (MIC)
    - Cryptographic message integrity code
    - Main purpose is to prevent forgeries
  - Extended Initialization Vector (IV) with sequencing rules
    - Implemented to prevent replays

Wi-Fi Protected Access (WPA)

- TKIP enhancements
  - Per-packet key mixing
    - It helps defeat weak key attacks that occurred in WEP
    - MAC addresses are used in creating an intermediate key
  - Rekeying mechanism
    - It provides fresh keys that help prevent attacks that relied on reusing old keys
- WPA also adds an authentication mechanism implementing 802.1X and EAP

Wireless Hacking

Equipment Required

innovate achieve lead

- Wireless adapter
- Chipset: To support writing own drivers
- Band support: Adapter to support both 2.4 and 5 GHz to operate on both bands.
  - Atheros with PCI/PCI-E/Cardbus/PCMCIA/Express Card interface
  - Railink RT73/RT2770F with USB interface
- Antenna support
- Interfaces: PCMCIA or USB are better from flexibility perspective
- Operating system: BackTrack or Kali
- Others
  - Antenna, GPS, Access Point

Wardriving

- Hackers use wardriving
  - Driving around with inexpensive hardware and software that enables them to detect access points that haven't been secured
- Wardriving is not illegal
  - But using the resources of these networks is illegal
- Warflying
  - Variant where an airplane is used instead of a car

How it Works?

- An attacker or security tester simply drives around with the following equipment
  - Laptop computer
  - Wireless NIC
  - An antenna
  - Software that scans the area for SSIDs
- Not all wireless NICs are compatible with scanning programs
- Antenna prices vary depending on the quality and the range they can cover
- Scanning software can identify
  - Company's SSID
  - Type of security enabled
  - Signal strength indicates how close the AP is to the attacker

Wireless Hacking

- Hacking a wireless network is similar to hacking a wired LAN
- Techniques for hacking wireless networks
  - Port scanning
  - Enumeration
- Two types of cracking:
  - **Passive cracking:** this type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
  - **Active cracking:** this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.

Wireless Hacking Tools

- Equipment
  - Laptop computer
  - A wireless NIC
  - An antenna
  - Sniffers
- Wireless routers that perform DHCP functions can pose a big security risk
- Tools for cracking WEP keys
  - AirSnort
  - WEPCrack

Aircrack

- Aircrack can be used for 802.11a/b/g WEP and WPA cracking.
- Aircrack uses algorithms to recover wireless passwords by capturing packets. Once enough packets have been gathered, it tries to recover the password.
- To make the attack faster, it implements a standard FMS attack with some optimizations.
- It supports most of the wireless adapters
- It requires deeper knowledge of Linux. If you are not comfortable with Linux, you will find it hard to use this tool.
- Ref: http://www.aircrack-ng.org/

NetStumbler

- Shareware tool written for Windows that enables to detect WLANs
  - Supports 802.11a, 802.11b, and 802.11g standards
- NetStumbler was primarily designed to
  - Verify WLAN configuration
  - Detect other wireless networks
  - Detect unauthorized Aps
  - Wardriving
- NetStumbler is capable of interface with a GPS
  - Enabling a security tester or hacker to map out locations of all the WLANs the software detects

NetStumbler

- NetStumbler logs the following information
  - SSID
  - MAC address of the AP
  - Manufacturer of the AP
  - Channel on which it was heard
  - Strength of the signal
  - Encryption
- Attackers can detect APs within a 350-foot radius
  - with a good antenna, they can locate APs a couple of miles away

Kismet

- Another product for conducting wardriving attacks
- Written by Mike Kershaw
- Runs on Linux, BSD, MAC OSX, and Linux PDAs
- Kismet can also act a sniffer and IDS
  - Kismet can sniff 802.11b, 802.11a, and 802.11g traffic
- Can detect wireless networks both visible and hidden, sniffer packets and detect intrusions
- For details refer: https://www.kismetwireless.net/

Kismet Features

- Ethereal and Tcpdump compatible data logging
- AirSnort compatible
- Network IP range detection
- Hidden network SSID detection
- Graphical mapping of networks
- Client-server architecture
- Manufacturer and model identification of APs and clients
- Detection of known default access point configurations
- XML output
- Supports 20 card types

AirSnort

- Created by Jeremy Bruestle and Blake Hegerle
- Can help access WEP-enabled WLAN
- Limitations
  - Runs only on Linux
  - Requires specific drivers
  - Not all wireless NICs function with AirSnort

WEPCRack

- Open-source tool used to crack WEP encryption
- WEPCrack uses Perl scripts to carry out attacks on wireless systems
- Has features to conduct brute-force attack
- For details refer: http://wepcrack.sourceforge.net/

WEP Cracking Tools

- **Aircrack:** network sniffer and WEP cracker. Can be downloaded from http://www.aircrack-ng.org/
- **WebDecrypt:** this tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters. http://wepdecrypt.sourceforge.net/

WPA Cracking Tools

- WPA uses a 256 pre-shared key or passphrase for authentications.
- Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords.
- The following tools can be used to crack WPA keys.
  - **CowPatty:** this tool is used to crack pre-shared keys (PSK) using brute force attack. http://wirelessdefence.org/Contents/coWPAttyMain.htm
  - **Cain & Abel:** this tool can be used to decode capture files from other sniffing programs such as Wireshark. The capture files may contain WEP or WPA-PSK encoded frames. https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml

Secure Wireless Network

innovate achieve lead

- Consider using anti-wardriving software to make it more difficult for attackers to discover your wireless LAN
  - Honeypots
  - FakeAP
  - Black Alchemy FakeAP
- Allow only predetermined MAC addresses and IP addresses to have access to the wireless LAN
- Limit the use of wireless technology to people located in your facility

Secure Wireless Network

- Consider using an authentication server instead of relying on a wireless device to authenticate users
- Consider using EAP, which allows different protocols to be used that enhance security
- Consider placing the AP in the demilitarized zone (DMZ)
- If you use WEP, consider using 104-bit encryption rather than 40-bit encryption
- Assign static IP addresses to wireless clients instead of using DHCP

Secure Wireless Network

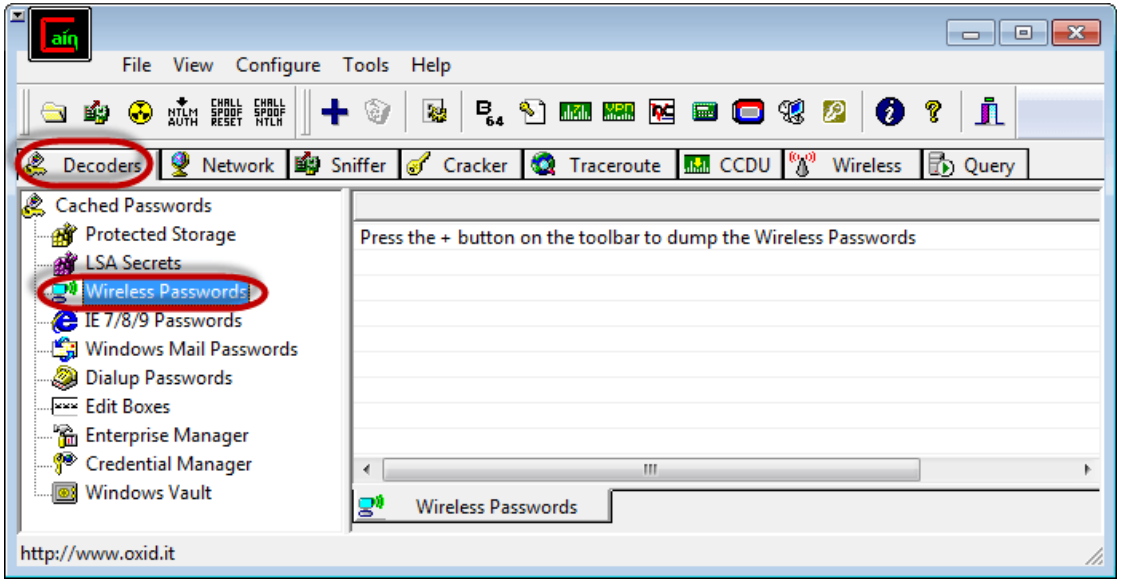
- Changing default passwords that come with the hardware
- Enabling the authentication mechanism
- Access to the network can be restricted by allowing only registered MAC addresses.
- Use of strong WEP and WPA-PSK keys, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- Firewall Software to help reduce unauthorized access.

Example: Cracking a Wireless Network

- A wireless network adapter with the capability to inject/intercept packets
- Be within the target network's radius. If the users of the target network are actively using and connecting to it, then your chances of cracking it will be significantly improved.
- Capture packets specially users login steps – pcap files
- Use the captured packets (pcap files) to find potential passwords using brute-force technique – SaaS services like CloudCracker etc

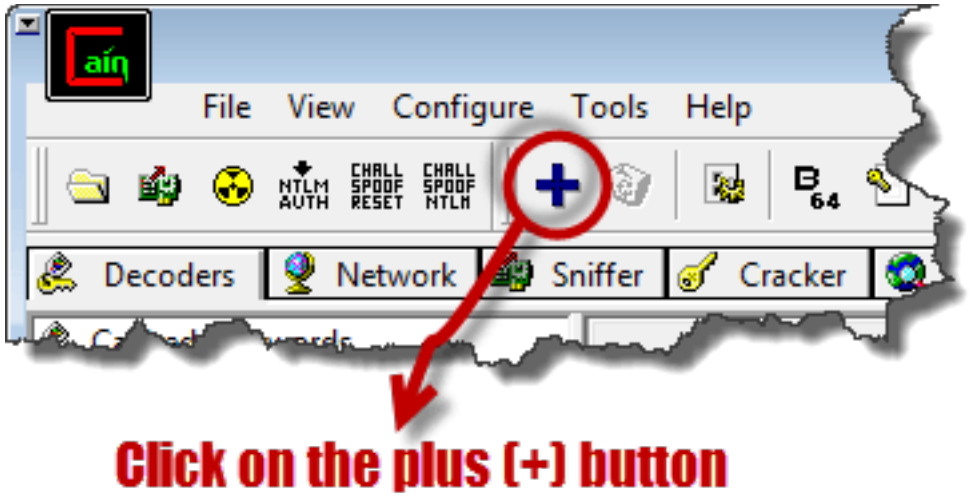
Example: Crack Wireless Password

- Use of Cain and Abel to decode the stored wireless network passwords in Windows.
- Provide useful information that can be used to crack the WEP and WPA keys of wireless networks.
- Download & Open Cain & Abel



Example: Crack Wireless Password

- Ensure that the Decoders tab is selected then click on Wireless Passwords from the navigation menu on the left-hand side
- Click on the button with a plus sign



Example: Crack Wireless Password

- Assuming you have connected to a secured wireless network before, you will get results similar to the ones shown below
- The decoder will show you the encryption type, SSID and the password that was used.

Adapter GUID	Descr	Type	SSID	Password	Hex
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{7825C2EF-C9F9-48F...	@netvwifimp.inf,%vwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A5437696278523740494...

Demo

- Kismet Demo

https://www.youtube.com/watch?v=3v_bwtHIToQ

https://www.youtube.com/watch?v=UYRXZxb4RWg

Thank You