Hacking nowadays has become very simple due to wireless standards and practices still rapidly evolving, it is important to understand the strengths and limitations of available technologies in order to implement a secure solution. Extending current security policies to encompass wireless devices requires an understanding of the security features of both wireless devices and wireless networks.

ABSTRACT
Hacking is the most exhilarating game on the planet. But it stops being fun when you end up in a cell with a roommate named “Spike.” But hacking doesn’t have to mean breaking laws. Hacking is so easy that if you have an on-line service and know how to send and read email, you can start hacking immediately.

Hacking emails
Main that people want to hack, their own personal gain.” Finally, www.prenhall.com hackers steal information from companies for their taste. It is the curiosities, which makes them want to know more about information, depending on computer systems & networks. Hacking is a state of who is extremely proficient or obsessive about programming, programming languages and or or computer systems & networks. Hacking is a state of mind. Curiosity is the main point; a hacker always wants to know more about information, depending on his/her taste. It is the curiosities, which makes them learn more and more quickly.

Hacking nowadays has become very simple due to the fact that there have been many hackers who have been helping out people so that they don’t have to break their heads when they have to hack. There are 3 main that people want to hack,

1) Hacking emails: This is one of the things that the people always want to do. Be it guys who want to see what’s happening in their girlfriend email. A company trying to see what his competitor is doing.

2) ftp Hacking: ftp means file transfer protocol. This is used to upload files onto servers and these have usernames and passwords and these can be hacked into to get information. ftp Hacking can also be done so that the site or information to be destroyed. The ftp and email Hacking is known as http brute force Hacking!

There are many tools that can be used for brute forcing. Eg : Munga Bungas http brute forcer - this is one of the best brute forcer available on the net todays. ftp Hacking software where the ftp can be hacked into and get into servers and retrieve information that can be used.

3) Remote Hacking: The remote Hacking means to get into a system that is on the net or the network and then getting information stored in that system. This is the best and the most difficult and most of all enjoying because this gives the most thrill.

RISKS IN WIRELESS MEDIUM
The Nature of the Wireless Medium: Traditional wired networks use cables to transfer information, which are protected by the buildings that enclose them. To access a wired network, a hacker must bypass the physical security of the building or breach the firewall.

On the other hand, wireless networks use the air, which is an uncontrolled medium. Wireless LAN signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls. Additionally, since the WLAN medium is airwaves, it is a shared medium that allows any one in proximity to “sniff” the traffic. The risks of using a shared medium is increasing with the advent of readily-available “hacker’s tools.” A variety of specialized tools and tool kits enable hackers to “sniff” data and applications, and to break both the encryption and authentication of wireless data.

Insecure Wireless LAN: Devices Insecure wireless LAN devices, such as access points and user stations, can seriously compromise both the wireless network and the wired network, making them popular targets for hackers.

Insecure Access Points: Access points can be insecure, due to improper configurations and design flaws.

Access points ship with default configurations that are insecure. They are pre-configured with a default
password; they broadcast service set identifiers (SSIDs); and they often require no encryption or authentication. If deployed with default settings, they become gateways that hackers use to access both the wireless and the wired network.

Figure 1 Common Wireless LAN Security Risk

WIRELESS HACKING

Wireless networks broadcast their packets using radio frequency or optical wavelengths. A modern laptop computer can listen in. Worse, an attacker can manufacture new packets on the fly and persuade wireless stations to accept his packets as legitimate. The step by step procedure in wireless hacking can be explained with help of different topics as follows:-

STATIONS AND ACCESS POINTS

A wireless network interface card (adapter) is a device, called a station, providing the network physical layer over a radio link to another station. An access point (AP) is a station that provides frame distribution service to stations associated with it. The AP itself is typically connected by wire to a LAN. Each AP has a 0 to 32 byte long Service Set Identifier (SSID) that is also commonly called a network name. The SSID is used to segment airwaves for usage.

CHANNELS

The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

WIRED EQUIVALENT PRIVACY (WEP)

It is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP. The WEP algorithm is intended to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always transmitted in the clear. WEP uses the RC4 encryption algorithm.

WIRELESS NETWORK SNIFFING

Sniffing is eavesdropping on the network. A (packet) sniffer is a program that intercepts and decodes network traffic broadcast through a medium. It is easier to sniff wireless networks than wired ones. Sniffing can also help find the easy kill as in scanning for open access points that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP, or in telnet, rlogin and ftp connections.

PASSIVE SCANNING

Scanning is the act of sniffing by tuning to various radio channels of the devices. A passive network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner. An attacker can passively scan without transmitting at all.

DETECTION OF SSID

The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Re-association Requests. Recall that management frames are always in the clear, even when WEP is enabled. When the above methods fail, SSID discovery is done by active scanning.

SSIDs advertised to a wireless station

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

**Default SSIDs**

- 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
  1. Enter IP address on your Web browser and provide your user logon name and password
  2. After a successful logon you will see the device’s main window
  3. Click on Wireless button to configure AP options
- SSID
- Wired Equivalent Privacy (WEP) keys
Steps for configuring a D-Link wireless router (continued)

- Turn off SSID broadcast
- Disabling SSID broadcast is not enough to protect your WLAN
- You must also change your SSID

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

The 802.11 standard defines a link-layer wireless protocol and is managed by the Institute of Electrical and Electronics Engineers (IEEE). Wi-Fi is a subset of the 802.11 standard, which is managed by the Wi-Fi Alliance. Because the 802.11 standard is so complex. The Wi-Fi Alliance assures that all products with a Wi-Fi-certified logo work together for a given set of functions. Wi-Fi Alliance defines the “right thing” to do. 802.11 provide wireless access to wired networks with the use of an access point (AP). The 802.11 standard divides all packets into three different categories: data, management, and control. These different categories are known as the packet type.

- Data packets are used to carry higher-level data (such as IP packets).
- Management packets are probably the most interesting to attackers; they control the management of the network.
- Control packets get their name from the term “media access control.” They are used for mediating access to the shared medium.
- Most 802.11 packets have three addresses: a source address, a destination address, and a Basic Service Set ID (BSSID).
- The BSSID field uniquely identifies the AP and its collection of associated stations, and is often the same MAC address as the wireless interface on the AP. The three addresses tell the packets where they are going, who sent them, and what AP to go through.

There are two very different encryption techniques used to protect 802.11 networks: Wired Equivalency Protocol (WEP) and Wi-Fi Protected Access (WPA). WEP is the older, extremely vulnerable standard. WPA is much more modern and resilient. WEP networks (usually) rely on a static 40- or 104-bit key that is known on each client. This key is used to initialize a stream cipher (RC4). Many interesting attacks are practical against RC4 in the way it is utilized within WEP. WPA can be configured in two very different modes: pre-shared key (or passphrase) and enterprise mode.

- The 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
The Architecture of 802.11

- 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 access point (AP) is a station that provides access to the DS
  - Data moves between a BSS and the DS through the AP

Connecting two wireless remote stations

- IEEE 802.11 also defines the operating frequency range of 802.11
  - In the United States, it is 2.400 to 2.4835 GHz
- Each frequency band contains channels
  - A channel is a frequency range
  - The 802.11 standard defines 79 channels
- If channels overlap, interference could occur

Table 11.2 Frequency Band

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Range</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely low frequency (ELF)</td>
<td>30–300 Hz</td>
<td>10,000–1000 km</td>
</tr>
<tr>
<td>Voice frequency (VF) or ultra low frequency (ULF)</td>
<td>300 Hz–3 kHz</td>
<td>1000–10 km</td>
</tr>
<tr>
<td>Very low frequency (VLF)</td>
<td>3–30 kHz</td>
<td>100–10 km</td>
</tr>
<tr>
<td>Low frequency (LF)</td>
<td>30–300 kHz</td>
<td>1–1 km</td>
</tr>
<tr>
<td>Medium frequency (MF)</td>
<td>0.001 Hz–3 kHz</td>
<td>1 km–100 m</td>
</tr>
<tr>
<td>High frequency (HF)</td>
<td>3–30 MHz</td>
<td>100–10 m</td>
</tr>
<tr>
<td>Very high frequency (VHF)</td>
<td>30–300 MHz</td>
<td>100 km</td>
</tr>
<tr>
<td>Ultra high frequency (UHF)</td>
<td>300 MHz–3 GHz</td>
<td>100 km</td>
</tr>
<tr>
<td>Super high frequency (SHF)</td>
<td>3–30 GHz</td>
<td>10–1 cm</td>
</tr>
<tr>
<td>Extremely high frequency (EHF)</td>
<td>30–300 GHz</td>
<td>1 cm–1 mm</td>
</tr>
</tbody>
</table>

COLLECTING THE MAC ADDRESSES

The attacker gathers legitimate MAC addresses for use later in constructing spoofed frames. The source and destination MAC addresses are always in the clear in all the frames.

COLLECTING THE FRAMES FOR CRACKING WEP

The goal of an attacker is to discover the WEP shared-secret key. The attacker sniffs a large number of frames An example of a WEP cracking tool is AirSnort (http://airsnort.shmoo.com).

DETECTION OF THE SNIFFERS

Detecting the presence of a wireless sniffer, who remains radio-silent, through network security measures is virtually impossible. Once the attacker begins probing (i.e., by injecting packets), the presence and the coordinates of the wireless device can be detected.

REFERENCES: