The Growing Phenomenon of Wireless Crime Forensic a Tracing and Tracing

Mr. Kapil Vyas, Mr. Ashish Sharma, Mr. Dalpat Songara.

Assistant Professors

* JECRC/F E & T, JODHPUR, INDIA

Abstract-

The wireless technology use is so widely spread illustrates that its benefits of the technology for now compensate the risks. Now the major bandwidth of the internet is being accessed more by the wireless links without concerning the security. The paper discusses the various aspects of wireless cyber crime with perspective of the venerability, detection and preventions of the malefic intentional use of the technology.

Key Words – Wireless forensic, Hitech Crime ,Wireless security. Wi-Fi threat.

I. Introduction

Currently, it is estimated that 75 percent of the wireless computer networks are vulnerable to attack. However, in spite of this statistic, the fact that wireless use is so widely prevalent illustrates that the benefits of the technology, for now, outweigh the risks.

These risks may become more problematic as the nation's critical IT infrastructure, namely, corporate sector, emergency services, and Government agencies, are becoming more and more tied to the Internet. This leads to an even bigger concern: the Internet is being accessed more and more frequently by wireless links connected to networks with inadequate security, which makes auditing and forensics all the more difficult. To counter or prevent the effects of these types of computer attacks, it is always best for organizations to ensure they are complying with basic network security guidelines. Although convenient and easy to deploy, wireless local area networks (WLANs) require proper planning, training, and an ongoing awareness of the security risks introduced by using wireless devices and networks. In this chapter we're going to cover threats, vulnerabilities, and security solutions related to Wi-Fi, PDAs, and cell

.

Ii Wireless Network Security Threats

The security risks in WLANs extend beyond those in a wired network to include the additional risks introduced by weaknesses in wireless protocols. The security threats posed by WLANs are considered in the following subsections.

Eavesdropping

Intercepting information that is transmitted over the WLAN is generally easier, as it can be done from a considerable distance outside of the building perimeter without any physical network connection. The information intercepted can be read if transmitted in the clear, or easily deciphered if only WEP encryption is used.

Traffic Analysis

The attacker gains information by monitoring wireless transmissions for patterns of communication and data flow between parties, and deciphers encrypted traffic that has been captured. Traffic analysis can result in the compromise of sensitive information.

Data Tampering

The information transmitted over the WLAN can be deleted, replayed, or modified by the attacker via man-in-the-middle attack. This can result in a loss of data integrity and availability.

Masquerading

The attacker gains unauthorized access to the information and network resources within the WLAN or other interconnected network by impersonating an authorized user. The attacker can cause further problems by launching attacks or introducing malicious code that can disrupt operations.

DENIAL -OF-SERVICE (Dos)

The attacker can jam the entire frequency channel that is used for wireless data transmission using a powerful signal generator, microwave, or a massive amount of broadcasted network traffic from a rogue wireless device. With high-gain antennas and WLAN attack tools, the perpetrator can cause denial-of-service without being close to the targeted WLAN, and although it is not impossible to direction-find (DF) the perpetrator, it is difficult and requires tools that are only now becoming available.

Wireless Client Attacks

The attacker can potentially gain access to the information shared or stored in the wireless client when it is connected to an unprotected ad hoc WLAN or an untrustworthy third-party WLAN. Additionally, the compromised wireless

client can potentially serve as a bridge to the internal network, thus allowing a perpetrator to gain access to or launch attacks against the internal corporate network and its resources.

OTHER ISSUES

Spread Spectrum Isn't Very Secure

Several of the 802.11 wireless LAN standards use spread spectrum, which is a modulation technique developed to prevent radio jamming. Spread spectrum, in general, is capable of changing the "spreading codes" in a way that makes decipherment impossible without knowing the correct codes. Wireless LAN vendors today still advertise the security that spread spectrum provides. This would be fine except that the 802.11 standard describes the spreading codes publicly so that companies can design interoperable 802.11 components. This means that a hacker or intruder would only need an 802.11-compliant radio NIC as the basis for connectivity, which nullifies the security benefits of spread spectrum

.Ssids ARE NOT DESINED AS PASSWORDS

The Service Set Identifier (SSID) is the name of a WLAN. All wireless devices on a particular WLAN must use the same SSID to communicate with each other. SSIDs were first introduced as a way to prevent people from connecting to the access point (AP) without foreknowledge of the SSID, which has now been incorporated into every AP as "Disabling broadcast SSID." So SSIDs serve a very useful function — identification of the AP or network; however, it should not be relied upon as a password.

WEP IS WEAK

The Wired Equivalent Privacy (WEP) protocol was designed to add security to WLANs. WEP was intended to give wireless networks the equivalent level of privacy of a comparable wired network. However, WEP occasionally produces typologically weak ciphers that are easily broken with modern tools. A step-by-step description of how the WEP protocol is cracked follows, to give you a better idea of the weakness of WEP and the speed with which it can be compromised:

1.A hacker runs Kismet, a wireless LAN discovery tool, to determine what wireless LANs are in the area. When the hacker discovers the SSID, the channel number it is operating on, and its BSSID (Basic Service Set Identifier—its Ethernet address), he has all the information needed to mount an attack to recover the WEP key.

2. If the SSID is unknown because the WLAN's owner has enabled mode that hides it (known as SSID Cloaking or SSID Broadcast Disable), the hacker can discover the SSID by waiting for a client to connect, in which case both the client as well as the AP disclose the SSID. Or the hacker can obtain the SSID by forcing an already connected client to disconnect and reconnect. This is done by sending a specially crafted packet pretending to be from the AP that tells the receiving client that it is no longer authenticated. The client has no way to tell that this is not actually coming from the AP, and so it attempts to rectify the problem by disconnecting from the AP and reconnecting, yielding the SSID in the process.

3. The hacker puts his wireless card into a monitor mode" in which the WLAN card eavesdrops on a WLAN without having to connect to it. He commands the WLAN card to monitor the channel on which the target AP is located, and begins capturing and saving all of the traffic monitored from that AP to disk in a file called a capture file.

4. The software used to capture the data notes the reception of packets encrypted with a weak Initialization Vector (IV), which in cryptography is a value used to initialize a cryptographic process. WEP misuses these IVs in an exploitable way, and when a certain number of weak IVs have been captured, the WEP key can be determined. Roughly 125,000 packets are required to crack most 40-bit WEP keys, and 200,000–250,000 packets for a 128-bit WEP key.

5. On a slow WLAN, capturing the requisite number of weak IVs can take some time. To accelerate the attack, the hacker will next inject a captured WEP frame back into the network to generate more traffic. This takes advantage of the fact that WEP has no "replay protection" mechanism to prevent this. An injection rate of 512 packets per second generally results in the required number of IVs being captured between 10 min for 40-bit and 30 min for 128-bit WEP. If no client is present on the WLAN to generate traffic that can be captured and reinjected, in most cases the attacker's own system can be made to do so.

6. After a sufficient number of IVs is captured, the hacker runs the AirCrack tool, which will attempt to crack and disclose the WEPkey.

7. Once the WEP key is known, the hacker can connect to the AP just as a legitimate client would — and the WLAN owner would be none be wiser.

WAR-DRIVING

War-driving is derived from the war-dialing exploits of the teenage hacker character in the 1983 movie War Games, who has his computer randomly dial hundreds of numbers. He eventually winds up tapping into a nuclear command and control system! With the growth of the Internet, scanning was the next version of this type of exploit. People often scan through large numbers of IP addresses looking for computers that are running certain types of servers.

The wireless age has introduced a new type of attack called war-driving.

Originally, war-driving was when crackers drove around in a car equipped with wireless gear looking for unsecured wireless networks to gain illicit access to. Over time, the term has evolved to include harmless types like us simply checking on the radio frequency (RF) environment.

- THE BASIC WAR-DRIVING KIT
- The basic kit consists of the following:
- Laptop computer

- Wireless NIC
- Antenna (optional)
- Software
- GPS unit (optional)

Why Are People War-Driving?
There is no clear answer to this question, because the act of war-driving can have so many different motivations. Technology is not bound to ethics. It is the application and use of that technology that brings ethics into it.
If someone is simply driving around a city searching for the existence of wireless networks, with no ulterior motive, it cannot be deemed illegal. However, if you are searching for a place to steal Internet access, or commit computer crimes, then war-driving is considered malicious and could be treated as such in court. Also remember that in the United States, simply receiving radio transmissions on the cellular telephone frequencies (895–925 MHz) is illegal.

A key differentiator here is that cellular interception takes place with equipment exclusive to the normal process of service, i.e., you don't use a cell phone to intercept someone else's call, you use a scanner. War driving (and wireless sniffing) uses the same equipment that you'd use to participate in a WLAN as a normal user. Further, because you have the right to monitor your own network, making monitoring tools illegal would certainly be questionable, especially in light of the current thinking that perhaps companies ought to be held liable for malicious activity occurring through their inadequately secured WLANs.

War-Chalking
War-chalking actually started out as something else. It was a secret sign language once used by hobos to alert fellow travelers of dangers or opportunities for food and work on the open road. Today, war-chalking is an extension of war-driving, in which people use chalk to place a special symbol on a sidewalk or other surface that indicates a nearby wireless network, especially one that offers Internet access.

War Flying
In yet another flavor of war-driving that has emerged in recent years, hobbyists are now taking their skills to the air. The term is appropriately named war flying and those using this technique are detecting hundreds of wireless LAN APs during short trips in private planes cruising at altitudes between 1500 and 2500 ft. On one war-flying tour over an area of San Diego County, a private plane detected 437 APs. Detection of so many APs is due to the increased range that wireless networks can broadcast upward because of lack of obstructions. However, the limit is currently around 2500 ft because most WLANs are vertically, not horizontally, polarized, and so most of the RF energy goes out parallel to the Earth's surface.

War-Driving And War-Chalking Ethics
In the previous subsections we have covered war-driving, war flying, and war-chalking; however, when we look beyond the definitions and techniques, we get into the ethical issues of these activities. Three questions come to mind:
1. Is it theft?
2. Is it harmful?
3. Is it stoppable?

Is It Theft?
According to the standard definition, theft is defined as "the felonious taking and removing of personal property with intent to deprive the rightful owner of it" Although war-chalking and war-driving activities identify and mark wireless networks, they do not remove or deprive the owner of his or her wireless connectivity. However, if common sense prevails here, this would be considered theft.

Wireless Crime Prevention Technique

In this new century we are entering a new age of policing, an age in which wireless technology will play a key role. Traditionally, police work has involved interviewing the public, searching the houses of suspects, and putting them under surveillance to discover whom the suspect was in touch with, where they traveled, etc. Today, in many cases, these techniques would reveal very little. In the future it will be far more useful to look at surveillance videos, review the suspect's e-mail and computer hard drive, and most importantly, gain access to cellular records as they will show where the suspect was and whom they were in contact with.

Is It Harmful?
War-chalking is only a process of identifying networks. It would be similar to going around a neighborhood and somehow making marks on public property identifying houses with weak security.

Is It Stoppable?
Not really, unless you are planning on installing lead walls. Owners of wireless networks can modify or shield their equipment, but it is by no means fool proof.

Proactive Measures
Now that we've seen an example of what's possible, let's look at some steps that can be taken to help protect a wireless network. In this section and the one that follows, we will cover some tools and best practices that will allow you to be proactive with our security. By using the same tools that hackers use to penetrate your network, you can to find and plug security holes beforehand. This combined

with using established security practices and policies, can help deter or prevent intrusions.
Tools for wireless networks:

Wlan Discovery Tools
- Netstumbler — Versions for Windows and Linux
- Kismet — Linux
- MacStumbler — Mac OS
- MiniStumbler — Pocket PC
- Mognet — Java

Wireless Network Sniffers
- AiroPeek — Windows
- AirTraf — Linux
- Ethereal — All OSs
- Sniffer Wireless — Windows and Pocket PC
- BSD AirTools — BSD

Wep Cracking Tools
- WEPCrack — Linux
- AirSnort — Linux
- BSD-Tools dweputils — BSD
- AirCrack — Linux and Windows
-

IV COMMON WI-FI SECURITY RECOMMENDATIONS: ACTIONS VERSUS REALITY

In the previous section we looked at some tools that will help you find out more about your wireless network and the information traveling across it. In this section we will take a closer look at what is commonly recommended
when securing wireless, and how effective those recommendations really are.

Recommended action: Turn SSID broadcasting off.Reality: Several software tools (such as Kismet) exist that will discover the SSID when a client connects — and common hacker tools can force a user to reconnect to the AP at will — thus giving up the SSID. In reality, this measure stops only two commonly used WLAN discovery tools from finding a WLAN, namely, Netstumbler and Windows XP.

Recommended action: Utilize static IP addresses.
Reality: Static IP address pools can be found quickly through simple traffic analysis, much quicker than you can eliminate DHCP from your network.

Recommended action: Turn 128-bit WEP encryption on.
Reality: WEP can be cracked in tens of minutes in essentially every case.

Recommended action: Change WEP keys periodically.
Reality: New WEP keys can be cracked just as quickly as old ones.

Recommended action: Enable MAC address filtering.
Reality: Simple traffic analysis will yield the authorized MAC addresses (which, after all, are the only ones passing traffic over the network). Because MAC addresses can be specified by a hacker for his WLAN card, this has no real security benefit. In fact, this "security tip" offers essentially zero security while requiring great effort to implement.

Recommended action: Utilize shared key authentication.
Reality: Again, WEP can be cracked quite rapidly.

Recommended action: Use personal firewalls.
Reality: A good idea to prevent anyone who does manage to connect with the AP from communicating with your mobile device and potentially obtaining data or doing harm. However, because attacks exist that fool the mobile device into believing that a hacker's system is a trusted one, this is not a panacea.

Recommended action: Administer wireless devices using secure protocols like SSH or HTTPS, instead of telnet or http. With the tunnel in place, anyone who tries to monitor the conversation between your laptop and the mail server will get something resembling line noise.
Reality: Unless the hacker is able to perpetrate a man-in-the-middle attack. SSH and HTTPS have been found vulnerable in the past to man-in-the-middle attacks in certain circumstances; wireless connections are easier to exploit in this regard than wired ones.

V. Personal Digital Assistants
Pda Threats And Vulnerabilities

Mobile Device Attacks
Although attacks on mobile devices are not as widely published or as prolific as the viruses and worms that infiltrate network security defenses, they do exist and can be equally dangerous. The open handheld operating systems are often left insecure, making the device highly susceptible to a variety of attacks. Some common attacks include: copying or stealing information from the device, loading malicious code onto the device, or destroying key files or applications on the device.

How A Pda Connects To Other Computers
A PDA connects to other computers by one or more of the following methods:

- Desktop synchronization
- Hardwired network interface card
- Wireless network interface card
- Bluetooth
- Wi-Fi

Viruses, Trojans, And Worms
As with desktop and laptop computers, PDAs and the programs they run can be vulnerable to malicious code, which include:

- Trojans: A program disguised as another program.
- Worms: Stand-alone programs that make full, running duplicationsof themselves, stealing system resources.

- Logic bombs: Programs within programs that perform destructive acts based on a trigger event.

One of the first reported wireless viruses was called Phage and was aimed at the Palm OS, back in 2000. Viruses depend on the type of PDA OS you are running. PDAs are also more likely to be a carrier of a virus than the actual target of an attack; however, this is probably of little comfort after a PDA has been synced with a workstation or worse, an enterprise.

Theft Of The Pda Device
PDAs and BlackBerrys are clearly more at risk for theft because of their size and weight. It's much easier to lift a device designed to go into your pocket as opposed to one that's not. The devices are often the main interest of the thief as they are typically worth a higher price tag despite their small size. However, this will not always be the case because as the data capacity and battery life increase, the data that resides on the device will interest the average thief.

Data Theft
Again, thanks to the portability of these devices and their ability to hold, in some cases, a variety of memory expansion cards, it often doesn't take much time for someone to quietly download all of your information to a removable flash card.

Mobile Code Exploits
Mobile code is software that is transmitted across a network from a server or other remote source to a local system and is then executed on that local system. Often, this is done without direct action by the user. This code may have flaws that can allow an attacker to compromise a PDA.

Authentication Theft
The theft of the device can also result in the theft of authentication information, which can allow access into additional resources or a larger network.

Dos Attacks
A DoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In the instance of a PDA, everything from a mobile code exploit to the theft of the actual device constitutes a DoS.

Session Hijacking
Session hijacking is when someone takes over a TCP session between two machines, or in this case, a PDA and another PDA or network. Most authentications only occur at the start of a TCP session, allowing the hacker to gain access to the PDA or its host network.

Vi Pda Security

Anti-Virus Software
As with workstations and servers, running an anti-virus program on your PDA will help reduce the risks of data loss or corruption, and help prevent your PDA from being a target of attack when it syncs to a computer or network. Norton, Symantec, F-Secure, and Kaspersky all produce PDA anti-virus products.

Other Pda Security Measures
The following are important PDA security measures:

- Database security and authentication
- Faraday bag (which blocks all wireless signals to the device)
- Encryption — Ccrypt, PDA Secure (TrustDigital)
- Firewalls — Mobile Firewall Plus
- Password enforcement — HotSync security, PDA Defense
- VPN — VPN 3000 (Cisco), MovianVPN

Combating Handheld Attacks
As we've seen, mobile device platforms have their own set of threats and vulnerabilities. These pose unique challenges to security administrators. Every mobile user and mobile enterprise needs to carefully evaluate its own device-side security needs.

The following best practices, from Bluefire Security Technologies, Baltimore, Maryland, provide a basic guide to begin the process:

1. Define handheld security policy
2. Centrally enforce and monitor handheld security
3. Enforce use of power-on passwords
4. Block unauthorized handheld network activity
5. Detect handheld intrusions
6. Protect handheld integrity
7. Encrypt sensitive data stored on handhelds
8. Protect traffic sent/received by handhelds
9. Maintain up-to-date anti-virus protection
10. Back up frequently

Vi. Wireless Network Security Threats
The security risks in WLANs extend beyond those in a wired network to include the additional risks introduced by weaknesses in wireless protocols.
The security threats posed by WLANs are considered in the following subsections. Eavesdropping Intercepting

information that is transmitted over the WLAN is generally easier, as it can be done from a considerable distance outside of the building perimeter without any physical network connection. The information intercepted can be read if transmitted in the clear, or easily deciphered if only WEP encryption is used. Traffic Analysis The attacker gains information by monitoring wireless transmissions for patterns of communication and data flow between parties, and deciphers encrypted traffic that has been captured. Traffic analysis can result in the compromise of sensitive information.

E911
E911 is a location technology promoted by the FCC that will enable mobile, or cellular, phones to process 911 emergency calls and enable emergency services to locate the geographic position of the caller.

When a person makes a 911 call using a land line, the call is routed to the nearest public safety answering point (PSAP), which sends the emergency call to the proper service, such as the police, the fire department, etc. The PSAP receives the caller's phone number and the exact location of the phone call. This is how things would work if you were calling from a landline.
But what about mobile phones?

Before 1996, all 911 calls made using a mobile phone would have toaccess their carriers first. The carrier would then have to verify subscription
of service. Once verified, the call would be routed to a PSAP. The FCC refined this process, and ruled that all 911 calls must go directly to the PSAP without receiving subscription verification from the cellular carrier.
Intrado of Longmont, Colorado, is a company that provides 911 solutions for wireless cellular carriers. Intrado has so far deployed Phase 1 of the E911 directive, which identifies the cell site from which a cellular call originates. More than 190 million 911 calls are placed annually, and almost 50 million of those are made from wireless phones.

Police Use Of Wireless Devices
The police and law enforcement forces have used the radio for decades. The maxim "You can't outrun a radio" when referring to a car chase with the police is just one small example. Today, police and law enforcement officials are using some newer programs that surpass the traditional radio.

Packetcluster
PacketCluster Patrol software allows patrol cars direct access to crime fighting information from a car-based laptop. This technology is in practical use in Salinas and Monterey County in California. Using a wireless network, more than 400 patrol officers can access records from county, state, and federal databases.

Totalroam
TotalRoam is another in-vehicle platform that is designed to manage data routing for wireless network communications. TotalRoam allows highway patrol officers to use the wireless system to instantly and directly access critical information from databases covering vehicle registration, outstanding warrants, and much more. TotalRoam will also enable the wireless transmission of information gathered by other onboard equipment, such as breathalyzers and GPS. Another significant quality of TotalRoam is its redundancy. Its multiple networking design guarantees continual communication, ensuring that during emergency situations officers will always have backup.

Hi-Tech Patrol Cars
In the Sacramento Police Department, all 190 police cars are being fitted with wireless IP networking equipment and onboard computers, allowing each officer to access any database the department would normally have access to. SACPD cars will also be fitted with equipment to allow them to view live video feed from police helicopters. This will help officers make much better decisions during a chase, as well as aid superior officers in making more informed decisions in, for example, hostage situations.
SACPD is also working toward moving to a paperless, or paper reduced, system by giving officers wireless PDAs to streamline the paperwork
process. Additionally, these systems will eventually be integrated with the electronic tagging systems used by the judicial and prison services.

Wireless Honeypots
To quote Lance Spitzner, the leader of the Honeynet Project, the definition of a honeypot is:
A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

A wireless honeypot, used properly, could reveal pertinent and accurate statistics about attacks on your infrastructure, including:

- The frequency of attacks
- The attacker's skill level
- Goals and methods

Wireless honeypots, similar to their wired counterparts, can help protect your networks by diverting the attacker's time and resources on fake targets. In the black hat community, hackers enjoy penetrating wireless networks for the following reasons:

- They are somewhat safe, because the attacker isn't directly connected to the network.
- They are easy to hack, because there are a huge number of open or unsecured access points (APs) around.
- They are fun to attack, because the wireless network is still considered relatively new.
- They allow for a great deal of anonymity.

Vii Wireless Crime Prevention Techniques

In this new century we are entering a new age of policing. An age in which wireless technology will play a key role. Traditionally, police work has involved interviewing the public, searching the houses of suspects, and putting them under surveillance to discover whom the suspect was in touch with, where they traveled, etc. Today, in many cases, these techniques would reveal very little.

In the future it will be far more useful to look at surveillance videos, review the suspect's e-mail and computer hard drive, and most importantly, gain access to cellular records as they will show where the suspect was and whom they were in contact with.

Viii Conclusion

Crime is also evolving in many ways and adapting to newer technologies. Criminals are among the early adopters of new technologies and emerging platforms. Crime is here to stay in the wire-free world. The extortionist, criminal or murderer who in the past sent a threat message by sticking letters cut out from newspapers on a sheet, now prefers sending a text message while spoofing the mobile number to avoid identification and tracing.

References

[1]. Wireless Crime and Forensic Investigation (Auerbach, 2007).
[2]. Cyber Crime Investigations - A. Reyes (Syngress, 2007).
[3]. Investigating Computer-Related Crime - a Handbook for Corporate Investigators (CRC, 2000)
[4]. Farely, T., Basic Wireless Principles, Privateline.com, January 3, 2006.
[5]. Galeev, M., Home networking with Zigbee, Embedded.com, April 2004.
[6]. Reed T., War Chalking, Airshare.org, November 2003.
[7]. Tyrrell, K., An Overview of Wireless Security Issues, SANS Institute, 2003.