Mobile And Digital Forensics

Satvik Gupta

April 6, 2023

Contents

Risks Created By Wireless Technology

1. Wireless is shared and uncontrolled.
2. Mobile devices are transient. They are always moving around. Detecting suspicious activity becomes difficult.
3. Ease of use - As wireless is easy to use, people become familiar with it and become comfortable and careless with security.
4. It's easier to attack.

Wireless Technologies in Use

PAN (Personal Area Network)

- WPANs are used in short distances, <10 m.
- Connect computers and peripherals
- High speed

Bluetooth

Infrared

- Line of sight
- Short range (0-2m)
- LoS makes it easy to think it's secure, but attackers can detect reflected light and filter out ambient noise, and gain access to the data.

Ultrawideband (UWB)

- Superfast, wireless.
- Doesn't use any carrier wave.
- Superfast pulses in timed sequences over a large continuous spectrum

ZigBee

- Home Area Network
- Designed to replace remote controls
- Cost effective, low power

Wireless USB

- 10m range
- 480 Mbps, upto 1 Gbps in future.

LAN

Wireless Local Area Networks

802.11

- AKA Wifi
- 1-2 Mbps, 2.4 GHz

900 MHz Packet Radio

- Cordless, pagers, medical equipment.
- Interference sometimes happens
- Transports IP based data.

MAN

A Metropolitan Area Network is designed to provide broadband connectivity to a densely populated area. Could be cities, counties, campuses. AKA *Last Mile Solutions.*

Microwave

- P2P,LoS
- AM Radio
- Less cost, Easy to Deploy
- High frequency

Free Space Optics

- Uses lasers instead of radio frequency
- High data rates
- Incorporates security of Fiber optic cables
- Transmits a LoS laser btw two points.

Ricochet

- Wireless ISP network solution for a particular geographic location
- Allows portable clients to move through an area and access Internet

WiMax

Worldwide Interoperability for Microwave Access, 802.16

- 2-11 GHz
- Long range
- High throughput ~70 Mbps

WANs

WANs are intended for communications between mobile and fixed devices worldwide.

Satellite

Use radio waves just like other wireless technologies. TElevision, GPS< ISPs, etc.

Cellular

- Cellular Digital Packet Data (CDPD)

  Uses unused cellular channels to transmit data packets.

- Global System for Mobile Comm. (GSM)

  Uses narrow band TDMA method to allow 8 simultaneous calls on the same radio frequency.

- 3GSM

  Will support multimedia, video, and Internet

- TDMA

  Each cellular channel is divided into 3 time slots to increase amount of data.

Blackberry

Email, File sharing, Voice and SMS, Calendar, Internet, Attachments, etc. btw Blackberry users.

Paging

SMS

Wireless Network Security Threats

Eavesdropping

Someone else can read the transmitted information, even from outside the building.

Traffic Analysis

Patterns of communication and data flow can be monitored and may yield information.

Data Tampering

Information can be deleted, or modified via MITM attack.

Masquerading

Attacker can impersonate an authorized user and gain access to information.

Denial of Service (DoS)

Attacker can jam frequency channels, using hardware blockers or by sending large amount of requests.

Wireless Client Attacks

Attacker can trick clients into connecting to an unsecured network and gain access to the data present on the client machine. The compromised client can now also be used to access the internal network and the data stored on it.

Other Issues with Wireless

Spread Spectrum isn't Secure

Spread Spectrum is a modulation technique used to prevent radio jamming.

In general, spread spectrum has **spreading codes**, that can be changed. Without knowing the correct code, it is impossible to decipher data sent through the spread spectrum.

However, the 802.11 standard publicly describes the spreading codes so that interoperable 802.11 components can be created. An attacker with a radio compliant with 802.11 would be able to connect.

SSIDs are not designed as passwords

SSID - Service Set Identifier.

- Were initially used to prevent people from connecting to the access point (AP) without knowing the SSID.
- However, they should not be relied upon as passwords.

WEP is weak

Wired Equivalent Privacy.

WEP occasionally produces cryptographically weak ciphers.

Steps to attack WEP.

1. Hacker runs Kismet to discover WLANs in the area. He gets its SSID, channel number and its BSSID (Basic SSID - the Ethernet Address).
2. APs can hide their SSIDs, using an option called SSID Cloaking/SSID Broadcast Disable.

   If this is the case, the attacker has to wait for a client to connect to the AP (the client and the AP will both disclose the SSID). The attacker can also force an already connected client to reconnect. This is done by sending a packet to the client, pretending to be from the AP. The packet tells the client that they have lost their connection with the AP (***You are no longer connected***). The client attempts to reconnect, and exposes the SSID.
3. The attacker puts his wireless card into Monitor mode. The card will eavesdrop on the WLAN (even without connecting to it.) He makes the card monitor the channel on which the target AP is. All the traffic monitored is saved in a *capture file.*
4. WEP uses Initialization Vectors (IVs), which are values used to start a cryptographic process. When a certain number of weak IVs have been captured, we can determine the WEP key. 125k packets are needed to crack 40-bit WEP keys. 200-250k packets for 128-bit WEP keys.
5. If the WLAN is slow, the hacker will need to accelerate the attack to capture the right amount of weak IVs. The attacker will inject already captured WEP frame back into the network. WEP has no replay protection mechanism.

   512 packets injected per second - 10 mins for 40-bit keys, 30 mins for 128-bit keys.
6. After sufficient amount of IVs are captured, the attacker runs AirCrack, which will attempt to crack and return the WEP key. Once the key is known, the attacker can connect to the AP in the same way a legitimate client would.

War Driving

People driving around in a car equipped with wireless gear, looking for unsecured wireless network. Generally they try to look for APs that are running a certain kind of server behind them, such as important security servers or financial servers, etc.

Sometimes people just do it harmlessly, for e.g, just checking the radio environment.

War Chalking

War driving + marking the places with chalk. Different symbols are used for open, closed, and WEP APs.

War Flying

War driving, but using airplanes,helicopters, etc. instead of cars. Due to increased range of wireless networks, hundreds of APs can be found in a short trip.

Security Recommendations vs Reality

Recommendation	Reality
Turn SSID Broadcasting off	SSIDs can be easily discovered as described above.
Use static IP Addresses	Static IP addresses can be found easily using traffic analysis
Turn 128-bit WEP on	WEP can be easily cracked
Change WEP keys	New keys can be cracked easily
Enable MAC Address Filtering	Traffic analysis will yield the authorized MAC Addresses. WLAN cards can specify their own MAC Address, so hackers can just claim to be using an authorized one
Utilize shared key auth	WEP keys can be cracked
Use personal firewalls	Hackers may be able to fool you that they are a trusted system
Use SSH/HTTPs	May be vulnerable to MITM sometimes

PDA (Personal Digital Assistants)

Common attacks:

1. Copying/Stealing information from the device
2. Loading malicious code onto the device
3. Destroying key files or applications on the device

Trojans

A program disguised as another program.

Worms

Programs that duplicate themselves over and over, and steal system resources in doing so.

Logic Bombs

Programs within programs that perform certain actions based on a trigger event. PDAs can also be carriers of such programs instead of the target.

Theft of the Device

Data Theft

Data can be easily copied from a PDA/Blackberry to a flash card within minutes.

Mobile Code

S/w transmitted from server to a local device, and then executed. This code may give the attacker access to the data on the PDA.

Auth Theft

Stealing a PDA may lead to auth information being stolen.

DoS Attacks

Any attack in which an organization is denied access to a resource can be termed DoS. For PDAs, anything from mobile code to device theft can be considered DoS.

Session Hijacking

A TCP session can be taken over by an attacker. TCP auth only occurs during the start, so an attacker can find ways to do this.

Providing Security to PDAs

- Use AntiVirus - Norton, Symantec, F-Secure, Kaspersky
- DB Security and Auth
- Faraday Bag - Block all wireless signals to the device
- Encryption - Ccrypt, PDA Secure
- Firewalls - Mobile Firewall Plus
- Password Enforcement - HotSync Security, PDA Defense.
- VPN - VPN 3000, Movian VPN

Best Security Practices

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