# Attacks on wireless networks

IT 220 | Wireless Networks

Daniel Rajaram

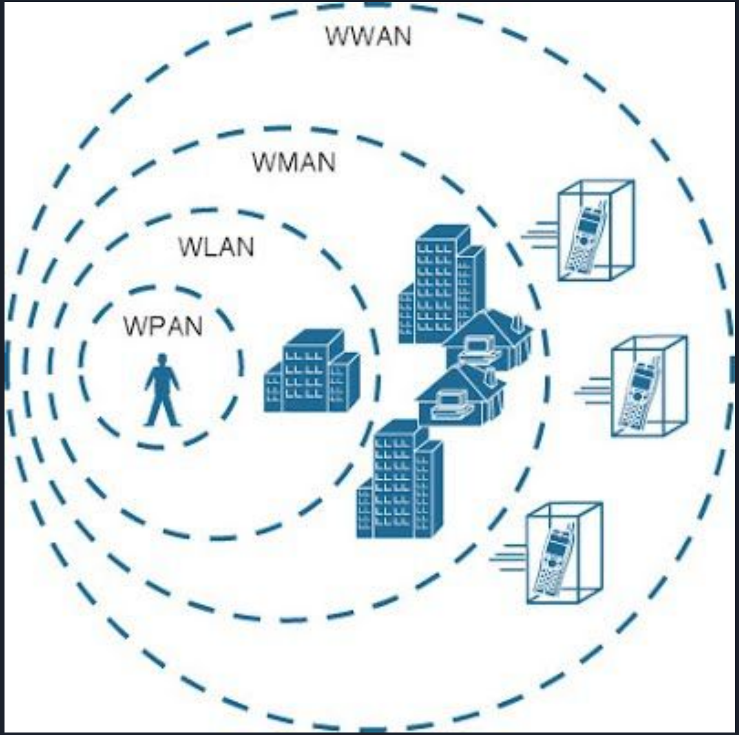
Professor: Dr. Robert Statica | Course: IT220

# Table of contents

- Attacks on wireless networks
- Types of wireless networks
- What is a wireless network attack?
- Types of attacks on wireless networks
- Wireless security and attacks
- Social engineering attacks
- How dangerous are wireless network attacks?
- Some examples of big wireless network attacks?
- Protection against and responding to wireless attacks

# Types of wireless networks

- Wireless personal area networks (WPAN)
- Wireless local area networks (WLANs)
- Wireless metropolitan area networks (WMAN)
- Wireless wide area networks (WWAN)



# What is a wireless network attack?

- Capturing information sent and received across a network
- Spy and gather data within the traffic of a network system
- Malicious intents such as stealing passwords and sensitive information
- Jamming and disrupting networks as a form of interference

# Types of Attacks on Wireless Networks

- Three Main types of attacks on wireless networks:
  - Attacks on enterprise organizations
    - Reading data, hijacking wireless connection, inserting traffic, denial-of-service attacks.
  - Attacks against mobile users
    - Evil Twin, Bluejacking, Read unencrypted transmissions, ad-hoc connection
  - Attacks against home users
    - Steal data, Read wireless transmissions, inject malware, download harmful content

# Attacks on Enterprise Organizations

- Reading data:
  - Most common attack, the attacker reads any confidential data that is being transmitted from open or misconfigured AP.
- Hijacking Wireless Connection:
  - Using an evil twin AP which is a way to trick corporate mobile devices to connect to imposter. Once connected Man-in-the-middle device receives data and passes it to recipient so neither devices are aware.
- Inserting Network Traffic:
  - Used to data packets to match specific applications or inject packets into network that will redirect traffic to an attackers server.
- Denial of Service (DoS):
  - An attack to prevent a device access to its normal functions. IEEE 802.11 is exploited because there is no verification requirement of source identity, attacker can pretend to be trusted client.

# Attacks Against Mobile Users

- Evil Twin
  - Public environment is filled with wifi networks and tricking victims into thinking they are connecting to a safe/reliable network instead of a compromised one.
- Bluejacking
  - Used for sending unauthorized/comprised data between bluetooth devices, usually on mobile devices.
- Ad-hoc connection
  - Additional hop or man-in-the-middle attack between mobile device and AP or other gateways.

# Attacks Against Home Users

- Steal Data:
  - Packet Sniffing is used like an Inserting Network Traffic attack where the attacker uses software or hardware to search for specific data in packets like, log-in credentials, account information ect.
- Download Harmful Content:
  - The famous trojan horse virus is an example of injecting malware into a home computer.
  - Fake applications or software disguised as legitimate applications can be used to corrupt important files.

# Social Engineering Attacks

- Social engineering is another major way that attacks can take place
- They involve more psychological tricks in order to fool an end user into making their network vulnerable
- There are different types of attacks that qualify as social engineering
    - Phishing
        - Involves making a victim click a link, typically distributed via email
    - Scareware
        - Tries to scare the end user into installing some fake software, with the pretense that if they don’t their computer could be destroyed with malware
    - Spear phishing
        - Involves infiltrating a network/enterprise
        - Involves impersonating someone at an enterprise in order to try and trick someone into opening a malicious link/file, typically also through email

# WEP-based attacks

- WEP has been considered extremely insecure for a while now
- A WEP-protected network can now usually be cracked in under a minute
- Key lengths are short and limited to hexadecimal characters which enables easy brute forcing
- Uses a static master key that can also be easily guessed
- Dynamic WEP was also available but easily cracked as well

# WPA-based attacks

- Created as a temporary solution to WEP, but cracked soon after
- Most devices only supported WPA with TKIP
- TKIP was heavily vulnerable to dictionary attacks
- AES was technically available but support was optional, not many devices supported it
- Industry moved to WPA2 soon after which mandated AES support

# WPA2-based attacks

- One attack that affects WPA2 is sniffing and decrypting traffic
- Attacker must know the PSK in order to do this
- After capturing the handshake, attacker can apply PSK and use sniffed session key to decrypt traffic
- Does not generally affect WPA2-Enterprise due to users usually having their own logins via EAP
- Easy to accomplish as long as the attacker has the PSK
- Solved by WPA3 using SAE

# WPA2-based attacks

- Another attack that affects WPA2 is KRACK
- Replay-based MITM attack
- Attacker does not need to know PSK
- Affects all WPA2 standards, including WPA2-Enterprise
- Achieved by exploiting and replaying part of the WPA2 handshake
- Not as easy to accomplish, but definitely possible
- Can usually be mitigated by keeping a device up to date or using WPA3

# How dangerous are wireless network attacks?

- Depending on the attack, the level of danger depends
- Based on many different factors
    - How easy is it to perform the attack
    - What is the scope of the attack?
    - Does it require other user interaction?
- Can be measured using a CVSS score
    - This is a rating on how severe certain network attacks are, and is based on a multitude of factors
- How does this rating work?

# CVSS Scoring System

- Framework maintained by Forum of Incident Response and Security Teams(FIRST)
- Has many different scoring pieces
- Exploitability
  - How exploitable is the attack?
- Scope
  - How much of the network does the attack effect?
- Impact
  - What is the outcome of the attack?
- There are also other components that help to balance the score
  - Temporal metrics measure how mature the attack is
    - The more mature the attack is the greater the chance of it being patched
  - Environmental metrics measures the actual importance of the data being breached
    - If the data isn’t important, the overall score drops

# Types of protections

- Access control
  - Granting or denying approval to use specific resources
- Wired equipment privacy (WEP)
  - Guard the confidentiality of data
  - Ensured only authorized parties can view it
- Authentication
  - Process in which access points accepts or rejects a wireless devices

# Some ways to minimize risks to wireless networks

- Change default passwords
- Restrict access
- Encrypt data on the network
- Protect service set identifier (SSID)
- Install firewall
- Maintain antivirus software
- Use file  sharing with caution
- Keep access points software patched and uptodate
- Check internet provider’s or router’s manufacturer wireless security options
- Connect using virtual private network (VPN)

# Citations

- EC-Council. “What Are Sniffing Attacks, and How Can You Protect Yourself? .” Cybersecurity Exchange, 12 June 2022, https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-sniffing-attacks/#:~:text=A%20sniffing%20attack%20occurs%20when,login%20credentials%2C%20and%20financial%20information.
- “Key Reinstallation Attacks.” KRACK Attacks: Breaking WPA2, https://www.krackattacks.com/.
- McAfee. “What Is a Trojan Horse?” McAfee Blog, 8 Sept. 2021, https://www.mcafee.com/blogs/internet-security/trojan-horse/.
- Okta Updated: 07/26/2022 - 3:43 Time to read: 6 m, and Okta. “Wired Equivalent Privacy (WEP): Definition & Risks.” Okta, https://www.okta.com/identity-101/wep/.
- “Security Tip (ST05-003).” CISA, https://www.cisa.gov/uscert/ncas/tips/ST05-003.
- Security, Panda. “What Is an Evil Twin Attack?” Panda Security Mediacenter, 13 Dec. 2021, https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/.
- “What Are CVSS Scores.” Balbix, 4 Aug. 2022, https://www.balbix.com/insights/understanding-cvss-scores/.
- “What Is Social Engineering: Attack Techniques & Prevention Methods: Imperva.” Learning Center, 29 Dec. 2019, https://www.imperva.com/learn/application-security/social-engineering-attack/.