# Network Penetration Testing

**Prof. Anthoniraj Amalanathan**

# Wireless Networks

- The wireless technologies of today are defined by the IEEE. The original wireless standard is IEEE 802.11.
- Modern wireless technologies used in corporations and home networks today,
- 802.11a - operate in the 5 GHz band. Speed up to 54 Mbps.
- 802.11b – operate at 2.4 GHz. Speed up to 11 Mbps.
- 802.11g – de-facto standard in most environments today. operate at 2.4 GHz. Speed up to 54 Mbps.

| Generation | IEEE standard | Adopted | Maximum link rate (Mbit/s) | Radio frequency (GHz) |
|---|---|---|---|---|
| Wi-Fi 7 | 802.11be | (2024) | 1376 to 46120 | 2.4/5/6 |
| Wi-Fi 6E | 802.11ax | 2020 | 574 to 9608 | 6 |
| Wi-Fi 6 | | 2019 | | 2.4/5 |
| Wi-Fi 5 | 802.11ac | 2014 | 433 to 6933 | 5 |
| Wi-Fi 4 | 802.11n | 2008 | 72 to 600 | 2.4/5 |
| (Wi-Fi 3)* | 802.11g | 2003 | 6 to 54 | 2.4 |
| (Wi-Fi 2)* | 802.11a | 1999 | 6 to 54 | 5 |
| (Wi-Fi 1)* | 802.11b | 1999 | 1 to 11 | 2.4 |
| (Wi-Fi 0)* | 802.11 | 1997 | 1 to 2 | 2.4 |

# Antennas and Access Points

- Wireless networks today use three types of antennas:
- **Omni-directional**: radiate their energy equally in all directions. If you want to go greater distances, you can use a high-gain, omni-directional antenna, which offers greater horizontal coverage at the sacrifice of vertical coverage.
- **Semi-directional**: used when you need short or range bridging, such as between two buildings near each other. These antennas direct their energy primarily in one general direction.
- **Highly directional**: These antennas can go long distances (up to 25 miles, so they are good for bridging buildings together). Because of the strength of these antennas, they are sometimes used to penetrate walls that other antennas are unable to.

# Wireless Security Technologies

- **Service Set Identifiers (SSIDs):** Wireless networks identify themselves with Service Set Identifiers (SSIDs). SSIDs are like shared passwords used between client machines and Access Points. When performing a penetration test, you should lookout the following:
  - Blank SSID ("\0\0\0"  three null characters is a valid SSID)
  - Broadcast SSID
  - Default SSID
- Wireless router or access points (AP) broadcast SSIDs so nearby devices can find and display any available networks.

# Securing Service Set Identifiers (SSIDs)

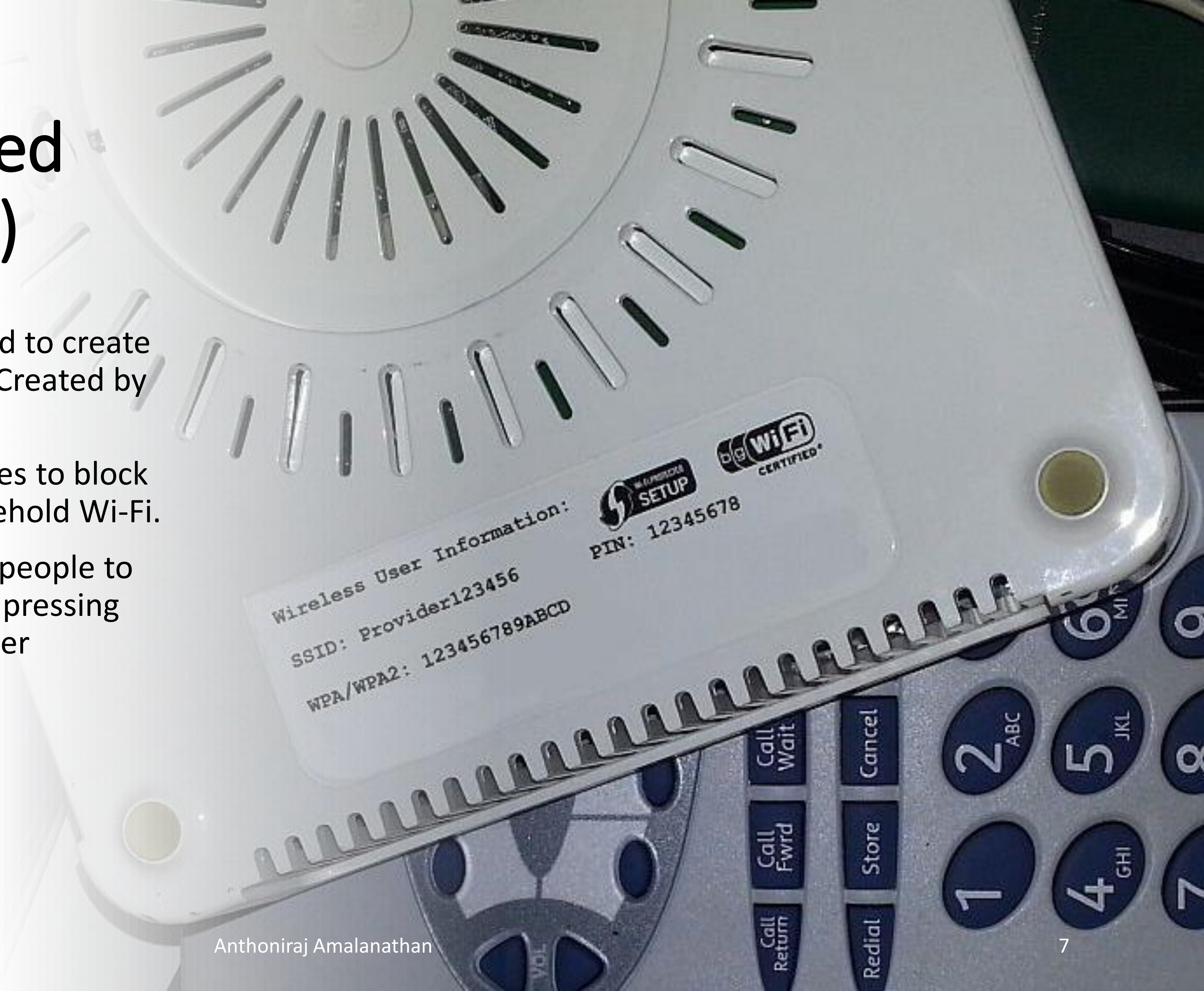
- Some of the most common mistakes that administrators make are the use of broadcasting SSIDs and default SSIDs.
- Broadcasting your SSID means that your AP periodically broadcasts its SSID to clients who are listening. You should disable SSID broadcasts and force clients to manually enter the SSID to gain access to the network.
- Default SSIDs are another mistake commonly seen. Here, wireless administrators fail to change the SSID from the factory default. For example, Linksys wireless routers use the default SSID of Linksys and are configured with the IP address of 192.168.1.1. If you see the Linksys SSID on a wireless network, you can most likely find the AP at the 192.168.1.1 IP address.
- Simply changing the SSID and turning off the broadcasting option is not enough to secure your wireless network. Active scanning tools such as Wireshark or NetStumbler can detect SSIDs even if you take these security measures. Nevertheless, you should change the SSID from the default and disable broadcasting to provide some security protection, however minor, to your wireless network.

# Wired Equivalent Privacy (WEP)

- WEP uses a secret key that is shared between a client and an Access Point (AP).
- This secret key is used with the RC4 (Rivest Cipher) algorithm to encrypt all communication between clients and the APs.
- WEP can operate with 64-bit or 128-bit encryption. The stronger the encryption, the more secure your network.

# Wi-Fi Protected Setup (WPS)

- WPS is a network security standard to create a secure wireless home network (Created by Cisco and introduced in 2006).
- Allows the owner of Wi-Fi privileges to block other users from using their household Wi-Fi.
- The owner can also allow specific people to use Wi-Fi. This can be changed by pressing the WPS button on the home router



Wireless User Information:
SSID: Provider123456
WPA/WPA2: 123456789ABCD
PIN: 12345678

# MAC Filtering

- In small networks, wireless administrators might restrict access to specific MAC addresses.
- The administrator can configure a filter on the Access Point to allow only certain MAC addresses to use a wireless network.
- Although such filtering might provide a mild restriction to malicious hackers, this security measure is easily evaded by spoofing MAC addresses.
- Using a packet sniffer such as **Kismet**, a malicious hacker can determine the MAC addresses used on a network. By spoofing a MAC address, they can gain access to the wireless network.

# 802.1x Port Security

- Because it is so easy to spoof a MAC address, IEEE devised another solution to provide added security through **network admission control**.
- The IEEE 802.1x port access control standard operates like a bouncer for your AP, deciding who gets access into your network.
- 802.1x uses the **Extensible Authentication Protocol over Wireless (EAPOW)** as a mechanism for message exchange between a RADIUS server and a client.
- Before a client can access a wireless network, it must authenticate through a RADIUS server. Authentication options include everything from a simple username and password to more secure options.

# IP security (IPSec)

- Probably the best option for securing your wireless network is IPSec.
- IPSec provides data integrity through hashing algorithms such as MD5 and SHA1, and data confidentiality through encryption algorithms such as DES and 3DES.
- Both the clients and the APs need to be configured for IPSec.
- IPSec might slow down your wireless network, but it remains the best option for securing a wireless environment.

# War Driving

- This is an information gathering method that includes driving around a premise to sniff out Wi-Fi signals.
- In war driving, a malicious hacker is armed with a laptop and a powerful antenna. While driving throughout a city, a malicious hacker can pick up and sniff wireless networks.
- Variants of war driving include
  - **war walking**, where a malicious hacker has a handheld device with wireless capabilities,
  - **war pedaling**, where a malicious hacker uses a bicycle instead of an automobile,
  - **war flying**, where a malicious hacker uses an airplane to scout out wireless networks.
  - **war sailing**, where people are using boats and going up and down a river or coastline searching for wireless networks.

# Wireless Pentesting Tools

- **Aircrack** is a suite of tools to perform Wi-Fi network assessments. The tools focus on different security layers such as packet capture, replay attacks, deauthentication, fake access points, and packet injection. (http://aircrack-ng.org/)
- **Kismet** is a wireless network and device detector. It acts as a sniffer, wardriving tool, and wireless intrusion detection framework. Kismet also works with Wi-Fi and Bluetooth interfaces, radio software and other capture hardware. (https://www.kismetwireless.net/)
- **Wireshark** is a network protocol analyzer, or an application that captures packets from a network connection. (https://www.wireshark.org/)
- **Wifiphisher**  is a mature tool within the wireless landscape. This tool is a rogue access point framework that creates a MiTM agent between wireless clients by performing targeted Wi-Fi association attacks**.** (https://wifiphisher.org/)
- **Reaver** is a tool that implements a brute force mechanism against Wi-Fi Protected Setup (WPS) registrar PINs to recover WPA/WPA2 passphrases. (https://github.com/t6x/reaver-wps-fork-t6x)
- **Pixiewps** is used to bruteforce offline the WPS pin (https://www.kali.org/tools/pixiewps/)
- **Airgeddon** is a multi-use bash script for Linux systems to audit wireless networks.