

# **CIT 270: SYSTEMS SECURITY I**

## **CHAPTER 8: WIRELESS NETWORK SECURITY**

# INTRODUCTION

---

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note 

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to **yellow words**. These highlighted words denote a topic that will almost always be on your chapter quiz.



# WIRELESS ATTACKS

---

**Bluetooth:** a wireless technology that uses short-range radio frequency (RF) transmissions and provides rapid device pairing.

**Ad Hoc Topology:** decentralised wireless network; no pre-existing infrastructure.

**Bluejacking:** an attack that sends an unsolicited message to Bluetooth-enabled devices; usually text, images and sound possible.

**Bluesnarfing:** an attack that accesses unauthorized information from a wireless device through a Bluetooth connection; often between a phone and laptop.

# WIRELESS ATTACKS

---

**Near Field Communication (NFC)**: set standards of communication between devices in very close proximity.

**Radio Frequency Identification (RFID)**: used to transmit information between an ID badge, inventory tag, book labels, and so on to a proximity reader.

**Wireless Local Area Network (WLAN)**: commonly called Wi-Fi and designed to replace or supplement a wired local area network.



# WIRELESS ATTACKS

## Institute of Electrical and Electronics Engineers (IEEE) WLAN Standards:

	Frequency	Max Data Rate	Indoor Range (feet / meters)	Outdoor Range (feet / meters)	Ratification Date
<b>802.11</b>	2.4 GHz	2 Mbps	65 / 20	328 / 100	1997
<b>802.11b</b>	2.4 GHz	11 Mbps	125 / 38	460 / 140	1999
<b>802.11a</b>	5 GHz	54 Mbps	115 / 35	393 / 120	1999
<b>802.11g</b>	2.4 GHz	54 Mbps	115 / 35	460 / 140	2003
<b>802.11n</b>	2.4 & 5 GHz	600 Mbps	230 / 70	820 / 250	2009
<b>802.11ad</b>	60 GHz	7 Gbps	32 / 10	N/A	2013
<b>802.11ac</b>	5 GHz	7.2 Gbps	115 / 35	460 / 140	2014

# WIRELESS ATTACKS

---

**Access Point (AP):** a centrally located WLAN connection device that can send and receive data; two main functions base station and bridge to a wired LAN.

**Ad Hoc Mode:** aka. *Independent Basic Service Set (IBSS)* is when devices can only communicate between themselves and cannot connect to another network.

**Wi-Fi Direct:** the Wi-Fi Alliance's technical specification of ad hoc networking; initially called Wi-Fi P2P

**Rogue AP:** an unauthorized AP that allows users (attackers) to bypass many of the network security configurations and opens the network up for attack.



# WIRELESS ATTACKS

---

**Evil Twin:** an AP that is set up by an attacker to mimic an authorized device; this allows attackers to conduct a wireless man-in-the middle attack.

**Wireless Replay Attack:** sending data captured by an Evil Twin to the original recipient at a later time; fake login.

**Jamming:** intentionally flooding the RF spectrum with extraneous RF signals called *noise* that creates interference and prevents communications.

**Disassociation Attack:** sending deauthentication or disassociation management frames causing the client to disconnect from the AP; wireless DoS.

# VULNERABILITIES OF IEEE WIRELESS SECURITY

---

**Wi-Fi Protected Setup (WPS):** an optional means of configuring security on a WLAN with little to no technology experience necessary; PIN or push method.

**Media Access Control (MAC):** a unique 48-bit identifier assigned to a network interface controller.

**MAC Address Filtering:** an access control method whereby the MAC address assigned to each network card is used to determine access to the network.

Organizationally Unique Identifier (OUI)

00-50-F2

Individual Address Block (IAB)

7C-62-E1



# VULNERABILITIES OF IEEE WIRELESS SECURITY

---

**Service Set Identifier (SSID)**: a user-supplied network name of a wireless network; normally broadcasted but can be hidden.

# WIRELESS SECURITY SOLUTIONS

---

**Wi-Fi Protected Access (WPA):** designed by the Wi-Fi Alliance to fit into the existing WEP engine with a personal version and an enterprise version.

**Temporal Key Integrity Protocol (TKIP):** a newer encryption technology that functions as a wrapper around WEP by adding an additional layer of security but preserving WEP's basic functionality:

1. require key length is increased from 64 bit to 128 bits.
2. the IV is increased from 24 bits to 48 bits; eliminating collisions.
3. a base key is created for each wireless device using a master key derived in the authentication process along with the senders unique MAC address.



# WIRELESS SECURITY SOLUTIONS

---

**Open Method:** a wireless network requiring no authentication to join it.

**Pre-shared Key (PSK):** authentication for WPA Personal using a secret key that has been previously shared; a shared secret; wifi password.

**Wi-Fi Protected Access 2 (WPA2):** second generation WPA with improvements and support for Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) and AES based encryption.



Professor Messer  
TKIP and CCMP


# WIRELESS SECURITY SOLUTIONS

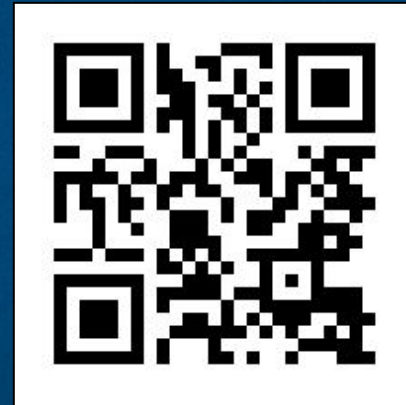
---

**Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)**: a general-purpose cipher mode algorithm providing data privacy, integrity, and authentication with AES.

**Advanced Encryption Standard (AES)**: is a subset of the Rijndael Block Cipher.



 [AES Rijndael Encryption Cipher Overview](#)



 [AES Rijndael Encryption Cipher Explained \(Full\)](#)



# WIRELESS SECURITY SOLUTIONS

---

**Enterprise Method** refers to **WPA2 Enterprise** that follows the IEEE 802.1x standard. This standard provides a greater degree of security by implementing port-based authentication and in its most secure configuration **certificate-based authentication**; this can also be used on wired networks.

- supplicant
- authenticator
- authentication server

**Extensible Authentication Protocol (EAP)**: a framework for transporting authentication protocols instead of the authentication protocol itself. EAP defines the format of the messages used for authentication and uses four types of packets: request, response, success, and failure.

# WIRELESS SECURITY SOLUTIONS

---

**Protected EAP (PEAP):** a common EAP protocol designed to simplify the deployment of 802.1x by using Microsoft Windows logins and passwords; creates encrypted channel between the client and authentication server which then protects the authentication exchange.

<u>EAP Name</u>	<u>Description</u>
EAP-TLS	This protocol uses digital certificates for authentication.
EAP-TTLS	This protocol securely tunnels client password authentication within TLS records.
EAP-FAST	This protocol securely tunnels any credential form for authentication (such as a password or a token) using TLS.



# WIRELESS SECURITY SOLUTIONS

---

**Rogue AP System Detection:** the best way to detect a rogue AP is by using a wireless probe:

- Wireless Device Probe – a standard wireless device such as a laptop configured to periodically scan and record wireless signals, sending the data back to a central server for analysis.
- Desktop Probe – same as above but an a wireless or radio card is installed in the desktop so it can perform the same scans.
- Access Point Probe – functionality on some AP to identify and know who their trusted AP neighbors are; not very popular.
- Dedicated Probe – a dedicated device designed to exclusively monitor the RF frequencies for transmissions; disguised like AP.

# WIRELESS SECURITY SOLUTIONS

---

**Standalone APs:** fat or thin clients that need a switch for some part of their management.

**Controller APs:** a single device (controller) that is configured and then used as the source for all AP settings.

Another means of protecting a wireless network is to choose the best type of AP for the needs of your network:

- **Fat AP** – good for home or small business use, everything needed to manage a wireless network is on the AP.
- **Thin AP** – best for medium to large business, only the bare minimum is on the AP and everything else is passed on to a managed switch.



# REFERENCES

---

“AES Rijndael Cipher explained as a Flash animation” AppliedGo, YouTube, 27 November 2017,  
<https://youtu.be/gP4PqVGudtg>

“AES Rijndael Encryption Cipher Overview” CoastRD, YouTube, 20 January 2012,  
[https://youtu.be/H2LIHOw\\_ANg](https://youtu.be/H2LIHOw_ANg)

Book [PNG]. Flat Icon. [https://www.flaticon.com/free-icon/book-opened-outline-from-top-view\\_30169](https://www.flaticon.com/free-icon/book-opened-outline-from-top-view_30169)

Common EAP Protocols supported by WPA2 Enterprise [Table 8-5]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 351. Boston, MA: Cengage.

IEEE WLAN Standards [Table 8-4]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 333. Boston, MA: Cengage.

Link Icon [PNG]. Share Icon. No license found, public domain inferred.

# REFERENCES

---

MAC Address [Figure 8-9]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 344. Boston, MA: Cengage.

Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.