UOW
MALAYSIA
KDU PENANG
UNIVERSITY COLLEGE

PART OF THE UNIVERSITY
OF WOLLONGONG AUSTRALIA
GLOBAL NETWORK

Fundamentals of Security in Ethical Hacking

DCS22104

Lesson 8: Hacking wireless networks with tools

Department of Computing

Course outline

Week	Topic
1	Introduction to ethical hacking and reconnaissance
2	Network enumerators and system vulnerabilities
3	Malware
4	Social engineering attacks
5	Hacking web servers and web applications
6	Session hijacking
7	Script injections
8	Hacking wireless network
9	Buffer overflow attacks
10	Cryptography
11	Evading IDS, firewall, and honeypot
12	Penetration testing

Assessments

#	Components	Marks(%)	Week
1	Test 1 (Topics 1 to 5)	10	DONE
2	Midterm examination	20	DONE
3	Test 2 (Topics 1 to 11)	20	12
4	Final examination	50	Exam week

Reviews on Lesson 7

- SQL stands for structured query language.
- It manipulates data in relational database management system (RDBMS).
- Short-circuit evaluation: ' OR '1' = '1.
- Comment injection attack: PeterAdam' #

Reviews on Lesson 7

Four approaches to prevent SQL injections. It manipulates data in relational database management system (RDBMS).

a. Escape key functions, such as addslashes() or mysqli_real_escape_string().

b. Separate SQL string into multiple lines of code.

c. SQL prepare statement which separate input data from SQL string.

d. Special character feature that translate special characters into normal text.

Topic learning outcomes

1. Identify the protocols used for wireless network.

2. Identify the strength of handshake technologies used in wireless network.

Lesson 8: Lecture and lab sessions

Start time	End time	Topics
1:00pm	1:30pm	Reviews on Lesson 7
1:30pm	2:00pm	Lecture 1: **Wireless network vulnerability**
2:00pm	2:15pm	Break time
2:15pm	2:45pm	Lecture 2: **Wireless network security**
2:45pm	2:50pm	References

Lecture 1: Wireless network vulnerability

Radio communication

- Radio communication in layer 1 of OSI.
- Radius range from 30 meters to 500 meters.
- A transceiver is used to transmit radio frequencies.
- Most wireless devices are of IEEE802.11 standards, which communicate at various frequency bands, usually 2.4GHz.

Service set identifier (SSID)

- Service set identifier (SSID) is used to identify a device in the wireless local area network (WLAN).
- 32 characters in length.
- SSID is broadcasted using beacon frames from a wireless access point with a router.

Advantages of a wireless network

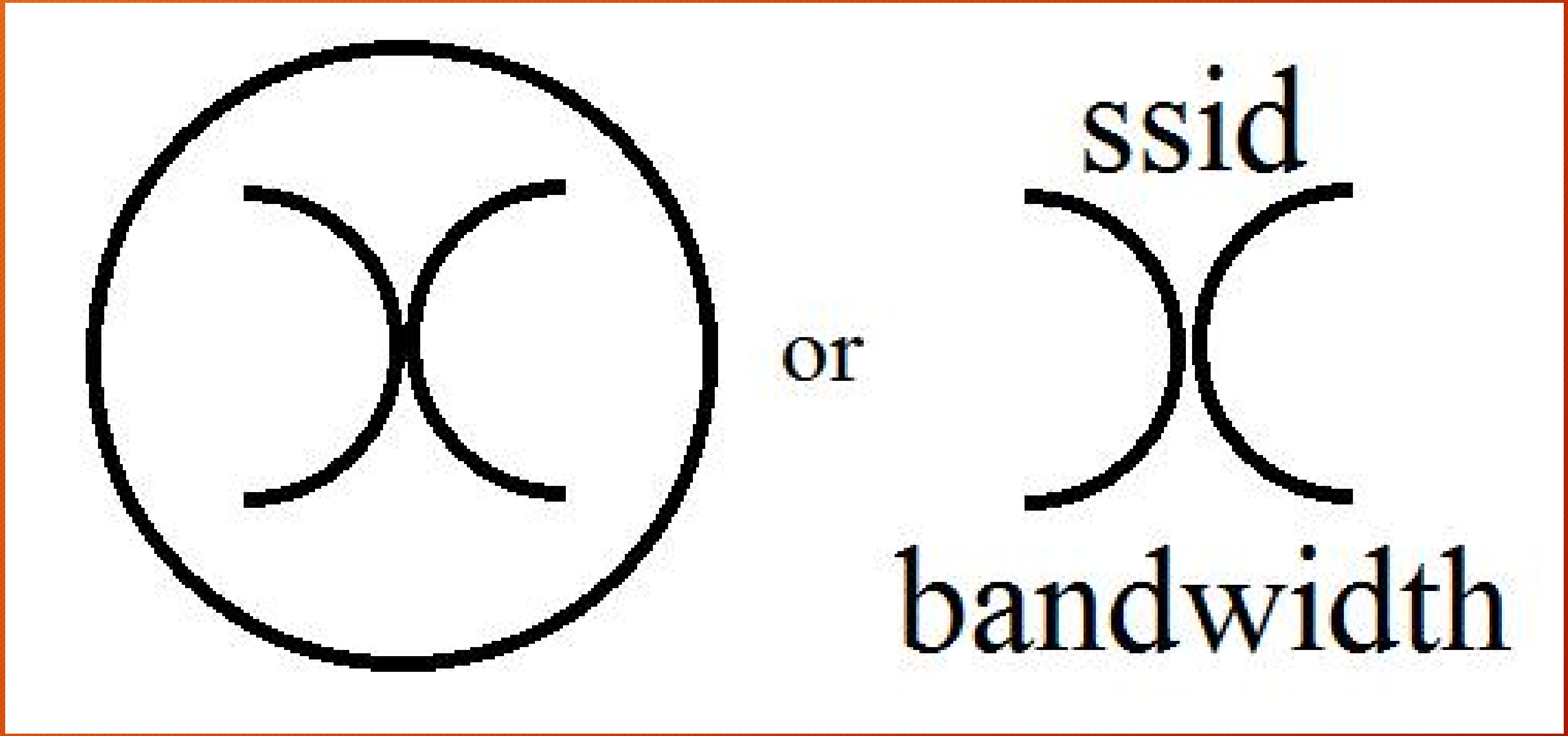
- No cable and plugs.
- High mobility. which is not fixed at a specific location.
- Easy tethering using phone as modem (PAM) to connect to the Internet.

Vulnerabilities

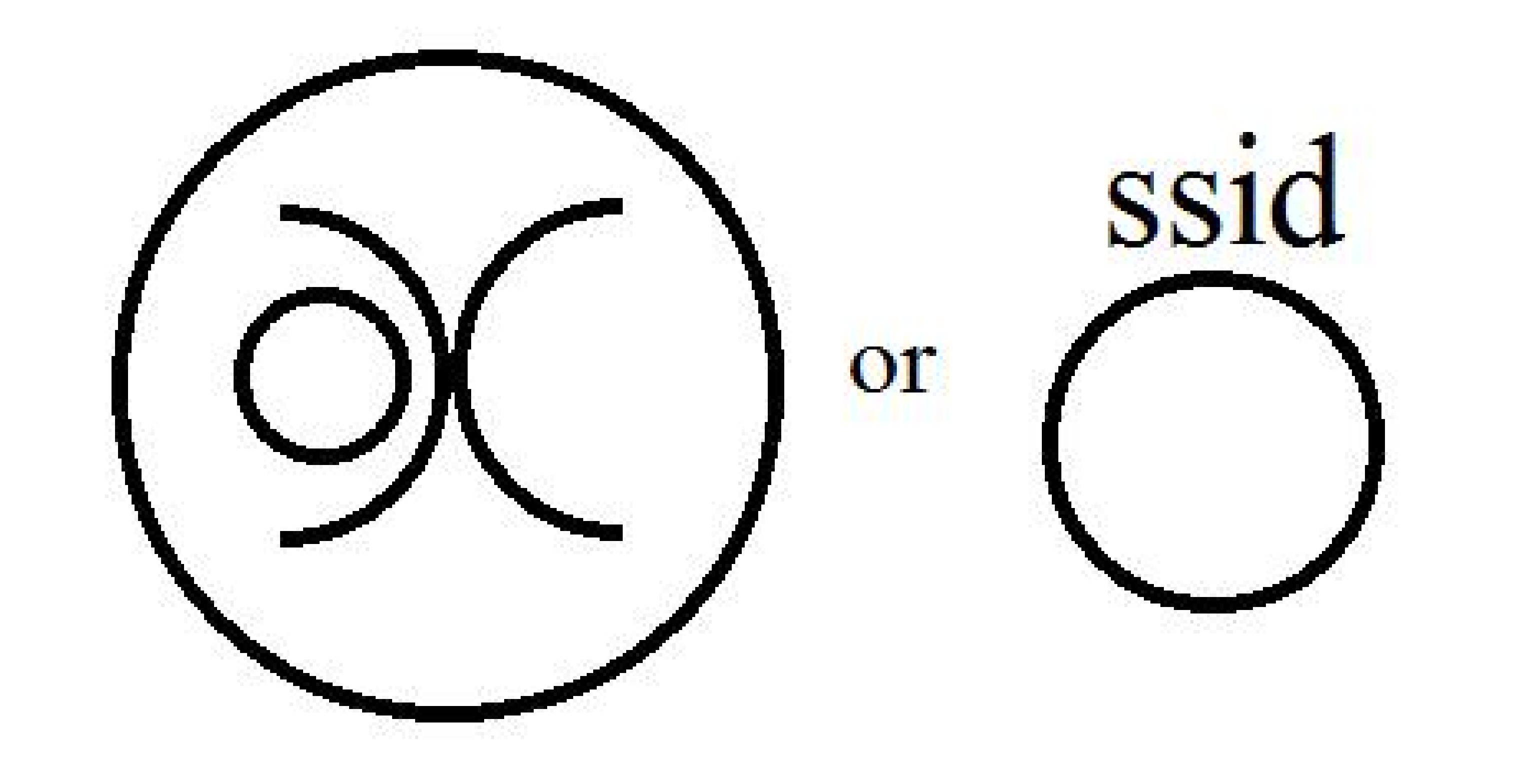
- No physical access required.
- Unknown network boundary.
- Within range could get attack.
- Leftover street signs.
- Unsecured or unencrypted wireless networks.
- Password retrieval using brute force attack.
- Session hijack using authentication credential.

Wireless network sign

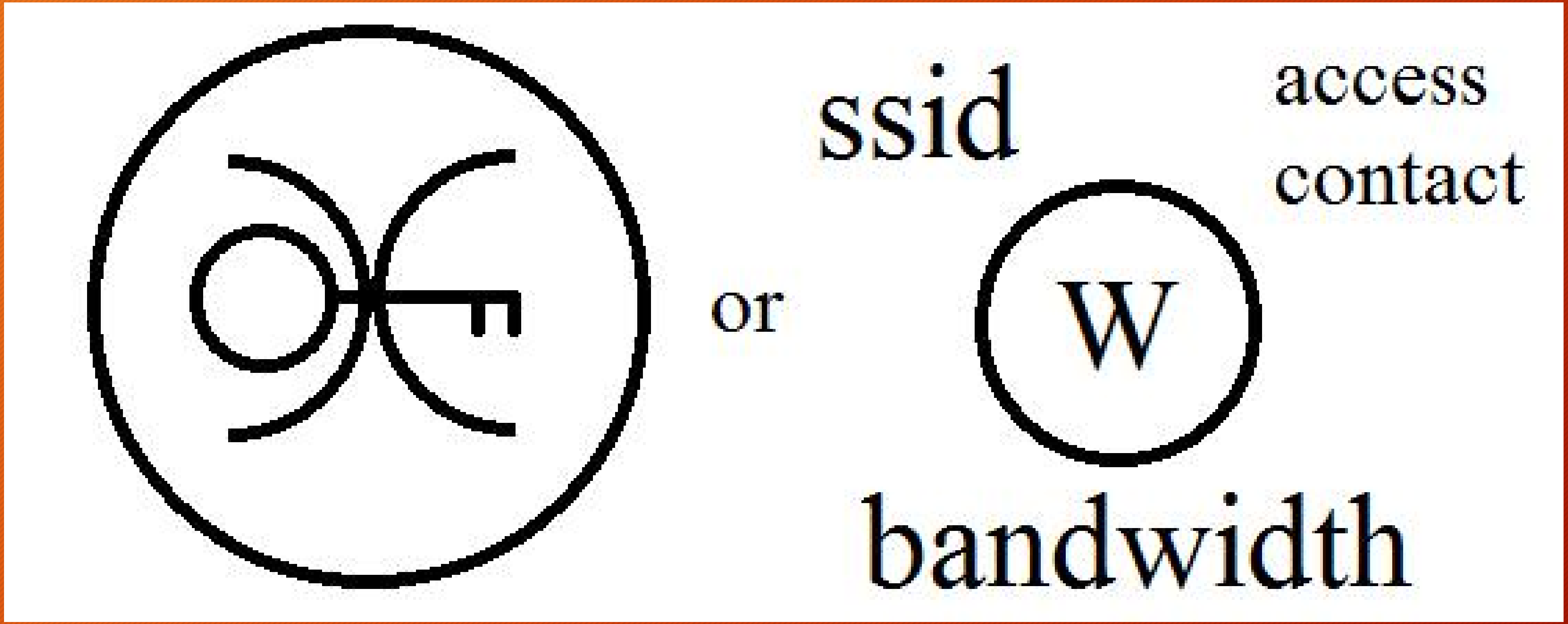
Open network sign



Closed network sign



WEP network sign



Exercise 1 (10 minutes)

1. Which layer of OSI that a radio communication device transmit data?

2. Which frequency bandwidth is the most common settings for wireless devices?

3. How a SSID is broadcast?

Break time

Duration: 15 minutes.

Lecture 2: Wireless network security

Wired equivalent privacy (WEP)

- It shares static key.
- 40 bits long, which is short.
- Weak encryption.
- Integrity check algorithm is public.
- No authentication.
- WEP can be cracked using free software, e.g. AirSnort.

Wi-Fi protected access (WPA & WPA2)

- It uses a dynamic encryption key.
- It includes real time authentication using token keys.
- It uses strong AES 256 bits encryption.
- It uses improved 64 bits integrity protection for data frames.
- It improves session initiation using forward handshaking operations.

Exercise 2 (10 minutes)

1. State three advantages of a wireless network.

2. State three security vulnerabilities for a wireless network.

References

- CEH course materials
- Goodrich, M (2010) *Introduction to Computer Security*, Addison Wesley, 1st Ed
- Purpura, P (2010) Security: An Introduction, CRC Press, 1st Ed
- Stallings, W (2007) Computer Security: Principles and Practices, Prentice Hall, 1st Ed
- Jacobson, D (2008) Introduction to Network Security, Chapman and Hall, 1st Ed
- Fischer, R (2008) Introduction to Security, Butterworth-Heinemann, 8th Ed