UOW
MALAYSIA
KDU PENANG
UNIVERSITY COLLEGE

PART OF THE UNIVERSITY
OF WOLLONGONG AUSTRALIA
GLOBAL NETWORK

Fundamentals of Security in Ethical Hacking

DCS22104

Lesson 9: Cryptography

Department of Computing

Course outline

Lesson	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	Cryptography
10	Buffer overflow attacks
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 8

A radio communication device transmit data in physical layer of OSI model.

2.4GHz is the most common frequency bandwidth for wireless devices.

SSID is broadcasted using beacon frames from a wireless access point with a router.

Reviews on Lesson 8

Three advantages of a wireless network.

a. No cable and plug.
b. High mobility, because it is not at a fixed location.
c. Easy tethering using phone as modem (PAM) to connect to the Internet.

Three security vulnerabilities for a wireless network.

a. Brute force attack is possible to retrieve password.
b. There is no physical access, user connections could not control physically.
c. Within range could get attack.
d. Session hijack is possible via ARP spoofing.

Lesson 9: Lecture and lab session

Start time	End time	Topics
1:00pm	1:30pm	Reviews on Lesson 8
1:30pm	2:00pm	Lecture 1: **Cryptography and its application**
2:00pm	2:15pm	Break time
2:15pm	2:45pm	Lecture 2: **Encryption and decryption**
2:45pm	2:50pm	References

Lecture 1: Cryptography and its application

Cryptography in information security

- It refers to the core developments of cryptosystem.
- It provides a layer of security to access data in a system.

Disadvantages of a password

- Password can be lost or forgotten by legitimate users.
- It is inconvenient for users to access their information.
- It could be shared, stolen, or revoked by malicious party.

Password vulnerabilities

- Brute-force attack.
- Common passwords (Date of birth, social security number, etc.)
- Possible passwords for a particular user.
- Search for system password file.
- Social engineering attacks. Ask from the user for their password.
- Dictionary attacks: Words, names, acronyms, common passwords.
- Reveal password format to public will be a danger.

Requirements for a strong password

- A strong password should included alphabets, numbers, and special characters.
- What is the possibilities for an eight characters long strong password?
  - (a) Uppercase and lowercase letters: 26 × 2 = 52.
  - (b) Numbers: 0 to 9 = 10.
  - (c) Special characters: 32
  - (d) Total possibilities: 52 + 10 + 32 = 94.
- 8 characters long: $94^8 + 94^7 + 94^6 + \ldots$. Thus, $\sum_{k=1}^{8} 94^k$.
- Meaningless for brute-force attack.

Password protection

- Stop or delay the brute-force attack.
- Restrict the number of times login attempts.
- Strong authentication through security questions and biometrics.
- Time embedded password, passcode = PIN + TOKEN CODE.

Exercise 1 (10 minutes)

1. Explain three vulnerabilities for a password.

2. What is the requirements for a strong password?

Break time

Duration: 15 minutes.

Lecture 2: Encryption and decryption

Symmetric encryption

- Use the same key for encryption and decryption.
- Example algorithms are stream ciphers and block ciphers.

Asymmetric encryption

- Different keys for encryption and decryption.
- Encryption key is the public key.
- Decryption key is the private key.
- Example encryption, such as Rivest-Shamir-Adelman (RSA).

Cryptosystem

- The objective is to make it difficult and not worth the effort to break it.
- There are three types of ciphers.

Types	Descriptions
Substitution ciphers	Characters are swapped.
Transposition ciphers	Permutation whereby the order of characters is rearranged.
Product ciphers	Combine two or more ciphers.

- n-gram is a string of characters of length n.

Caesar cipher

- It is a substitution cipher.
- Each letter is replaced by the third letter following it.

Plain:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphers:	XYZABCDEFGHIJKLMNOPQRSTUVW

- Encryption process

Plaintext:	SECRET MESSAGE
Ciphertext:	PBZOBQ JBPPXDB

- Exhaustive search possible, since this cipher has only 26 possible keys.

3 rows rail-fence cipher

- A plain text message is transposed into several rows.

Plain:	SECRET MESSAGE
Encryption process:	S...E...S...E (3 dots) .E.R.T.E.S.G. (1 dot) ..C...M...A.. (prefix: 2 dots, letters in between: 3 dots, postfix: 2 dots)
Ciphers:	SESE ERTESG CMA

Stream ciphers: Encryption

- Encryption key is based on one time pad (OTP).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Encryption process.

Plaintext:	P	R	O	T	E	C	T	E	D
Numeric plaintext, np:	16	18	15	20	5	3	20	5	4
OTP:	D	I	M	I	T	R	I	C	A
Numeric OTP, no:	4	9	13	9	20	18	9	3	1
np + no:	20	27	28	29	25	21	29	8	5
Ciphertext:	T	A	B	C	Y	U	C	H	E

Stream ciphers: Decryption

- Encryption key is based on one time pad (OTP).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Decryption process.

Ciphertext:	T	A	B	C	Y	U	C	H	E (9-grams)
Numeric ciphertext, nc:	20	1	2	3	25	21	3	8	5
OTP:	D	I	M	I	T	R	I	C	A (9-grams)
Numeric OTP, no:	4	9	13	9	20	18	9	3	1
nc - no:	16	-8 26	-11 26	-6 26	5	3	-6 26	5	4
Plaintext:	P	R	O	T	E	C	T	E	D

Shannon’s criteria

- Need certain degree of secrecy.
- Set keys and encryption algorithm should be simple.
- Simple implementation.
- Limited propagation of errors.
- Size or storage of cipher text should be restricted.

Commercial principles

- Mathematical theory sound.
- Verified by expert analysis including external experts.
- Has stood the test of time.
- Fix flaws in encryption algorithms.

Data encryption standard (DES)

- 56 bits fixed length key.
- 16 iterations of encryption are performed on the plaintext including substitutions and permutations.
- Each iteration uses its own key.

Advanced encryption standard (AES)

- Symmetric key algorithm
- Developed by Belgian cryptographers.
- 128 bit blocks of plaintext.
- 10 rounds for 128 bit keys.
- 12 rounds for 192 bit keys.
- 14 rounds for 256 bit keys.
- Basic operations involved substitution, shift row, mix columns and add subkey.

Exercise 2 (10 minutes)

1. State a different between symmetric and asymmetric encryption algorithms.

2. What is the objective of a cryptosystem?

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