UNIVERSITY OF GHANA

BSc COMPUTER SCIENCE

FIRST SEMESTER EXAMINATIONS: 2017/2018

CSIT 431: DATA NETWORK SECURITY II

MARKING SCHEME

INSRUCTIONS
ANSWER QUESTION 0NE COMPULSERY
ANSWER ANY THREE OF THE FOLLOWING QUESTIONS FOR 15 MARKS EACH
TIME ALLOWED: ***TWO AND A HALF (2½) HOURS***

[60 MARKS TOTAL]

Q1. **Ability Micro finance has experienced network attacks on their online banking and personal finance system infrastructure at various stages which has caused them a huge financial loss due to security implementation issues.**
You have been employed as the Chief Security Officer (CIO) to analyze and identify the threats, vulnerabilities and attacks at each level of security on the network.
Q1a. With the aid of a diagram, identify all the risk access spots on the banks online internet from the customer's computer or mobile device to the application server. [10 Marks]
Q1b. Explain at each stage on the diagram, the type of vulnerability that can be exploited, threat that can be initiated and the type of security measures that must be implemented. [20 Marks]

ANSWER 1A

By organising the risk access spots will ensure security controls are being identified before it can be implemented and will also help enforce organisational regulations.
To organise the resources available to you, all the security resources must be identified e.g.:

Controls

1. Authentication – Checks weather user is true
2. Multifactor authentication – e.g. ATM Card &PIN
3. Authorisation – Give access to user
4. Approval Levels

Server

1. Client
2. Web
3. Cache
4. Application
5. Database

Authentication

1. User ID

2. Password
3. Encryption
4.

Service Providers

1. IP Address
2. Routers & Switches
3. Hubs
4. Operating System
5. Gateway
6. Bridges
7. Port Addresses

ANSWER 2A
Students to explain these vulnerabilities and attacks

1. Computer/Mobile Device: Vulnerabilities on online App, Browser, Password. Attackes: Cross site Scripting,
2. Encryption: HTTP(S) Vulnerable to various attacks as ID and Data theft, Intellectual Property,
3. Firewall: IP Spoofing, I
4. Logon Screen: Session Hijacking and User ID Password Theft.
5. Webserver: Vulnerable to Cross Site Request Forgery, DoS attack
6. Application Server:

Q2a. **With examples, define firewall and explain it implementation concepts. [5 Marks]**
Q2b. Using the principle of **Work Factor & Cost of Circumvention, e**valuate the five

different types of firewalls and their vulnerabilities. [10 Marks]

ANSWER 2A

A firewall is a configuration mechanism (tool) for maintaining control over the traffic that flows into and out of our network(s).

The concept of firewall implementations:

1. Placed on the border between our internal network and the Internet to prevent network traffic of a sensitive nature from being accessed by those that have no reason to do so.
2. Configured to examine the packets that are coming in over the network.
3. This examination determines what should be allowed in or out.

Whether the traffic is allowed or blocked can be based on a variety of factors and largely depends on the complexity of the firewall.

1. E.g. we might allow or disallow traffic based on protocol being used, allowing Web and e-mail traffic to pass, but blocking everything else.

ANSWER 2B

Packet Filtering Firewall

Is one of the simplest of firewall technologies that examines at the contents of each packet in the traffic individually and makes a gross determination, based on the source and destination?

1. IP addresses
2. The port number
3. The protocol being used

Of whether the traffic will be allowed to pass.

Vulnerability on the Packet Filtering

Each packet is examined individually and not in concert with the rest of the packets comprising the content of the traffic, it can be possible to slip attacks through this type of firewall.

Stateful Packet Inspection Firewalls

Function on the same general principle as packet filtering firewalls

1. But they are able to keep track of traffic at a granular (Rough) level.

While a packet filtering firewall only examines an individual packet out of context

A stateful firewall is able to watch the traffic over a given connection, generally defined by the:

- Source and destination IP addresses,
- the ports being used,
- the already existing network traffic.

A stateful firewall uses what is called a state table to keep track of the connection state and will only allow traffic through that is part of a new or already established connection.
Most stateful firewalls can also function as a packet filtering firewall, often combining the two forms of filtering. E.g.

- This type of firewall can identify and track the traffic related to a particular user initiated connection to a web site,
- And knows when the connection has been closed and further traffic should not legitimately be present.

Deep Packet Inspection Firewalls
Add yet another layer of intelligence to our firewall capabilities.

1. Deep packet inspection firewalls are capable of analyzing the actual content of the traffic that is flowing through them.
2. Although packet filtering firewalls and stateful firewalls can only look at the structure of the network traffic itself in order to filter out attacks and undesirable content
3. Deep packet inspection firewalls can actually reassemble the contents of the traffic to look at what will be delivered to the application for which it is ultimately destined.

Deep Packet Inspection Firewalls
Open the package and inspect its contents, then make a judgment as to whether the package could be shipped based on its contents.
It is used by top security fires to detect anomaly and any forms of threat patterns on the data network.

Proxy Servers
Are ultimately a specialized modified of a firewall. These servers provide security and performance features, generally for a particular application, such as mail or Web browsing.
Proxy servers can serve as a choke point in order to allow us to filter traffic for attacks or undesirable content such as malware or traffic to Web sites hosting adult content.

1. They also allow us to log the traffic that goes through them for later inspection
2. They serve to provide a layer of security for the devices behind them, by serving as a single source for requests

Proxy servers are nearly ubiquitous in the business world, largely due to the filtering capability they provide. It is used:

1. To keep the large amounts of spam that flow over e-mail from reaching their users and lowering productivity.
2. To filter web traffic in such environments in order to keep employees from visiting web sites that might have objectionable material
3. To filter out traffic that might indicate the presence of malware.

Again the major issue with them is delay introduced with additional step of inspection.

Demilitarized Zone or DMZ

Is generally a combination of a network design feature and a protective device such as a firewall.

DMZs are used as part of Network Security Design to increase the level of security on our networks by segmenting them properly. such as:

1. Mail servers
2. Proxy servers
3. Software as a service application
4. Web servers

To ensure their security and the security of the devices on the network behind them.

We can putting a layer of protection between the device, such as our mail server and the Internet, and between the rest of our network and the device.

This allows only the traffic that needs to reach the mail server to do that for instance:

1. Internet Message Access Protocol (IMAP)
2. Simple Message Transfer Protocol (SMTP) on ports 143 and 25, respectively to reach our mail server, and the same ports to pass through on our network.

Presuming that no other services are running on the same system, we could restrict the traffic going into and out of the DMZ where our mail server sits to those particular ports

3a. With the aid of a diagram explain Symmetric and Asymmetric Encryptions models and the mathematical formulas used to encrypt data.

3b.Using the four Cryptanalytic Attacks vectors, explain how attack are initiated from Cypher Text-only attack to Chosen-Cypher text attack.

ANSWER 3A

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.

It is also known as conventional encryption.

◆ Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm.

Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text.

The two types of attack on an encryption algorithm are cryptanalysis:

- based on properties of the encryption algorithm
- brute-force, which involves trying all possible keys.

◆ Traditional symmetric ciphers use substitution and/or transposition techniques.

- Substitution techniques map plaintext elements (characters, bits) into cipher text elements.
- Transposition techniques systematically transpose the positions of plaintext elements.

2. Or conventional / private-key / single-key
3. Sender and recipient share a common key
4. All classical encryption algorithms are private-key

Symmetric Cipher Model

1. Two requirements for secure use of symmetric encryption:
    - a strong encryption algorithm
    - a secret key known only to sender / receiver
2. mathematically have:

Y = E(K, X)
X = D(K, Y)

1. Assume encryption algorithm is known and implies a secure channel to distribute key

ASSYMETRIC /PUBLIC KEY ENCRYPTION

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys. One a public key and one a private key.

◆ Asymmetric encryption transforms plaintext into ciphertext using a one of two keys and an encryption algorithm.

- Using the paired key and a decryption algorithm, the plaintext is recovered from the ciphertext.

2. Asymmetric encryption can be used for confidentiality, authentication, or both.
3. The most widely used public-key cryptosystem is RSA. The difficulty of attacking RSA is based on the difficulty of finding the prime factors of a composite number.

Asymmetric Keys

1. Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
2. Public Key Certificate
3. A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key.

Bob has two keys: a private key, SB, which Bob keeps secret, and a public key, PB, which Bob broadcasts widely.

- **In order for Alice to send an encrypted message to Bob, she need only obtain his public key, PB, use that to encrypt her message, M, and send the result, $C = E_{PB}$ (M), to Bob. Bob then uses his secret key to decrypt the message as $M = D_{SB}$ (C).**

Public Key Encryption Steps:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. Each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Public-Key Cryptosystem for Confidentiality & Authentication

1. Encrypting a message, using the sender's private key. This provides the digital signature.
2. Encrypt again, using the receiver's public key.
3. The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus, confidentiality is provided.

4. $Z = E(PU_b, E(PR_a, X))$
5. $X = D(PU_a, D(PR_b, Z))$

ANSWER 3B

Cryptanalyst has access to ciphertext. The goal is to determine the plaintext or, better yet to discover the K
Crypt analyst has access to plaintext-ciphertext pair. The goal is to determine the key, K.
Cryptanalyst choose a plainrtext and get its ciphertext based on the use of key, K.
Cryptanalyst choose a ciphertext and get its plaintext based on the use of key, K.

4. Explain the difference between WEP and WPA/2. With examples give reason why you would select one against the other. [10 Marks]

ANSWER
WEP (Wireless Equivalency Protocol)
WAP (Wireless Access Point)

WEP is not the best protection and Generally not as secure as the more sophisticated WPA/ WPA2 encryption.

1. If a hacker can sniff packets on a WEP encrypted network, it is only a matter of time until the password is cracked.
2. If enough traffic can be intercepted by an attacker, then it can be broken by brute force. E.g. Two Nigerians and the CID
3. The time it takes to crack WEP only grows linearly with key length
4. A 104-bit key doesn’t provide any significant protection over a 40-bit key when faced against a determined cracker.

Shared Key and Open System Authentications

In Shared Key, the client request authentication and the Wireless Access Point sends a text which the client has to encrypt using the WEP key and send it back

- If it matches then the WAP (Wireless Access Point) authenticates and associates it with the client.

In Open System Authentication any client can associate with WAP

- The client is authenticated regardless of the key it possesses and begins to receive packets.
- The client would need the correct key at this point to read the packets.

2. A WEP key is usually 128bit comprised of 26 hexadecimal values and a 24bit Initialization Vector (IV).
3. Each packet is encrypted using RC4 algorithm with the 26 hexadecimal values and a random IV.
4. The packet is sent along with the IV in plain text.
5. The client then decrypts the packet using the hex key and the included IV.

Wi-Fi Protected Access (WPA) is a software/firmware improvement over WEP.

- All regular WLAN-equipment that worked with WEP are able to be simply upgraded and no new equipment needs to be bought.
- WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP.

2. TKIP (Temporal Key Integrity Protocol) encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices.
3. The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

B, Explain the following kali Linux penetration testing software (Aircrack-ng) suite commands used in WEP and WPA Security. [5 Marks]

ANSWER 2B

kali Linux Penetration Testing Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.

1. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff:
    - 802.11b
    - 802.11g
    - 802.11n traffic
2. The program runs under Linux and Windows.

ANSWER

The Kali Linux Pentest software commands suite includes:

1. aircrack-ng - Cracks WEP and WPA (Dictionary attack) key
2. airdecap-ng - Decrypts WEP or WPA encrypted capture files with known key.
3. airmon-ng - Placing different cards in monitor mode.
4. aireplay-ng - Packet injector (Linux, and Windows).
5. airodump-ng - Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks.

5. With the aid of a diagram explain the three security objectives and the threat issues? [7M arks]

5b. Identify the CIA goals and the tolls required to ensure security controls [8Marks]

ANSWER 5A

The CIA triad gives us a model that explains security concepts, and tends to be very focus on

security as it pertains to data.
The confidentiality, integrity, and availability triad.

1. Confidentiality
    - “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.” Confidentiality of ATM PIN Number, Account Information
2. Integrity

- "Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity." E.g ensure information is correct

3. Availability
   - "Ensuring timely and reliable access and use of information."
   - E.g. have my information whenever I need them 24/7

ANSWER 5B
CONDIDENTIALITY

1. **Confidentiality** is the avoidance of the unauthorized disclosure of information.
   - Confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.

TOOLS FOR CONFIDENTIALITY

1. **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a "need to know."
   - This need to know may be determined by identity, such as:
     - a person's name
     - or a computer's serial number,
     - or by a role that a person has, such as being a manager or a computer security specialist.
2. **Authentication:** the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of
   - something the person has (like a smart card or a radio key fob storing secret keys),
   - something the person knows (like a password),
   - something the person is (like a human with a fingerprint).