Cyber Security Assessment

# Task 1: Part a

# Frauds and Scams over the Internet

Given below are the most common and frequent scam and fraud attacks on a computer network over the internet.

## Man-in-the-middle Attack

This attack is based on the interception of the communication between two parties i.e. users or clients over the internet. Basically the client and server are connected using the TCP connection. So, the attacker creates another TCP connect by splitting the client and server connection. Now user is connected to attacker’s machine and that is then connected to server. In this way all of the communication between user/client and server is intercepted by the attacker.

### Prevention of Attack

The man-in-the-middle attack can be prevented using strong encryption on both sides i.e. on the client’s machine and on the server side.

## Phishing Attacks

These attacks attempt to steal sensitive data and access to credible resources of a system or a user by fraudulent electronic communication and deceiving the victim to compromise its information and resources to the attacker. Mostly these attacks are activated when the user/victim clicks a malicious link or downloads a harmful software of file.

### Prevention of Attack

There are four measures to protect yourself against phishing attacks

1. Using a security software that detect these attacks and helps protect your computer
2. If you use multi-factor authentication, phishing attacks can be avoided
3. Frequently updating your software, computers, mobile phones etc.
4. Save your data as a backup on some machine or on a cloud platform.

## SQL injection and Cross-Site Scripting (XSS) Attack

These attacks are mostly done via web applications. Basically these are a type of code injection attack where the malicious script or code is injected into the web applications and the attacker gains the control over the data and resources of that application. It Is used to steal information, redirect users to malicious websites and gain control over resources like database, cookies and admin credentials etc.

### Prevention of Attack

The best measure to avoid and protect your application against these attacks is to encode and filter special characters in the user input. Also the encryption does not allow attackers script to run on the server.

## Part b:

## Protection of the Network from Data Theft over the Internet:

Some of top most effective techniques and measures to prevent attacks over the internet are given below. These measure help us to secure the information, data and resources.

### End-to-End encryption:

Even if the communication is intercepted, it is not meaningful or understandable and can’t be decrypted without the encryption keys.

### Multi-factor Authentication:

This measure will help avoid the phishing attacks and secure your system from data theft and unauthorized communication.

### Encoding the User Input:

It is fundamentally the most important part to handle the malicious input and secure your application from code injection attacks. There are different types of encoding respective to the user input i.e. HTML, JavaScript, attribute, URL and script encoding.

# Task 3: Part a

## Denial of Service (DoS) Attacks:

The main goal of these type of attacks is to exhaust the system resources, so that it does the respond in the intended way. Given below are some of the most frequent and destruction denial of service (DoS) attacks.

### TCP SYN Flood Attack:

It occurs during the TCP handshake protocol at the beginning of the communication when the server is acknowledging and authenticating the user. Send massive amount requests to a server that fills up its queue and it no longer responds in the intended way or it may crash in this situation.

### Smurf Attack:

It causes a distributed denial of service attack by broadcasting large number of “Internet Control Message Protocol (ICMP)” packets over the network using a broadcasting IP address.

### Botnets Attack:

It includes bots or zombie systems that attack the targeted system on the behalf of an attacker. A large number of these bots together create a distributed denial of service (DDoS) attack. This makes the DDoS attack more complex and untraceable as the bots/machines are spread across a wide area of coverage with respect to geographical locations.

# Task 4: Part a

## Software Tools for Protection against Malware and Spyware

There are numerous tools in the industry right now. All of them have their own specialty and area of influence. These tools work best in the defined and respective context or scope of the system and most of them are system specific i.e. used for a specific purpose or type of malware. Some of the leading malware protection software and tools are given below.

### McAfree Antivirus Software:

It is one of the best tools for protecting your system against malware and spyware. It contains a virus database that is maintained and updated regularly with the data collected through a web crawler. It collects the names of all the malicious software names and harmful file extensions that may cause damages to the user system and compromise its data and resources.

It strengthens the firewall of a computer using the virus database. Scans the whole computer for any malware or corrupted files and deletes or kills any file and software that contains a malware.

### Avast Antivirus:

Avast provides a smart scan which detects malware and outdated software and removes any files or software that compromises the security of computer. It matches all the files with the virus records and virus definitions in order to find the untrusted or malicious software.

One of main benefits of Avast is the “Boot-Time Scan”. This is done during the startup of the system, this is the time when malware are inactive and can’t do any damage. So scanning at this time clean the system before any malware is launched. Thus malware is detected and removed from the computer before it can counteract or activate itself.

### Norton:

It is considered as one of top defenders against malware. It allows the users to scan there system for any malware and suspicious behavior. It has a large database for virus definitions that helps improve the security and malware detection for a computer.

Norton has an emulator for untrusted software and it runs these types of software in a separate environment to analyze the behavior of these programs. So, in this way the malicious software can be emulated and executed without harming the system.

### MalwareBytes:

Fast and efficient scanning is one of the key features of this tool. MalwareBytes Anti-Malware completely removes the existing virus infections. It has its own “Chameleon” technology which allows it to get installed and execute on the infected systems which do not allow other security software to operate.

The best feature of this tool is the “real-time protection” and “heuristic scanning method”. Previously unknown malicious software infections are detected by analyzing their behavior and influence on the computer system. This makes this modern security software very efficient and effective. In this way it takes care of new and emerging threats.

### BitDefender:

It contains a distributed architecture. For different types of files and malware it has unique scanning engines. It has different kinds of plug-ins and each one is responsible for detection and removal of a specific malware. It can be deployed and used in different environments based upon its impressive modularized architecture.

BitDefender is completely independent of the platform and it is easily portable. It provides compatibility at binary level. This software tool is largely independent from the host operating system and this makes the detection more efficient without having any compatibility issues for any system.

## Part b:

## Cryptography Methods

### Triple Data Encryption standard (DES):

The original data encryption standard (DES) was replaced by the triple DES. The older versions were cracked by the hackers and the system exploitations were successful. So, the triple DES became the new method for securing the networks. It is highly recommended and one the most widely used symmetric algorithm in the industry.

It uses 3 individual keys, each consisting 56 bits. It makes a hardware encryption solution that is dependable and can be used in financial services and other industries.

### Advanced Encryption Standard (AES):

It is the standard encryption algorithm trusted by the U.S government. It is in 128-bit form and very efficient and effective. In case of severe type of encryption it uses 256 bits for this purpose.

It is qualified to be impenetrable to all kinds of attacks except the brute force attack. AES has the potential to become the standard in the encryption and eventually used in the private sector.

### Blowfish:

It is a symmetric cipher. Creates blocks of 64 bits for each message and then encrypt them one by one. It is extremely fast in terms of speed and highly effective in the domain of encryption. It is freely available in public domain.

It is one of the most flexible methods for encryption. Applications of blowfish can be found in the big industries like e-commerce, secure payments and password management tools. It is highly effective in securing the networks and protecting passwords and important information.

## Part c:

### Recommended Cryptography Methodology:

Based on the information collected on the cryptography methods for secure networks and algorithms described in the above section. My recommendations consist of the two advanced methodologies for this purpose:

1. Advanced Encryption Standard (AES): It is highly effective and also used by the American government as the standard of encryption for protecting computer networks. It is foolproof against most of the attacks.
2. Blowfish: It is fast and flexible. It is widely used in e-commerce industry and for securing payments which is very crucial element of an e-commerce website and network. So, it is one of the best option for securing networks.