# Computer Security Principles - Summary Questions

## Lecture: Course Overview

1. Distinguish between hacktivists, cyber criminals and Nation States in terms of cyber security actors.
2. With the aid of a diagram describe the concept of “Defence in Depth” in the context of cyber security
3. Describe the following areas which may put you at risk when connected to the network.

   Key loggers, Spyware, Cookies, Viruses, Worms, Back Doors, Trojans, Bot attack, web beacon, ransomware,

## Lecture: Security Concepts

1. Give an account of the CIA triad in the context of network security.
2. Discuss the three potential levels of impact on a company should there be a breach of security.
3. List four categories of assets present in a computer and describe how each of these asset types may be compromised in terms of Confidentiality, Integrity and Availability.
4. List four categories of attack that may take place on a company’s assets. Which class of attack would be most difficult to detect and mitigate against?
5. List three attack surface categories and give examples of attacks that could be launched against each of these surfaces.
6. List four fundamental security design principle and give brief overview of each.
7. Describe the following terms used in Computer Security Strategy:
   Security Policy, Security Implementation, Assurance and Evaluation.

## Lecture: Viruses

1. Describe what is meant by the following statement “Viruses have restricted propagating mechanisms and are parasitic in nature”
2. What is a virus?
3. Give an account of any four of the following types of virus (Note that you should be able to explain all) -
   Boot, File Infector, Macro, Resident, Direct Action, Overwrite,

Directory, Email, Companion, FAT, multipartite, polymorphic, XSS, Browser hijacker.

4. With the aid of a diagram give a detailed account of Cross-Site Scripting.
5. What is obfuscation technique? Give an account of the four virus obfuscation techniques:

   Encryption, Polymorphism, Metamorphism, Stealth

6. Name and describe four types of virus payloads (non, non-destructive, destructive, Droppers)

## Lecture: Worms

1. What is the major difference between worms and viruses?
2. What is an ODE (0 Day Exploit) worm?
3. Distinguish between a polymorphic and a metamorphic worm. Which are more difficult to deal with?
4. What is a multi-exploit worm?
5. Give an account of Flash Technique in relation to worm.
6. List steps you can take to safeguard against worm attacks?
7. Give an account of the STUXNET attack.

## Lecture: Botnets & Rootkits

1. What is a botnet?
2. How are distributed denial of service (DDOS) attacks carried out?
3. Describe 8 potential uses of botnets.
4. What is a Rootkit and mention two malicious applications of rootkits.
5. Give account of two primary functions of rootkits.
6. How do rootkits operate?
7. List four steps that can be taken to defend against rootkits.
8. How do you deal with a kernel level rootkit?

## Lecture: Social Engineering

1. What is social engineering in the context of computer security?
2. Discuss how the formation of inappropriate trust relationships is the basis for social engineering.
3. How do social engineers gain a foothold in an organisation’s IT system?
4. Discuss four of the following techniques for social engineering ( You should be able to explain all)
5. Pretexting, Phishing, Spear Phishing, IVR/Phone Phishing, Trojan Horse, Shoulder Surfing, Dumpster Diving, Road Apples, Quid pro quo
6. Describe four social engineering example scenarios.

7. List five policies that a company or an individual can implement to reduce the risk of social engineering.
8. Give account of the saying “There is no delete button on the web”.
9. What is a person’s digital footprint and distinguish between active and passive collection of data.

## Lecture: Anti-Virus & Firewall

1. Distinguish between a false positive and a true negative statistics in terms of virus detection capabilities of Anti-Virus software
2. Describe in detail three methods implemented by anti-virus software to detect malware.
3. Distinguish between signature-based, malicious activity based and Heuristic based virus detection techniques.
4. List three possible actions AV software can take if software is suspected as being malicious.
5. Comment on the ability of signature based detection in combating ODE (zero-day-exploits), polymorphic and metamorphic viruses.
6. Discuss in detail the three modes of operation of Heuristic virus detection.
7. In the context of virus detection what is a sandbox and where does it find use?
8. List 5 approaches that will help in eliminating virus threats.
9. What roles do firewalls play in computer security?
10. Draw a block diagram illustrating the operation of a personal firewall.
11. Name and describe the three modes of operation in firewall.
12. Distinguish between packet filter and stateful inspection modes of operation in a firewall.
13. Name and describe four firewall analysis mechanism.
14. What additional services can a firewall offer to clients in addition to traffic filtering?

## Lecture: Browser Usage

1. Describe three web browsing dangers.
2. Describe four ways through which web browsers can be breached.
3. Give an account of the mode of operation of the following: No Script, Web of Trust, AdBlock Plus, Ghostery, HTTPS Everywhere, Better Privacy, RequestPolicy, FlashBlock, Click&Clean, Disconnect and Site Advisor browser add ons.
4. Describe two security advantages that Google Chrome has over its competitor browsers.
5. Describe five safe browsing tips.

## Lecture: Privacy and Cookies

1. Describe a risk associate with the use of Google products (gmail, youtube etc) and how can they be counteracted.
2. List five channels through which information can leak from a personal computer.
3. List six types of information stored on a webserver logfile in response to connecting a browser navigating to a page on that server.
4. What are cookies used for?
5. What privacy risks do cookies present?
6. Give examples of private information we might inadvertently leak through our google searches.
7. Are Gmail emails private?
8. Give account of inter website tracking.
9. Give account of intra website tracking.
10. Draw a block diagram illustrating “cross-site tracking”
11. Describe behavioural targeting. What are its benefits to companies?
12. Give account of how a user’s home, work PC and laptop can be linked together.
13. What is AdSense? Give account of how it can be used to track user activities online.
14. Describe counter measures to protect your online identity

## Lecture: BYOD

1. List three major security issues associated with Android Smartphone
2. List security issues associated with Apple IOS
3. List ten steps you can take to secure you mobile phone.
4. List five mobile malwares.
5. What types of data should never be stored on a mobile phone.

## Lecture: Authentication

1. What is an authentication factor?
2. Describe with the aid of examples the three classes of authentication factors.
3. Give an example of two-factor authentication using a token card.
4. Give an example of biometric authentication. Why are users often unhappy with biometric authentication?
5. Explain how magnetic cards have inbuilt two-factor authentication that prevents card cloning.
6. Describe how the use of Smart Cards be compromised through side-channel attacks.
7. What is the principle of least privilege?
8. Describe how the “principle of least privilege” improves a system’s stability, security and easy of deployment of systems.
9. What is the golden rule relating to the use of passwords?

10. Describe classes of weak passwords.
11. Describe how you would choose a strong password.

## Lecture: Cryptography

1. Define the following terms: Cryptography, Cryptanalysis.
2. What is conventional cryptography?
3. Distinguish between symmetric and asymmetric cryptography
4. Give two advantages and two disadvantages of symmetric cryptography
5. Give a brief account of Asymmetric Cryptography in terms of public and private keys.
6. What do you understand by the term “session key”?
7. What do you understand by the term “key stretching”?
8. What do you understand by the term “ciphertext”?
9. Give account of how cryptographic strength can be measured.
10. With the aid of a block diagram briefly describe the principle of operation of a Digital Signature.
11. What is a hash function and how is it used in digital signatures.
12. List the three components of a Digital Certificate.
13. How are digital Certificates distributed?
14. Explain the terms PKI and CA in the context of Digital Certificate management
15. What is Certificate Revocation and how is it implemented?
16. Give a detailed account of how PGP works in terms of Encryption, Decryption, keys, Signing and Certificates.
17. Describe the web of trust process in PGP.

## Lecture: Wireless Security

1. Describe Piggybacking, War Driving home wireless threats and the problems associated with them.
2. Give account of an initialization vector attack.
3. List five things that can be done to protect a home wireless
4. Describe five threats associated with public wireless access
5. Describe the following wireless attacks:
6. Wireless Replay, Sinkhole, Evil Twin, WEP and WPA attacks, WPS attacks, BlueJacking, BlueSnarfing
7. List 4 steps you would take to protect yourself when using wireless networking in public places