Security in Computing & IT

Revision questions
Part 1

Week 1

- Explain the following terms in one sentence each: confidentiality, privacy, integrity, availability and authenticity of information.
- What is security by obscurity and what is security via legislation?
- What is a covert channel? Explain it on a simple example.
- What is the difference between a security policy and a security mechanism?

Week 2

- Explain the following security terms: vulnerability, exploit, attack, threat, threat agent
- What is CVSS? What are the metric groups used in CVSS? What are the metrics in each group?
- Explain the following malware types: virus, worm, Trojan horse, logic bomb, Easter egg
- Explain the following attack types: dictionary attack, replay attack, password sniffing, spoofing, denial of service.
- Explain the following terms: injection attack, rootkit, social engineering.
- What are the main steps when responding to an incident?
- What is the aim of DOS attacks? Explain the main DDOS attacks types.

Week 3

- What is a security mechanism? What are its main tasks? What types of mechanisms are used in computing? Give an example of each.
- What is the difference between pervasive and specific security mechanisms? Give an example for each.
- What are the security trade-offs?
- How can you measure risk?
- What is encryption? What is the role of an encryption key?
- What is the basic difference between symmetric key encryption and asymmetric key encryption?
- Compare symmetric and asymmetric key encryption (keys, security, complexity, speed)
- What is a stream cipher and what is a block cipher?
- Explain each of the following methods: describe their characteristics and most important features. AES, RSA, Diffie-Hellman.
- Explain cipher block chaining and electronic code book (ECB) encryption.
- What is a hash (or secure digest) function and what are its main features?
- What is a digital signature used for? How is it produced?

Week 4

- What is the difference between identification and authentication?
- What are the three main authentication factor types? Give a real-life example of multifactor authentication.
- What is single sign-on?
- Explain the challenge-response authentication method. How is it used with passwords?
- Explain the difference between http Basic and http Digest authentication
- Explain the following three password protection methods: exponential backoff, blacklisting, reverse Turing test
- What is a one-time password? Explain one method of generating it.
- What is biometric authentication? What is the difference between physiological and behavioural methods?
- What is iris recognition used for in computing, and how?
- What are the main problems in fingerprint authentication?
- What are the major issues in face recognition?
- What is an X.509 certificate for? What does it contain and how is it secured? What is a Certificate Revocation List?
- Explain the role of a Certificate Authority in Public Key Infrastructure.
- For what purpose is the Kerberos protocol used? Who are the participants in the protocol?

Week 5

- What is the difference between authentication, access control and authorisation? What is the connection between them?
- Explain the terms ‘subject’ and ‘object’ in relation to access control.
- What is the access control matrix? What are the columns and rows representing?
- What is an access control list and what is an access control capability? Which one is easier to maintain and why? Which method is used in (i) Windows and in (ii) Unix?
- Mention at least two methods used by the Apache web server for access control.
- What are the two types of access control in a network? Explain them briefly.
- Compare mandatory and discretionary access control. What is the basic difference, and what other features differ?
- How are privileges assigned to a user in role-based access control?
- Explain what a role hierarchy is and how it is related to permission inheritance.
- What is a private role in RBAC?
- Explain the following terms with relation to RBAC: separation of duty, cardinality and prerequisite roles.
- What is SELinux? State its most important features in one sentence.

Week 6

- Explain the following security principles: least privilege, economy of mechanism, open design, complete mediation, permission basis, separation of privilege, least common mechanism, ease of use
- What is the difference between user-oriented access control and data-oriented access control?
- What is security by separation? Explain it in the context of physical, temporal, logical and cryptographic separation.
- Explain the memory layout of a user program. What segments are there, and what do those segments contain? How does segmentation help security?
- What is virtual memory and what is the major limitation in protecting it?
- File access control is based on two major factors. What are they?
- What is file permission inheritance? How can it be overridden?
- Explain temporarily acquired file permissions. What can they be based on? Give an example for each method.
- What type of storage system failures affect file system reliability? List them, and explain each.
- Explain the key concepts of redundant array of independent disks (RAID).
- Explain the Unix file protection model (what type of access control it uses, how permissions are set and how access authorisations are granted).
- Explain the Windows file protection model (what type of access control it uses, how permissions are set and how access authorisations are granted).