Security in Computing & IT

Revision questions
Part 2

Week 7

- On what levels has database integrity to be provided?
- Explain a method used to ensure that updating data in a database is done in a reliable manner.
- Explain a usual method used to prevent data loss in a database.
- What is two-phase updating and why is it used?
- What does a database monitor do?
- What access constraints can be imposed on sensitive data?
- Explain why the following types of disclosures can violate confidentiality: bounds of data values, existence, probable value, negative query result.
- What is the difference between data suppression and data concealing?
- What are the major security threats in database queries and database updates?
- What is a statistical inference attack on a database? Explain it on an example.
- What is a direct inference attack on a database? Explain it on an example.
- What is an indirect inference attack on a database? Explain it on an example.
- Why is data aggregation a threat to privacy?
- What is an SQL injection attack? Explain it on an example.
- Compare the hot-swap and off-line backup methods. How are they done and what are the advantages of each?
- Compare the incremental and mirroring backup methods. How are they done and what are the advantages of each?
- Why is backup separation important? What types of separation are the most prevalent?
- Compare the multilevel database integrity lock and the multilevel database sensitivity lock. What do they have in common, and how do they differ?
- What are the major issues with distributed databases?

Week 8

- Wired media can be easily tapped for eavesdropping. Is this statement true for every wired media? Explain the case for coaxial cable, twisted pair and optical fibre.
- What are the major security issues with wireless communication?
- Compare wired and wireless media security. Explain the advantages and disadvantages of both.
- What is the main function of a firewall?
- How many network nodes can a firewall protect?
- What are the basic differences between a dedicated firewall device and firewall software running on the protected device?
- What is a packet filter and what is a proxy? What is common in them, and how do they differ?
- Name at least two Internet-related security protocols, and indicate in which OSI layer they are used.

- What are the main aims of a host compromise?
- How can direct flooding be used in a denial of service attack? Can indirect flooding be used?
- What is a botnet? Describe how it is organised, how it works and name one famous one. (Look at lectures 2, 8 and 12 as well)
- How does a person-in-the-middle attack work? How does it differ from traffic diversion?
- Explain three ways of session hijacking.
- What are the most frequent targets when network administration is attacked?
- What are the main differences between audit trails and logs?
- What are the advantages and disadvantages of network-based, host-based, application-based and target-based intrusion detection?
- What are the basic differences between misuse and anomaly based intrusion detection?
- Explain the steps in kill chain analysis.
- What are the roles of red and blue teams in penetration testing?

Week 9

- What are the major security threats of embedded content in web pages?
- What are the main security issues related to communication produced by web scripting?
- Explain the *sandbox* web security policy.
- Explain the *same origin* web security policy.
- What are the possible dangers when using a URL to find a web page? Is typing it in, cutting and pasting or clicking on a link more secure? Why?
- What is cross-site scripting? How does it work? Explain at least two types of XSS attacks.
- What are the possible consequences of a cross-site script attack? Name at least four.
- How can the possibility of cross-site scripting attacks be reduced by the web site maintainer and by the browser/user?
- What is cross-site request forgery? Why is it extremely dangerous?
- What are the most frequent variants of CSRF? How can the browser/user mitigate the danger, and how can the web site maintainer reduce the risk?
- What is clickjacking? How does it work?
- How can the browser/user mitigate the danger of clickjacking, and how can the web site maintainer reduce the risk?
- What is cross-site framing? Explain the method.
- What is cross-site double clicking? Explain the method.
- Explain what a web crawler does and for what purpose.
- Explain the three main policies a web crawler should observe.
- Explain at least four blackhat methods that are used by unscrupulous web site maintainers to improve the search ranking of a web page.
- What is the purpose of search engine optimisation poisoning?
- How are blackhat methods used in search engine optimisation poisoning?

Week 10

- Consider physical security and software security of (i) mobile computers and (ii) fixed hosts. Explain which one is more important in case (i) and in case (ii) and why it is so.
- What is the main security issue when a mobile computer is attached to a (i) wired network and when to a (ii) wireless network.
- Explain the major security issue in WiFi hotspots.
- Explain at least three major security issues in WiFi home networks.
- Explain at least four reasons why WEP has been superseded by better protection methods.
- What are the main security advantages of WPA/WPA2 over WEP?
- What security services are available in Bluetooth?
- What are the Bluetooth security levels for services and for devices?
- Explain at least three Bluetooth vulnerabilities.
- Explain two major protection methods used by the manufacturer to protect iPhones.
- What is 'jailbreaking an iPhone'?
- Name at least three methods used to propagate mobile phone malware.
- Explain how (mobile) malware evolves.
- What is phishing and how does it work?
- What is spear phishing and what is vishing? (Look at lecture 12 too)
- What is pharming? (Look at lecture 12 too)
- Mention at least four different types of information that can be obtained by spying on mobile phones.
- Describe some mobile spyware/malware detection and defence methods.

Week 11

- What are the major security and privacy concerns in cloud computing, and how can they be addressed?
- What is the business model of social network sites? How does that affect privacy?
- What is the purpose of a privacy policy e.g. in a social network? How effective are those policies in practice?
- Explain why trust modelling in social networks can be considered simplistic.
- Why does personal data need more protection than financial data?
- What is the major concern with single sign-on between social sites?
- What limitations need to be considered on personal information directly published on the web?
- Explain two ways of indirect publishing of personal data by social network friends.
- Explain the indirect publishing of personal data by social network applications.
- Why do employers monitor social network sites? Explain at least two reasons.
- Explain at least four ways of criminal use of social network sites.
- What information can be collected from social network sites by law enforcement agencies?
- Describe three types of services that use location as the main input parameter.
- Explain the main components of location-based services.
- Explain the primary functions of the Office of the Australian Information Commissioner briefly.

Week 12

- Explain the steps in processing a credit card payment via the Internet.
- What technology is available to prevent phishing?
- Explain the reason for authenticating emails, and describe two email authentication methods.
- Describe three methods of mobile banking.
- Explain a popular digital currency. How does it work and how can be it attacked?
- What are the six major requirements of the Payment Card Industry Data Security Standards?
- Explain what the Darknet is. What is the Darknet market?
- What is Blackhole and what are the most important features of it?
- What are the advanced technological features of botnets?