Information Security Tutorials [ETCS-401]

Dr. A K Yadav
Amity School of Engineering and Technology
(affiliated to GGSIPU, Delhi)
akyadav1@amity.edu
akyadav@akyadav.in
www.akyadav.in
+91 9911375598

December 10, 2020

Tutorial 1

1. Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA. Define each of these terms.
2. Give a concrete example where confidentiality is more important than integrity.
3. Give a concrete example where integrity is more important than confidentiality.
4. Give a concrete example where availability is the overriding concern.
5. From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important?

6. Discuss a significant World War II event where broken Enigma messages played a major role.
7. How effective is the CAPTCHA? How user-friendly is the CAPTCHA?
8. Why do you hate CAPTCHAs?

Tutorial 2

1. When you want to authenticate yourself to your computer, most likely you type in your username and password. The username is considered public knowledge, so it is the password that authenticates you. Your password is something you know.
   - 1.1 It is also possible to authenticate based on something you are, that is, a physical characteristic. Such a characteristic is known as a biometric. Give an example of biometric-based authentication.
   - 1.2 It is also possible to authenticate based on something you have, that is, something in your possession. Give an example of authentication based on something you have.

1.3 Two-factor authentication requires that two of the three authentications methods (something you know, something you have, something you are) be used. Give an example from everyday life where two-factor authentication is used. Which two of the three are used?

2. Malware is software that is intentionally malicious, in the sense that it is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.
   2.1 Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, why have you been so lucky?
   2.2 In the past, most malware was designed to annoy users. Today, it is often claimed that most malware is written for profit. How could malware possibly be profitable?
3. What is war dialling and war driving? What is war carting?
4. Suppose that we have a computer that can test 2^{40} keys each second.

4.1 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{88}?

4.2 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{112}?

4.3 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{256}?

5. What kind of attacks are possible on mobile/cell phones? Explain with example.
6. Explain the countermeasures to be practised for possible attacks on mobile/cell phones.
7. What kind of cyber security measures an organization should have to take in case of portable storage devices? Prepare security guidelines which can be implemented in an organization.
8. Explain the various measures for protection of laptops through physical and logical control measures.

Tutorial 3

1. What is security breach? Explain the impact it has on an organization.
2. What are Personal Information (PI) and Sensitive Personal Information (SPI)? Explain with appropriate examples.
3. What is meant by "insider threat"? How does it affects an organization?
4. Are information security and cyber security two independent domains? Explain your answer with example to support your rationale.
5. What are four dimensions of privacy? Do they all relate to data security? Justify your answer with suitable example.
6. What are some key challenges to organization discussed in the last classes?

7. What is Information Classification? How can you classify information?
8. What is the role and responsibilities of Information custodian?

Tutorial 4

1. If your were a owner of an organization, what actions you were taken to secure information of your user?
2. Supreme Court of India limited use of Aadhaar in some scheme of Indian government and in some scheme the court permitted. Why? Explain your view.
3. What is MAC address and IP address?
4. Explain ARP poisoning with example.
5. What do you mean by Protocols? Give example of some day to day life protocols and some example of security and authentication network protocols.
6. What is the role of ports in Internet? List some port number with their services.

7. Explain protocols and applications of the layers of network models.
8. What is the difference between TCP and UDP protocols? On which layer of OSI model they work?

Tutorial 5

1. What are the different networking devices?
2. On which layer of OSI model, the above networking devices operate?
3. What is the role of router in Information Security?
4. What are the differences between Switch and Bridge?
5. What are the differences between Router and Gateways?
6. Why do we need Information Security?
7. Define Cultural mores, Ethics and Laws. Explain with some real life example.
8. What is the difference between Ethics and Laws. Give some example of ethics which is not laws and some example of ethics which is not acceptable as per laws.
9. What are the different laws for Information Security?

Tutorial 6

1. Give some example of ethical difference between different cultures.
2. List some International Laws and Legal Bodies for Information Security. Explain in brief.
3. What is the difference or relationship between Policy and Law?
4. How can you stop unethical and illegal Behaviour?
5. Explain some Codes of Ethics for any Professional Organizations.
6. What are the three steps of Risk Management? Explain in detail.
7. What are the Security Threats to E-Commerce?
8. How can you protect yourself from the E-Commerce Threats?
9. What are the different Business Transactions taking place on web?

Tutorial 7

1. What are the different electronic payment system are used now a days?
2. What do you mean by Digital Forensics? What are the different types of Digital Forensics?
3. Why physical security of a system is important?
4. How can we insure physical security of information? .
5. Explain the role of access control, authentication and user identification in the context of security.
6. If a certain human physiological characteristic is to be used in biometrics, it has to satisfy certain criteria. Explain these criteria.

7. Explain how matching and enrolment processes work in biometrics and what purposes they serve together.
8. What are the key success factors for biometric systems to work? Illustrate with examples wherever possible.
9. Explain the basic steps involved in the process flow of any biometric systems.

Tutorial 8

1. What are the relative advantages and disadvantages of biometrics?
2. What are the criteria used while selecting a biometric characteristics to design a biometric system?
3. Present your understanding about the critical technical issues in a biometric system design.
4. Is the issue of data protection related with biometrics? Explain with suitable arguments.
5. Using the Internet resources, find out details of at least four finger recognition systems or devices and do comparative feature analysis.
6. Explain the meaning of various key terms associated with cryptography.

7. Explain the concept of ciphers. What are the various types of ciphers that exist?
8. What is the difference between block cipher and stream cipher systems?

Tutorial 9

1. Explain the role of cryptography in information systems security.
2. With a suitable illustration, explain the working of digital signatures. What is a message digest?
3. What is the role of a trusted certificate in message authentication? Explain how it is useful in e-commerce?
4. Why is key management essential? Discuss the various functions under key management.
5. With suitable diagrams, explain the working of symmetric and asymmetric encryption methods.
6. Compare private- and public-key methods in terms of their relative advantages and disadvantages.

7. How do you place steganography in the context of cryptography? Explain how (digital) watermarking is related to steganography.
8. Explain the scientific principle on which the concept of quantum cryptography is based.
9. Explain what firewalls are and why do organizations need them.

Tutorial 10

1. Explain various approaches to the deployment of firewalls. Why is the concept of 'demilitarized zone' so important?
2. What is the role played by a proxy server?
3. What are the different types of firewall configurations that you are aware of? Explain how they function.
4. Explain the role of routers and intrusion detection systems in the context of firewalls.
5. Discuss key design and implementation issues for firewalls. Explain the critical role of firewall policies that the organizations must consider.
6. Explain how network security matters in the modern digital world in which today's extended enterprises operate.

7. Explain the concept of network trust.
8. What are the three main types of networks that must be considered when defining a security policy?
9. Explain the various methods of attack on a network.

Tutorial 11

1. Why is security perimeter an important concept? Explain with suitable examples. What considerations should be made in the design of perimeter security?
2. What is an intrusion detection system? Explain the need for having an intrusion detection system in place.
3. Explain the various stages followed by intruders to attack networks.
4. What are the two most well-known conceptual approaches to the design of intrusion detection systems? Compare them in terms of their relative advantages and disadvantages.
5. What are the various categories of intrusion detection systems?

6. What are the characteristics of a good intrusion detection system?
7. Why do organizations perform network penetration tests?
8. Do routers play a role in intrusion detection? Explain.
9. What can organizations do to ensure security of their network routers? Explain with examples.

Tutorial 12

1. Describe the challenges faced by the intrusion detection systems.
2. What care needs to be taken while implementing intrusion detection systems in organizations?
3. Using suitable diagram(s) explain what virtual private networks are and why do organizations need them.
4. Explain the crucial role of VPNs in today's net-centric digital enterprises.
5. In the context of security, how do tunnelling protocols work for VPNs? Why is authentication important?
6. What are the business scenarios under which different kinds of VPNs get used?

7. What are the various VPN technologies available today? Explain.
8. Describe the various well-known VPN architectures as discussed in the due course.
9. In the light of what you have learned, provide a comprehensive view of parameters that put forth the strong need for VPN security.

Thank you

Please send your feedback or any queries to **akyadav1@amity.edu**
You can contact me on **+91 9911375598**