Information Systems Security: exercises on foundational techniques for cybersecurity

Diana Berbecaru
< diana.berbecaru @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

AA 2023-2024

Outline

- **questions (multiple-choice)**
  - part 1: security properties
  - part 2: security attacks
  - part 3: risk management

Questions:
Security properties

Question 1

- **Alice wants to open a communication channel with Bob. Which of the following security properties she must implement in order to check that she is really communicating with Bob?**
  - A. non-repudiation
  - B. integrity
  - C. availability
  - D. peer authentication
  - E. data authentication
  - F. privacy
  - G. accountability

© D.Berbecaru (Politecnico di Torino, 2023)

Question 2

- **Assume Alice sends a message to Bob. Bob knows that he has to perform data authentication. What does it mean?:**
  - A. Bob must register the received data in a database
  - B. Bob must identify Alice (e.g. check her identity card)
  - C. Bob must verify that the data really comes from Alice (for example, by verifying some sort of evidence attached to the data that only Alice may have created)
  - D. Bob must demonstrate his identity to Alice

Question 3

- **Assume Alice wants to connect to two systems run by Bob. Alice and Bob must always perform the mutual authentication. What does it mean?:**
  - A. Alice authenticates to every system run by Bob and each of the two systems of Bob authenticate to Alice
  - B. Bob authenticates to Alice
  - C. Alice authenticates to the two systems run by Bob
  - D. each of the two systems of Bob authenticate to Alice
  - E. Alice and Bob must identify themselves, e.g. by exchanging their identity cards

Question 4

- **Assume Alice is entering a password (or a PIN) to access her smartphone. Which security property is implemented by her smartphone for this operation?**
  - A. confidentiality
  - B. integrity
  - C. authentication
  - D. availability
  - E. authorization

Question 5

- **In Windows OS there are two types of users: normal and administrator. Assume a normal user tries to install a program and this operation is denied by the OS. Which security property the OS has implemented for software installation operation? (we assume the user has already logged in successfully with his credentials):**
  - A. authentication
  - B. authorization
  - C. traceability
  - D. availability

Question 6

- **Alice writes some data on her disk. The disk is placed in a secure place. After some time she wants to check whether the data has been modified. Which security property does she have to implement?**
  - A. authentication
  - B. authorization
  - C. traceability
  - D. integrity
  - E. availability

Question 7

- **Alice wants to protect the entrance in a building with a card reader. Which security property/properties must implement the card reader placed at the entrance?**
  - A. authentication
  - B. authorization
  - C. non-repudiation
  - D. integrity

© D.Berbecaru (Politecnico di Torino, 2023)

Questions:
Basic Security Attacks

Question 8

- **What is a replay attack?**
  - A. an attack in which some data (in clear or protected for confidentiality) can be intercepted and then sent more than once to the destination
  - B. an attack in which only data in clear can be intercepted and then sent more than once to the destination
  - C. an attack in which an attacker intercepts the data, then sends it to another attacker who will send it to the destination

© D.Berbecaru (Politecnico di Torino, 2023)

Question 9

- **What is a sniffing attack?**
  - A. an attack in which data (in clear or protected) is intercepted while in transmission
  - B. an attack in which only data in clear can be intercepted
  - C. an attack in which an attacker intercepts the data, then modifies it, then finally sends it to the destination

Question 10

- **What is an IP spoofing attack?**
  - A. an attack in which the attacker creates fake date and inserts it into a connection
  - B. an attack in which an attacker modifies the IP source address and sends it to a destination
  - C. an attack in which an attacker modifies the IP destination address and sends it to the destination
  - D. an attack in which an attacker modifies both the source and the destination addresses in an IP packet

© D.Berbecaru (Politecnico di Torino, 2023)

Question 11

- **What kind of countermeasures are applicable for an IP spoofing attack aimed to gain unauthorised access to a remote resource?**
  - A. instruct the browser's users to carefully check the URL they are connecting to
  - B. avoid the use of broadcast networks
  - C. avoid the use of the IP address as "credential" to authenticate and get access to any remote resources
  - D. install (and regularly update) an anti-malware application on each device

Question 12

- **What is a Denial of Service attack?**
  - A. an attack in which the attacker keeps a host busy by exhausting its resources (e.g. mail) so that it cannot provide its services
  - B. an attack in which the attacker keeps a host busy by flooding it with traffic (e.g. DNS or ICMP) so that it cannot provide its services
  - C. an attack in which an attacker keeps a host busy by exhausting its resources (e.g. by injecting a malware that makes continuous calculations) so that to block the use of the host
  - D. an attack in which an attacker denies the use of a host to a user because he/she is not authorized

© D.Berbecaru (Politecnico di Torino, 2023)

Question 13

- **What is Distributed Denial of Service (DoS) attack?**
  - A. attack in which the attacker (master) exploits multiple deamons installed on compromised nodes to run (upon command) a software implementing the DoS attack against one victim
  - B. attack in which an attacker (master) distributes the DoS software to multiple nodes that run independently the attack against different victims
  - C. attack in which attackers (masters) collaborate and decide along with the zombies which type of DoS attack to run

Question 14

- **Bob is an attacker who decides to activate a shadow server to attack Alice. What kind of attacks can he perform against Alice (to provoke damage)**
  - A. replay attack
  - B. Denial of Service
  - C. redirect Alice to fake web sites
  - D. packet sniffing

Question 15

- **Alice wants to communicate securely with Bob (server). What kind of security properties must she implement to protect from Man in the Middle attack? Note: we assume Alice and Bob have trusted devices and software**
  - A. server authentication, data authentication, confidentiality of the data exchanged, integrity of the data exchanged
  - B. server authentication, confidentiality of the data exchanged, integrity of the data exchanged, serialization of each packet
  - C. server authentication, data authentication, confidentiality of the data exchanged, integrity of the data exchanged, and serialization of each packet
  - D. privacy of the data exchanged, server authentication, data authentication, integrity of the data exchanged, serialization of each packet

© D.Berbecaru (Politecnico di Torino, 2023)

Questions:
Risk Management

Question 16

- **In risk analysis, assets are:**
  - A. any ICT resource, data, and people present or working inside a company
  - B. any ICT resource, data, and people used for providing a service
  - C. the ICT resources, data, people, and location used in providing a specific service
  - D. the ICT resources, data, people, and location used in providing the services offered by the company

© D.Berbecaru (Politecnico di Torino, 2023)

Question 17

- **In risk analysis, vulnerabilities are:**
  - A. weaknesses in the software that could be exploited by an attacker
  - B. weaknesses in the design, implementation, configuration and management that could be exploited by an attacker
  - C. actions an attacker performs to damage an asset
  - D. weaknesses in the design, implementation, configuration and management that could harm assets if exploited by an attacker or by occurance of unintentional events (natural disasters, mistakes performed by individuals)

© D.Berbecaru (Politecnico di Torino, 2023)

Question 18

- **In risk analysis, a security control is:**
  - A. a set of operational and management processes, and security mechanisms (including software techniques, algorithms and protocols) used to protect against threats
  - B. functional and non-functional requirements that need to be satisfied in order to achieve security
  - C. a set of operational and management processes, and security mechanisms (including software techniques, algorithms and protocols) adopted to reduce risks

© D.Berbecaru (Politecnico di Torino, 2023)

Question 19

- **In risk analysis, a risk is:**
  - A. a qualitative (e.g., low, medium, high, very high) or quantitative (e.g. 10, 15, 25) value calculated based on the impact and the probability of occurrence of a security event
  - B. a cost calculated based on the countermeasures to be selected and implemented to protect against a security event
  - C. possible deliberate action/accidental event that can produce the loss of a security property

© D.Berbecaru (Politecnico di Torino, 2023)

Question 20

- **What are the security controls and procedures?**
  - A. documents expressing ‘how’ you implement the policies, both for the technical details (such as specific techniques, algorithms used) and organizational details
  - B. documents expressing the vulnerabilities of a system or product
  - C. documents expressing the flaws in the implementation of a system of product

© D.Berbecaru (Politecnico di Torino, 2023)

Question 21

- **Which of the following is not a purpose of doing a risk analysis?**
  - A. delegate responsibility
  - B. quantify impact of potential threats
  - C. identify risks
  - D. define the balance between the impact of a risk and the cost of the necessary countermeasure

© D.Berbecaru (Politecnico di Torino, 2023)