COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 1

ITU-T (International Telecommunication Union, Telecommunication Standardization Sector)

- The X.800 *Security Architecture for Open Systems Interconnection (OSI)* gives a systematic way of defining and providing security requirements http://www.itu.int/rec/T-REC-X.800-199103-I/e

The Requests for Comments (RFC) document series is a set of technical and organizational notes about the Internet; published by the Internet Engineering Task Force which develops Internet standards.

- RFC4949 *Internet Security Glossary* - obsoletes RFC2828 https://www.rfc-editor.org/info/rfc4949

National Institute of Standards and Technology (NIST)

- FIPS 199 – *Standards for Security Categorization of Federal Information and Information Systems.* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
- NIST SP 800-12 *An Introduction to Information Security* – obsoletes NIST95 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

1. Do X.800, RFC 4949, FIPS 199, and NIST SP 800-12 define each of the following concepts:
    a. cyberspace
    b. cybersecurity
    c. computer security
    d. information security
    e. data security
    f. network security

    If yes, are the definitions consistent?

    If not, is there a similar concept defined in the document in question?

Solution:

X.800

a. It does not define 'cyberspace'.
b. It does not define 'cybersecurity' or 'cyber security'.
c. It does not define 'computer security'.
d. It does not define 'information security'.
e. It does not explicitly define 'network security' but we note that X.800 is focused on network architecture and placement of security services and mechanisms on different network layers.

The only term related to the above that X.800 defines is 'security'. In Anex A, it is defined as

> 'The term "security" is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.'

RFC 4949

a. While the term 'cyberspace' is not defined, it is mentioned on page 100, and it is implied that it is related to 'structures of computer networks'.
b. It does not define 'cybersecurity' or 'cyber security'.
c. 'Computer security' is defined as 'Measures to implement and assure security services in a computer system, particularly those that assure access control service.'
d. 'Information security' is defined as 'Measures that implement and assure security services in information systems, including in computer systems (see: COMPUSEC) and in communication systems'
e. It does not explicitly define 'network security' but it refers to it in several places and refers to 'communication systems' in the definition of 'Information Security'.

FIPS 199

a. It does not define 'cyberspace'.
b. It does not define 'cybersecurity' or 'cyber security'.
c. It does not define 'computer security', although the document is authored by the 'Computer Security Division' of NIST.
d. 'Information security' is defined as 'The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.'
e. It does not define 'network security'.

NIST SP 800-12

a. It does not define 'cyberspace'.
b. The term 'cybersecurity' is used to replace the term "Information Assurance' that is defined as 'Measures that protect and defend information and information systems by

ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.'

c. It does not define 'computer security', although the document is authored by the 'Computer Security Division' of NIST, and uses it as a keyword.
d. 'Information Security' is defined as 'The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.'
e. It does not define 'network security'.

The definitions are more or less consistent. There are some inconsistencies, for example, in NIST SP 800-12, Information security refers to confidentiality, integrity, and availability while Information assurance refers to availability, integrity, authentication, confidentiality, and non-repudiation. Information Security refers to information systems, and sometimes also includes information itself; in RFC 4949 it also includes communication systems.

2. Do RFC 4949, FIPS 199, and NIST SP 800-12 define security services, mechanisms, and attacks? If yes, are the definitions consistent with X.800?

Solution:

Security Services

a. **X.800**
b. **RFC 4949:** A processing or communication service that is provided by a system to give a specific kind of protection to system resources. (See: access control service, audit service, availability service, data confidentiality service, data integrity service, data origin authentication service, non-repudiation service, peer entity authentication service, system integrity service.) Security services implement security policies, and are implemented by security mechanisms.
c. **NIST 199:** Referred to 'Security Objectives'; not explicitly defined except that 'The FISMA defines three security objectives for information and information systems:' and then confidentiality, integrity and availability are listed.
d. **NIST SP 800-12:** Refers to 'Security Objectives' as 'The first step in the management process is to define security objectives commensurate with risk for the specific system. Although this process may begin with an analysis of the need for integrity, confidentiality, and availability, it may not stop there. A security objective needs to be specific, concrete, well defined, and stated in such a way that it is a clearly achievable objective. Stakeholders play an important role in developing comprehensive, yet practical, policy. Therefore, it is imperative to remember that policy is not created by management personnel only.'

Security Mechanisms

a. **X.800**
b. **RFC 4949:** A method or process (or a device incorporating it) that can be used in a system to implement a security service that is provided by or within the system. (See: Tutorial under "security policy". Compare: security doctrine.)
Usage: Usually understood to refer primarily to components of communication security, computer security, and emanation security.
Examples: Authentication exchange, checksum, digital signature, encryption, and traffic padding.
c. **NIST 199:** Refers to 'Security Controls', which it defines as 'The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
d. **NIST SP 800-12:** Refers to 'Security Controls' which it defines as 'The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, availability, and integrity of the system and its information.' – same as NIST 199.

Security Attacks

a. **X.800**
b. **RFC 4949:** An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat. (See: penetration, violation, vulnerability.)
   A method or technique used in an assault (e.g., masquerade). (See: blind attack, distributed attack.)
c. **NIST 199:** It does not define security attacks but talks about 'a breach of security (i.e., a loss of confidentiality, integrity, or availability)' and discusses the impact of the breach (low, moderate, high)
d. **NIST SP 800-12:** Defines 'threats' and 'vulnerabilities' together as 'A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source. 6 Vulnerabilities leave systems susceptible to a multitude of activities that can result in significant and sometimes irreversible losses to an individual, group, or organization. These losses can range from a single damaged file on a laptop computer or mobile device to entire databases at an operations center being compromised. With the right tools and knowledge, an adversary can exploit system vulnerabilities and gain access to the information stored on them. The damage inflicted on compromised systems can vary depending on the threat source.'

3. What security services are specified in X.800, RFC 4949, FIPS 199, and NIST SP 800-12?

Solution:

a. **X.800:**
   - Peer entity authentication
   - Data origin authentication
   - Access control
   - Data confidentiality
   - Traffic flow confidentiality
   - Data integrity
   - Non-repudiation with proof of origin
   - Non-repudiation with proof of delivery

b. RFC 494
   - Access control service
   - Audit service
   - Availability service
   - Data confidentiality service
   - Data integrity service
   - Data origin authentication service
   - Non-repudiation service
   - Peer entity authentication service
   - System integrity service

c. NIST 199
   - Confidentiality
   - Integrity
   - Availability

d. NIST SP 800-12
   - Confidentiality
   - Integrity
   - Availability
   - Other objectives as defined by the organisation

4. What security mechanisms are specified in X.800, RFC 4949, FIPS 199, and NIST SP 800-12?

Solution:

a. **X.800:**
   - Encipherment
   - Digital signature
   - Access control mechanisms
   - Data Integrity
   - Authentication exchange
   - Traffic padding
   - Routing control
   - Notarization

b. RFC 494
   - Authentication exchange
   - Checksum
   - Digital signature
   - Encryption
   - Traffic padding
   - …

c. NIST 199
   - technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability

d. NIST SP 800-12
   - Access Control: account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination
   - Awareness and training: security awareness training, role-based security training, and security training records.
   - Audit and accountability: security assessments, system interconnections, plans of action and milestones, and continuous monitoring
   - Configuration management: baseline configuration, configuration change control, security impact analysis, least functionality, and software usage restrictions
   - Contingency planning: contingency plan, contingency training, contingency plan testing, system backup, and system recovery and reconstitution
   - Identification and authentication: device identification and authentication, identifier management, authenticator management, authenticator feedback, and re-authentication
   - Individual participation: consent, redress, privacy notice, privacy

act statements for federal agencies, and individual access

- Incidence response: incident response training, incident response testing, incident handling, incident monitoring, and incident reporting
- Maintenance: controlled maintenance, maintenance tools, nonlocal maintenance, maintenance personnel, and timely maintenance
- Media protection: media access, media marking, media storage, media transport, and media sanitization
- Privacy authorisation: authority to collect, purpose specification, and information sharing with external parties
- Physical and environmental protection: physical access authorizations, physical access control, monitoring physical access, emergency shutoff, emergency power, emergency lighting, alternate work site, information leakage, and asset monitoring and tracking
- Planning: system security plan, rules of behavior, security concept of operations, information security architecture, and central management
- Program management: information security program plan, information security resources, plan of action and milestone process, system inventory, enterprise architecture, risk management strategy, insider threat program, and threat awareness program
- Personal security: personnel screening, personnel termination, personnel transfer, access agreements, and personnel sanctions
- Risk assessment: security categorization, risk assessment, vulnerability scanning, and technical surveillance countermeasures survey
- System and services acquisition: allocation of resources, acquisition process, system documentation, supply chain protection, trustworthiness, criticality analysis, developer-provided training, component authenticity, and developer screening
- System and communication protection: application partitioning, denial of service protection, boundary protection, trusted path, mobile code, session authenticity, thin nodes, honeypots, transmission confidentiality and integrity, operations security, protection of information at rest and in transit, and usage restrictions
- System and information integrity: flaw remediation, malicious code protection, security function verification, information input validation, error handling, nonpersistence, and memory protection

5. What security attacks are specified in X.800, RFC 4949, FIPS 199, and NIST SP 800-12?

Solution:

a. **X.800:**
   - Masquerade
   - Replay
   - Modification of messages
   - Denial of Service
   - Wiretapping
   - Traffic analysis
   - Trapdoor
   - Trojan horse

b. RFC 494
   - Active wiretapping
   - Denial-of-service
   - Birthday attack
   - Blind attack (type of attack)
   - Brute force
   - Buffer Overflow
   - Chosen-cyphertext attack
   - Chosen-plaintext attack
   - Cyphertext-only attack
   - Cut-and-paste attack
   - Dictionary attack
   - Man-in-the-middle attack
   - …

c. NIST 199
   - Loss of confidentiality
   - Loss of integrity
   - Loss of availability

d. NIST SP 800-12
   - Social media
   - Social engineering
   - Advanced Persistent Threat
   - Insider threats: Destroying hardware or facilities; Planting malicious code that destroys programs or data; Entering data incorrectly, holding data, or deleting data; Crashing systems; Changing administrative passwords to prevent system access
   - Malicious hacker threats
   - Malicious code threats; Trojan horse, worm, logic bomb, ransomware

6. Create tables showing security services, security mechanisms and security attacks based on those defined by ITU-T Recommendation X.800, and their brief descriptions, as indicated below.

Security Services	
Confidentiality	The protection of data from unauthorized disclosure.

Security Mechanisms	
Encipherment	The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Security Attacks	
Release of message contents	Opponent learning the content of a message.

a. Create a matrix to show the relationship between security services and mechanisms, as indicated below.

	Encipherment							
Confidentiality	Yes							

b. Create a matrix to show the relationship between security services and attacks.
c. Create a matrix to show the relationship between security mechanisms and attacks.

Solution:

Security Services	
Peer entity authentication	This service is provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection.
Data origin authentication	The data origin authentication service provides the corroboration of the source of a data unit. The service does not provide protection against duplication or modification of data units.
Access control	This service provides protection against unauthorized use of resources accessible via OSI. These may be OSI or non-OSI resources accessed via OSI protocols. This protection service may be applied to various types of access to a resource (e.g., the use of a communications resource; the reading, the writing, or the deletion of an information resource; the execution of a processing resource) or to all accesses to a resource.
Confidentiality	These services provide for the protection of data from unauthorized disclosure
Traffic flow confidentiality	This service provides for the protection of the information which might be derived from observation of traffic flows.
Data integrity	These services counter active threats and detect any modification, insertion, deletion or replay.
Non-repudiation with proof of origin,	The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.
Non-repudiation with proof of delivery	The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

Security Mechanisms – we list only specific security mechanisms	
Encipherment	Encipherment can provide confidentiality of either data or traffic flow information and can play a part in or complement a number of other security mechanisms as described in the following sections. Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithm: a) symmetric (i.e. secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice versa; and b) asymmetric (e.g. public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or

	vice versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key". Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret.
Digital signature	These mechanisms define two procedures: a) signing a data unit, and b) verifying a signed data unit. The first process uses information which is private (i.e. unique and confidential) to the signer. The second process uses procedures and information which are publicly available but from which the signer's private information cannot be deduced. The signing process involves either an encipherment of the data unit or the production of a cryptographic checkvalue of the data unit, using the signer's private information as a private key. The verification process involves using the public procedures and information to determine whether the signature was produced with the signer's private information. The essential characteristic of the signature mechanism is that the signature can only be produced using the signer's private information. Thus when the signature is verified, it can subsequently be proven to a third party (e.g. a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.
Access control	These mechanisms may use the authenticated identity of an entity or information about the entity (such as membership in a known set of entities) or capabilities of the entity, in order to determine and enforce the access rights of the entity. If the entity attempts to use an unauthorized resource, or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail. Any notification to the sender of a denial of access for a connectionless data transmission can be provided only as a result of access controls imposed at the origin. Access control mechanisms may, for example, be based on use of one or more of the following: a) Access control information bases, where the access rights of peer entities are maintained. This information may be maintained by authorization centres or by the entity being accessed, and may be in the form of an access control list or matrix of hierarchical or distributed structure. This presupposes that peer entity authentication has been assured.

	b) Authentication information such as passwords, possession and subsequent presentation of which is evidence of the accessing entity's authorization; c) Capabilities, possession and subsequent presentation of which is evidence of the right to access the entity or resource defined by the capability. Note – A capability should be unforceable and should be conveyed in a trusted manner. d) Security labels, which when associated with an entity may be used to grant or deny access, usually according to a security policy. e) Time of attempted access. f) Route of attempted access, and g) Duration of access.
Data integrity	Two aspects of data integrity are: the integrity of a single data unit or field; and the integrity of a stream of data units or fields. In general, different mechanisms are used to provide these two types of integrity service, although provision of the second without the first is not practical. Determining the integrity of a single data unit involves two processes, one at the sending entity and one at the receiving entity. The sending entity appends to a data unit a quantity which is a function of the data itself. This quantity may be supplementary information such as a block check code or a cryptographic checkvalue and may itself be enciphered. The receiving entity generates a corresponding quantity and compares it with the received quantity to determine whether the data has been modified in transit. This mechanism alone will not protect against the replay of a single data unit. In appropriate layers of the architecture, detection of manipulation may lead to recovery action (for example, via retransmissions or error correction) at that or a higher layer.
Authentication exchange	A mechanism intended to ensure the identity of an entity by means of information exchange. Some of the techniques which may be applied to authentication exchanges are: a) use of authentication information, such as passwords supplied by a sending entity and checked by the receiving entity; b) cryptographic techniques; and c) use of characteristics and/or possessions of the entity.
Traffic padding	The insertion of additional bits into a data stream to frustrate traffic analysis attempts. Traffic padding mechanisms can be used to provide various levels of protection against traffic analysis. This mechanism can be effective only if the traffic padding is protected by a confidentiality service.

Routing control	End-systems may, on detection of persistent manipulation attacks, wish to instruct the network service provider to establish a connection via a different route.
Notarization	Properties about the data communicated between two or more entities, such as its integrity, origin, time and destination, can be assured by the provision of a notarization mechanism. The assurance is provided by a third party notary, which is trusted by the communicating entities, and which holds the necessary information to provide the required assurance in a testifiable manner. Each instance of communication may use digital signature, encipherment, and integrity mechanisms as appropriate to the service being provided by the notary. When such a notarization mechanism is invoked, the data is communicated between the communicating entities via the protected instances of communication and the notary.

Security Attacks	
Masquerade	A masquerade is where an entity pretends to be a different entity. A masquerade is usually used with some other forms of active attack, especially replay and modification of messages. For instance, authentication sequences can be captured and replayed after a valid authentication sequence has taken place. An authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges.
Replay	A replay occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).
Modification of messages	Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect, as when, for example, a message “Allow 'John Smith' to read confidential file 'Accounts'” is changed to “Allow 'Fred Brown' to read confidential file 'Accounts'”.
Denial of service	Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. The attack may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as the security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.
Wiretapping	Unauthorised disclosure of message content.

Traffic analysis	An attacker learns the identity of communication parties, and the frequency and length of exchanged messages.

	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Yes	Yes			Yes			Yes
Data origin authentication	Yes	Yes						Yes
Access control			Yes					
Confidentiality	Yes						Yes	
Traffic flow confidentiality	Yes					Yes	Yes	
Data integrity	Yes	Yes		Yes				Yes
Non-repudiation with proof of origin,		Yes						Yes
Non-repudiation with proof of delivery,		Yes						Yes

	Masquerade	Replay Modification	Modification of messages	Denial of service	Wiretapping	Traffic analysis
Peer entity authentication	Yes					
Data origin authentication	Yes					
Access control	Yes					
Confidentiality					Yes	

Traffic flow confidentiality						Yes
Data integrity		Yes	Yes			
Non-repudiation with proof of origin,	Yes					
Non-repudiation with proof of delivery,	Yes					

	Masquerade	Replay Modification	Modification of messages	Denial of service	Wiretapping	Traffic analysis
Encipherment					Yes	Yes
Digital signature	Yes	Yes	Yes			
Access control	Yes	Yes	Yes	Yes	Yes	
Data integrity		Yes	Yes			
Authentication exchange	Yes	Yes	Yes	Yes	Yes	
Traffic padding						Yes
Routing control				Yes	Yes	Yes
Notarization	Yes	Yes	Yes			

7. (Stallings, 2022) The following are the levels of impact on organisations or individuals should there be a breach of security (i.e., confidentiality, integrity or availability), defined in FIPS PUB 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)

- **Low:** The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
  AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- **Moderate:** The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
  AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- **High:** The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
  AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

  The generalized format for expressing the security category, SC, of an information type is:

  SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)},

  where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

  For example, an organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as:

  SC public information = {(confidentiality, NA), (integrity, MODERATE), (availability, MODERATE)}.

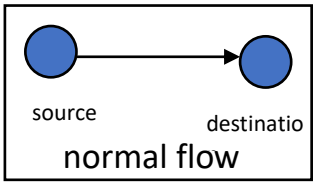
Provide a security category for each of the following assets:

a. A student maintaining a blog to post public information.
b. An examination section of a University managing sensitive information about exam papers.
c. An information system in a pathological laboratory maintaining the patient's data.
d. A student information system used for maintaining student data in a University contains both personal, academic information, and routine administrative information (not privacy related). Assess the impact for the two data sets separately and the information system as a whole.
e. A University library contains a library management system which controls the distribution of books amongst the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data sets separately and the information system as a whole.

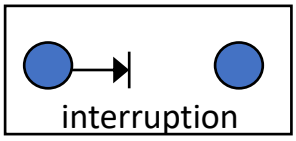
Solution hint: Check the examples given in FIPS 199.

8. Consider the normal flow of data and the five attacks depicted in the picture below. For each attack, identify the security service that is breached by the attack.

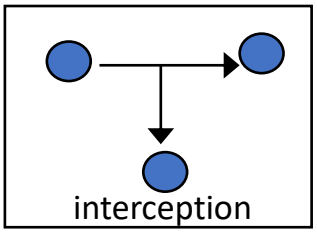
a)



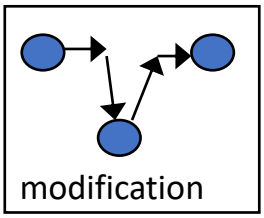
b)



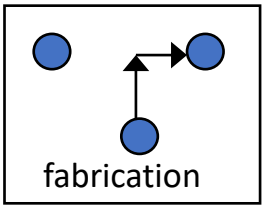
c)



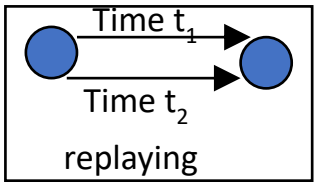
d)



e)



f)



Solution:

a) Normal flow – no service breached.
b) Availability
c) Confidentiality
d) Integrity
e) Authenticity
f) This is a tricky one – X.800 defines this as a matter of integrity, but one could argue that this attack breaches authenticity.

9. For each of the following attacks, identify the security service breached by the attack.
    a. Ransome attack
    b. Identity theft
    c. Digitally disappearing
    d. Deepfake

Solution:

a. Availability
b. Authenticity
c. Integrity
d. Authenticity

10. (Adapted from Stallings, 2022) True or False?
    a. The OSI security architecture focuses on security attacks, mechanisms, and services.
    b. Security attacks are classified as either passive, aggressive, or passive-aggressive.
    c. “Data security” is a subset of “network security”.
    d. “Information security” is a subset of “cybersecurity”.
    e. Cybersecurity focuses on prevention of security attacks, rather than on detection, mitigation and recovery.

Solution:

a. T
b. F
c. F
d. T
e. F