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?

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?

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

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

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

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.

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.

- <u>**High:**</u> 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.

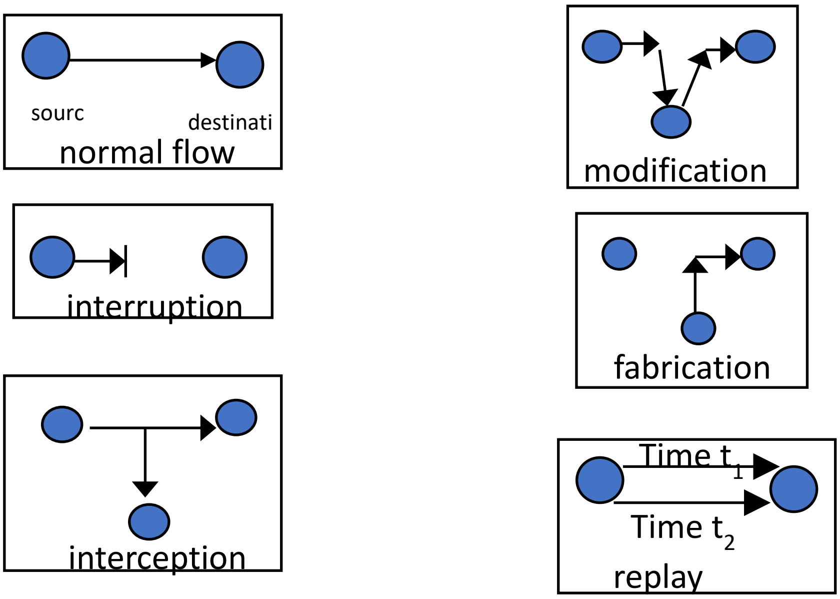
For example, an organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a 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.

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.



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

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. The main focus of cybersecurity is on prevention of security attacks, rather than detection, mitigation and recovery.