The University of Newcastle
School of Electrical Engineering and Comping

COMP3260/6360 Data Security
Week 2 Workshop – 1st and 3rd March 2021

The following tables show security services, security mechanisms and security attacks based on those defined by ITU-T Recommendation X.800.

Security Services	
Peer entity authentication	Used in association with a logical connection to provide confidence in the identity of the entities connected.
Data origin authentication	In a connectionless transfer, provides assurance that the source of received data is as claimed.
Access control	The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
Confidentiality	The protection of data from unauthorized disclosure.
Traffic flow confidentiality	The protection of the information that might be derived from observation of traffic flows.
Data integrity	The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Non-repudiation	Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Availability	Ensuring timely and reliable access to resources (data) to authorised parties.

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.
Digital signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).
Access control	A variety of mechanisms that enforce access rights to resources.
Data integrity	A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
Authentication exchange	A mechanism intended to ensure the identity of an entity by means of information exchange.
Traffic padding	The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
Routing control	Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
Notarization	The use of a trusted third party to assure certain properties of a data exchange.

Security Attacks	
Release of message contents	Opponent learning the content of a message.
Traffic analysis	Opponent learning the location and identity of communication hosts, as well as frequency and length of exchanged messages.
Masquerade	One entity pretending to be another entity.
Replay Modification	Capture of data and its subsequent retransmission to produce an unauthorised effect.
Modification of messages	Altering some portion of the message, or delying or reordering the message.
Denial of service	Preventing or inhibiting the normal use or management of communication facilities.

1. Create a matrix to show the relationship between security services and mechanisms.

2. Create a matrix to show the relationship between security services and attacks.

3. Create a matrix to show the relationship between security mechanisms and attacks.

4. 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 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.

5. TRUE or FALSE? Provide a brief justification.

   a. The set {9,8,7,6,5,4} is a complete set of residues modulo 6.

   b. The set {4,5,6,7,8,9} is a complete set of residues modulo 7.

   c. The set {10,6,4,22,33} is a complete set of residues modulo 5.

   d. The set {44,5,61,6,8} is a complete set of residues modulo 5.

   e. The set {0,4,3,2,1} is a complete set of residues modulo 5.

6. Use the Fast Exponentiation Algorithm to compute the following.

   a. 3^{1354} mod 10

   b. 7^{8897} mod 15

   c. 19^{4562} mod 22

   d. 21^{56900}mod 40

   e. 3^{49} mod 170

7. Which ones of the sets and operations below satisfy requirements for a group, Abelian group, ring, commutative ring, integral domain and field?

   a. Whole numbers with addition and multiplication

   b. Integers, including 0 with addition and multiplication

   c. Integers modulo n with addition and multiplication

   d. Rational numbers with addition and multiplication

8. Apply Chinese Remainder Theorem to find x in the range [0,59] such that

x mod 4 = 3
x mod 3 = 2
x mod 5 = 4

9. Using Chinese Remainder Theorem solve for x in the range [0, n-1].

a) 5x mod 17 = 1
b) 19x mod 26 = 1
c) 17x mod 100 = 1
d) 2x mod 57 =1