The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security

Week 2 Workshop Solutions – 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	Opponent learning the location and identity of communication hosts, as well

analysis	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 denying 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.

Solution:

	Encipherment	Digital signature	Access control	Data integrity	Authentication exchan	Traffic padding	Routing control	Notarization
Peer entity authentication	Yes	Yes			Yes			
Data origin authentication	Yes	Yes						
Access control			Yes					
Confidentiality	Yes						Yes	
Traffic flow confidentiality	Yes					Yes	Yes	
Data integrity	Yes	Yes		Yes				
Non-repudiation		Yes		Yes				Yes
Availability				Yes	Yes			

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

Solution:

	Release of message contents	Traffic analysis	Masquerade	Replay Modification	Modification of messages	Denial of service
Peer entity authentication			Yes			
Data origin authentication			Yes			
Access control			Yes			
Confidentiality	Yes					
Traffic flow confidentiality		Yes				
Data integrity				Yes	Yes	
Non-repudiation			Yes			
Availability						Yes

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

Solution:

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

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.

<u>Solution idea:</u>

The following are not solutions but rather examples from FIPS 199 that are relevant to the above questions:

a. 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.

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

b. A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate.

   SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}

c. A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

d. The management within the contracting organization determines that:
   i. for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and
   ii. for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

The resulting security categories, SC, of these information types are expressed as:

SC contract information = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)},

and

SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

e. The management at the power plant determines that:
   i. for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and
   ii. for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability.

The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(confidentiality, NA), (integrity, HIGH), (availability, HIGH)},

and

SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}.

5. TRUE or FALSE?

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.

Solution:

a. TRUE

b. FALSE – For example, 10 is not congruent to any element of the set.

c. TRUE

d. FALSE – For example, 7 is not congruent to any element of the set.

e. TRUE

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

Solution:

a. 3^{1354} mod 10
$= 9^{677}$ mod 10
$= 9 \times 9^{676}$ mod 10
$= 9 \times 81^{338}$ mod 10
$= 9 \times 1^{338}$ mod 10
$=9$

b. 7^{8897} mod 15 = 7

c. 19^{4562} mod 22 = 9

d. 21^{56900}mod 40 = 1

e. 3^{49} mod 170 = 3

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

Solution:

a. We define "whole numbers" as positive integers, i.e., {1,2,...}. Whole numbers with addition do not form a group, as there is neither identity nor inverse element; the same is the case with whole numbers with multiplication.

b. We define integers as {..., -2, -1, 0, 1, 2,...}. Integers with addition form an Abelian group. Integers with multiplication do not form a group as there is no inverse element. Integers with addition and multiplication form an integral domain but do not form a field as there is no multiplicative inverse.

c. Integers modulo n with addition form an Abelian group. Integers modulo n with multiplication may or may not form an Abelian group, depending on the choice of n. Likewise, integers modulo n with addition and multiplication form an integral domain and may or may not form a field, depending on the choice of n. If n is a prime number, they do form a field as then every element except 0 has a multiplicative inverse.

d. Rational numbers with addition and multiplication form a field.

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

Solution:
Chinese Remainder Theorem: Let $d_1, d_2, \ldots, d_t$ be pairwise relatively prime, and let $n = d_1 \times d_2 \times \cdots \times d_t$. Then the system of equations

$$x \bmod d_i = x_i, i = 1, \ldots, t$$

has a common solution x in the range $[0, n-1]$.The common solution is

$$x = \left(\sum_{i=1}^{t} \frac{n}{d_i} y_i x_i \right) \bmod n$$

where y_i is a solution of $\frac{n}{d_i} y_i \bmod d_i = 1, i = 1, \ldots, t$.

We have $x_1 = 3, x_2 = 2, x_3 = 4$. Further, we have $d_1 = 4, d_2 = 3, d_3 = 5$ and so $n = 4 \times 3 \times 5$.

We first need to find y_1, y_2 and y_3 such that

$$\frac{60}{4} y_1 \bmod 4 = 1$$
$$\frac{60}{3} y_2 \bmod 3 = 1$$
$$\frac{60}{5} y_3 \bmod 5 = 1$$

We get:

$$15 y_1 \bmod 4 = 1$$
$$20 y_2 \bmod 3 = 1$$
$$12 y_3 \bmod 5 = 1$$

That is,

$$3 y_1 \bmod 4 = 1$$
$$2 y_2 \bmod 3 = 1$$
$$2 y_3 \bmod 5 = 1$$

We get $y_1 = 3, y_2 = 2$ and $y_3 = 3$.

We now get the solution:

$x = (15 \times 3 \times 3 + 20 \times 2 \times 2 + 12 \times 3 \times 4) \bmod 60 =$
$((15 \times 3 \times 3) \bmod 60 + (20 \times 2 \times 2) \bmod 60 + (12 \times 3 \times 4) \bmod 60) \bmod 60 =$
$(15 + 20 + 24) \bmod 60 = 59$

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

<u>Solution:</u>

a) $5x \bmod 17 = 1$

As 17 is a prime number, we cannot apply Chinese Remainder Theorem. We can use Extended Euclid's Algorithm, or Euler's Totient function (you should do both of these for practice), but since the modulus (17) is fairly small, we can simply apply a brute force strategy to find the multiplicative inverse:

5×1 mod 17 = 5
5×2 mod 17 = 10
5×3 mod 17 = 15
5×4 mod 17 = 3
5×5 mod 17 = 8
5×6 mod 17 = 13
5×7 mod 17 = 1

Thus the multiplicative inverse of 5 modulo 17 is 7.

b) $19x \bmod 26 = 1$

We have

$26 = 2 \times 13$, $d1 = 2$, $d2 = 13$

$19x1 \bmod 2 = 1 \rightarrow x1 \bmod 2 = 1$, $x1 = 1$
$19x2 \bmod 13 = 1 \rightarrow 6x2 \bmod 13 = 1$, $x2 = 11$

$x \bmod 2 = 1$
$x \bmod 13 = 11$

We now need to find y_1 and y_2 such that

$(26/2)\ y_1 \bmod 2 = 1$
$(26/13)\ y_2 \bmod 13 = 1$

$13y_1 \bmod 2 = y_1 \bmod 2 = 1$
$2y_2 \bmod 13 = 1$

We get $y_1 = 1$ and $y_2 = 7$.

We now get the solution

$$x = (13 \times 1 \times 1 + 2 \times 7 \times 11) \bmod 26 = 11$$

Thus the multiplicative inverse of 19 modulo 26 is 11.

c) $17x \bmod 100 = 1$

We have

$100 = 2^2 \times 5^2$, $d_1 = 2^2$, $d_2 = 5^2$

$17x1 \bmod 4 = 1 \rightarrow x1 \bmod 4 = 1$, $x1 = 1$
$17x2 \bmod 25 = 1 \rightarrow x2 = 3$

$x \bmod 4 = 1$
$x \bmod 25 = 3$

We now need to find y1 and y2 such that

$(100/4)\ y_1 \bmod 4 = 1$
$(100/25)\ y_2 \bmod 25 = 1$

$25y_1 \bmod 4 = 1 \rightarrow y_1 \bmod 4 = 1$
$4y_2 \bmod 25 = 1$

We get $y_1 = 1$ and $y_2 = 19$.

We now get the solution

$$x = (25 \times 1 \times 1 + 4 \times 19 \times 3) \bmod 100 = 53$$

Thus, the multiplicative inverse of 17 modulo 100 is 53.

d) $2x \bmod 57 = 1$

We have

$57 = 3 \times 19$, $d_1 = 3$, $d_2 = 19$

$2x1 \bmod 3 = 1 \rightarrow x_1 = 2$
$2x2 \bmod 19 = 1 \rightarrow x_2 = 10$

$x \bmod 3 = 2$
$x \bmod 19 = 10$

We now need to find y1 and y2 such that

$(57/3)\, y_1 \bmod 3 = 1$
$(57/19)\, y_2 \bmod 19 = 1$

$19y_1 \bmod 3 = 1 \rightarrow y_1 \bmod 3 = 1$
$3y_2 \bmod 19 = 1$

We get $y_1 = 1$ and $y_2 = 13$.
We now get the solution

$x = (19\times1\times2 + 3\times13\times10) \bmod 57 = 29$

Thus, the multiplicative inverse of 2 modulo 57 is 29.