SENG2250/6250 System and Network Security

School of Electrical Engineering and Computing

Semester 2, 2020

Lab 1 Solutions

Part 1 Review Questions

1. What is the C.I.A triangle in security services?

   Answers

   a. Confidentiality: prevent the asset from being access from an unauthorised party.
   b. Integrity: prevent an unauthorised party from modifying the origin of message/source.
   c. Availability: relates to the reliability of a system.
   d. Authenticity: The origin of assets should be assured and the assets should be unforgeable by unauthorised parties.

2. Describe which CIA property would be related to each of the attacks (interruption, interception, modification, and fabrication)?

   Answers

   a. Interruption: availability
   b. Interception: confidentiality
   c. Modification: integrity, authenticity
   d. Fabrication: integrity, authenticity

3. Which security service is being targeted in a man-in-the-middle (MITM) attack?

   Answers

   Integrity/authenticity

4. Think about what an adversary could do in a communication channel.

   Answers

   Passive and active attacks, such as interruption, interception, modification and fabrication.

5. How can a TTP help users to establish a secure channel (generally)?

   Answers

   For example

   a. TTP can deliver a secret key to participants.
   b. TTP can also generate then deliver the secret key to participants.

Part 2 Exercises

6. **Brute Force Attacks**: It tries to attempt all possible passwords until the correct one is found. It is also known as an exhaustive key search. Assume that an adversary can (randomly) try 100,000 different passwords per second.

   Answers

   Assume that a password is randomly generated, the expected number (E) of attempts can be calculated by (can you explain why we could in this way?)

   $$E = \frac{bestcase+worstcase}{2}.$$

   Let the expected time be t, then $t = \frac{E}{r}$, where r is the number of attempts per second.

   a. If a password consists of 8 digits, what is the expected (average) time to find the correct password?
      $\approx 500s$
   b. If a password consists of 8 characters, including numbers and/or lower-case English letters, what is the expected time to find the correct password?
      $\approx 14105550s$
   c. If a password consists of 6 characters, including numbers and/or lower-case English letters, what is the expected time to find the correct password?
      $\approx 10884s$
   d. What can you find from the above results?
      The number of possible key letters and password length can significantly impact the security of the password.
   e. Consider a login system, what is your strategy to slow down the attack?
      For example, set some restrictions, such as the number of attempts in a period of time.

7. **Modular Arithmetic**: solve the following questions by using a calculator (e.g., https://www.calculators.org/math/modulo.php)
   a. $(651 \times 7213)\ mod\ 47\ = 34$
      $651\ mod\ 47 \times 7213\ mod\ 47\ = 34$
      $(651\ mod\ 47 \times 7213\ mod\ 47)\ mod\ 47\ = 34$
   b. $(651 + 7213)\ mod\ 47\ = 15$
      $651\ mod\ 47 + 7213\ mod\ 47\ = 62$
      $(651\ mod\ 47 + 7213\ mod\ 47)\ mod\ 47\ = 15$
   c. Does it matter where you calculate the modulus in the above two cases (be aware of the order of operations)?

8. **Multiplicative inverse**: solve the following questions by using a calculator

$$3 \times 21\ mod\ 31 = 1$$
$$11 \times 17\ mod\ 31 = 1$$
$$15 \times 29\ mod\ 31 = 1$$
$$23 \times 27\ mod\ 31 = 1$$

   21, 17, 29 and 27 are called the multiplicative inverse of 3, 11, 15 and 23 under modulus 31, respectively.
   a. Read the definition of the multiplicative inverse: https://planetcalc.com/3311/.
   b. What is the multiplicative inverse of $19\ mod\ 31$? 18
   c. What is the multiplicative inverse of $1625876299\ mod\ 51$? 11
   d. Can you find any other inverse(s) of 3 modulus 31? What about 11, 15 and 23? What inference you may have from it?

   No, there is (at most) one modular multiplicative inverse for a number under a particular modulus.

9. **Programming**: modular exponentiation $(b^e\ mod\ n)$ is an essential operation for many modern cryptographic algorithms. For example

$$2^0 = 1, 2^1 = 2,\ 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$$

   where modulus $n = 11, b = 2, e = 0,1, \ldots, 10$.

   Write a (C/C++/Java/Python) program for the modular exponentiation operation based on the following pseudocode.

$$3^3\ mod\ 7 = 6$$
$$10^8\ mod\ 133 = 93$$
$$3785^{8395}\ mod\ 65537 = 355$$