COMP90043: Cryptography and Security

Week 2 Workshop Activity Solutions

Semester 2, 2016

(Problems are from the text by Stallings, 5th & 6th edition)

Before we begin, take a few minutes to discuss the following:

1. When considering Data, stored digitally, how would you determine the satisfaction of the following criteria:

   a) Confidentiality
   Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

   b) Integrity
   Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

   c) Availability
   Ensuring timely and reliable access to and use of information.

   d) Authentication
   Is the property of being genuine and being able to be verified and trusted.

   e) Accountability
   Is a security goal that requires all actions of an entity to be traced uniquely to that entity.

   f) Which one of the three do you think is the MOST important?
   This is dependent on many factors.

2. Number Theory

   a) Modulo Arithmetic
   Two integers *p* and *q* are said to be congruent modulo *n*, if *(p mod n) = (q mod n)*. This is written as *p ≡ q (mod n)*.
   Solve the following pairs of numbers using modulo arithmetic:
   i. 73 mod 23 = **4**
   ii. -11 mod 7 = **4**
   iii. $(-13)^2$ mod 9 = **7**

   b) Greatest Common Division (GCD)
   Definition: A GCD between the two numbers p and q is the largest number *m* which divides the two numbers *p*, and *q*.
   Find the GCD for the following pairs of numbers:
   i. GCD(60, 24) = **12**
   ii. GCD(30, 105) = **15**
   iii. GCD(1473, 1562) = **1**

3. Security Attacks and Threats
    a) Define a Security Threat and a Security Attack
    A Security Threat is a possible danger that might exploit a vulnerability
    A Security Attack is an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

    b) Define the following attacks:
        i. Denial of Service:
        is an attack which prevents of inhibits the normal use or management of communications facilities.

        ii. Release of Message Contents
        is an attack in which the contents of a message or transmission are either directly or indirectly released.

        iii. Message Modification
        Is an attack which aims to alter a part or whole of a legitimate message as a means of delaying or reordering in order to produce an unauthorized effect.

        iv. Masquerade
        A masquerade takes place when one entity pretends to be a different entity.

        v. Traffic Analysis
        is an attack which aims to analyse data and information going across the network in order to infer the details of the message and/or communication.

        vi. Replay
        Is an attack that passively captures a data unit and subsequently retransmits it to produce an unauthorized effect.

    c) From the above, identify which constitute as active attacks and which constitute as passive attacks?
    An active attack is one that involves some modification of the data stream or the creation of a false stream. From the above, the following constitute as active attacks:
        i. Denial of Service
        ii. Message Modification
        iii. Masquerade
        iv. Replay

    A passive attack involves the eavesdropping or monitoring of transmissions with the goal of obtaining information that is being transmitted. From the above, the following constitute as passive attacks:
        i. Release of message contents
        ii. Traffic Analysis

4. Homework
On your own, please read up on the Euclidean Algorithm, and the Extended Euclidean algorithm to understand how the principles of modulo arithmetic are applied in order to obtain the GCD for two given integers. We will be applying these concepts in coming weeks.