SENG2250/6250 System and Network Security

School of Electrical Engineering and Computing

Semester 2, 2020

Lab 1 Security Fundamentals Review

Objectives

- Review the knowledge of Topic 1 introduction to security fundamentals.
- Review the knowledge of math for the understanding of coming lectures.
- Implement cryptographic operations in programming.

Part 1 Review Questions

1. What is the C.I.A triangle in security services?
2. Describe which CIA property would be related to each of the attacks (interruption, interception, modification, and fabrication)?
3. Which security service is being targeted in a man-in-the-middle (MITM) attack?
4. Think about what an adversary could do in a communication channel.
5. How can a TTP help users to establish a secure channel (generally)?

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.
    a. If a password consists of 8 digits, what is the expected (average) time to find the correct password?
    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?

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?

d. What can you find from the above results?

e. Consider a login system, what is your strategy to slow down the attack?

7. **Modular Arithmetic**: solve the following questions by using a calculator (e.g., https://www.calculators.org/math/modulo.php)

   a. $(651 \times 7213) mod\ 47 = ?$

      $651\ mod\ 47 \times 7213\ mod\ 47\ \ = ?$

      $(651\ mod\ 47 \times 7213\ mod\ 47)\ mod\ 47\ \ = ?$

   b. $(651 + 7213)\ mod\ 47\ \ = ?$

      $651\ mod\ 47 + 7213\ mod\ 47\ \ = ?$

      $(651\ mod\ 47 + 7213\ mod\ 47)\ mod\ 47\ \ = ?$

   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

$$3 \times 21\ mod\ 31 = ?$$

$$11 \times 17\ mod\ 31 = ?$$

$$15 \times 29\ mod\ 31 = ?$$

$$23 \times 27\ mod\ 31 = ?$$

21, 17, 29 and 27 are called the multiplicative inverse of 3, 11, 15 and 23 under modulus 31, respectively.

   a. Find the definition of the multiplicative inverse: e.g., https://planetcalc.com/3311/.

   b. What is the multiplicative inverse of $19\ mod\ 31$?

   c. What is the multiplicative inverse of $1625876299\ mod\ 51$?

   d. Can you find any other inverse(s) of 3 modulus 31? What about 11, 15 and 23? What inference could you have from it?

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 $n = 11, b = 2, e = 0,1, \dots ,10$.

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

```
function powmod(base b, exponent e, modulus n) {
    if n  = 1
        return 0
    t = 1
    rs = 1
    while (t <= e) {
        rs = (rs * b) mod n
        t = t + 1
    }
    return rs
}
```

Using the above implementation to find the solutions to

$3^3 \, mod \, 7 =?$
$10^8 \, mod \, 133 =?$
$3785^{8395} \, mod \, 65537 =?$

Part 3 Discovery

10. Find a security attack/breach and summarise the following information about the attack/breach.
    a. What is the goal of the attacker?
    b. How does the attack work? Brief description.
    c. What is the consequence?
    d. What solutions applied to resolve the issue, if any?