CS 546 Computer Security (Spring 2019)

Homework #3, 82 points, Due on 5/02/2019 class time

- **Q1(30 points): Confidentiality, Integrity and Authenticity**
  Suppose that host A and B are connected by insecure public networks. Assume that A and B have synchronized system time. Let M be a plaintext message and K be a secret key shared by A and B. Let

  - $CBC(X, K)$ denotes the ciphertext of a plaintext X after a secret key encryption (CBC mode) using a key K.
  - $MD(X, K)$ denotes the message digest of a plaintext $X|K$.
  - $RSA(X, I)$ denotes the ciphertext of a plaintext X after an RSA public key operation using I's public key.
  - $RSA\{X, I\}$ denotes the ciphertext of a plaintext X after an RSA private key operation using I's private key.

  If A sends out a packet to B that the packet's headers encapsulate one of the following.

  1. $CBC(M + timestamp, K)$ and IV.
  2. *Residue of* $CBC(M + timestamp, K)$, M and IV.
  3. $CBC(M + A's\ IP\ address, K)$ and IV.
  4. $MD(M, K)$.
  5. $MD(M + A's\ IP\ address, K)$ and M.
  6. $MD(M + timestamp, K)$ and M.
  7. $RSA\{M + timestamp, A\}$ and M.
  8. $RSA(M + timestamp, B)$.

  (a)(10 points) Please list the numbers above to indicate which packets achieve the security goal confidentiality.

  (b)(10 points) Please list the numbers above to indicate which packets achieve the security goal integrity.

  (c)(10 points) Please list the numbers above to indicate which packets achieve the security goal authenticity.

- **Q2(12 points): Hash Function Applications**

  Cryptographic hash function is a one-way function, which means the original message cannot be recovered from the message digest. Thus, it cannot be used as an encryption algorithm. Please describe three possible usages of cryptographic hash functions, which can either obtain some security goals or improve efficiency of some cryptographic operations. Your answer should not include the most common usage - password hashing.

- **Q3(20 points): Cryptology Computation**

  (a)(10 points) Using the square and multiply technique, we can compute the modular exponentiation operation with a large exponent. Let both a and b be positive integers and $1 < a < b$. How many modular multiplication operations are required to compute $a^{172} \bmod b$?

  (b)(10 points) In an elliptic curve cryptosystem, multiplying a scalar number k to a point G on a curve $E_p(a, b)$ will result in another point Q on the curve. That is $Q = k \cdot G$, where both $G, Q \in E_p(a, b)$.

  Now given a point G and $k = 110$, how many elliptic curve additions are required to compute $Q = 110 \cdot G$?

- **Q4(10 points): Buffer Overflow/format String Vulnerability**

```
int main(int argc, char *argv[])
{
   char buff[50];

   if (agrc < 2)
   {
      printf("Syntax: %s <input string>\n", argv[0]);
      exit(0);
   }

   strcpy(buff, argv[1]);
   return 0;
}
```

Assume you are an attacker, you can exploit the buffer overflow vulnerability of above codes. In addition to crash the program, can you gain the control of the program to execute arbitrary codes and how?

- **Q5(10 points): SQL Injection**

  The following SQL query that requires user input could be vulnerable to SQL Injections.

  ```
  SELECT fname, lname FROM employee WHERE ssn = 'user input';
  ```

  Assume you are an attacker, please provide a user input that may maliciously return the salaries for all employees with the last name "Smith" from the employee table.