Second semester examinations

2019/20

CYBERSECURITY

Name: Yuyang.Wan
ID:1715687

1.Explain what are Secure Multi Party Computations and give a detailed example of their possible application. Discuss possible benefits of, and potential issues with your proposed application. (20 marks)

Secure Multi Party Computations is technology aimed at the situation when set of participants want to compute a joint function of their private inputs while they don't want to divulge their own input, in another word, MPC technic can get use of data without leaking primitive data.

Multi Party Computations can be applied on Oblivious Transfer. Assuming there is a medical instruction platform holds all kind of medical instruction with cost for patient. It is obvious that patients want to keep their condition secret while platform wants to keep unpaid instructions secret. Indication platform S(Sender) has two instructions M_0 and M_1. Patient R(Receiver).

In the condition of R wants to receive M_0.

S generates random a; R generates random b

$A=g^a$ is sent to R; $B=g^b$ is sent to S

Compute $k_0=Hash(B^a)$, $k_1=Hash((B/A)^a)$

$e_0=M_0$ encrypted by k_0, $e_1=M_1$ encrypted by k_1 Send e_1, e_0 to R

Potential benefit is the instruction platform can send all the instructions each time even patients requires for different instruction, and don't have to worry about information leaking. Patients don't have to worry about personal information leaking.

Potential issue is the encryption process involves too much computation, when it comes to large amount of request it will be too time consuming.

2. The following algorithm has been proposed to compute a hash function.
Generate some key K for the AES algorithm. Encrypt M with K and take the last 64 bits of the result as the hash of M.
What are the main disadvantages of this algorithm? Can the algorithm be improved by taking the first 64 bits of the result instead of the last 64 bits?
(12 marks)

Cannot be applied to a block of data of any size

Output size of hash function is too small

It can’t resist related-key attacks.
It is very easy to find any to find M with same algorithm result. Especially when padding is used.
It is possible to compute M by result. An AES algorithm is reversible while hash function means to be non-reversible.
Yes, it can be improved limitedly. By taking the first 64 bits of the result instead of the last 64 bits, padding will no longer leads to a mass of same algorithm result.

3. What is a purpose of using multiple layers of encryption in CryptDB approach to querying encrypted databases? Give an example of the situation where using three layers of encryption is justified. If needed you may either define some queries in SQL or describe them in the natural language.
(20 marks)

CryptDB can ensure that server won’t be able to stole the information while user can still use server to do computation. Using multiple layers of encryption is mainly to ensure the security of the data, while ensuring that it can support encryption operations, which is a compromise design. Different encryptions can support different operations some may support addition wile some support comparison. To implement all the operations on the database, we have to use multiple layers of encryption.
Take student achievement system as example, the OPE(order preserving encryption), DET(Deterministic), HOM(Homomorphic encryption) will be used.
OPE will enable users to rank the achievement of students
DET will be used to retrieve specific data and same values
HOM will supports manipulate data in crypted form.

4. The company X has proposed a very fast and reliable biometric unlock system for their smartphones.
It recognizes the owner’s face with different face expressions, open and closed
eyes, etc with very high probability. What are the possible issues of using this system as the only authentication method granting access to the smartphone?
(8 marks)

Biological information is unique and cannot be modified. When personal Biological information is stolen by attacker, it is in an irreversible state, user can’t change their face to protect their device which is to say their device cannot be restored to protected state.
Others cannot be authorized to use the smartphone when the device owner is not around because Biological information cannot be provided remotely.
The user will not be able to use the device providing that the user receives facial injuries or wear mask in the epidemic because facial recognition involves every part of the face unlike iris scanning.

5. What could be the purpose of the following protocol, where both parties use RSA publickey
algorithm, skA is the secret key of A, pkB is the public key of B, and s is the secret message by B?
Message 1. $A \rightarrow B : \{\{k\}_{sk\,A}\}_{pk\,B}$;
Message 2. $B \rightarrow A : \{s\}_{k}$
Explain the rationale behind and the possible issue with this protocol. How can the issue be fixed? (15 marks)

The purpose of the protocol is to share more convenient Symmetric Key with more secure Public Key Cryptography while add digital signature to Symmetric Key for authentication.
pk B can ensure only B can decrypt to retrieve the message {k} sk A because B is the only one who holds sk B
sk A is a digital signature which can prove to B that key K is send by A because A is the only one who holds skA
When K is sent to B it will be used to encrypt secret message.
The issue is this protocol is defenseless facing middle attack like reflection attack. This issue can be fixed by using certification authority, CA binds public key to particular entity, prevents attacker uses their own set of keys to steal message in the middle.

6. The following schema for password-based encryption has been proposed recently. The password is split into two parts: the first part is short and easy to remember, the second part is randomly generated and kept secret - nobody knows it. When it comes to decryption the user enters his/her first part of the password, and the second secret part is brute-forced by the decryption algorithm and if successful, the ciphertext is decrypted. Discuss possible advantages and disadvantages of such a schema and compare it with possible alternative solutions. (25 marks)

Advantage:

-The first part of the password is more memorable as a short key. While as safe as long password facing brute force attack because of the second part of the password.
-The second part of the password sometimes called pepper is significantly smaller than the typical salt.
-The second part of the password is randomly generated and irrelated to the first part means the full password will be random and of enough length makes attacker impossible to directly attack the password.
-The second part of the password is randomized and kept secret making it impossible for attackers to crack the password by cracking the pepper

Disadvantages:

-A password or pass-phrase is potentially guessable. If the attacker guesses out the password by user's personal information, it will easy to crack the password.
-It may take users long time to brute-forced the second part of the password considering

the hardware since second part has to be long enough to avoid whole password being cracked.

Alternative solutions:

PBE algorithms use a user's password together with salt and iteration count.
Salt and pepper both prevent dictionary attacks.
The salt is not a secret value, it may be transmitted along with the ciphertext to the receiver while pepper should be kept secret.
Iteration will make the key derivation procedure more complicated, and more time consuming. However, it's still faster than the schema above.
Both of the schemas can protect password from brute force attack.
The length of random password generated by schema above is fixed it may be fragile to rainbow table attack. The salt and iteration can resist rainbow table attack efficiently.
Both schema is fragile if the user uses easily guessable password.
Therefore we should be checking for those weak classes of passwords at the door and not allowing them in. Personal information should not be allowed to be used as password.