Assignment One

Yuming JIANG 460444981

Hangyuan Yu 460469308

1 Poker and Cyphers

A. Attacks

I used the known plaintext attack. Because the ciphertext and plaintext pair is chosen by Slim and Rusty. I just identify two pairs of their ciphers. I can not select neither the message nor the ciphertext.

B. PRNGs

The using of Unix rand() random number generator is not secure since it uses the linear congruential method which has a certain small key space to guess the seed. Once the seed is found, the list of "random" number can be easily calculate and predict. This method takes the "mod" operation, so if its function is something like Xn+1 = (aXn + b) mod c, the period of this PRNG is at most c. As a result, it is more likely to be predicted.

C. PRNGs II

I think this PRNG is not secure enough. As this PRNG uses the time as the seed. Everybody knows the time and can use this as the seed to predicate the next random number. So to make this PRNG more secure, I should change the seed to Thermal noise of hard drives, Low-order bit fluctuations of voltage readings, User input or Geiger counter click timing.

D. Hash Function

The best MAC out of a hash function is constructed in this way:

MACk(m) = h((k $\oplus$ opad)|h((k $\oplus$ ipad)|m))

The hash function we use to generate the MAC is SHA-256. In this way, the process follows the Merkle-Damgård construction. First, a message in large size is cut into smaller blocks. The block size is usually equal to or larger than 512 bits. In this case, we use 512 bits block size. Then a compression function is used to generate the hash MAC. The opad and the ipad in the above function means outer padding and inner padding represent a hexdecimal constant value. The key for generating the MAC should be at least 256 bits in length and should also be generated randomly. Once everything is ready, we start to calculate the HMAC. The first block contains the initial vector (IV), key $\oplus$ ipad, and the message. The operation $\oplus$ is to make the key and the inner padding do a XOR calculation. Then three parts together calculates a result in the given compression function. This result will be the next key vector to calculate the next results and so on. When it reaches the final block, if the message size is not enough to fill a block, a padding block (PB) is used to fill the block into 512 bits. Finally, the key and the outer padding will do a XOR operation and be the vector to calculate the final HMAC together with the result calculated by the last block of message.

E. Polyalphabetic Substitution Cyphers

If the ciphertext message contains a series of hexadecimal number or just some unreadable

strings, the cipher used should be one of the modern symmetric cipher. If the ciphertext message, for example English, only contains the characters in the alphabet of English, the cipher used should be a polyalphabetic substitution cipher.

I will calculate the index of coincidence of this ciphertext message. First, I will divide the ciphertext message into n-size characters set. Second, I will compute the aggregate delta I.C. for all n columns ("delta bar"). Third, I will compare these n Delta-bar I.C. values with the I.C. values of English and Spanish. If the most similar value is English, the plaintext was sent by a Columbian paramilitary group, otherwise, it was sent by a Californian drug dealer.

2 General Questions

A. DoS

DoS, which is known as denial of service attack, is implemented by visit a website or send large volume of data to the server to process, or request great number of times requests to the server at one time to make the targeted computer system become slow or totally break down. The principle is based on occupying the targeted computer system's resources to make it not available for others so that the service will be slow or even stopped.

B. Time attack

Timing attack is one of the side channel attacks. It will take time to execute the cryptographic algorithms. This execution can differ based on the input. Attackers can measure this time and work backwards to the input.

The execution time for the RSA decryption depends on the number of '1' bits in the key. If the system does not hide the finish time of the decryption, attackers can use the public key to encrypt a lot of messages and let the system to decrypt these. Attackers will measure the decryption finish time and work backwards to the RSA private key.

C. RSA

It is not secure at all. If one knows the public key, he can calculate the ciphertext using the public key with all text. Since the input text (origin message) for the RSA encryption has only three kinds: either "Sammy the Knife", "Big Kevsta" or "Teflon Hook", the encrypted ciphertext also has three kinds, one to one in correspondence. Therefore, if one tries to compare the ciphertext emailed by others with the three ciphertext he generates on his own, he would know who others elect.

D. Attacks on Asymmetric Algorithms

I think the rate of improving attacks on asymmetric cryptosystems is greater than symmetric cryptosystems. Because the security of asymmetric cryptosystems is based on the presumed difficulty of a small set of number-theoretic problems. With the increasing of the computing speed, the problem may be solved very easily. For symmetric cryptosystems, even the basic cipher is not secure, people can use the basic cipher to construct stronger ciphers.

The end game for attacks on asymmetric algorithms is that attackers can use future computing machine to solve the set of number-theoretic problems very quickly, hence the whole algorithms can not be used.

E. Avalanche Effect

The avalanche effect in DES means that even if a little change in the input of the DES will result in a indistinguishable change in the output. There are mainly three major building blocks which cause this effect. Two of them are S-boxes and P-boxes, the other one is the construction structure which is the block cipher. Both S-boxes and P-boxes maintain the characteristic of diffusion. Diffusion means the change of one bit in either original text and the ciphertext will result in half of the bits change on the other side. The S-boxes and P-boxes are used in the round function, which is the major part of the Feist Network. In addition, since DES is a iterated block cipher. The current result is calculated together with the result from the last block. This causes diffusion, which will further result in avalanche effect in DES.

3 Protocols

A.

To convince Bob that some other value $\neq$ is the committed value, Alice can ask Bob to calculate h(x||r) with x received during the open phase and r received during the commitment phase, denote the result of this calculation as . Bob can check if received during the commitment phase. As MD5 has the Collision Resistance property, if they are the same, x received during the open phase should be the same as the committed value.

B.

Bob can use the collision attack to find x||r with given y during the commitment phase. The best collision attack can only take times attempt, this won't take too much time with a regular pc. After finding x||r, Bob can use r to determine the committed value.

C.

Commitment phase:

First, Alice generates random strings r, s, and computes y = SHA256(r||s||x). Second, Alice sends Bob r and y.

Revelation Phase:

Alice sends Bob the remaining data of s and x. Then Bob verifies that SHA256(r||s||x) is the same as the y he received.

With this scheme, even Bob brute force the value of r||s||x, Bob can not determine the value of x, because s is kept secret.

4 Network and Software Security

A. SSL

Whether a website has a 256-bit certificate is not the standard to prove that the website is secure. When getting the website's certificate, it should be checked if one of the trusted Certification Authority has signed the certificate. Sometimes the verification can be cancelled with Online Certificate Status Protocol by the attackers and this make the users do not know the website is not secure. Sometimes there can even be some fraudulent certificates.

B. Salting Passwords

The password is usually stored in the database. However, it is so dangerous to store the password

in plaintext. Even Storing the hashed password is considered not secure as well. To make sure the password is safe even if the database is stolen, we use salt attaching to the password to generate hash. By salting the password, it will become harder for the attackers to use rainbow table attack or dictionary attack because the original password is adding a random salt which cannot be guessed using information in a database or a dictionary. In addition, adding a salt in the password can increase the password strength. It can increase the length of the password so that brute force the hash become much more harder.

The difference between the salt and the secret salt is that salt can be either public or secret. Actually, the salt is not necessary to be kept secret. An attacker won't know in advance what the salt will be, so they can't pre-compute a lookup table or rainbow table. It is important that the salt can not be reused. Using a single salt also means that every user who inputs the same password will have the same hash. This makes it easier to attack multiple users by cracking only one hash

C. OS Fingerprinting

The operation systems can be identified by so called OS fingerprinting, which is corresponded with the TCP/IP stacking fingerprinting. The TCP/IP stacking fingerprinting is fetched when the computers communicate through layer 4 in the OSI model using TCP/UDP. The TCP/IP stacking fingerprinting is the configuration attributes in this level of communication. With this information, one can get a OS fingerprinting by sending packets to the target machine and get the response. There is a tool called Nmap network scanning which can get active OS fingerprinting. Another way is to use pof, it can provide passive traffic fingerprinting behind the communication, which can also get the OS fingerprinting to indicate the target operation systems through network.

D. Internet

Benefits:

If everyone on the internet ran the same operation systems, it will be easier to implement security defense with low costs. Attacking and defending in the network is a resource game. By using the same operation systems, companies will have lower costs to main just one type of system with the same interfaces instead of managing multiple systems. To be more specific, the costs of human resources as well as the training costs will be reduced. In addition, implementing security project on the same system will be much easier than integrating multiple systems together. Using the same operation systems can form the security standard more easily to further reduce the costs.

Drawbacks:

However, due to running the same operation systems, there are also many drawbacks. For example, one of them is that if the attacker can successfully implement an exploit, he can apply it to all the computers running the same operation systems. It will become much more dangerous if all the people use the same operation systems.