Final Lab Exercise - Written Questions

58119125 Jiang Zhuoyang

1. Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme?

Answer:

Yes, there is a flaw caused by defect of XOR Encryption.

If the string1 sent by A to B is intercepted and the string2 replied by B to A is intercepted, the original key is obtained by XOR calculation of the two strings

2. Assume that passwords are limited to the use of the 95 printable ASCII characters and that all passwords are 10 characters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions per second. How long will it take to test exhaustively all possible passwords on a UNIX system?

Answer:

The time to test exhaustively all possible passwords on a UNIX system will be:

$$\frac{\mathbf{95^{10}/6.4*10^6}}{\mathbf{60*60*24*365}} \approx 296653.5(years)$$

3. Because of the known risks of the UNIX password system, the SunOS-4.0 documentation recommends that the password file be removed and replaced with a publicly readable file called /etc/publickey. An entry in the file for user A consists of a user's identifier IDA, the user's public key, PUa, and the corresponding private key PRa. This private key is encrypted using DES with a key derived from the user's login password Pa. When A logs in, the system decrypts E(Pa, PRa) to obtain PRa.

a. The system then verifies that Pa was correctly supplied. How?

b. How can an opponent attack this system?

a.Answer:

The system gets the Pa when user A logs in and decrypts E(Pa, PRa) with Pa to obtain PRa.

The public key PUa is also stored in /etc/publickey.

Because of the mutual inverse between PUa and PRa, the system can check the PRa to verify if Pa is correctly supplied.

b.Answer:

Because of the visibility of /etc/publickey, attacker can just guess the password Pa brutally to compute PRa. For example, the attacker can use an arbitrary string to test out the password and PRa.

4. A company named Wukong wants to offer a secure, cloud-based backup system. When the user updates a local file, her Wukong client opens a TCP connection to a Wukong server, and uses the Diffie-Helman protocol to establish a secret symmetric key *K* with the server. Then, the client generates the following string *s*:

$$s =< documentName, documentContent, userName, userPassword, randomNumber >$$

and sends the following message to the Wukong server:

$$EK\ (s, \mathrm{MAC}K\ (s))$$

where $E_K(m)$ denotes encrypting message *m* using key *K*, and $MAC_K(m)$ denotes computing a MAC message authentication code of message *m* using key *K*.

The server decrypts the message, verifies the user's password *userPassword*, and verifies the integrity of the message using the MAC. If all of the checks succeed, the server stores the document. If the server sees more than 10 messages with the wrong password, all future accesses to that account are blocked. How can a network attacker reliably obtain the user's password

Answer:

Wukong does not do authenticate with users, so that attacker can pretending to be Wukong to get the user's password.

5. Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests. Consider a server system with a table for 256 connection requests. This system will retry sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30 second intervals, before purging the request from its table. Assume that no additional countermeasures are used against this attack and that the attacker has filled this table with an initial flood of connection requests. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? Assuming that the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth does the attacker consume to continue this attack?

Answer:

The time between two emptying operations:

$$T_{full} = 30 * 5 + 30 = 180(s) = 3(m)$$

The number of requests that attacker needs to send between two emptying operations is 256.

So that, the number of requests to send for continuing this attack is:

$$n_0 = \lceil \frac{256}{T_{full}} \rceil = 86(t/s)$$

The TCP SYN packet is 40 bytes in size, so that the size of one request is:

$$s = 40(byte) = 320(bit)$$

So that the bandwidth for continuing this attack is:

$$B = \frac{n_0 * s}{60} \approx 458.67(\text{bps})$$

6. Which certifications should be in your list of credentials if you decide to pursue a career in Cyber Security? Please list THREE certifications you think are the most demanded (hottest) certifications in cyber security.

Answer:

1. CISSP
2. CISM
3. CISP