NAME: SAMUEL MWANGI

REG: P15/1461/2012

COURSE TITLE: COMPUTER NETWORK SUCURITY

COURSE CODE: CSC 411

LECTURER: PROF OKELLO ODONGO

1. **Assume a re-usable password authentication system that uses of an “encrypted” password file based on a one-way function, f(pw). Describe the dictionary attack on such a system. Explain how use of “salt” makes the dictionary attack difficult.**

Dictionary attack mostly applies to shorter and ordinary passwords. In the above case, an attacker prepares a dictionary (list) of probable matching passwords in a file in plain text then encrypts the words. The attacker then obtains the password file and compares for a matching entries of their encrypted words and the encrypted passwords in the password file since the encryption is a one way function (No need of decrypting).

Using salt involves using a random value together with the passwords for each user then encrypting the passwords. In this case, duplicates are not revealed making a dictionary attack more difficult.

2. **Briefly explain the capabilities based access authorization mechanism. Explain how the MAC (Message Authentication Code) could be employed to secure a capability against forgery.**

Involves using an **unforgeable token or ticket** for a subject referring to a particular object and **specifies operations that can be performed** on that object by the subject. Mostly applied in large distributed systems. A capability structure has a check-field that locks the capabilities of the subject. It contains the object reference, Operations and a secret-key. The check-field function is one way.

Message Authentication Code (MAC) is a cryptographic checksum on data that uses a session key to defeat both accidental and intentional modifications of the data. The key is only known by the sender and the recipient. In capability access authorization mechanism, the token can be taken as the message and a MAC is provided that is only known by the sender and the recipient. In this case, the recipient only expects a message from a particular sender whose key is known thus no forgery.

3. **Describe the memory protection mechanism based on the segmented memory architecture.**

In this architecture, a **program is organized as a collection of logical segments** (data, code, and stack data). Each segment has a **unique ID and an offset denoted as: <SegID, offset**>. For all segments, an address table is maintained by the OS- cached in the memory management unit (MMU). All references pass through the MMU which does **address translation and access rights checks**

How it works.

A **program that references memory specifies their request privilege level** (RPL). On the other hand the **descriptor of the target specifies the program instruction protection level** otherwise known as descriptor privilege level (DPL). The **Current Privilege level (CPL)** of the executing program is also considered. For different situations the MMU does the following:-

- **Data access** – The MMU checks whether the **DPL** is lower or equal to both CPL and RPL to allow access
- **Call to Conforming Code -** DPL must be at a higher or equal privilege level to both CPL and RPL
- **Call through a call gate** – gateDPL must be at a lower or equal privilege level to both CPL and RPL. TargetcodeDPL must be at a higher or equal privilege level to both CPL and RPL

For any situation if the above conditions does not apply, the MMU generates an privilege violation interrupt.

4. **Consider the design and implementation of a biometric authentications system in which the template is stored in a card (token) carried by the owner. Explain how such a system works assuming that the card is to hold only the PIN of the owner, name of the owner, and a "signature" of the biometric template. (Note signature constructed using message digests (hash) and public key cryptography. I.e., describe the enrolment and the verification processes.**

Enrollment

The name and biometric template of the user are captured. When capturing the biometric template **several of them are captured to arrive at a true sample representative** via an averaging process. The **template is then hashed (utilizes algorithmic numbers) to protect it against modifications**. The user's **public key is also applied on the template to associate the template with the user**. The hashing and encryption of the template creates the signature of the biometric template. The user is then assigned a pin. The user name, pin and the signature are then stored in the card to be carried by the owner.

Verification

User provides the card then **claims identity by providing a PIN which should match the one the card**. To **verify the claim, a biometric sample of the user is taken and subjected to hashing and encryption as applied during enrolment (it is one way function)** to obtain a sample biometric signature. The signature is then compared to the one the card. If they match, the user is verified.

5. Explain why I/O protection is necessary for the successful realization of file access control mechanism such as that based on ACL.

How it Works

Process or programs have privilege levels for each operation on device drivers or instructions. For each request for an operation, either read write or execute, the privilege level (like rights in ACL) is checked if it allows the operation to take place.

Why it is necessary

- Prevents **programs from interfering (unauthorized access)** with the I/O instructions and secondary storage devices
- Prevent programs **from interfering with the I/O operations of other programs**
- Facilitates **authorized sharing of I/O and secondary storage devices**.

6. Briefly describe the Diffie-Hellman key exchange system. Explain how it might be susceptible to man-in-the-middle attack. Explain how certificate authority system may be used to secure the Diffie-Hellman exchange from the man-in-the-middle vulnerability

Diffie-Hellman key exchange system uses numbers raised to powers to generate decryption keys.

How it works

Assuming there are two users Alice and Bob in a communication network, they **both agree on keys *p* and *q*** in a channel they know to be secure. Key ***p*** is a **prime number** while ***q*** is a **generator of *p***. Alice then chooses positive personal number ***a*** and bob chooses positive personal number ***b*** . Both ***a and b*** should be less than modulus ***p*** and **should be kept secret by each of the parties.**

Alice computes $a^* = q^a \bmod p$

Bob computes $b^* = q^b \bmod p$

Alice sends ***a**** to Bob and Bob sends ***b**** since both can be sent over an insecure medium. A number x can be generated by both parties as illustrated below:-

For Alice $x = (b^*)^a \bmod p$

For Bob $x = (a^*)^b \bmod p$

They can then use key ***x*** in their own chosen encryption technique in their communication.

Susceptibility to man-in-the-middle attack

An intruder can obtain ***p, q, a**** and ***b*.*** They only need to compute for ***a*** and ***b*** using discrete algorithms

Using a Certificate Authority (CA)

A certificate authority provides third party authentication of public keys. Alice and Bob can identify to the CA and each authenticates themselves. The CA issues a certificate to each.

During transmission of information, **each participant publishes their certificate** and the other can **verify its validity by confirming the trusted attached certificate signature.** Only the certificate authority can create and modify the certificate.

7. **The time it takes to encrypt a message of n 64-bit blocks using a 64-bit key symmetric key cryptography algorithm is T * n. The time to encrypt the same using a public key cryptography algorithm is $T * 10^4 * n$. How much faster, compared to the public key system, would a hybrid cryptographic system (described in the lecture notes) based on the above be? Show clearly how you have arrived at the answer.**

Overview

In symmetric key cryptography, involves two parties using **the same private key** to both encrypt and decrypt information. **Public** key cryptography, on the other hand, is where **two different keys are used** – a public key for encryption and a private key for decryption. Hybrid cryptography in the above case **would combine both public key and symmetric key cryptography** algorithms - use public key to encrypt the 64-bit key and then use symmetric key to encrypt the whole message.

Calculation

To encrypt the message, the symmetric key will take **T*n**. To encrypt key, public key algorithm will take $\mathbf{T * 10^4 * n}$.

But since the key is 64 bit and is equivalent to one block, then **n = 1** Hence Hybrid = $\mathbf{(T * 10^4) + T*n}$ implying that hybrid is $\mathbf{(T * 10^4 * n) / (T * 10^4) + T*n}$ faster.

Assuming that T is 1 second and n is 50, then hybrid is $\mathbf{(1* 10^4 * 50) / (1 * 10^4) + 1*50}$ faster which is equal to 45.75. Hence we can say that hybrid is n times faster than public key mechanism.

8. **In the context of a manual messaging systems, a common forgery attack involves the attacker cutting a signature from an intercepted message and pasting that signature on another bogus message. Show that the digital message authentication system based on message digests and public key cryptography is relatively immune to this kind of attack. In this context explain the importance of “collision resistance property”.**

In the digital message authentication system using message digest and public key cryptography, the signature is generated as follows

On the sender’s side

- ✓ The sender generates a small, eg128bit, digest from the message to be sent.
- ✓ The digest is then encrypted using the secret key to generate a short authenticator, now called the signature.
- ✓ The signature is then sent together with the message to the recipient.

On the Recipient’s side

- ✓ The recipient applies the same digest generation algorithm to the message to obtain the recipient computed digest.
- ✓ The received signature is decrypted to obtain the received digest.
- ✓ Compares the computed with the received digest.
- ✓ If there is a match then sender is authenticated and the message’s integrity is confirmed.

In the above scenario, if an attacker cuts a signature from an intercepted message and pastes that signature on another bogus message, the recipient will apply the same digest generation algorithm to the bogus message, and decrypt the received signature to obtain received digest which will not match, because the messages used by sender would not be the same as used by the recipient. This would therefore alert the recipient that the message has been tampered with.

Collision Resistance

A hash function H is collision resistant if it is hard to find two inputs that hash to the same output. A function that is not collision resistant allows an attacker to take an authentic digitally signed message, find a different message that produces the same digest (the collision), then substitute the fake message for the real one while keeping the same signature value. The recipient trying to validate the signature won't be able to tell the difference. This destroys the value of digital signatures. Hence, an effective cryptographic hash function needs to be collision resistant.

References

1. Class notes.

2. *What are the differences between symmetric and public key cryptography. Also give an example of when you would use each one.* Retrieved from http://www.programmerinterview.com/ on 20th November 2015.

3. *Hybrid Encryption.* Retrieved from https://www.techopedia.com/definition/1779/hybrid-encryption on 19th November 2015.

4. Contributed by Dr. Ron Peterson, Posted by Margaret Rouse, *Diffie-Hellman key exchange (exponential key exchange definition).* Retrieved from http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange on 19th November 2015.

5. William Stallings (16th November 2015). *Cryptography and Network Security Principles and Practices, Fourth Edition.*