Quiz 6

CSE-644 INTERNET SECURITY

DR. SYED SHAZLI

2/28/2023

Anthony Redamonti
SYRACUSE UNIVERSITY

1) What's the difference between Public key and Symmetric key? Why do we need public key method?

A symmetric key is used to encrypt the data before transfer and decrypt the data after transfer (same key is used to encrypt and decrypt the data). Public key encryption, also known as asymmetric key encryption, is the use of a public and private key pair. A large random number is fed into a key generation program that outputs the pair of keys. The public key is used to encrypt the data, and the private key is used to decrypt the ciphertext into plaintext. Anyone with a public key can encrypt a message, but only those who know the private key can decrypt it.

The public key encryption is needed to solve the key exchange problem. The symmetric key encryption struggled to find a secure method of sharing the key between the sender/receiver. The key used to be sent via Fed-Ex or USPS (unsecure). James Ellis first introduced the idea of the public key encryption, in which the public key is sent over the network in plaintext and is used only for encryption. The user keeps the private key secret and uses it to decrypt incoming messages.

2) What is Diffie_Hellman Key Exchange (math formula)? How do you explain it in a public key exchange? (which can be considered public key, which can be considered private key)

The Diffie-Hellman key exchange algorithm uses a discrete logarithm to securely transmit keys between the sender/receiver. The following formula was used to transmit the number "x" : g^(x) * mod(P) = b. Even if g, P, and b are known by an attacker, it is difficult to find x. The receiver will also send their key "y" as a discrete logarithm to the sender.

Public key 1 = g^(x) * mod(P)
Public key 2 = g^(y) * mod(P)

The sender can then perform the following operation: (g^(y)mod(P))^(x) * mod(P). X is known to the sender. The formula simplifies to g^(xy)*mod(P). The number is only known between the sender/receiver.

Shared private key = g^(xy) * mod(P)

3) What is man-in-the-middle attack? (explain it in a little tech detail, such as describe which key is used to do this attack and why it can succeed).

An attacker can intercept the traffic between the sender/receiver and change the public key by altering the content of the packets. The public key sent to the receiver will be intercepted and modified by the attacker (man-in-the-middle attack). The receiver will use the attacker's public key to encrypt a message. The attacker can decrypt the message and forward the message with the correct encryption to the sender. The attacker will then have the ability to decrypt the messages from both the sender and receiver.

4) What is the disadvantage of public key? It is used mostly for what encryption? Why?

The disadvantage of public key encryption is that it is susceptible to the previously discussed man-in-the-middle attack. A digital signature is used to prevent the alteration of the public key. The digital signature is verified by a trusted third party to match the public key with its owner.

Public key encryption is used primarily for encrypting communications between a server/client. The sender authentication makes use of the digital signature. The public/private key pair in combination with the digital signature ensure a robust method of encrypting data between a sender/receiver.