Computer Systems Class Notes

November 17th, Third Hour
Raymond Cheng

Network Level Threats

Machines accepting messages from other machines are susceptible to attacks. Below are some common network threats:

- **Worms** are self replication programs. Unlike viruses, they do not attach themselves to other code. It is possible to spawn multiple copies on the host. Of the worms, the Morris worm was perhaps the most famous. It attached itself through an exploit in finger. It would then spread itself through rsh, dictionary attacks against local user accounts and e-mail.
- **Port scanning** is the act of querying machines to determine vulnerability.
- **Denial of service** aims to overwhelm target with requests such that it cannot respond to legitimate requests. More worrisome is the **distributed denial of service attack**. There is no easy way to filter out unwanted traffic.These distributed attacks are typically carried out by botnets.
- Botnets are also a good way to generate spam.

Cryptography

Suppose we are communicating over a network and the network is insecure. By insecure, we mean that messages are not authenticated. We want to guarantee that the other party is who we think they are. To effect this, cryptography modifies the message to restrict the list of possible senders/receivers. This is typically done via secret keys.

An encryption algorithm contains:

- Set of keys k
- Set of message M
- Set of ciphertext C (encrypted messsege)
- Function E: K -> (M -> C)
- Function D: K -> (C -> M)

We want E (encrypt) and D (decrypt) to be efficient functions. Furthermore we want to ensure that observing the ciphertexts will not reveal the decryption function.

There are two general types of encryption: symmetric and asymmetric.

- **Symmetric encryption** is very efficient; it can be done easily in hardware. The key is the same for both encryption and decryption. Common examples are DES, AES and RC4. There are two types of symmetric encryption:
    - **Block cipher**: these operate on fixed length group of bits called blocks. one block of message -> one block of ciphertext. To further strengthen the encryption, cipher block chaining is employed. Here the current block's encryption is dependent on the encryption of the previous blocks.
    - **Stream cipher**: these operate on non fixed length messages with varying number of bits.
- **Asymmetric encryption** is generally expensive. It take 1000x longer than symmetric encryption.
    - There are pair of keys k_1, k_2 such that $E(k_1)$ and $D(k_2)$. $k_1$is typically the public key, and $k_2$the private. This allows anyone to write the $k_2$holder an encrypted message.
    - Most common implementation is RSA.

There are some strategies employing encryption:

- We can use an asymmetric encryption to encrypt a symmetric encryption key. This allows us to take advantage of the symmetric encryption speed.
- We can give everyone the private key and keep the public key private. Thus everyone can decrypt messages, but not encrypt them. This is used for authentication.
- To ensure that an unencrypted message is authentic. The sender can create a hash of the message, and encrypt the hash. Everyone decrypts the hash and verifies it against the unencrypted message.