Network and Computer Security

Summary

Contents

1 Cryptography **2**

1.1 Cryptographic Services . . . 2
1.2 Cryptographic Building Blocks . . . 2
1.2.1 Symmetric Cipher . . . 2
1.2.2 Asymmetric Cipher . . . 3
1.2.3 Cryptographic Hash . . . 3
1.2.4 Composite Building Blocks . . . 3
1.3 Symmetric Criptography . . . 3
1.3.1 Symmetric Stream Ciphers . . . 4
1.3.2 Symmetric Block Ciphers . . . 4
1.4 Hash Functions . . . 8
1.4.1 Message Integrity Codes . . . 8
1.5 Asymmetric Ciphers . . . 9
1.5.1 One-way Functions . . . 9
1.5.2 Algorithms . . . 9
1.5.3 Digital Signatures . . . 10

2 Networks **11**

2.1 Network Models . . . 11
2.1.1 OSI and Internet . . . 11
2.1.2 Address Resolution . . . 11
2.2 Network Vulnerabilities . . . 12
2.2.1 Physical Layer . . . 12
2.2.2 Data Link Layer . . . 12
2.2.3 Network Layer . . . 13
2.2.4 Transport Layer . . . 13
2.2.5 Application Layer . . . 15

Chapter 1

Cryptography

It is a widespread and dangerous belief that encrypting everything provides protection against anything. In reality, when the algorithm is known it is necessary to prevent several types of attacks, such as ciphertext-only, known-plaintext, chosen-plaintext or chosen-ciphertext. Cryptography must, then, protect the information against unauthorized insertion of information, modification of information in transit, replay of information and access to information.

1.1 Cryptographic Services

To this end, we need the following cryptographic services:

- Confidentiality: a service used to keep the content of the information from all, but those entities authorized to have it. Has the drawbacks of making debugging harder and may lead to information loss if the key is lost. Can be assured through symmetric of assymetric cipher.
- Integrity: a service that detects data manipulation by unauthorized entities (not the same thing as error detection codes). An intruder should not be able to substitute a false message for a legitimate one. Can be assured through MIC or a digital signature.
- Authenticity: a service used to ascertain the identity or the origin of a message. Can be assured through MIC or a digital signature, tough freshness requires adding a nonce to the message.
  - Entity authentication: verify the identity of an entity
  - Data origin authentication: confirm the creator of the message
  - Non-repudiation: a service which prevents an entity from denying. Can be assured by a digital signature. previous commitments or actions

1.2 Cryptographic Building Blocks

1.2.1 Symmetric Cipher

Uses the same key to cipher and decipher. In cryptographic function notation:

- $E(M, K)$: cipher message M with key K
- $D(C, K)$: decipher cryptogram C with key K

1.2.2 Asymmetric Cipher

A public/private pair of keys is used (KU/KR). In cryptographic function notation:

- $AE(M, KR)$: cipher message M with private key KR
- $AD(C, KU)$: decipher cryptogram C with public key KU

It is also possible to cipher with the public key and then decipher with the private key.

1.2.3 Cryptographic Hash

A cryptographic hash function does not use a key, instead receives an input message and returns a digest of the data. In cryptographic function notation:

- $H(M)$: hash of message M

The digest value is deterministic, has fixed size, a unique representation, is non-reversible and sensible to input changes.

1.2.4 Composite Building Blocks

- Hybrid cipher: a random symmetric key is generated and used to cipher the message. This key is then ciphered with the public key of the receiver and is sent along with the ciphered message. The receiver must decipher the symmetric key with its private key and use it do decipher the message
- Message integrity code: the MIC is created by creating the digest of the message and ciphering the result. It can then be used to check the integrity of the message by generating a new hash and comparing to the sent one.
- Digital signature: a digital signature is created by ciphering a digest with the private key. The receiver can then decipher with the public key and verify the identity of the sender.

1.3 Symmetric Criptography

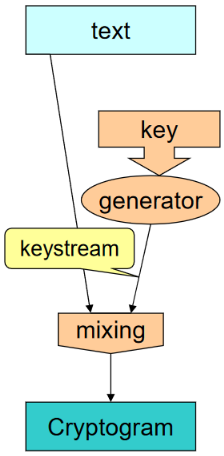
Symmetric ciphers use a single secret key that may be shared by 2 or more communicating parties. This allows confidentiality to all those who have the key and message authentication, with good performance. The main problem lies in key distribution

For N communicating parties, $N \times (N - 1)/2$ keys are needed for them to be able to communicate 1 - 1 secretly.

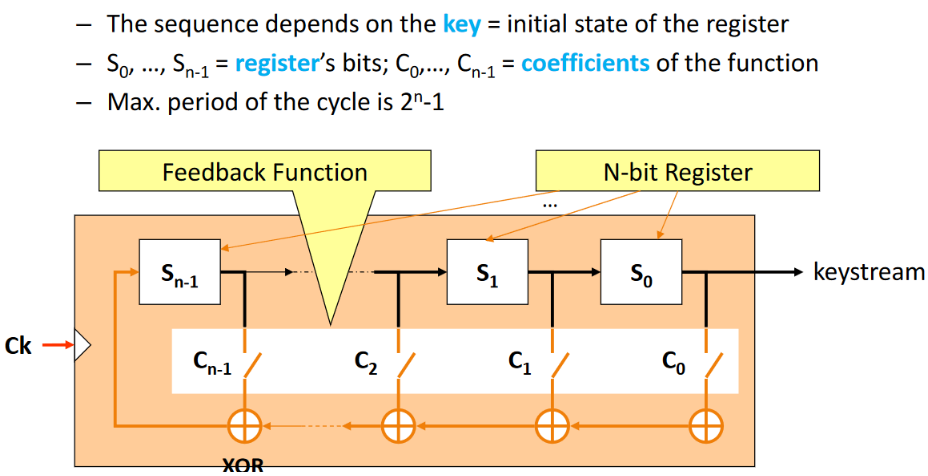
An example of a symmetric cipher is the one-time pad, where the message is XOR'd with the key. The security is based on the assumption that the key is never reused.

1.3.1 Symmetric Stream Ciphers

Symmetric stream ciphers are pratical approximations to the one-time pad. Keystreams are generated in a deterministic way from a fixed size key (approximation to real random sequence generators).



In this type of cipher, if the plain text is known, the keystream is exposed. The secure pseudo-random generators are sometimes based on LFSRs (Linear Feedback Shift Registers). It consists on a state machine that produces a cyclic sequence of bits:



1.3.2 Symmetric Block Ciphers

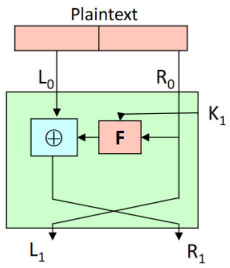
These are also based on approximations, using Shannon's notions of confusion (repeated application of a complex function to a large block) and diffusion (permutation, substitution, expansion and compression).

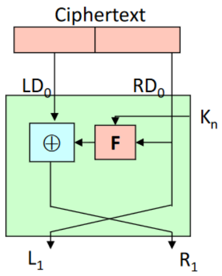
Feistel Network

The feistel network is a complex function most commonly used in block cipher algorithms. It applies a round function F over multiple rounds:

- Each round uses a different round key (K_i), obtained from the key (K)
- Text is split in left (L) and right (R) parts

The cipher and decipher processes are the same, with the keys used in the inverse order.





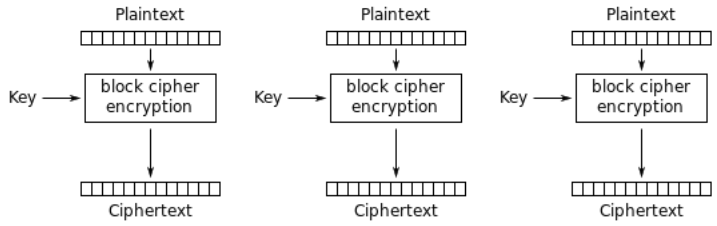
DES

The DES algorithm uses 64 bit blocks with 56 bit keys. It applies the feistel network algorithm on several rounds, after an initial permutation of the 64 bits, according to a fixed table.

Block Cipher Modes

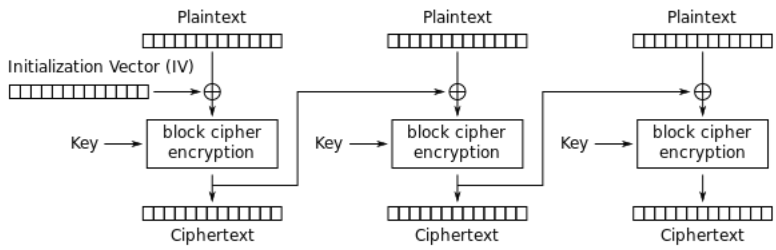
When using a plaintext of different size than the block, a cipher mode must be used.

- *Electronic Code Book* (ECB)
  - Encryption using independent blocks
  - Weakness in reproducing patterns from the original text; identical blocks produce the same ciphertext



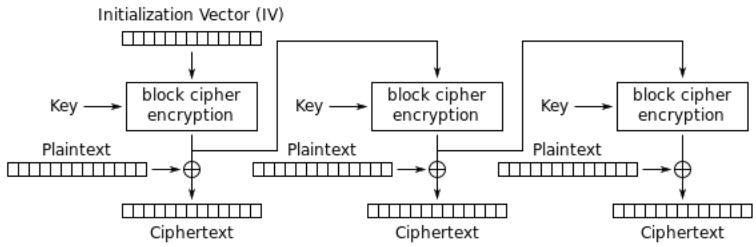
Electronic Codebook (ECB) mode encryption

- *Cipher Block Chaining* (CBC)
  - Plaintext is XORed with the ciphertext of the previous block before encryption
  - Reduces the risk of pattern replication
  - Uses an initialization vector in the first block (necessary for decryption) and requires padding: bits to compose entire blocks of the size required by the algorithm



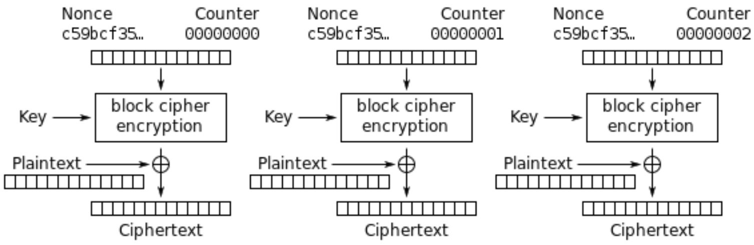
Cipher Block Chaining (CBC) mode encryption

- *Output Feedback* (OFB)
  - Retains the advantages of CFB, and the ciphertext is not used in the next block, allowing block cipher operations to be performed in advance, enabling parallel XOR as soon as the text (plaintext or ciphertext) is available



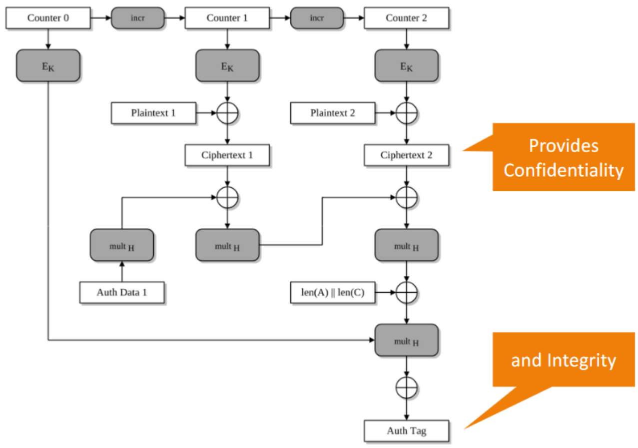
Output Feedback (OFB) mode encryption

- *Counter Mode* (CTR)
  - Standard cipher mode in AES
  - Uses a nonce and a counter, which must be different in each cipher operation



Counter (CTR) mode encryption

- *Galois Counter Mode* (GCM)



Padding

Sometimes it may be necessary to pad the last block, when the message size is not divisible by the block length. This may be done by:

- Padding with zero (null) bytes, spaces (0x20), all bytes of the same value
- Padding with random bits
- Padding with 0x80 (1000 0000) followed by zero (null) characters
- Padding with the PKCS#5 scheme: Sequence of bytes, each of which equal to the number of padding bytes (e.g. if 24 bits of padding need to be added, the padding string is "03 03 03": 3 bytes times 8 bits equals 24)

AES

AES is the current encryption standard. Supports keys of 128, 192 and 256 bits with 128 bit blocks. It runs in 10, 12 or 14 rounds, in which it substitutes bytes, shifts rows, mixes columns and adds the round key XOR state with key material)

1.4 Hash Functions

These are cryptagraphic functions, but not ciphers. They must be:

- Collision resistance: Computationally infeasible to find two inputs that give the same hash
- Preimage resistance: Given a hash, it's computationally infeasible to find an input that produces that hash
- Seconde preimage resistant: Given a hash value and the corresponding input, it's computationally infeasible to find a second input that generates that same hash

The most common algorithms are:

- MD5 (128 bits): very weak
- SHA-1 (160 bits): weak
- SHA-2 (256 to 512 bits)
- SHA-3 (256 to 512 bits)

Attacks on hash functions are sometimes done by brute force ($P(collision) = 2^{m-1}$) and most often through the birthday attack (pick M, M', M'', M'''... and obtain hashes until any 2 are identical) ($P(collision) = 2^{m/2}$).

1.4.1 Message Integrity Codes

The objective is to detect changes to a message. It allows the checking of a message's integrity and, with freshness can provide authenticity, thus, it's sometimes called MAC.

Under the assumption that the sender and recipient have a shared secret key K, the idea is to send the messgae and the MAC; if the message (or the MAC) is modified by an attacker, the recipient will be able to detect it. Attacker cannot create a valid MIC because he does not have K.

Implementations of MAC could be as follows:

- Hash the message and encrypt the digest
- Using a keyed-function (CMAC, usually with CBC)
- Using a keyed-hash (HMAC)

1.5 Asymmetric Ciphers

Asymmetric cryptography uses a pair of public/private keys. It allows for confidentiality, authentication and integrity (digital signatures). Has the advantage of only needing N key pairs, but the performance is much worse.

For confidentiality, the public key is used to cipher and the private to decipher. For authentication it's the opposite.

1.5.1 One-way Functions

Also known as trapdoor functions. The idea is for the function to be easy to compute in one direction, but hard to invert. These are usually used in asymmetric cryptography.

1.5.2 Algorithms

RSA

In this algorithm, the plaintext is divided into blocks, which are treated as a number. The keys are generated as follows:

- Choose two prime numbers p and q
- Define $n = pq$ and $z = \phi(n) = (p-1)(q-1)$
- Choose $e < n$ such that e is coprime with z
- Calculate d such that $ed \mod z = 1$
- The public key is $K_u = (e, n)$, and the private key is $K_r = (d, n)$

To encrypt, compute:

$$E(K_u, m) = m^e \mod n = c$$

And to decrypt:

$$D(K_r, c) = c^d \mod n = m$$

RSA is often used to produce signatures. To sign M we calculate $S = (hash(M))^d \mod n$ and to verify we check $hash(M) == S^e \mod n$. Only the owner of the private key can sign, but anyone with the public key can verify the signature.

ECC

Elliptic curve cryptography offers the same security as RSA with smaller bit sizes. In this case, the "hard" problem is the elliptic curve logarithm:

- $Q = k \cdot P$, where Q, P belong to an elliptic curve (e.g. $y^2 = x^3 - 3x + b \mod p$)
- Easy to compute Q, given k and P
- Hard to find k, given Q and P
- P is a base point (parameter of the curve)

1.5.3 Digital Signatures

Digital signatures use an asymmetric cipher and a hash function. The basic algorithm is as follows:

- Sign: $S(doc) = E(K_r, hash(doc))$
- Validate: $D(K_u, S(doc)) == hash(doc)$

Today often ECDSA is adopted (with elliptic curve encryption).

Chapter 2

Networks

2.1 Network Models

2.1.1 OSI and Internet

There are seven layers in the OSI model:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

The network is not just computers and servers, there are also:

- Hubs: Send signals everywhere
- Switches: Send frames only where they need to go
- Routers: Look at the IP address from the incoming packet and forwards it. Have MAC address too.
- Gateways: Access point to other networks, with possible change of addressing and networking technology.

2.1.2 Address Resolution

In layers 2 and 3, MAC and IP addresses are used, respectively. IP addresses identify the network and the machine and MAC addresses may be converted to IPs with the ARP protocol. Some network ranges were reserved for private addressing.

2.2 Network Vulnerabilities

2.2.1 Physical Layer

Hubs

Hubs broadcast information on a shared medium, thus, are at threat of information leakage through sniffers.

Anyone can connect to a hub even if it is physically secure.

Sniffers

Usually, network adapters operate in a non-promiscuous mode (only listen to what is sent to their MAC). Sniffers, on the other hand, read all frames, regardless of MAC.

It is possible to indentify sniffers using tools (with several methods: latency, dns, os-specific, ...) or using the ARP method:

- Machines cache ARPs
- Send a non-broadcast ARP with our correct MAC address
- Then send a broadcast ping with the right IP but wrong MAC address
- Only a machine which has our correct MAC address from the sniffed ARP will respond

To prevent sniffing, switches may be used instead of hubs (does not fully solve). It is also possible to prevent the effectiveness of sniffing by using one-time passwords and encryption.

2.2.2 Data Link Layer

Switches typically send frames only to the destination MAC address, and thus, reduce the sniffing problem. There are, however, some ARP vulnerabilities present:

- MAC flooding: attacker sends several unsolicited ARP messages, overwhelming the switch with entries. When the table is filled, some switches stop accepting connections and others revert to Hub mode
- ARP Spoofing/Poisoning: An attacker sends a non-requested ARP message with a false IP-MAC address correspondence. ARP messages are in no way signed, so it is easy to falsify a message from any given MAC

Some preventive measures include the use of tools like *arpwatch*, to monitor the ARP to IP translation and the use of switches with fixed tables (with a cost in flexibility).

2.2.3 Network Layer

Routers support the indirect delivery of IP datagrams through the use of routing tables. Some threats in this layer include:

- Packet integrity: Data is not authenticated, so an attacker can change the source address of IP packets
- Information lead and DoS: Users have little to no guarantee concerning the routing path taken by the packets. An attacker might corrupt the routing tables by sending routing-update messages and effectively hijack the route

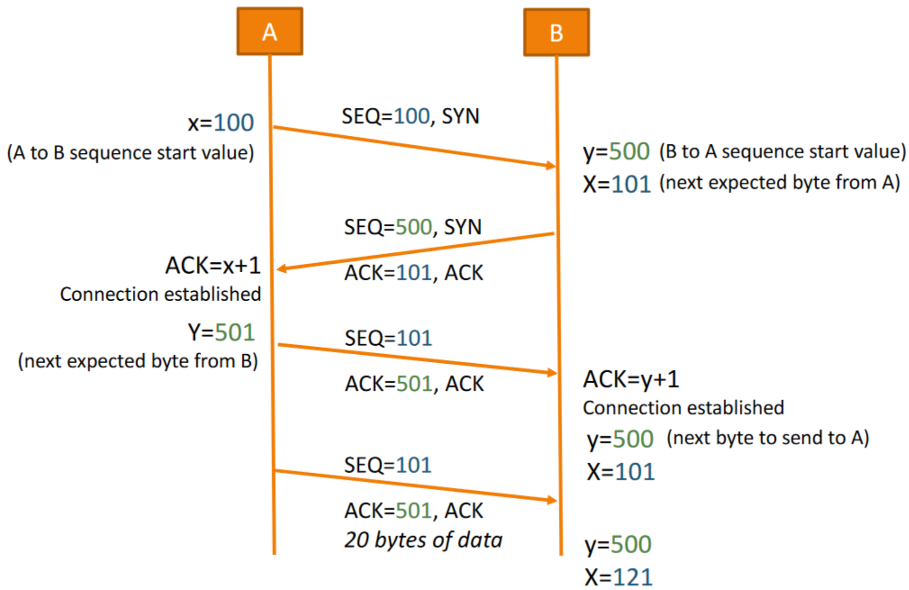
2.2.4 Transport Layer

UDP

UDP can be used to send and receive individual packets, without an established connection. It's just a thin addition to IP and is vulnerable to the same attacks.

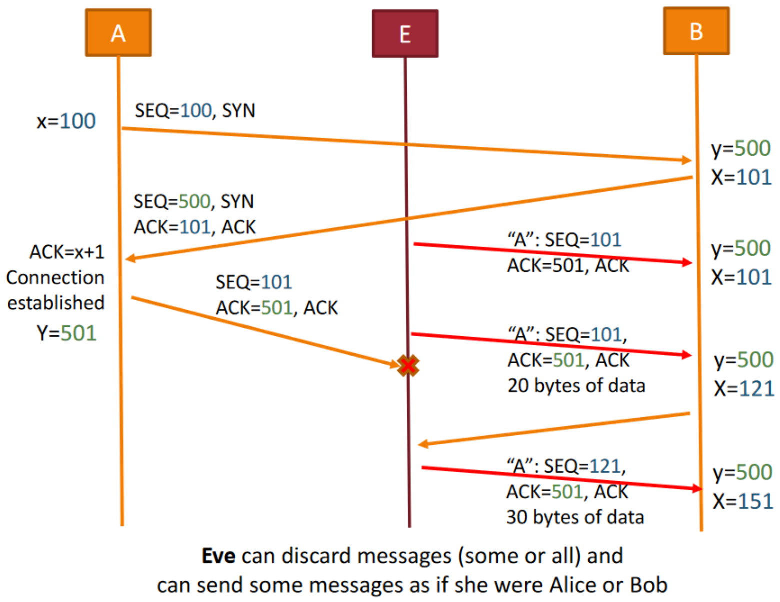
TCP

TCP can be used establish a connection to send and receive a data stream of bytes. An example of a TCP handshake:

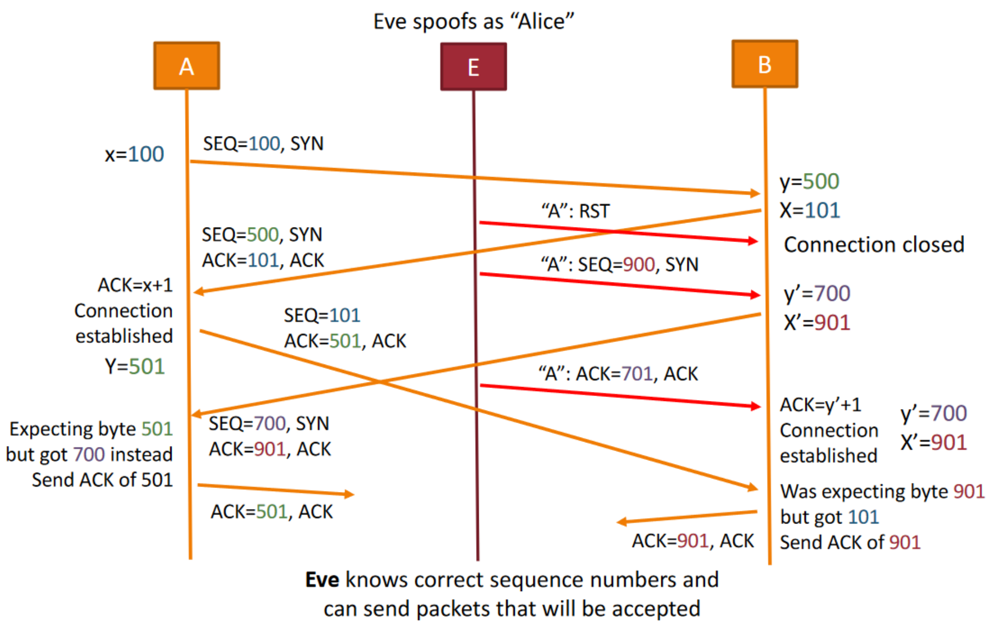


There are different techniques for TCP hijecking, depending on the attacker's capability to intercept communications:

- Full adversary-in-the-middle: the attacker is positioned to fully intercept the communication and can intercept the sequence numbers and take over the connection. The tool *shijack* is capable of doing this.



- Weak adversary-in-the-middle TCP hijack: the attacker can only eavesdrop and spoof packets (cannot drop packets). Attacker must now exploit de-synchronization between hosts. Once the sender and the receiver are desynchronized, only the attacker can create data segments with correct numbers



The de-synchronization can be forged during the creation of a TCP/IP connection with a reset and with false acknowledgements. It can also be done for an already established connection by sending blank data to displace sliding windows.

- Blind TCP hijack: The attacker cannot capture return traffic from the host connection and only blindly sends malicious or manipulated packets. The attacker does not receive any confirmation of the desired effect through a packet capture and for the attack to be successful, the attacker must guess the sequence numbers of the TCP packets

Another common TCP attacks is syn flooding. It consists of overloading a host with incomplete TCP/IP connection requests. There is no definite solution for IPv4 SYN flooding; SYN cookies may also be used to mitigate flooding:

- Bob generates the initial sequence number α such as:
  - α = h(K, SSYN)
  - h is a one-way hash function
  - K: a secret key known only by the server
  - SSYN: source IP address of the SYN packet
- At arrival of the ACK message, Bob calculates α again
  - If knows K and received the source IP
- Then, it verifies if the ACK number is correct
- If yes, it assumes that the client has sent a SYN message recently and it is considered as normal behavior

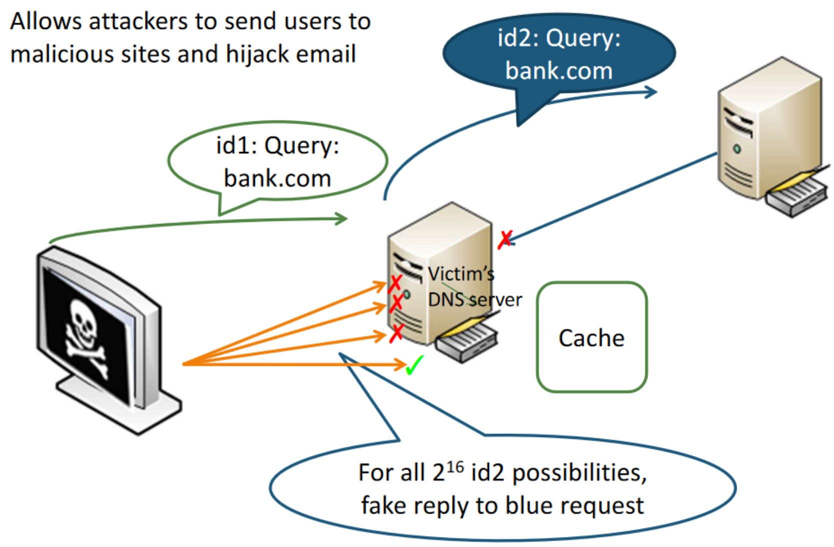
Cooperation with firewalls and attack detectors is also helpful:

- Handshake relay: firewall stands in front of server and protects it until the handshake is complete
- Gateway: firewall keeps the connection alive on server and terminates it if the client leaves the connection open but without traffic

2.2.5 Application Layer

DNS

DNS translates domain names to IP addresses. In 2008 the Kaminsky attack was found:



The attack is successful if it can guess the query ID value.

DNSSEC is DNS with digitally signed responses. Each zone has its own key-pair for signing and public Keys are published in the DNS itself. DNSSEC provides integrity and authenticity for RRs of the signed zones.

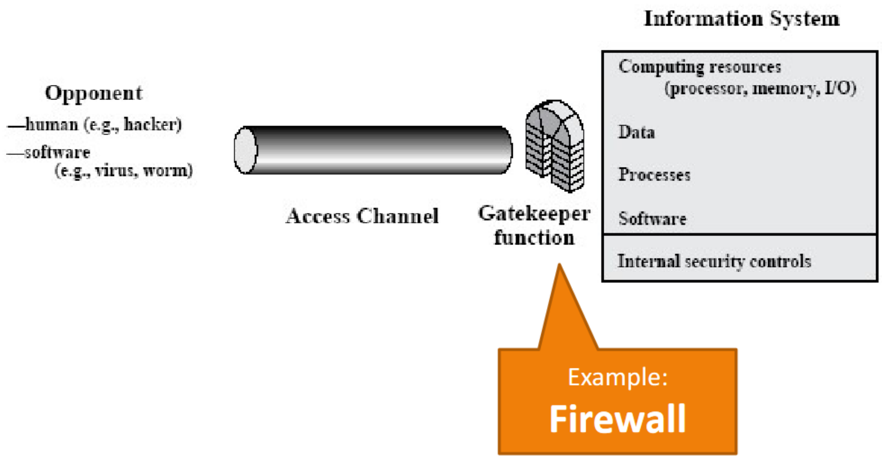
RCE

Remote code execution is a class of software security vulnerabilities. Most programming languages have some way to generate code in runtime and execute it, which has the potential of being abused by a malicious actor.

To prevent code injection, one must avoid using data as code as much as possible, as well as sanitize inputs.

2.3 Network Security Models

Gatekeeper for access control:



Secure communication channel: