Computer security fiche

Pierre Colson

Contents

Markdown version on *github*
Compiled using *pandoc* and *`gpdf` script*

CIA

- **CIA** : Confidentiality, Integrity, Availability
  - Confidentiality : The recsource is protected from unauthorized read access. (ex of mesure for protection : encryption)
  - Intergrity : The resource is protected from unauthorized write (change or delete) access. (ex of mesure for protection : message authentication code)
  - Availability : The resource can be accessed by authorized subjects in an unaltered way. (ex of mesure for protection : firewall)

Cryptography

- **RSA** is based on the hardness of factorization of large number into two prime number.

Digital signature and MAC

- **Message Authenticaton Code (MAC)** is used to guarantees integrity. The schema assumes that twos parties A and B agree on a common secret K_{AB}. If party A wants to send a message M to B, A computes $mac = F(K_{AB}, M)$, appends this code to the message and sends the result to B. The other party extract the message M and the code *mac* from the same received data, computes its own code using the message and the same key and compares the results with the code *mac*. If the match successes then the receiver is assured that
  - the message has beed generated by A
  - the message has not been altered.
- **Digital signature** use asymmetric cryptography. The sender signs the message by encrypting the ahsh of the message with his private key. The recipient can verify by decrypting this with the sender's public key and check that the resulting hash is indeed the same as one obtained by hashing the message.

Digital envelopes

- **Digital envelopes** : Preapare a message. Generate a random symmetric key. Encrypt the message with the symmetric key. Encrypt the symmetric key unsing public key encryption with re recipients public key. Attach the encrypted symmetric key to the end of the message and send it to the recipient. They are use to use symmetric key encryption for performance when sending a message, without having to agree on a secret first.

Intrusion detection

- A **host based instruction detection system** monitors the activities and the events occuring on a single host. Usaually a host based instruction detection system is interact with the host OS to intercept the events.
- A **network based instruction detection system** (IDS) monitors network traffic that transit a particular region, thsu checking the network activities of several hosts, but being no able to check internal host activities.
- **Anomaly detection** is suitable against denaila of service attack (they increase traffic and connection attempts compared to normal usage) and scanning attacks (they generate atypical traffic flow patterns).
- Signature-based intrusion detection can only detect intrusions that are already identified as such in the IDS.

Firewalls

- A **firewall** must be a *statefull* inspection firewall to keep track of the opened TCP connections.
- **packet filter firewall** is a stateless firewall.
- **Network Layer Firewall** only has addresses and ports, no other application-specific knowledge, falter, vulnearble to IP spoofing.
- **application level firewall** can take application-specific information into account, slower, no end-to-end encryption.

Principles

- The **principe of secure/fail-safe defaults** : The default, i.e., when no other specific rule exists, should be safe.
- The **principle of complete mediation** : All requests for a ressource must be checked.
- The **principle of psychological acceptability** states that security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present. Configuring and executing a program should be as easy and as intuitive as possible, and any output should be clear, direct, and useful.

Authentication

- There are two parts to authentication : identification and verification. To see who is doing the request and making sure it's really them using identifier (username) and credential (password, dongle, biometrics).
- To keep an attacker form easly finding out whether two users have the same password we can hash passwords using individual salts for each user.
- Kerberos provides mutual authentication between a user and a server, i.e., not only is the user authenticated to the server but the user can be sure that the server is authentic as well.

Malware

- **Viruses** spread by attacking their executable code to other executable programs. To spread among different host one of the affected program msut be copied by some other mechanism (e.g. the user itelf).
- **Worms** spread bu attacking vulnerability of running programs and services. They do not necessarly change the ninary code saved in the storage. A Worm can spread among multiple hosts by attacking the services running on the target host. properties that make then sucesssful :
  - Zero delay exploits, they make use of unknow vulnerabilities
  - Multi-exploit, they make use of several vulnerabilities.
  - Metamorphic, worms change their behavior patters to avoid detection
  - Multiplatform : They work not only on one operating system, but perntrate sevral different ones or exploit crosse platform scripting languages.
- **Encrypted virus** behavior :
  - Infection of a victim executable
    - the virus generates a new encryption key K
    - the virus encrypts its payload V
    - the virus copies the cyphertext $E(K, V)$ into the victim P
    - the virus copies a small code (dec) and the decryption key
  - Execution of the virus

    * the bootsrat code (dec) is executed
    * it decrypts in memory the payload
    * it executes (jumps to) the decrypted payload V
    * when the payload termianates it executes the victim V

- **ransomware** : Once the ransomware is triggered
  - it connects to a remote server asking for a public key. The remote server (controlled by attacker) generates a fress asymmetrci key pair and sends the public key to the ransomware (alternatively, the ransomware generates the keys, deliver the key pair to a remote server and delete locally the private file).
  - it encrypts local files using the public key and deletes the original file
  - once a large number of documents have been encrypted, the malware requires a payment to disclose the public key.
    A simpel counter mesure is to ensure that important files are backed up on a different computer.

Buffer Overflow

- To prevent buffer offerflow we should use safe libraries that check bounds and do other buffer management or use random canaries that are put in the buffer and if they are changed, it means there was a buffer overflow.
- Guard Pages are used to detect buffer overflows and buffer over-reads.

Social Engineering

- Typical strategies for social engineering are :
  - Stress victims by pleading urgency and dire consequences. This works because is impedes rational decision making.
  - Help victims solves a problem first. This works because the pressure of reciprocity increase
- Social engineering exploits often positive human traits, not lack of intelligence.

Access control

- In discretionary access control, the owner of a resource can give access rights to others.
- In role-based access contol, the user's identity is not as important as what tole they have at the moment. Users can have several roles and switch between them.
- The **Start-porperty of Bell LaPadula** prevents a subject to write into an abject of less security level. If this property is not guarantee, a subject that can read classified information can copy this information in an unclassified object. This object can be later accessed by uwer with low security level, allowing the classified information to be leacked.
- **Chinese Wall Model** ensure that information can not flow between two corportions being in conflict of interest The "object" (unit of information) are grouped into "datasets". Each datasets represents a corporation. Moreover, each datasets belongs to one or more conflict of interest class (CI) There are two main rules to respect :
  - (ss-rule) a subject can read an object if :
    * the obejct is in a datasets that has been already accessed by the subject or
    * the object belongs to a CI that has never been accessed by the subject
  - (*-rule) a subject can write an object O if
    * the subject can read the object and
    * the subject can not read objects outside the dataset of O

Denial of service

- **SYN-spoofing attack** : The attacker sends a SYN with a spoofed source address to a Server. The server sends a SYN-ACK to the cleint according to the spoofed and keeps re-sending SYN-ACKs after time-outs until is assume a failed connection request. A non existent or busy client connot send a RST lessage to stop this earlier and thus the server will fill up the table of connections.
- **Ingress filtering** forces hosts connected to an ISP to only deliver packets using IPs assigneted by the ISP. The same filter is not efficient in other routers since they can not validate if the IP of a packet is licit or not.
- DOS that does not saturate the network : infinite zip for example.

Secure hash functions

- Requirements :
  - can be efficiently applied to data of any size,
  - produces a fixed-lengh output,
  - the function is relatively easy to compute
  - is one-way,
  - is strong collision resistant.

Privacy

- **GDPR** is a regulation of EU menber countries for how to change their privacy laws.