Appunti Information System Security

Brendon Mendicino

October 10, 2022

Contents

1 Introduzione

Security Principles:

- security in depth: there must be more layers in security;
- security by design: you design the system to be secure;
- security by default: the security feature are turned on even if you don't want to;
- least privilege: when someone operates in the system, that program must have the minimun permession to allow the basic work;
- need-to-know: which data can be accessed by a program or by a huan, a program must operate only on the sufficient data it needs;

Security propreties:

Peer authentication When a person tries to perform an operation on system it has to proof it's identity to the system, but even the system hhas to authenticate itself to the accessing user, this is called mutual authentication (when both peer have to authenticate).

Data authentication Non-repudiation: undeniable proof of the data creator; there needs to be several facetes:

- authentication;
- integrity of the data;
- identification;
- ...

Authorization (access control) Someone has to give you the Authorization to perfrom some kind of action.

Privacy (communication) Someone listening to a conversation means to vilate the privacy.

Privacy (data, actions, position) Keeping some data encrypted inside a disk to protect them from someone accessing them. By law the internet provider are required to keep track of all the visited websites up to some years in the past, those can be accessed in case of an investigation. The internet provider needs to keep track at any time of the position of the connected device.

Integrity (data modification) The manager of the network can in some way modify the data shared by the systems, it can also cancel some parts of the data or filtering specific ones.

Replay attack If the data is encrypted they can no longer be modified by an external actor. The data cannot be changed but it can be send more that once, a **replay attack**. This can be solved by giving an ID to every transaction.

Data protection:

- data in transit: data must be sucered while travelling between systems;
- data at rest: even whene the data is parked on the disk is not modificated in any way;
- data at work: data at some point is copyed in the RAM to perform some kind of action, and if an external program modify them inside the RAM it will be never kwnown;

Basic Problems Networks are insecure:

- most of the communication are in clear;
- LANs operate in broadcast;
- geographical connections are not made through end-to-end dedicated lines but through shared lines and third-party routers;
- weak user authentication;
- there is no server authentication;
- the software contains many bugs;

2 Some classes of attacks

IP spoofing : creating an IP packet that contains a different address, typically the level 3 and level 2 address. It's a tecnique to hide somenes identiy. The attacks are: data forging a packet in someone else name, or currupting them. The countermeasures are: to never use an address-based authentication.

Packet sniffing : the ability to read the packets addressed to another network node, this is very to do in broadcast area networks (all intranet networks are broadcast). This attack allows to read the payload of the packets sniffed, the countermeasures are: to don't use broadcast networks (not possible), to encrypt the payload of the packets.

Denial-of-Service (DoS) : keeping an host busy so that it cannot perform any other relevant action. Some examples are:

- mail or log saturation;
- ping flooding;
- SYN attack

The purpose of the attack is to block the use of a system. There are no countermeasures, the only possiblity is to monitor.

Distributed Dos The attacker is using many computers (deamons, zombie, ...), usally infected with a malware, those machines contrlled by another master are called **Botnet**. To control the machines the attacker may uses encrypted channels, using a CC structure (Command and Control).

Attack: some of the deamons are turned into masters contrlling all the deamons, the attacker unplugs from the network avoind being monitored, some time later the masters give the command to the deamons and they start attacking all the vectim.

Shadow/fake server There are two kind of tecnique to fake a server:

- being in the same network (sniffing packet), if I (the attacker) respond to the user faster than the server, now your connection is opened with me, now the victim exchanges informatios with the attacker;
- creating a fake DNS to my own versions of the servers, providing wrong services, capturing data;

The countermeasures are: server authentications.

Connection hijacking (MITM, Data Spoofing) The attacker takes phisycal control of some node, becoming a **Man In The Middle**, letting the comunications of two cominacotrs get through my node, reading all the traffic, being able to perform any action. The countermeasures: even if the channel is already opend and the peers are already identified, the attackers can still take control of the comunications, to prevent this kind of attaks there needs to be some kind of authentication inside of the packets, even then also serializations is needed, beacause the attacker can swap the order of the packets.

Trojan A trojan is program containing a malicious payload. The networks are becoming more protected but terminals are becoming more vulnerable (smartphone, smartTV, IOT, ...). The attacker could trick the user into download an extension, or pirated copies of games, this programs could contain things like keyloggers. This attacks are colled:

- MATE: Man At The End;
- MITB: Man In The Browser;

Zues Also kwown as Zbot, this malware is installed on millions on devices, it can be user to:

- perfom keylogging or form grabbing;
- to load other malware, like CryptoLocker ransomware;

It was very difficoult to discover.

Sotware Bugs Bugs in a sotware are explotable, thanks to them DoS can be performed.

Virus & Co. (malware)

- virus: damages the target and replicates itself thanks to humams, requires involuntary complicity;
- worm replicates itself sucking all the available resources and the propagating;
- trojan: a vector for malware;
- backdoor: entry point not known but the developers;
- rootkit: something isntalled in the computer that provides root access to the attacker, remaining unnoticed;
- PUA: Potentially Unwanted Applications, some applications not very dangerous but performing annoying operations;

Ransomware It's a kind of malware that is oriented on getting a ransom, typically performed by ecrypting the disk or changing passwords. The only way of unlocking the device is to reset it, or

Solcial Engineering :

- phishing:
- psychological pressure: asking for help, or impersonating a person of interest imposing to perform some action;

Fake Mail It can be possible to take an old email (send to the victim), copying it and changing the attachment with a malware.

Important classes of attacks:

- Stuxnet (2010): new king of attack, it was a worm + virus for Windows, it was the first time to attempt to damage a SCADA system. It contained in itself an attack based on a known vulnerability (patched), a known vulnerability (not patched), and 2 zero-day vulnerability. This malware was used to destroy a nuclear plant in Iran (in fact in Iran the spread was 51%), destroying most of the machines, the facility was isolated from internet, the only way it could have accessed it was via USB, the malware spread thanks to shared disks and old sotfware with bugs, the malware aslo used digital signature validate by Microsoft;
- Mirai: it was a cyberworm exploiting IOT vulnerabilities, trasforming the victim in botnets for a large scale attack. All this devices ware because they have little to none protection. The software was compiled with static libraires, cross compiled and also open source. It also abserves the victim before contactin the C&C, if it detects some secuirty protection it contacts a fake C&C.

The pillars of security

- Planning;
- Avoidance;
- Detection;
- Investigation;

3 Foundations

Cryptography It's a mathematical algorithm that consists in: a clear message gets encrypted with a key, send to the receiver, that will decrypt the message with a second key to read the original message.

- message in clear: called: **plain text** or **P**;
- ecrypted message: called **chipertext** or **C**;

Kerchoff's principle:

- the keys needs to be secret;
- the keys are managed by a trusted system;

- the keys needs to be of adequate lenght;

If this three priciples are met then the ecryption and decryption algorithms can be public.

Security through obscurity (STO)

Secret key/symmetric cryptography The key is shared

$$C = enc(K, P) \text{ or } C = PK$$

$$P = dec(K, C) = enc^{-1}(K, C)$$

The main problem of symmetric cryptography is how to share the shared key.

DES is an **obsolete** symmetric algorith with 64 bit block and 56 bit key. AES is a **state of the art** symmetric algorithm that uses 128 bit block and 128-192-256 bit key.

The XOR function If the input is random the output has the same probability (the 0:1 have 50% probability of outcome).

DES It used 64 bits as a key but only 56 bits were for the key, the other 8 bit were parity bits, this algorithm was created to run fast on hardware.

Triple DES (3DES) 3DES works with 2 keys, following the algorithm:

$$C' = enc(K_1, P)\ C'' = dec(K_2, C')\ C = enc(K_1, C'')$$

3DES with 3 keys:

$$C' = enc(K_1, P)\ C'' = dec(K_2, C')\ C = enc(K_3, C'')$$

The reason why it's not good to encrypt twice with the same algorithm, the reason is beacause of the attack **meet-in-the-middle**, which allows to decrypt the data with 2^{n+1} attempts if the keys are n-bit long, this is not a good enough improvemnt for the incresed volume of work added, or worse if the algorithm is part of a group there could exist a K_3:

$$enc(K_2, enc(K_1, P)) = enc(K_3, P)$$

Meet-in-the-middle attack Hypothesis:

- n-bit key;
- known P and C such that $C = enc(K_2, enc(K_1, P))$;

Note:

- $\exists M$ such that $M = enc(K_1, P)$ and $C = enc(K_2, M)$;

Actions:

- compute 2^n for $X_i = enc(K_i, P)$;
- compute 2^n for $Y_j = dec(K_j, C)$;
- if X_i and Y_j are matched then K_i and K_j are found;
- false positives can be discarded with other (P, C) couples;

Application of block algorithms How a block algorithm is applied to a data quantity different from the alogorithm's block size?

- ECB (Electronic Code Book): if we have to encrypt some data, we simply split the data in equal size blocks and encrypt every block with the same key, this is very insecure, for example an attcker could swap two ciphertext, also if there is a known plaintex the attacker could find the matching key and then decrypt all the ciphertext;
- CBC (Cipher Block Chaining): we also split the data, we take every blcock, and before ecrypting the the block we xor it with the previous encrypted block, for the initial block we use a IV (Initialization Vector, C_0), for this reason the first block is the most vulnerable. In decryption to recover the plain text, the decrypted block will need to be xor-ed with the previous block (proprety of the xor function);

Padding with explicit lenght

- Schneier: the last byte has the value of bytes of padding, the other bytes are null;
- SSL/TLS: the bytes of padding are all at the value as the lenght of the padding;

If the data is an exact multiple of the block lenght, then the padding will have to be added in anyhow, if the that is the case the last block will be entirely of padding.

Ciphertext stealing (CTS) CTS permits to use any block algorithm without requireing any padding to be added.

CTR (Counter mode)