POLITECNICO
DI TORINO

Recap Computer System Security (02KRQOV)

Jacopo Nasi
Computer Engineer
Politecnico di Torino

I Period - 2018/2019

October 16, 2018

Contents

License

Acknowledgments

Questo breve riepilogo non ha alcuno scopo se non quello di agevolare lo studio di me stesso, se vi fosse di aiuto siete liberi di usarlo.
Le fonti su cui mi sono basato sono quelle relative al corso offerto (**Computer System Security (02KRQOV)**) dal Politecnico di Torino durante l'anno accademico 2018/2019.
Non mi assumo nessuna responsabilità in merito ad errori o qualsiasi altra cosa. Fatene buon uso!

1 Introduction Security ICT System

Why is securoty an important issue? Nowadays that everything is online and connected to a world wild network, the security over the ICT system has become fundamental. A lack of the secutiry could generate lose for milions of money. Also data breach become a problem.
Everydays technology improve and drive innovation but security must be improved together with the innovations.
With the increase of the number of connected devices, the IoT (Internet of Things), security start to facing a lot of more problem, the complexity of the scenario has become really really big. From personal devices, like desktop, laptop, fridge or car, by communications networks, and to distributed services, everything must be secured!

Complexity enemy of security based on one of the first axiom of engineering: *"The more complex a syste, is, the more difficult its correctness verification will be."*. Keep a system as simple as possible is always a good idea. The KISS rules (***Keep It Simple, Stupid***) is one of the most important rule over the system security.

Definition of ICT Security "It is the set of products, services, organization rules and individual behaviours that protect the ICT system of a company.

It has the duty to protect the resources from undesired access, guarantee the privacy of information, ensure the service operation and availability in case of unpredictable events (C.I.A. = Confidentiality, Integrity, Availability).

The objective is to guard the information with the same professionalism and attention as for the jewels and deposit certificates stored in a bank caveau.

The ICT system is the safe of our most valuable information; ICT security is the equivalent of the locks, combinations and keys required to protect it."
— **Italian Bank**

An important part of the security study is the Risk Estimation, is a fundamental step that take in account all the assets and events to evaluate the risk of something. The flow is showed in figure 1:
Where the assets is composed by everythings needed by a service to work, both soft and hard part, also human resources. The vulnerabilities, intrinsic of an asset, represent the weakness of it. The threats is a deliberate action, or an accidental event, that can produce the loss of a security properties exploting a vulnerability. The event is also characterized by an impact and a probability

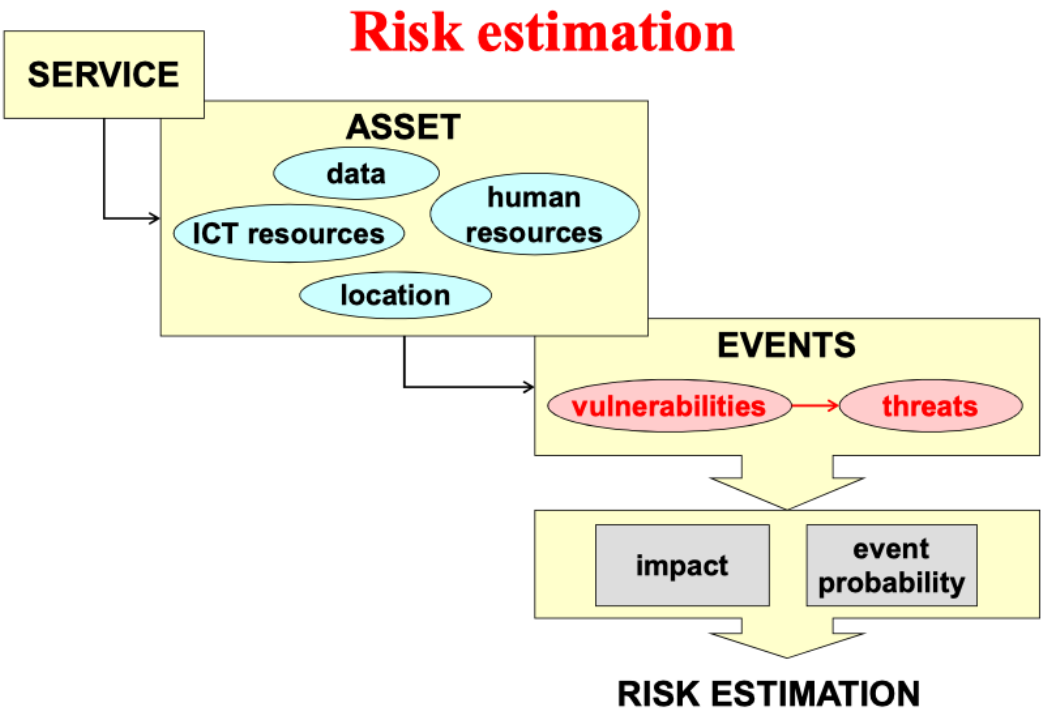

Figure 1: Risk Estimation

that could be high, low or other middle values.
Direct following of the risk estimation is the Analysis and management of security. After the evaluation of risks, is necessary to:

1. Select Countermeasures
2. Implement Countermeasures
3. Audit (check if works)

The security implement is not a phase of the developmente process, is part of each sigle part of it. Security can't be compute at the end of the development, it must be implement from the beginning of the process. **Security is a process, not a product!** The following figure 2 show the parallel line followed by the security development.

An important definition, before speaking about security itself, is the **Window of Exposure** the represent the time when an attack could be perfomed and there are no countermeasures to avoid it. This window could potentially be infinite and this is the real problem. The figure 3 show how this windows id divided in different part:

As already says, security is not a product but is a proccess. Computer flaws are inevitable and this is way we can't use devote our security to only secured products. The only way to effectively do business is an insecure world is to put processes in place that recognize the inheritent insecurity in the products. **The**

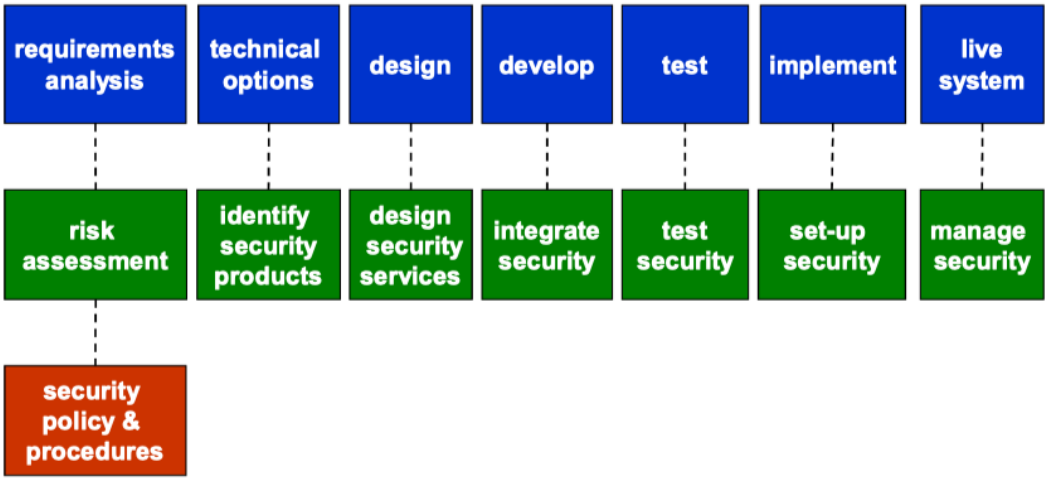

Figure 2: Security Life Cycle

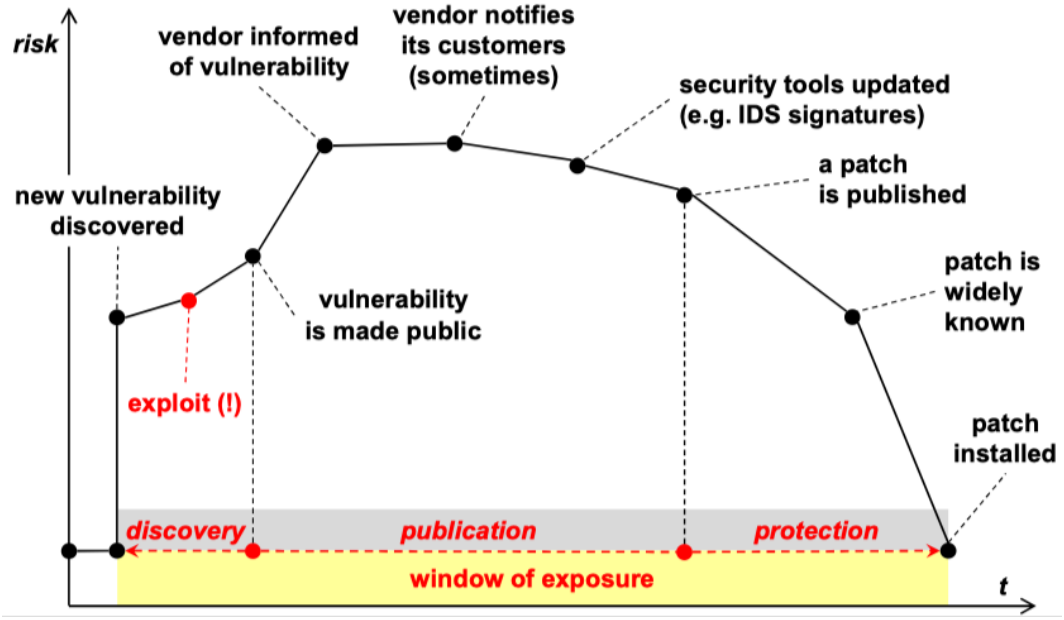

Figure 3: Window of Exposure

trick is to reduce your risk of exposure regardless of the products or patches.

Security Principles Here some of the most important security principles:

- Security by Design
- Least Privilege: Only correct rights and the only few needed
- Need-to-know: Access to the only piece of stuff that are needed

- Security by Default
- Security in Depth: More the importance of the system, more the obstacles

Security Properties The following list show the most importante properties of the security world:

- Authentication (Simple/Mutual): Source (or both) must prove themself
- Data Origin/Authentication
- Authorization and Access Control
- Confidentiality/Privacy/Secrecy
- Non Repudiation: Formal proof, acceptable by a court of justice, that gives undeniable evidence of the data creator
- Availability
- Accountability
- Integrity: Modification, Filtering

Where is the enemy? The enemy normally is supposed to be outside of our system but is not simple as it seems. The possible locations are:

- Outside our organization (Firewall)
- Outside our organization, with exceptionn of our parters (VPN)
- Inside our organitazion
- Everywhere!

The last item is probably the more true. The distinction between internal/external and good/bad guys is no more sufficent. From the *Verizon Data Breach Invetigation Report* the percentage of source of attacks is: 20% Internal and 80% External, probably the internal percentage is a little bit higher due to the fact that Verizon is a provider and can't show the internal side so much.

Basic Problems There are some basic problem for security:

- Networks are insecure:
  - Clear communications
  - LAN use broadcast
  - Not E2E geographical connections

- Weak user Authentication
- No server Authentication
- **Software with bugs!**

Classes of Attacks Some of the most common type of attacks:

- IP Spoofing / Shadow Server
- Packet Sniffing
- Connection Hijacking / Data Spoofing
- Denial-of-Service (Distributed DoS)

The **IP Spoofig**, or source address spoofing, is forginng the sourcce network address, typically performed at LV3 (IP), but also at LV2 can be performed. The typical attacks are: Data Forging and unauthorized access to systems.
The **Packet Spoofing** it reads the packet addresses to another network node, it easy to do in LAN or at the switching nodes. It allows to intercept password, data and other stuffs.
The **Denial-of-Service (DoS)** it keeps a host busy so that it can't provide its services. There are a lots of examples: mail/log saturation, ping flooding, SYN attacks. The main problem of this kind of attacks is that there are no countermeasures. The **Distributed DoS** are similar to the previous one but perfomed by a greater number of hosts (botnet), controlled by a master. The power is the same of a normal DoS multiplied by the number of deamons of the botnet. There are also some techniques to improve the attack like using a reflector to hide the attacker's track. One of the more important DDoS was performed agains Yahoo! during Feb 2000.
The **Shadow Server** is a technique that host that manage the attacks show itself (to victims) as a service provider without having the right to do so. It provide a "wrong" serice to victims, like bank sites or other stuffs.
Connection Hijacking / MITM, AKA Data Spoofing, is performed when attacker takes control of a communicatio channel to insert, delete, or manipulate traffics. It can edit data is all forms, and change the messages of the communications. Another similar for is the **Trojan / MITB**, it used the fact that network channels are more protected, but users terminals not. The behaviour is to install a keylogger to store everything. It could be also passed via browser extension.
The are other application-leve problems:

- Buffer Overflow
- Cookies
- Clear password in DB

- "invent" a protection system

We make now some clearance about name of malwares:

- Virus: Damage the target and replicate itself, propagated by humans (require complicity)
- Worm: Damage target because replications (resource saturation)
- Trojan: Malware vector
- Backdoor: Unauthorized access point
- Rootkit: Privileged access tools, hidden and stealth
- Ransomware: Make hosts unreadable (can be also silent)

Non technological problems Prorably the greatest majority of the problems and leaks come from here! The are some basic problems: due to low awareness, mistakes, tendency to trust and other facts the major cause of leaks are humans.
The **Social Engineering** are sets of techniques used to asks the involutary user's partecipatio to the attack action, usually the naïve users are targeted (e.g. *"do change immediately your password with the following one, because your PC is under attack"*), also experienced users are targeted (e.g. by copying an authentic mail but changing its attachment or URL).
One of the most used technique is the **Phishing** (fishing) where the attacker try to stole information (fishing) from the target (fish), it can be achieved, for example, by showing acquaintance with the company's procedures, habits and personnel helps in gaining trust and make the target lower his defences. Is often performed by using fake mail, SMS or IM. The normal procedures works by attarcting the fish in a shadow server where it will leave of the sensitive informations or persuade to install plugins or other stuffs. Two variants exist, **spear phishing** (include several personal data to disguise the fake message as a good one, e.g. mail address, name of Dept/Office, phone no.) or **whailing** (targeted to VIP such as CEO or CIO). The **Pharming** is a set of several techniques to re-direct a user towards a shadow server, chaging the hosts file, nameserver, poisoning cache of DNS. Some important examples of this techniques are T.J.Maxx attack, Transformed3 phishing or Stuxnet.
The typical path of attackers is showed in figure 4.

From this brief introduction we can define he three pillars of security:

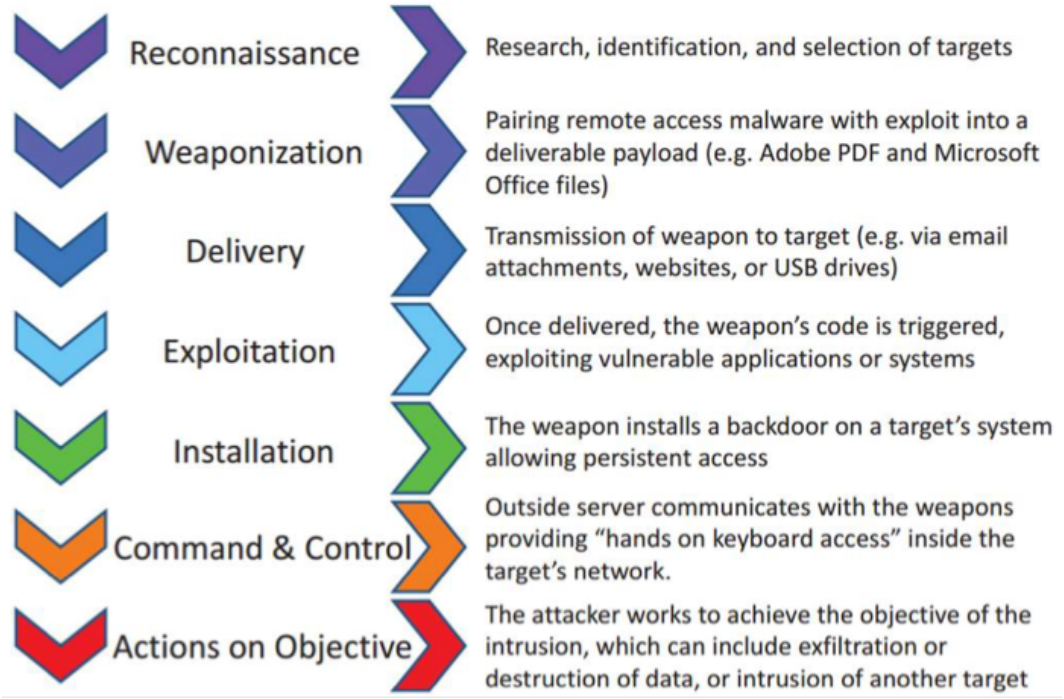

Figure 4: Cyber (intrusion) Kill Chain

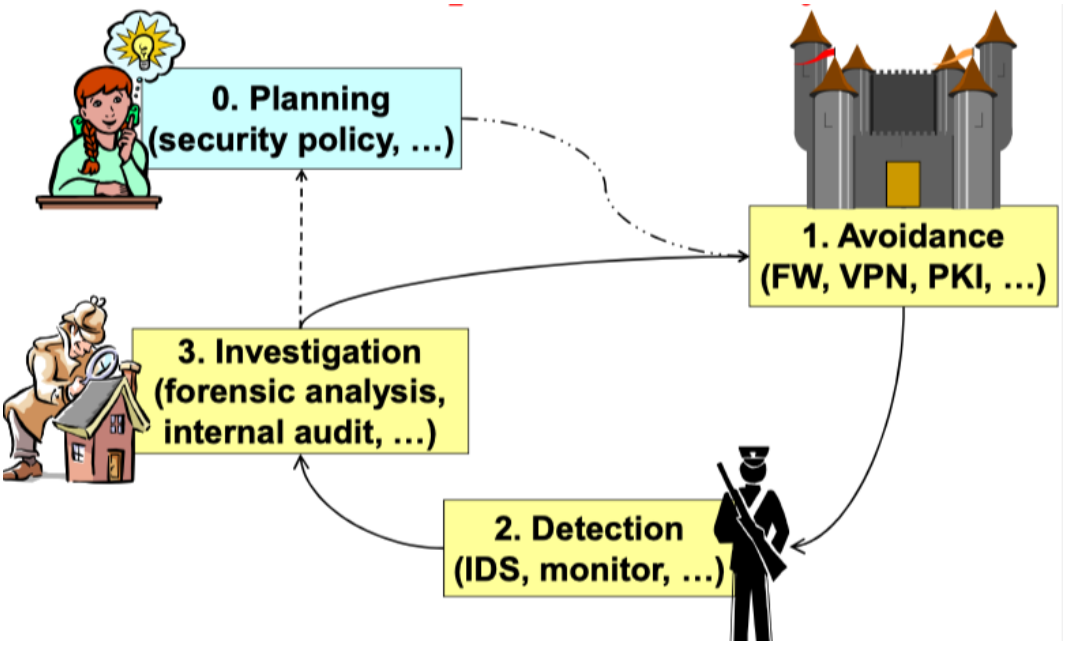

Figure 5: Pillars of Security

and we can define the main figures:

- Hacker: Good and skilled
- Cracker: Bad but skilled

- Script Kiddie: Bad but NOT skilled
- Wannabe Lamer: Not good at all

2 Basic of ICT security

2.1 Cryptography Introduction

The basic principles of Cryptography are showed in the following figure

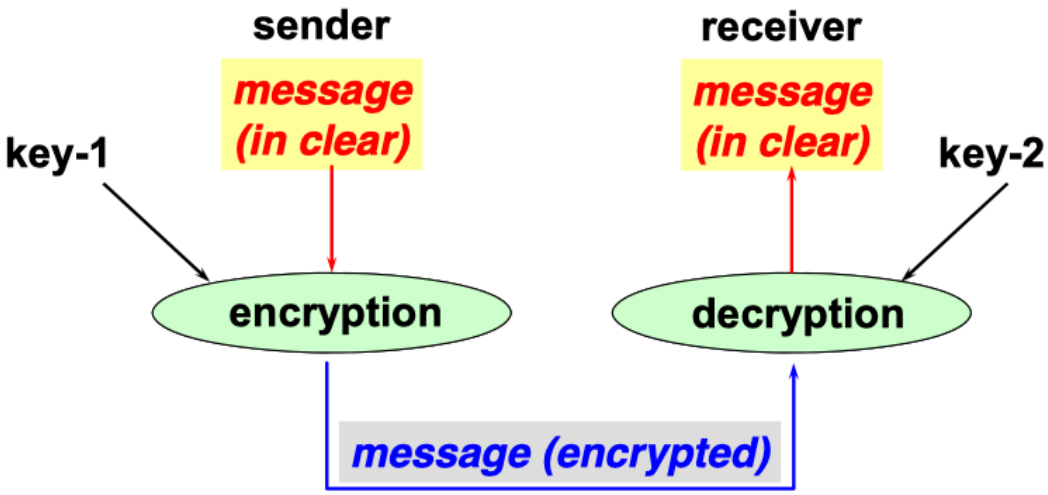

Figure 6: Cryptography flow

Some important terminology. The message in clear is called:

- Cleartext or plaintext
- Refer with **P**

Instead the encrypted message:

- Ciphertext
- Refer with **C**

Some principles of Cryptography, written by Kerchoffs, are: If the keys:

- Are kept secret
- Are managed only by trusted systems
- Are of adeguate lenght

then...

- it has no importance that the ecryption and decryption algorithms are kept secret
- on the contrary it is better to make the algorithms public so that they can be widely analysed and their possible weaknesses identified

In computer system STO (Security Through Obscurity) is not good.
An important operator of this world is the XOR function that is the ideal confusion operator, because it not change the probability. Is also a primitive operation present in all CPUs.

2.2 Symmetric Cryptography

Are all the algorithms based on a secret key shared between sender and receiver, used for encrypt and decrypt. Figure 7 show the general flow of this kind of algorithms. The advantage are low computational cost, in fact is used for data encryption.

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

One of the main problem is *"How to share (securely) the secret key among sender and receiver?"*. T

Figure 7: Symmetric General flow

There is not a confirmation of correct decryption, is up to the user to understand if the result is correct or not, in any case a result is provided with any key.

DES (Data Encryption Standard) one of the first used by US government. Is now obsolete, is based on a key of 64 bits, composed by:

- Key: 56 bits
- Parity: 8 bits

This means that the actual bit of resistence is 56. It's based on 64 bits of data blocks. It is also designed to be efficent in hardware with poor performance, the flow is:

1. XOR
2. Shift
3. Permutation (not so good performance)

3DES is the triple repeted application of DES, it used two of three 56 bits keys. Is different from passe to a keys long 56*3 because the key lenght will not match with that number of bits. It can be computed in two ways:

- 2 Keys: $C = enc(K_1, dec(K_2, enc(K_1, P)))$
- 3 Keys: $C = enc(K_3, dec(K_2, enc(K_1, P)))$

The central step of decryption is made to generated mess.
An important issue of the encryption is the doubling of an algorithms. Double application of encryption algorithms is subject to a know-plaintext attack named **meet-in-the-middle** which allows to decrypt data with at most 2^N+1 attempts (if the keys are N-bits long). Thus the double version is never used, it double the computation time and increase they key lenght of only one bit. The formulas are:

$$C = enc(K2, enc(K1, P))$$

$$dec(C, K2) = dec(K2, enc(K2, enc(K1, P)))$$

$$dec(C, K2) = enc(K1, P)$$

The attacker can compute ENC(K1, P) for all values of K1 and DEC(K2, C) for all possible values of K2, and add only 1 bit of strenght for 2 keys of the same size.

IDEA