POLITECNICO
DI TORINO

Recap Computer System Security (02KRQOV)

Jacopo Nasi
Computer Engineer
Politecnico di Torino

I Period - 2018/2019

October 8, 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

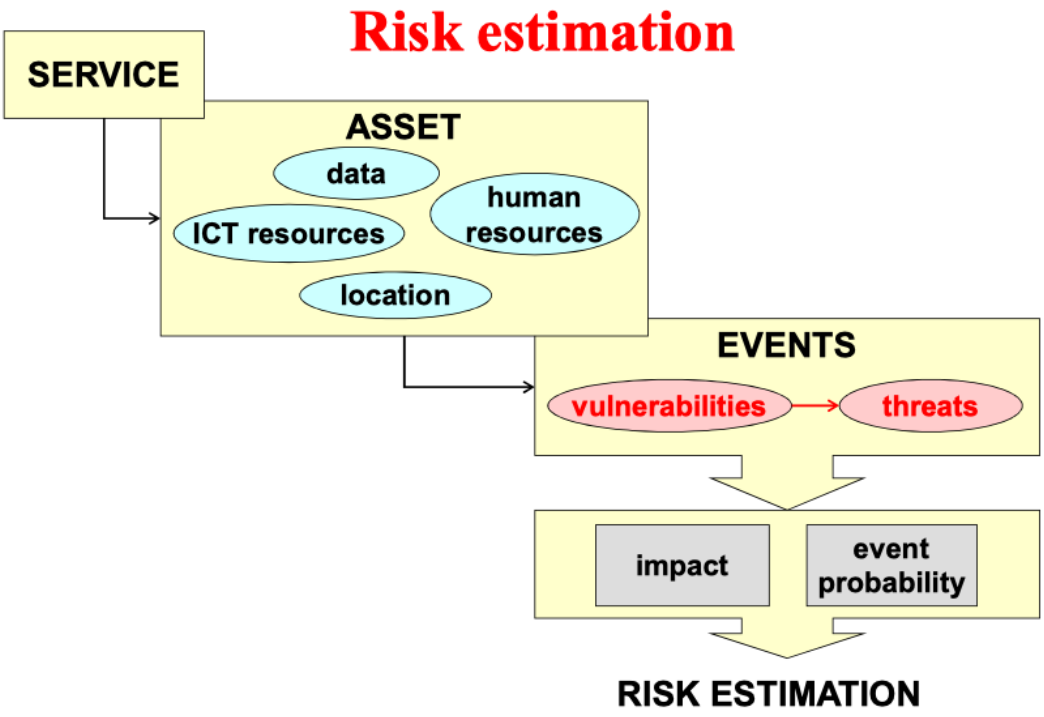

Figure 1: Risk Estimation

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**

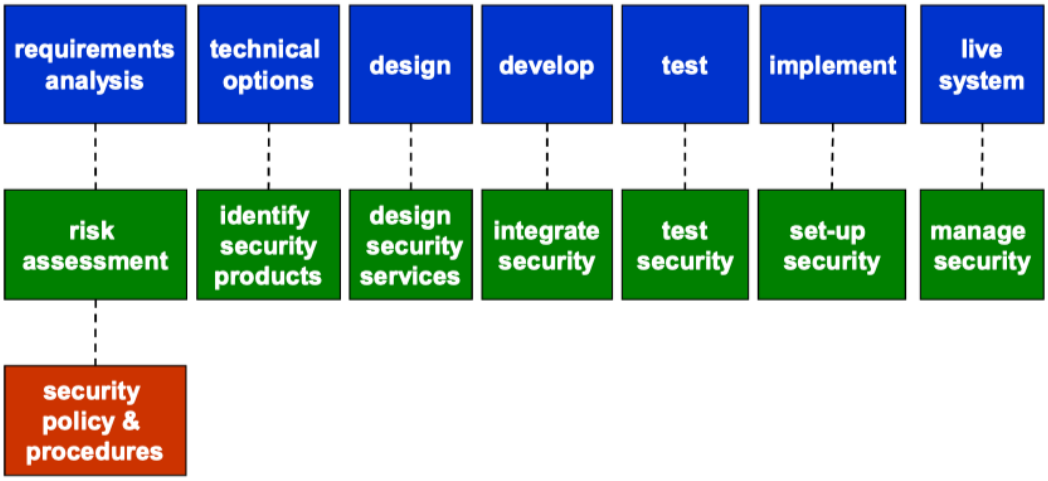

Figure 2: Security Life Cycle

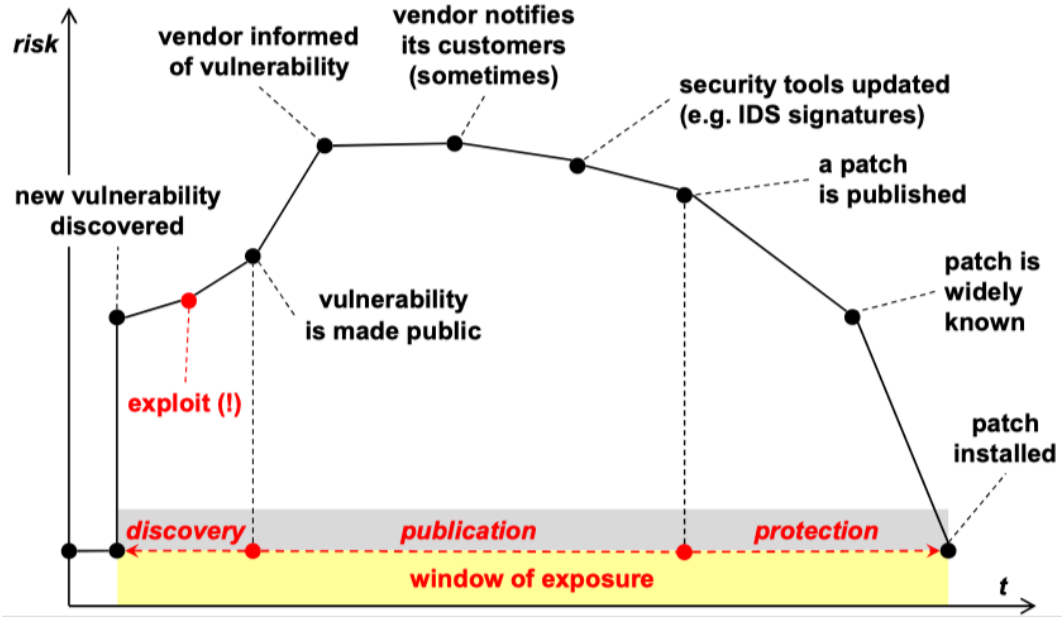

Figure 3: Window of Exposure

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