Intersem – INF114

Cybersecurity Basics

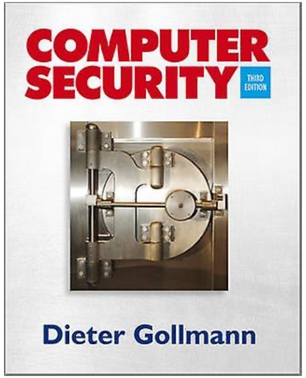
Jean Leneutre
Telecom Paris, LTCI, INFRES/ACES
jean.leneutre@telecom-paris.fr
01 75 31 97 78

Course outline

- Content
  - Context & Definitions
  - Security Properties
  - Security Risk Management Concepts
  - Main Security Functions
  - Some Security Standards

To Go Furthers

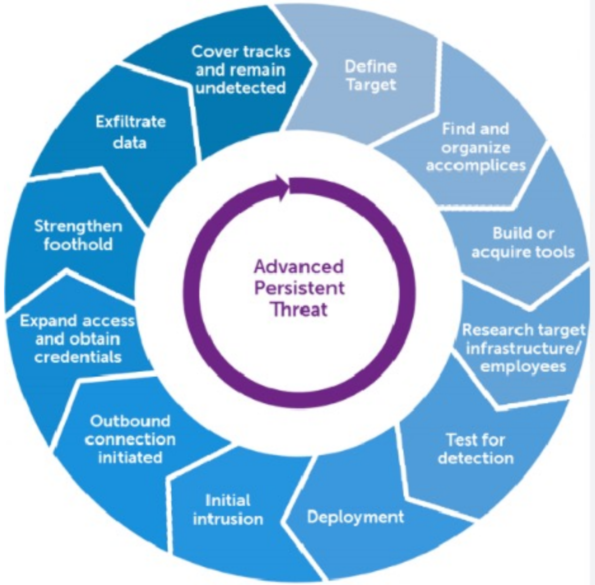
- Reference textbook :
  - Dieter Gollmann, *Computer Security*, John-Wiley, 3rd edition 2013.
  - Stallings and Brown, Computer Security: Principles and Practice (2014, 3/e; Prentice Hall).



Context & Definitions

Context & Definitions

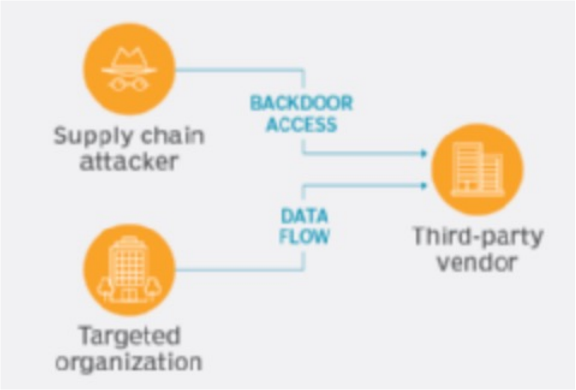
- New trends in an ever evolving cyberthreats landscape (1)
  - *Advanced Persistent Threats (APTs)*
    - — *Complex and stealthy attack with a long life cycle*
    - — *Origin of the attack: a state or a state sponsored group*
    - — *Motivation: economic or political*
    - — *Impact: loss of digital sovereignty*
    - — *Examples: Operation Aurora targeting targeting several companies such as Google (2009), Stuxnet targeting Iran's nuclear program (2010)*


Advanced Persistent Threat
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

https://en.wikipedia.org/wiki/Advanced_persistent_threat

Context & Definitions

- New trends in an evolving cyberthreats landscape (2)
  - *Supply chain attacks*
    - *Exploit vulnerability in the supply chain*
    - *Target a hardware or software component provided by a third party during its manufacturing or distributing phase*
    - *Example: United States federal government data breach (2020)*
      - *Third party attacked: IT Infrastructure company Solar Wind (Orion software monitoring Windows hosts)*
      - *Impact: confidential data leaks*
      - *200 US federal institutions impacted and 18000 non federal customers*



Context & Definitions

- New Trends in an ever evolving cyberthreats landscape (3)
  - *AI-based and Generative AI-based attacks*
    - *Attacks using AI techniques such as machine learning to improve their efficiency*
    - *Examples*
      - *PassGAN: A password guesser tool based on Generative Adversarial Networks (GAN)*
      - *DeepLocker: highly evasive malware using videoconference systems to identify a specific target using Deep Neural Networks (DNN)*
  - *Attacks targeting AI-based cyber mechanisms*
    - *Attacks specifically targeting automatic decision-making mechanisms based on machine learning techniques*
    - *Example*
      - *MalGAN: tool that bypasses intrusion detection systems based on machine learning, by submitting to the detection model, slightly modified data (called adversarial examples) so that they are misclassified and not detected as attacks*

Context & Definitions

- New Trends in an ever evolving cyberthreats landscape (4)
  - *Rise of Quantum Computing in a near future?*
    - *Impact on classical cryptographic algorithms*
    - *Example: RSA asymmetric algorithm*
    - *Shor’s algorithm in quantum computing model: can factor large numbers exponentially faster than classical algorithms*
    - *Need for post-quantum cryptographic algorithms*

IBM Quantum SystemOne

Context & Definitions

Cybersecurity

- Implicitly security of information or functions processing information in cybersystems
  - System and software security: security of information processed by a system or a software
  - Network security: security of information transiting in a network
  - Hardware security: security of information processed by a hardware

- Information (or Information System) security vs. Cybersecurity
  - An Information System is the set of entities that store, process, manage, and distribute information in an organization
  - Entities = humans, data, hardware, software, …
  - Information security encompasses Cybersecurity and includes also for instance Physical Security (control of physical access to buildings)

Context & Definitions

- Usual definition of Cybersecurity(as a specific case of Information Security)
  - Information Security = set of properties about information including at least
    - ***Confidentiality***: no non-authorized *observation* or *divulgation* of information
    - ***Integrity***: no non-authorized *modification or alteration* of information
    - ***Availability:*** no non-authorized *retention* of information or function processing information
  - Some other properties depending on the context
    - ***Accountability***: to be able to determine who is responsible for any action affecting security
    - ***Non repudiation***: unforgeable evidence that a specific action occurred
    - ***Anonymity***, ***Unlinkability***, ***Differential Privacy***, *…: properties defined in the context of data security and privacy*
    - ***Non-interference***, ***Non-deducibility***, …: formal properties defined in the context of information flow control

Context & Definions

- An alternative definition (as a specific case of Information Security)
  - Operational definition of security
    - Information security deals with the prevention, detection, mitigation (correction), and recovery of unauthorized actions by users
    - Unauthorized actions cover both intentional actions (attacks) and non-intentional actions (errors)
  - Assumes the existence of a *security policy* defining what are the authorized actions
    - *Security Policy*: A specification that defines the *security objectives* of an organization; it has to state what needs to be protected; it may also indicate how this is to be done.
    - *Security Objectives*: A statement of intent to protect an identified resource from unauthorized use.
    - *Organizational security policy*: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes resources to achieve specified security policy objectives.
    - *Technical security policy*: The set of restrictions and properties that specify how a computing system prevents information and computing resources from being used to violate an organizational security policy.
    - A technical security policy defines access control lists and firewall settings, … etc.

Context & Definitions

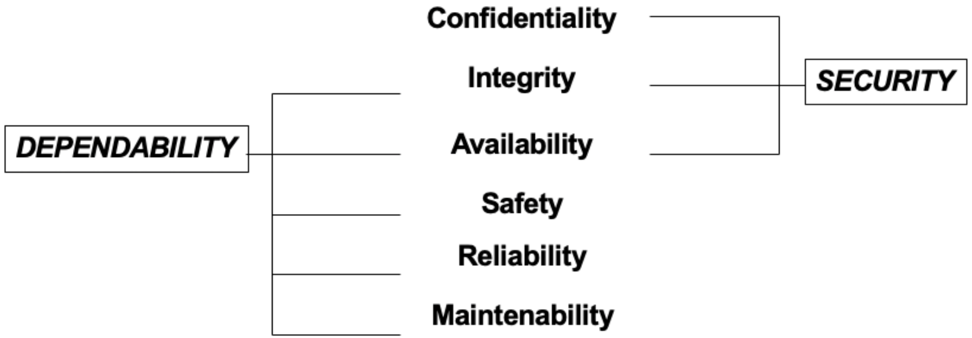
- Security objective (or requirement or need)
  - A statement linking a given information and a security property with some attributes
    - Examples
      - Confidentiality of the new commercial strategy plan of a company between the director & the deputy directors
      - Confidentiality of a password between a client and a server
      - Availability of a given information takes less than one second
    - Interdependencies between security objectives
      - Mutual exclusion
        - Example: a strong confidentiality objective on a given information may require the systematic use of robust cryptographic mechanisms that may impact availability objective
      - Causality relation
        - Example: the confidentiality objective on a given information may be enforced by encrypting all the files containing this information using a cryptographic key, based on the assumption that this cryptographic key is also confidential

Context & Definitions

- Security vs Safety
  - Security
    - Protect information (of functions processing information) against non authorized actions
    - Assets
      - Immaterial assets: information and function processing information
      - Material assets: concrete entities on which information are stored or managed (example a copy of a file containing information stored on a server)
  - Safety (in french « Innocuité » but sometimes translated as « Sécurité »)
    - Protect against harmful events (hazards)
    - Assets:
      - Security of humans
      - Tangible possessions

Context & Definitions

- Security vs. Dependability
  - Dependability (translated in French as « Sûreté de fonctionnement »)
    - Dependability of a computing system is the ability to deliver service that can justifiably be trusted
    - Dependability = integrity + availability + safety + reliability + maintenability



Picture from [Avizienis & alii, 2004]

- Dependability is usually assessed both through formal approach (based on verification of properties) or quantitative approach (based on metrics)

[Avizienis & alii, 2004] A. Avizienis, J. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing”, IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, 2004.

Context & Definitions

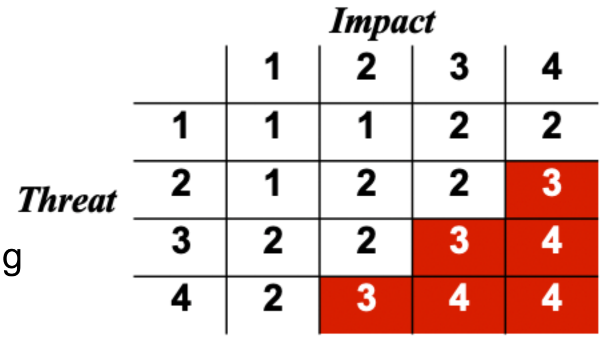
- How to assess the security of a system?
  - Formal approach
    - Example: verification of authentication protocol
    - Used in the context of certification for small system (Common Criteria*)
  - Quantitative approach
    - Derive the probability of a potential attack based on past experiences
    - Measure the *attack surface* of a system (number of interfaces, number of dangerous instructions used in a code, …)
    - ➢ Quantitative approaches rarely used to assess security in operational context
  - Qualitative approach
    - Security risk analysis: identify and assess security risks that threat assets and impact the system
    - Process based on human expertise
    - Risk Management method: EBIOS (ANSSI), MEHARI (CLUSIF), …

* https://www.ssi.gouv.fr/administration/produits-certifies/cc/

Context & Definitions

- What is a security risk?
  - Several definition depending on the risk management method
  - But generally: a risk is a couple made of a threat scenario (a potential attack or undesired event) and an impact (the consequence of the threat)
  - The threat scenario is characterized by the likelihood (L) that the attack will materialize/succeed
  - The impact is characterized by its severity (S) in term financial loss, level of damage,…
  - The risk level R is a function of L and S

  - Example: given 4 levels for L and 4 levels for I, the following matrix computes R
  - Risk treatment
    - Removing, reducing, transferring or taking the risk
    - Residual risk: risk still existing after the risk processing



		Impact			
		1	2	3	4
Threat	1	1	1	2	2
	2	1	2	2	3
	3	2	2	3	4
	4	2	3	4	4

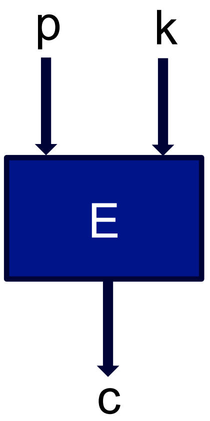
Security Properties

Security Properties: Focus on Confidentiality

- Usual informal definition used in cybersecurity
  - No non-authorized divulgation of information
    - May be applied not only to its content but also to its existence
  - Only authorized entities are able to observe a given information
    - Must be specified in the security policy
  - Examples of access operations that must be controlled
    - Read access to a file in an OS, listing the content of a repertory, read access to a database, …
  - Security mechanisms providing confidentiality
    - Encryption of a file using a cryptosystem, access control to a file system based on ACL (access control list), …
  - Examples of attacks targetting confidentiality
    - Cryptanalysis of a ciphering algorithm, sniffing the trafic in a wired network, eavesdropping of wireless communication, eavesdropping computer electromagnetic radiations that leaks information on data processed (TEMPEST)
  - Privacy (« Intimité »)
    - Confidentiality of personal information

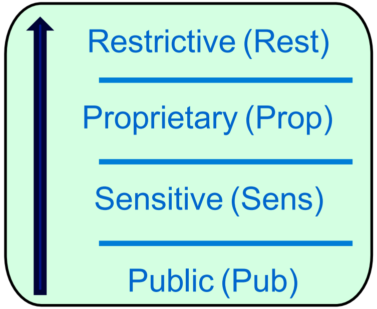
Security Properties: Focus on Confidentiality

- *Perfect Secrecy (Unconditional secrecy)*
  - Formal definition from Information theory used in cryptography
  - Consider a cryptographic algorithm E that given a secret k uniformly random (cryptographic key), transform a clear message p (plaintext) into an encrypted message c (cipher)
  - Intuitively perfect secrecy holds when ciphertext c gives absolutely no additional information about p (except its maximum possible length)
  - If k is unifomly random, for an attacker observing only a ciphertext c, all possible values of plaintext are equally likely
  - Example: Vernam Cipher (One Time Pad), a new key has to be generated for each encryption … (see course on cryptography)



Security Properties: Focus on Confidentiality

- Confidentiality in a Multi-Level Security (MLS) setting (1)
  - Used by some operating systems
  - Assign confidentiality labels to information (confidentiality classification)
  - The order between the labels maybe total or partial
  - Example of confidentiality labels with total order (Rest>Prop>Sens>Pub)



Restrictive (Rest)

Proprietary (Prop)

Sensitive (Sens)

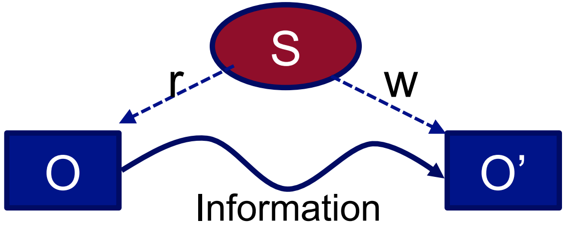
Public (Pub)

Label	Meaning
Rest	Information must be accessible only to identified persons from the staff on a need-to-know basis
Prop	Information must be accessible only to the (internal) staff involved
Sens	Information must be accessible only to staff and partners
Pub	Information is public

— Confidentiality defined as a requirement on *Information Flow*

Security Properties: Focus on Confidentiality

- Confidentiality in a Multi-Level Security (MLS) setting (2)
  - Information flow
    - Object: material assets (a file containing information under protection)
    - There is an information flow from an object o to an object o’, if when observing information related to o’, it is possible to learn information about o.
    - Examples: an active entity *s* (for instance a process) can read object *o* and can write to object *o’*.



    - Exemple: Information flow from variable *h* to *l*:

```
var l, h
l := h
```

Security Properties: Focus on Confidentiality

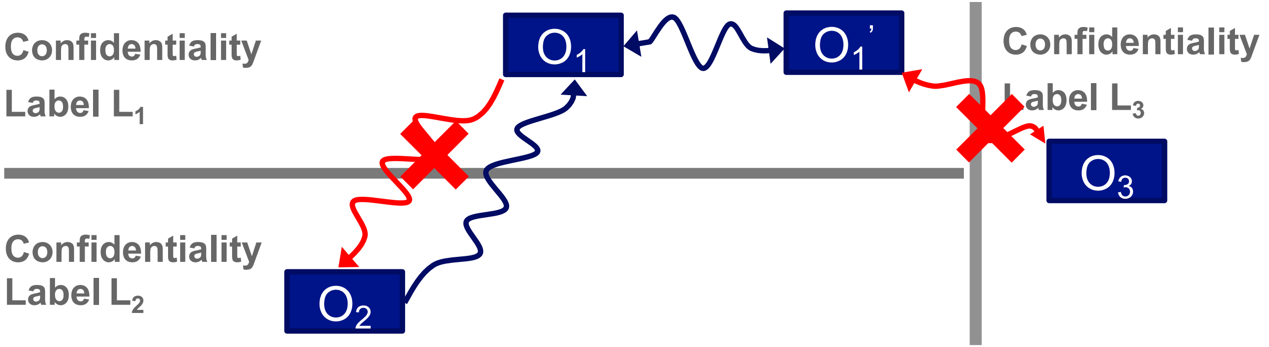
- Confidentiality in a Multi-Level Security (MLS) setting (3)
  - Bell Lapadula model (BLP)
    - No information leaks from a higher label to a lower label
    - An information flow is authorized from an object o to an object o’ iff l(o)≥l’(o) (where l(o) and l(o’) denote resp. the labels of o and o’)

$L_1 > L_2$

L_1 n.c. L_3

L_2 n.c. L_3

(n.c. means non comparable)



    - Example: BLP policies in Security-Enhanced Linux (SELinux)

Security Properties: Focus on Confidentiality

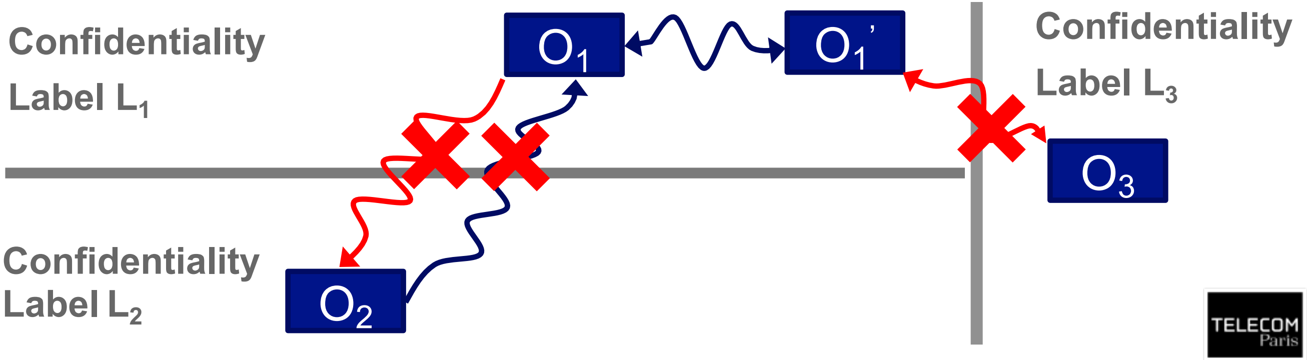
- Confidentiality in a Multi-Level Security (MLS) setting (4)
  - Multiple Independent Levels of Security (MILS)
    - Strict separation model: information flows stay internal to a label
    - An information flow is authorized from an object o to an object o' iff l(o)=l'(o')

$L_1 > L_2$

L_1 n.c. L_3

L_2 n.c. L_3

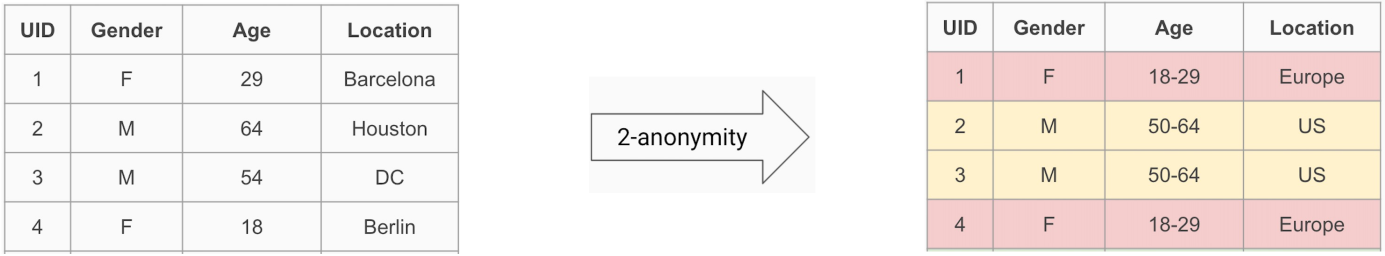
(n.c. means non comparable)


Confidentiality Label L_1
O_1
O_1'
Confidentiality Label L_3
O_3
Confidentiality Label L_2
O_2

Security Properties: Focus on Confidentiality

Privacy properties

- **Anonymity**: the state of being not identifiable within a set of subjects, the anonymity set
  - Example: anonymity of a sender of a message
  - Anonymity in databases
    - K-anonymity: the information for each person contained in a release of a dataset cannot be distinguished from at least k-1 individuals whose information also appear in the release



UID	Gender	Age	Location
1	F	29	Barcelona
2	M	64	Houston
3	M	54	DC
4	F	18	Berlin

2-anonymity

UID	Gender	Age	Location
1	F	18-29	Europe
2	M	50-64	US
3	M	50-64	US
4	F	18-29	Europe

- Other measures for anonymity in databases: L-diversity, T-closeness

Security Properties: Focus on Confidentiality

- Privacy properties
  - **Pseudonymity:** The use of pseudonyms (alias) as identifiers to hide the true identity
    - However an attacker may know that several actions have been performed by the same pseudonyms
  - **Unlinkability**: Incapability of stating the relation between two observed events in the system
    - Example: an attacker cannot know whether two given messages have been sent by the same subject
  - **Differential Privacy**: Mathematical guarantee that individual-level information about participants in a database is not leaked.
    - Consider an algorithm that analyzes a dataset and computes statistics about it
    - This algorithm is differentially private if by looking at the output, one cannot tell whether any individual's data was included in the original dataset or not
    - Anything the algorithm might output on a database containing some individual's information is almost as likely to have come from a database without that individual's information
    - Example: Apple iOS 10, Intelligent personal assistant technology (2016)

Security Properties: Focus on Integrity

- Usual definition of integrity:
  - No non-authorized modification of information,
  - Only authorized entities are able to **modify** a given information
  - Examples of access operations that must be controlled
    - Write access to a file in an OS, deleting the content of a repertory, write access to a database, …
  - Security mechanisms providing integrity
    - Access control, detection of loss of integrity based on cryptographic mechanisms using hash functions
  - Examples of attacks targetting integrity
    - Insertion of virus modifying the code of a program, Domain Name Server (DNS) spoofing (also known as DNS cache spoofing)
  - Different meaning depending of the context
    - No modification: integrity of communication(detection & correction of modifications due to transmission errors or intentional manipulation)
    - Modifications must satisfy some properties: integrity of relations in a database (consistency), integrity of a variable in a program
    - Modifications must only be performed by trusted entities (human, process)

Security Properties: Focus on Integrity

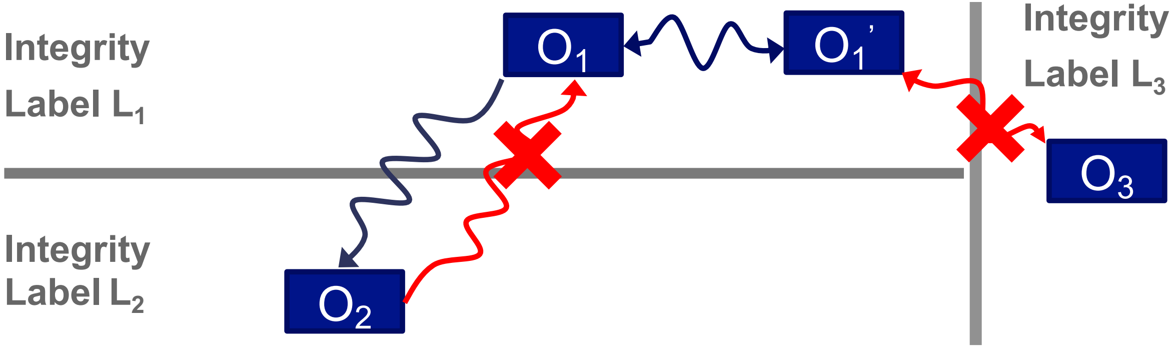
- Integrity in multi-level security :
  - BIBA Model
    - No information leaks from a lower label to a higher label
    - An information flow is authorized from an object o to an object o’ iff I(o)≥I’(o) (where I(o) and I(o’) denote resp. the labels of o and o’)

$L_1 > L_2$

L_1 n.c. L_3

L_2 n.c. L_3

(n.c. means non comparable)



Security Properties: Focus on Availability

Availability

- No retention of information or functions processing information
  - *Authorized entities can* ***use or execute*** *functions processing information and* ***obtain*** *information when it is needed*
  - Examples of access operations
    - Execution of a program in the cloud, execution of the services provided by a network, downloading a file from a server…
  - Security mechanisms providing availability
    - Redundancy mechanisms and load balancing in network, supervision based on Intrusion Detection System (IDS)
  - Examples of attacks targetting availability
    - *Jamming attack* in a wireless network, *Denial of Service (DoS)* caused by a flooding attack on a server, …
  - Several levels of requirements depending of the context
    - Presence of information or usability of services
    - Ability to answer to a request
    - Ability to answer to a request in bounded time (for instance in real-time systems)
    - Fairness in resource allocation (for instance in a multi-user operating system or in a network)
  - A security property difficult to ensure !

Security Properties: Other properties

- **Accountability** (“Imputabilité”)
  - To be able to determine who is responsible for any action against the security policy
    - Requires **Auditability**: to be able to trace the events impacting security during a given period
    - Requires Identification/Authentication
  - Mechanisms providing accountability
    - Log file + integrity mechanism + authentication of users
    - Blockchain
- **Non Repudiation**
  - To be able to ensure that an entity cannot deny previous commitments or actions
    - Impossibility for an entity to deny the reception or emission of a message
    - Needs to provide an evidence that an action has been performed
      - Proof of integrity of messages + proof of origin of data + assurance of timeliness
    - May be obtained through use of digital signatures and time-stamps

Security Properties: Other Properties

- Properties defined on information flows
  - Capture both confidentiality and integrity aspects
  - **Non interference** [Goguen & Meseguer, 1982]: Enforces that an attacker should not be able to distinguish two computations from their outputs if they only vary in their secret inputs
    - Suppose we have only two labels *high* and *low*, with *high>low*
    - A variation of confidential (high) input does not cause a variation of public (low) output.
    - Let M be a memory configuration, and M_L and M_H be the projections of the memory to the low and high parts
    - Let $=_L$ be the function that compares the low parts of the memory configurations, i.e. $M =_L M'$ iff $M_L = M'_L$
    - Let $(P,M) \rightarrow^* M'$ be the execution of the program P starting with memory configuration M and terminating with the memory configuration M'
    - Non-interference for program P holds if:

$$\forall M_1\ \forall M_2\ .\ (M_1 =_L M_2 \wedge (P,M_1) \rightarrow^* M_1' \wedge (P,M_2) \rightarrow^* M_2') \Rightarrow M_1' =_L M_2'$$

[Goguen & Meseguer, 1976] J. A. Goguen and J. Meseguer, “Security policies and security models,” in Proc. IEEE Symp. on Security and Privacy, Apr. 1982, pp. 11–20.

Security Properties: Other Properties

- Properties defined on information flows
  - **Non interference** (continued)
    - Example: h (resp. l) variable with high (resp. low) label
      - h := l+4 is secure (sastifies non-interference)
      - (if l = 5 then h := h + 1 else l := l + 1) is secure because the final value of l only depends on the initial value of l
      - (if h = 3 then l := 5 else skip) is non secure because the value of depends on the value of h
    - Application to programming languages (language based security)
      - Non interference can be enforced using a type system
      - JIF: a security-typed programming language that extends Java with support for information flow control, enforced at both compile time and run (http://www.cs.cornell.edu/jif/)
  - **Non Deducibility** [Sutherland, 1986]
    - A subject can detect the activity of a subject with a higher label if she/he is unable to interpret it
    - Non-interference: a subject cannot detect the activity of a subject with a higher label.
    - Non-interference ⇒ Non-deducibility

D.Sutherland, ‘‘AModelof Information,’’ inProc.of the9thNationalComputer SecurityConference,Gaithersburg,MD.,September,1986.

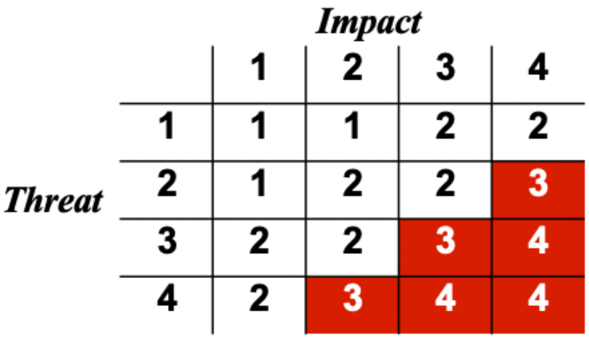
Security Properties: Other Properties

- Other dependability properties
  - **Reliability**
    - Capacity of a system to provide a correct service
    - Characterized by the probability that a component or the system works on a time interval [0,t]
    - Metrics: Mean Time Between Failures (MTBF)
  - **Maintenability**
    - Capacity of a system to work again after a fault
    - Metrics: Mean Time To Repair (MTTR)

Security Risk Management Concepts

Security Risk Management Concepts

- Reminder: What is a security risk?
  - A risk is a couple made of a threat scenario (a potential attack or undesired event) and an impact (the consequence of the threat)
  - The threat scenario is characterized by the likelihood (L) that the attack will materialize/succeed
  - The impact is characterized by its severity (S) in term financial loss, level of damage,…
  - The risk level R is a function of L and S

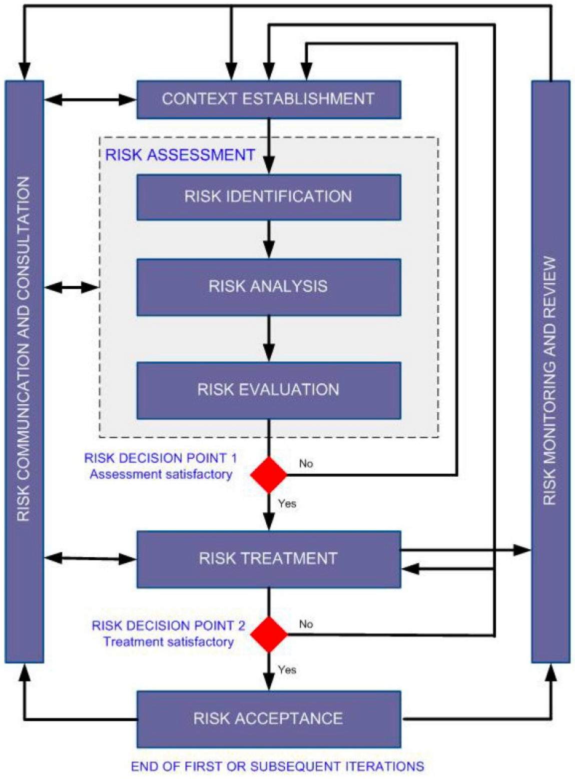


		Impact			
		1	2	3	4
Threat	1	1	1	2	2
	2	1	2	2	3
	3	2	2	3	4
	4	2	3	4	4

- Risk Management process
  - Standard: ISO 27005
  - Method: EBIOS Risk Manager (ANSSI, https://cyber.gouv.fr/en/publications/ebios-risk-manager-method)

Security Risk Management Concepts

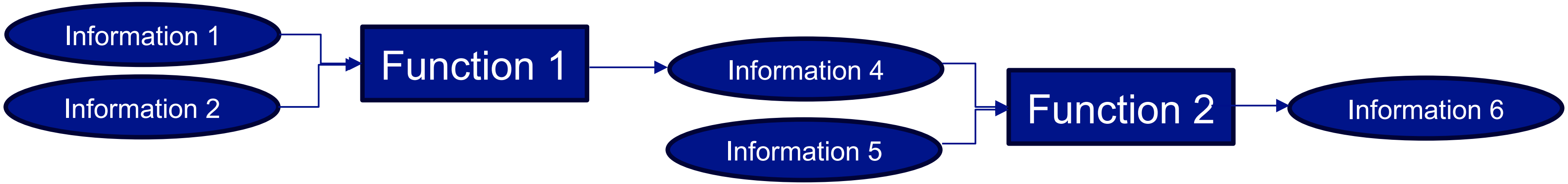
- **ISO/IEC 27005 risk management process (currently under revision)**
  - **Context establishment**: aims at collecting all the relevant information for the risk management activities, in particular the expectations of the stakeholders, and the constraints of the organization (budgetary, technical, …)
  - **Risk assessment**: decomposed into the **risk analysis** step (identification and estimation of the different components of the risk) and the **risk evaluation** that compares and prioritizes the risks;
  - **Risk treatment:** specifies for each risk an option of treatment (reduce, retain, avoid, transfer) and accordingly provides a set of security measures; the security reduction process is sometimes called ***security hardening***;
  - **Risk acceptance**: ensure that residual risks are explicitly accepted by the leaders of the organization.



Schema from [ISO/IEC27005]

Security Risk Management Concepts

- Assets identification & modelling
  - Immaterial asset (or essential asset, business assets)
    - Information that must be protected
      - Examples: list of user names, list of passwords, value of a cryptographic key, specification of a new software
    - Function processing information(service, business process)
      - Examples: function that generate passwords, ciphering algorithm, ….
    - Dependencies between immaterial assets



- Avalaibility requirement on Information 6 may be impacted if Function 2 is not available, but also if Function 1 is not available

Security Risk Management Concepts

Assets identification & modelling

- Material asset (or supporting asset)
  - Datas (files), Databases, Hardware, Sofware, Network device
  - Include also locations (server room) and humans (system administrator)
  - Attack scenarios will exploit vulnerabilities related to material asset

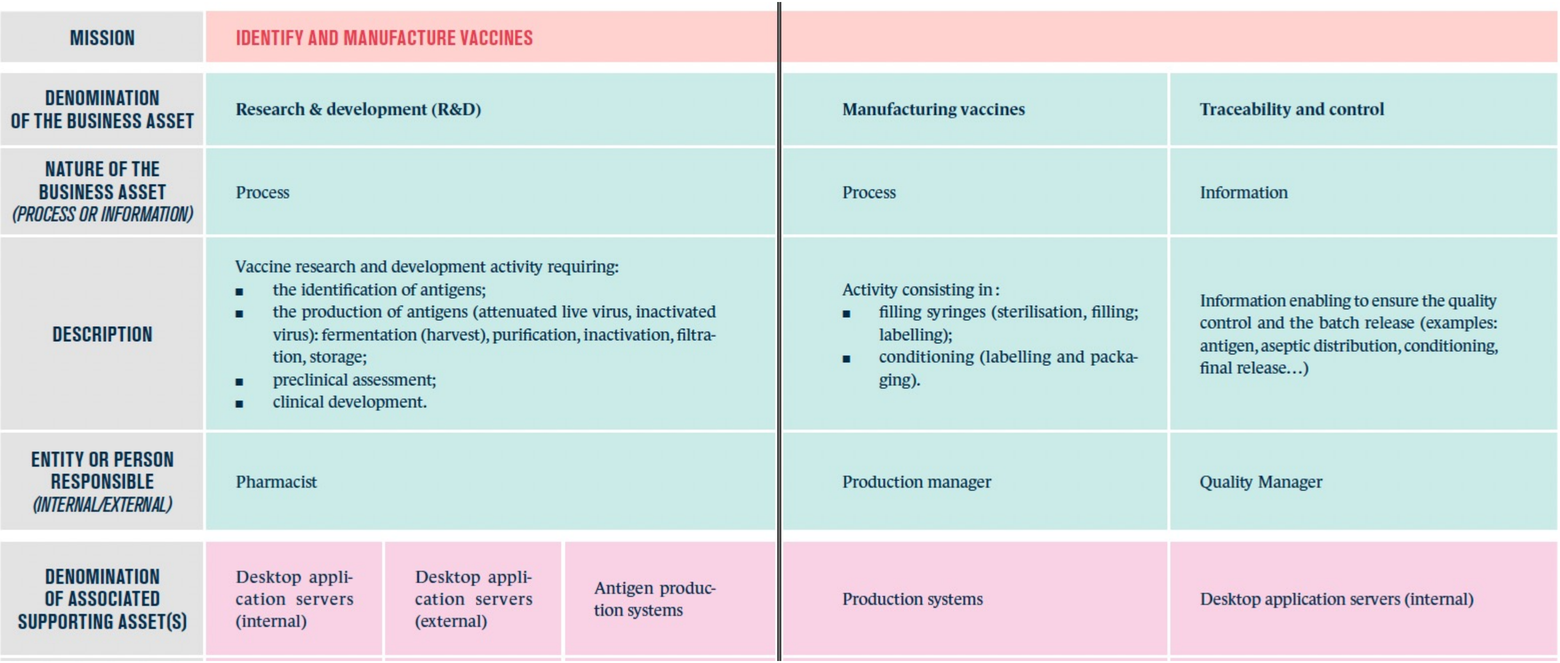
- Link between immaterial and material assets

	MA_1	MA_2	MA_3	MA_4	MA_5
IA_1	X		X	X	
IA_2	X				X
IA_3		X	X		
IA_4			X	X	X

Security Risk Management Concepts

Assets identification & modelling

- Example: Biotechnology company manufacturing vaccines (EBIOS RM Guide)



MISSION	IDENTIFY AND MANUFACTURE VACCINES				
DENOMINATION OF THE BUSINESS ASSET	Research & development (R&D)			Manufacturing vaccines	Traceability and control
NATURE OF THE BUSINESS ASSET *(PROCESS OR INFORMATION)*	Process			Process	Information
DESCRIPTION	Vaccine research and development activity requiring: ▪ the identification of antigens; ▪ the production of antigens (attenuated live virus, inactivated virus): fermentation (harvest), purification, inactivation, filtration, storage; ▪ preclinical assessment; ▪ clinical development.			Activity consisting in : ▪ filling syringes (sterilisation, filling; labelling); ▪ conditioning (labelling and packaging).	Information enabling to ensure the quality control and the batch release (examples: antigen, aseptic distribution, conditioning, final release…)
ENTITY OR PERSON RESPONSIBLE *(INTERNAL/EXTERNAL)*	Pharmacist			Production manager	Quality Manager
DENOMINATION OF ASSOCIATED SUPPORTING ASSET(S)	Desktop application servers (internal)	Desktop application servers (external)	Antigen production systems	Production systems	Desktop application servers (internal)

Security Risk Management Concepts

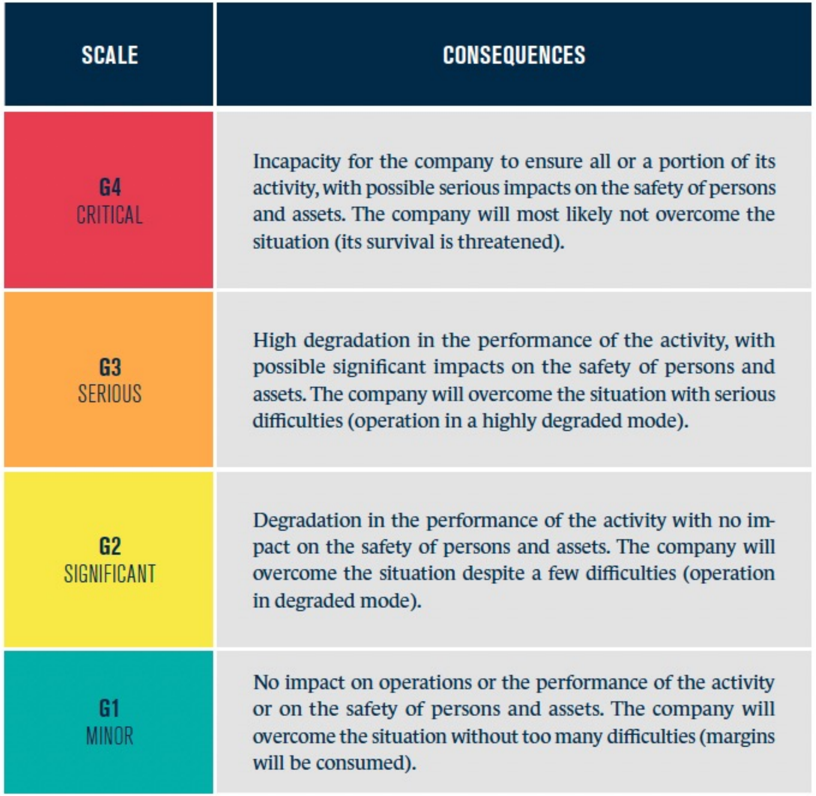
- Impact Assessment
  - Security objectives (security needs)
    - For each Immaterial Asset specify what is the need in term of security properties (CIA)
    - May use a scale for each property
    - Ex.: Immaterial entity IA_1 has a security need in term of availability of level A4, and in term of confidentiality of level C3
  - **Feared event**
    - Non availability of IA_1
    - Impact: financial cost, loss of brand image, loss of competitive advantage, …
    - Severity of impact assessed according to a scale based on business expertise

Availability level	Meaning
A1	Asset may be unavailable for more than 72 hours
A2	Asset must be available within 72 hours
A3	Asset must be available within 24 hours
A4	Asset must be available within 4 hours

Confidentiality level	Meaning
C1	Information is public
C2	Information must be accessible only to staff and partners
C3	Information must be accessible only to the (internal) staff involved
C4	Information must be accessible only to identified persons from the staff on a need-to-know basis

Security Risk Management Concepts

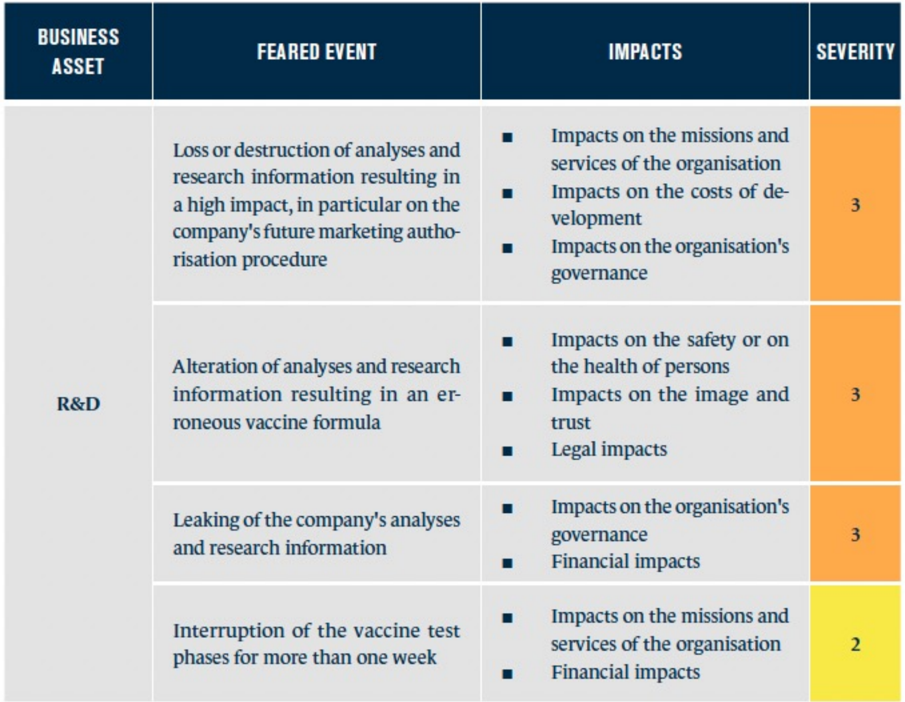
- **Impact assessment**
  - Example: Severity scale (EBIOS RM Guide)



SCALE	CONSEQUENCES
G4 CRITICAL	Incapacity for the company to ensure all or a portion of its activity, with possible serious impacts on the safety of persons and assets. The company will most likely not overcome the situation (its survival is threatened).
G3 SERIOUS	High degradation in the performance of the activity, with possible significant impacts on the safety of persons and assets. The company will overcome the situation with serious difficulties (operation in a highly degraded mode).
G2 SIGNIFICANT	Degradation in the performance of the activity with no impact on the safety of persons and assets. The company will overcome the situation despite a few difficulties (operation in degraded mode).
G1 MINOR	No impact on operations or the performance of the activity or on the safety of persons and assets. The company will overcome the situation without too many difficulties (margins will be consumed).

Security Risk Management Concepts

- Impact Assessment
  - Example: Feared events for R&D Business assets (EBIOS RM Guide)



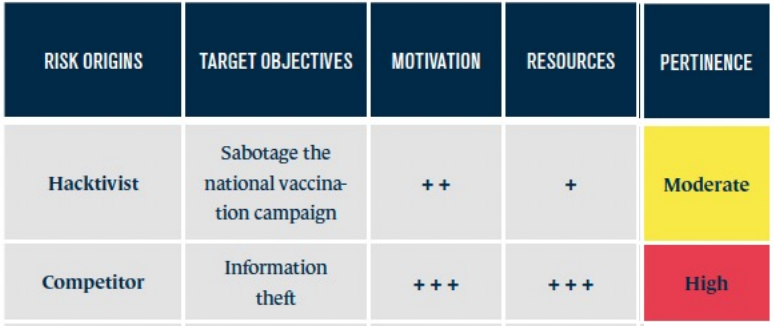
BUSINESS ASSET	FEARED EVENT	IMPACTS	SEVERITY
R&D	Loss or destruction of analyses and research information resulting in a high impact, in particular on the company's future marketing authorisation procedure	■ Impacts on the missions and services of the organisation ■ Impacts on the costs of development ■ Impacts on the organisation's governance	3
	Alteration of analyses and research information resulting in an erroneous vaccine formula	■ Impacts on the safety or on the health of persons ■ Impacts on the image and trust ■ Legal impacts	3
	Leaking of the company's analyses and research information	■ Impacts on the organisation's governance ■ Financial impacts	3
	Interruption of the vaccine test phases for more than one week	■ Impacts on the missions and services of the organisation ■ Financial impacts	2

Security Risk Management Concepts

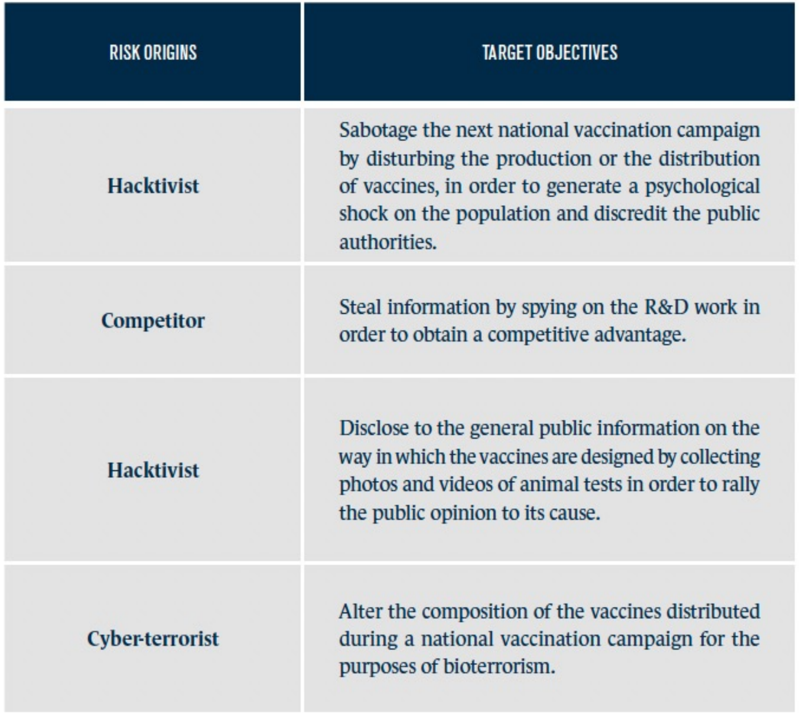
- Source of the threat (origin of the risk)
  - Type
    - Human origin (user or hacker), natural origin (river, …)
    - Non intentional cause or intentional cause (***attacker***)
  - Attacker model (profile, potential)
    - Motivation
    - Expertise (technical skills)
    - Available resources (financial resources, time, exploits…)
  - The attacker model limits the set of attacks that the attacker can perform
    - Example: Dolev Yao model, formal model used when analyzing security protocols (presented in latter courses)

Security Risk Management Concepts

- Source of the threat (origin of the risk)
  - Example: Biotechnology company manufacturing vaccines (EBIOS RM Guide)



RISK ORIGINS	TARGET OBJECTIVES	MOTIVATION	RESOURCES	PERTINENCE
Hacktivist	Sabotage the national vaccination campaign	+ +	+	Moderate
Competitor	Information theft	+ + +	+ + +	High



RISK ORIGINS	TARGET OBJECTIVES
Hacktivist	Sabotage the next national vaccination campaign by disturbing the production or the distribution of vaccines, in order to generate a psychological shock on the population and discredit the public authorities.
Competitor	Steal information by spying on the R&D work in order to obtain a competitive advantage.
Hacktivist	Disclose to the general public information on the way in which the vaccines are designed by collecting photos and videos of animal tests in order to rally the public opinion to its cause.
Cyber-terrorist	Alter the composition of the vaccines distributed during a national vaccination campaign for the purposes of bioterrorism.

Security Risk Management Concepts

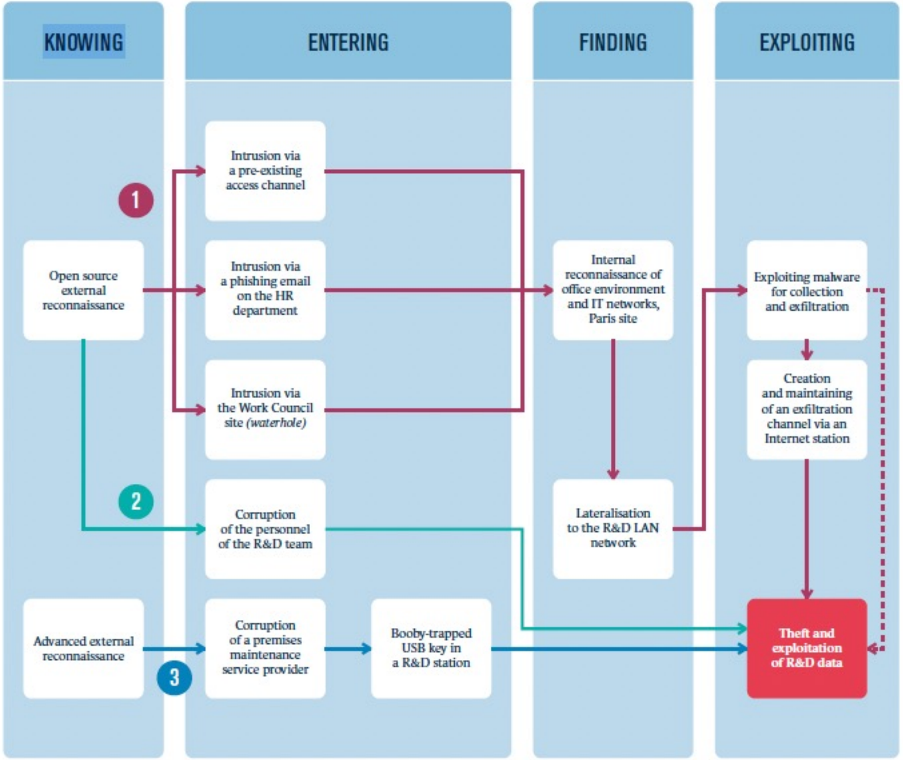
- Vulnerability
  - Security flaw in a component of the system (material asset)
    - Problem in the requirements, functional specification, design, implementation or during the deployment
  - Example
    - A system program written in C with known flaws (no verification of buffer size)
  - *Principle of the weakest link in a chain*
    - Vulnerability level of a system = vulnerability level of its weakest component (easier to exploit for the attacker)
  - Vulnerability database: identify, define, and catalog publicly disclosed cybersecurity vulnerabilities
    - Example: CVE (Common Vulnerabilities and Exposures, https://www.cve.org/)
  - Vulnerability scoring system: assign severity score to vulnerability
    - Example: CVSS (Common Vulnerability Scoring System, https://nvd.nist.gov/vuln-metrics/cvss)
  - Vulnerability scanner: tool that identify vulnerabilities in an application, operating system or network
    - Use a vulnerability scanner
    - Perform version fingerprinting

Security Risk Management Concepts

- Attack (or exploit, or attack pattern, or atomic attack)
  - Pattern of actions employed by the source of attack to exploit a known vulnerability on a given material asset
  - Example: A hacker perform a **buffer overflow attack** exploiting a non verification of input size in a system program written in C
  - Attack Database: collection of known attack patterns
    - Example: MITRE CAPEC (Common Attack Pattern Enumeration & Classification, https://capec.mitre.org/index.html)
- Attack scenario (or threat scenario)
  - A combination of attacks performed by the source of attack to reach an objective
  - Formalism to represent attack scenarios: *attack trees*, *attack graphs* (presented in course on attacks)
  - Attack phases
    - Knowing: collect of information
    - Entering: inital access to the system
    - Finding: locate the sought data
    - Exploiting: attack the supporting assets for the data targeted

Security Risk Management Concepts

- Attack scenario (threat scenario)
  - Example: Biotechnology company manufacturing vaccines (EBIOS RM Guide)
    - A competitor steals research work by creating a data exfiltration channel that directly concerns the information system of R&D



KNOWING

ENTERING

FINDING

EXPLOITING

1

2

3

Open source external reconnaissance

Advanced external reconnaissance

Intrusion via a pre-existing access channel

Intrusion via a phishing email on the HR department

Intrusion via the Work Council site *(waterhole)*

Corruption of the personnel of the R&D team

Corruption of a premises maintenance service provider

Booby-trapped USB key in a R&D station

Internal reconnaissance of office environment and IT networks, Paris site

Lateralisation to the R&D LAN network

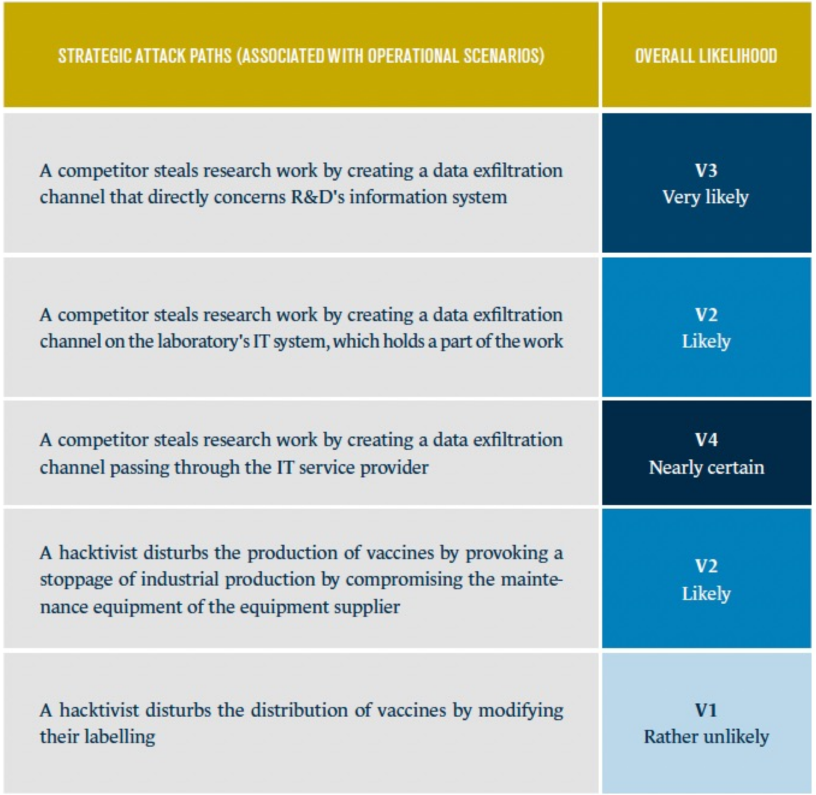
Exploiting malware for collection and exfiltration

Creation and maintaining of an exfiltration channel via an Internet station

Theft and exploitation of R&D data

Security Risk Management Concepts

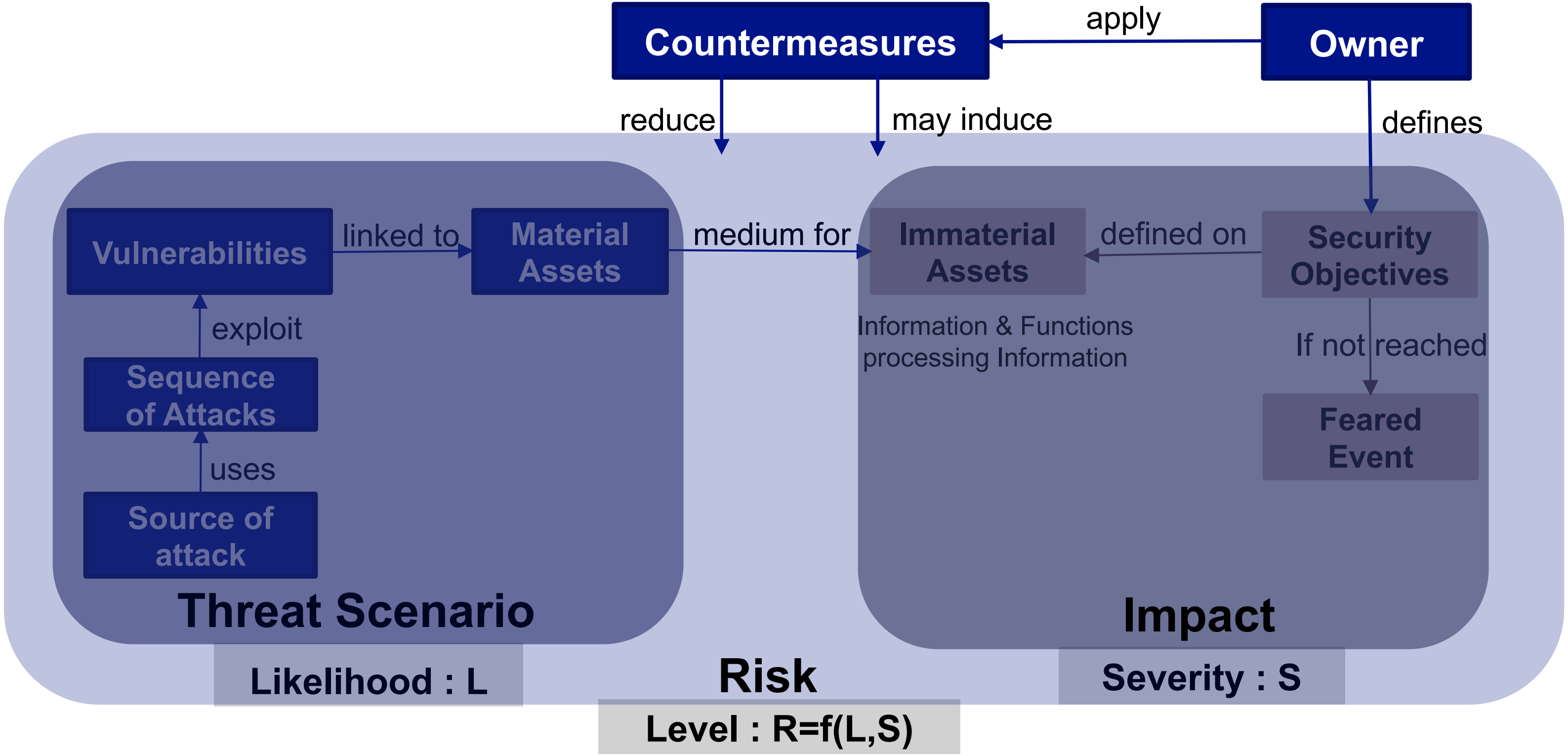
- Attack scenario (or threat scenario) likelihood assessment
  - Based on the probability of success of each attack step of the scenario
  - Computed in some attack graph tools using CVSS
  - Example: Biotechnology company manufacturing vaccines (EBIOS RM Guide)



STRATEGIC ATTACK PATHS (ASSOCIATED WITH OPERATIONAL SCENARIOS)	OVERALL LIKELIHOOD
A competitor steals research work by creating a data exfiltration channel that directly concerns R&D's information system	V3 Very likely
A competitor steals research work by creating a data exfiltration channel on the laboratory's IT system, which holds a part of the work	V2 Likely
A competitor steals research work by creating a data exfiltration channel passing through the IT service provider	V4 Nearly certain
A hacktivist disturbs the production of vaccines by provoking a stoppage of industrial production by compromising the maintenance equipment of the equipment supplier	V2 Likely
A hacktivist disturbs the distribution of vaccines by modifying their labelling	V1 Rather unlikely

Security Risk Management Concepts

- A view of cybersecurity risk

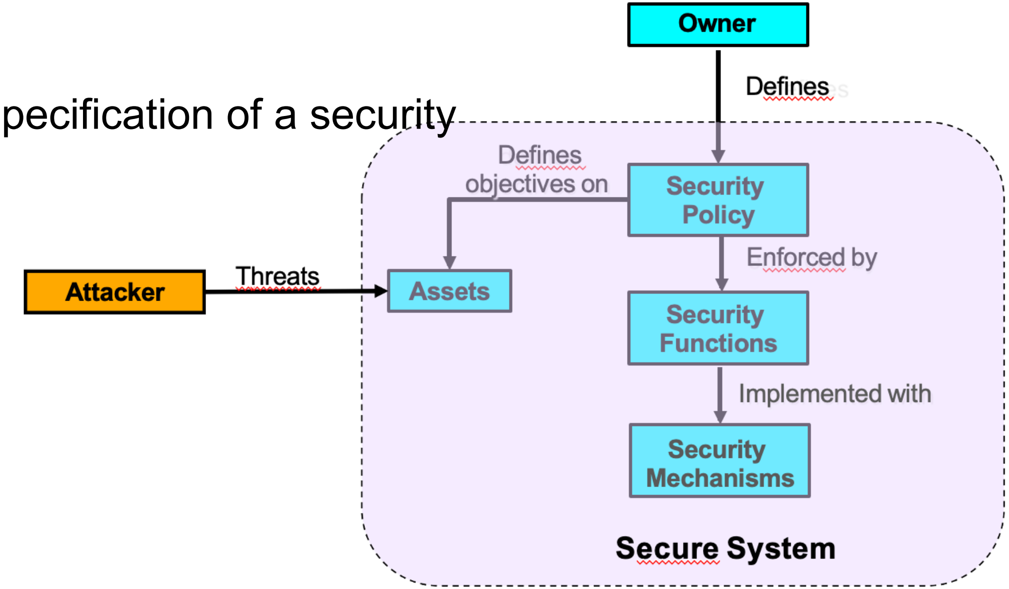


Security Functions

Security Functions

- Secure system
  - Security function (services: functional specification of a security countermeasure (algorithm or protocol)
    - Example : classes of security functions introduced in Common Criteria (CC):

      FIA: Identification and Authentication
      FTA: Target of Evaluation Access
      FAU: Security Audit
      FPR: Privacy
      FCO: Communication security
      FDP: Protection of user data
      … and others (11 classes)



  - Security mechanism: implementation via hardware or software of a security function
    - Ensures that the system does not accept non-authorized actions

Security Functions

- Identification/Authentication
  - Identification
    - Declaration of an identity by an entity
    - Example: entering your login
  - Authentication
    - Process that checks the identity of an entity (entity authentication) or the origin of a message (data origin authentication)
    - Example : verification of password entered after the login
    - Pre-requisite for security of communications and access control
    - Functionalities associated to authentication
      - Identity management: add identitites, remove
      - Ensure confidentiality and integrity of authentication credentials / information

Security Functions

- Identification/Authentication
  - Entity Authentication (A authenticates B)
    - Provides assurance to a first entity A about the identity of a second entity B, with whom A is interacting (A has the guarantee that B was active during the entity authentication process)
    - Requires some freshness information
    - Mutual authentication: A authenticates B and B authenticates A
  - Data Origin Authentication (also known as message authentication)
    - Provides assurance to a first entity that receives a message, about the identity of the entity that originated the message
    - Does not protect against replay attack

Security Functions

- Identification/Authentication
  - Entity Authentication concepts
    - Prover = entity that tries to be authenticated
    - Verifier = entity that checks the identity of the prover
    - Proof = information used by the prover to prove its identity to the verifier
  - Types of proof for entity authentication
    - Based on Knowledge (password, PIN code, cryptographic key)
    - Based on ownership (smartcard, USB token)
    - Based on biometric properties
    - Based on on biometric behavior
  - Strength of entity authentication: based on the quantity of information revealed about the proof
    - Password based authentication, biometric authentication: weak entity authentication
    - One Time Password, challenge-resposne protocols, 0-knowledge protocol: strong authentication
    - Multi-factor authentication: same level as its strongest authentication mechanisms

Security Functions

- Access control
  - Function controlling that subjects (users and processes) can only access to information and resources, if they have the corresponding authorizations
  - Example: access control to a system file, firewall in a network
  - Functionalities associated to access control
  - Functions that manage the authorization specifications
- Audit
  - Function ensuring that information concerning events potentially impacting security is recorded, so that a further examination is able to determine whether there has been a security problem
  - Example: log file in an OS, intrusion detection system in a network
  - Functionalities associated to access control
    - Functions ensuring the integrity or recorded events

Security Functions

Attack life-cycle and security countermeasures

- Dissuasion: measures that deter the attacker from performing the attack
  - Use imputability mechanisms so that the attacker knows that his actions will be recorded
- Protection: measures that prevent the attack
  - Training of non expert users to security
  - Cryptography (art of secret): hide information to third parties
  - Steganography (art of dissimulation): hide information in another content (hide both information and its existence)
  - Identification/Authentication: check the identity of users
  - Acces control (filtering using a firewall)
- Misinformation: measures that deceive the attacker
  - Use Honeypots to obtain information on the attacker (Cyber Threat Intelligence, CTI) or slow down the attacker

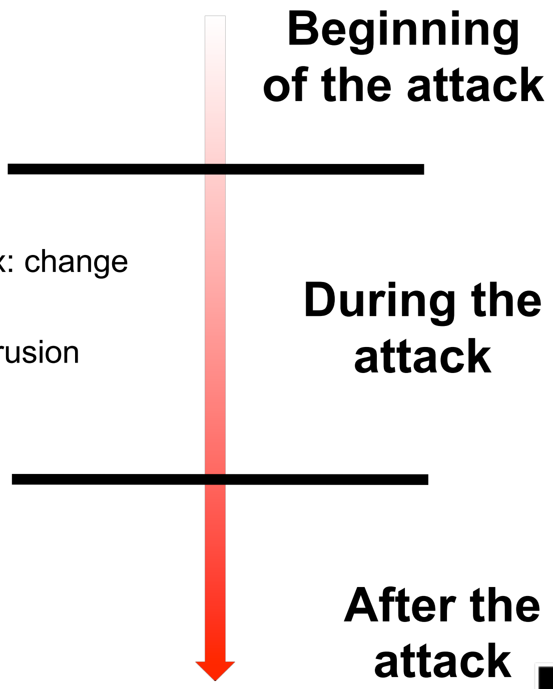
Before

the

attack

Security Functions

- **Attack life-cycle and security countermeasures**
  - Supervision: measures to detect the attack
    - Intrusion Detection System (IDS)
  - Correction: measures to stop or to mitigate the attack
    - Reactive Moving Target Defense: dynamic reconfiguration the system (ex: change the IP addresses)
    - Confinement: quarantine isolation, modification of filtering rules (IPS, Intrusion Prevention System)
    - Ensure availability during an attack (load balancing)
  - Recovery: measures to recover the losses after the incident
    - Understand the attack and search evidence: Computer Forensics
    - Repair the damages (restore the resources in their initial state)
    - Fix the vulnerabilities to prevent future similar attacks
    - Legal action against cyber-criminals, against a third party



Security Standards

(Some) Cybersecurity international standards

- ISO/IEC 73: *Risk management vocabulary*
- ISO/IEC 27000 family*: Information security, cybersecurity and privacy protection*
  - Set of standard to manage information security Information security management system (ISMS)
  - ISO/IEC 27000: Overview and vocabulary
  - ISO/IEC 27001: Specifies requirements for an ISMS
  - ISO/IEC 27002: Detailed catalog of information security controls that might be managed through the ISMS
  - ISO/IEC 27005: Provides guidelines and techniques for managing information security risks
    - Not a complete Risk Management method (does not specify or recommend any risk management method)
- ISO/IEC 15408: *Common Criteria for Information Technology Security Evaluation (CC)*
  - Originates out of previous standards TCSEC (Orange Book) and ITSEC
  - Guidelines for the evaluation and certification of information security products and systems

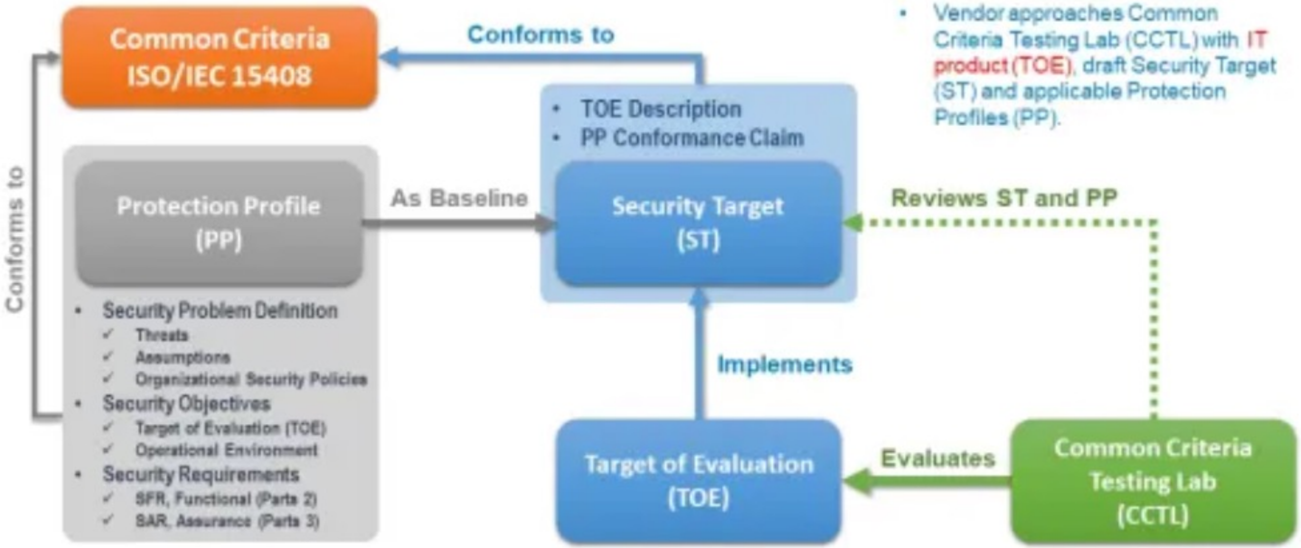
Common Criteria certification scheme (1)

- Separation of functional & assurance requirements for security functions
  - Functional requirements: define desired security behavior (Audit, Identification & Authentication, Cryptographic Support, …)
  - Assurance requirements: ensure that the claimed security measures are effective and implemented correctly (Vulnerability Assessment, Tests, Configuration Management, …)
- Seven *Evaluation Assurance Levels (EALs)*
  - EAL1-2: black box evaluation
  - EAL 3-6: grey box evaluation
  - EAL 7: white box evaluation

EAL	Requirements
EAL1	Functionally. tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested and reviewed
EAL5	Semi-formally designed and tested
EAL6	Semi-formally verified design and tested
EAL7	Formally verified design and tested

Common Criteria certification scheme (2)

- Evaluation process (in France)
  - Vendor of a security product developed following the Common Criteria guidelines contacts ANSSI
  - ANSSI ask to an accredited evaluation center (CESTI) to perform the evaluation



Common Criteria ISO/IEC 15408

Conforms to

- TOE Description
- PP Conformance Claim

- Vendor approaches Common Criteria Testing Lab (CCTL) with IT product (TOE), draft Security Target (ST) and applicable Protection Profiles (PP).

Conforms to

Protection Profile (PP)

As Baseline

Security Target (ST)

Reviews ST and PP

- Security Problem Definition
  - ✓ Threats
  - ✓ Assumptions
  - ✓ Organizational Security Policies
- Security Objectives
  - ✓ Target of Evaluation (TOE)
  - ✓ Operational Environment
- Security Requirements
  - ✓ SFR, Functional (Parts 2)
  - ✓ SAR, Assurance (Parts 3)

Implements

Target of Evaluation (TOE)

Evaluates

Common Criteria Testing Lab (CCTL)

Certificate

Common Criteria certification scheme (3)

- Impact of Certification
  - International Market Entry Assurance
  - Government Procurement Mandate
  - Competitive Marketplace Advantage
  - Sector-Specific Preference (defense, critical infrastructure)
- Example of certified products
  - Complete list available on ANSSI site