Introduction to Security and Privacy (International Master)

Dr. Ing. Karima Boudaoud

karima.boudaoud@univ-cotedazur.fr

Université Côte d'Azur - IUT Nice Côte d'Azur - Polytech Nice Sophia

Laboratoire I3S- CNRS

Content of the course

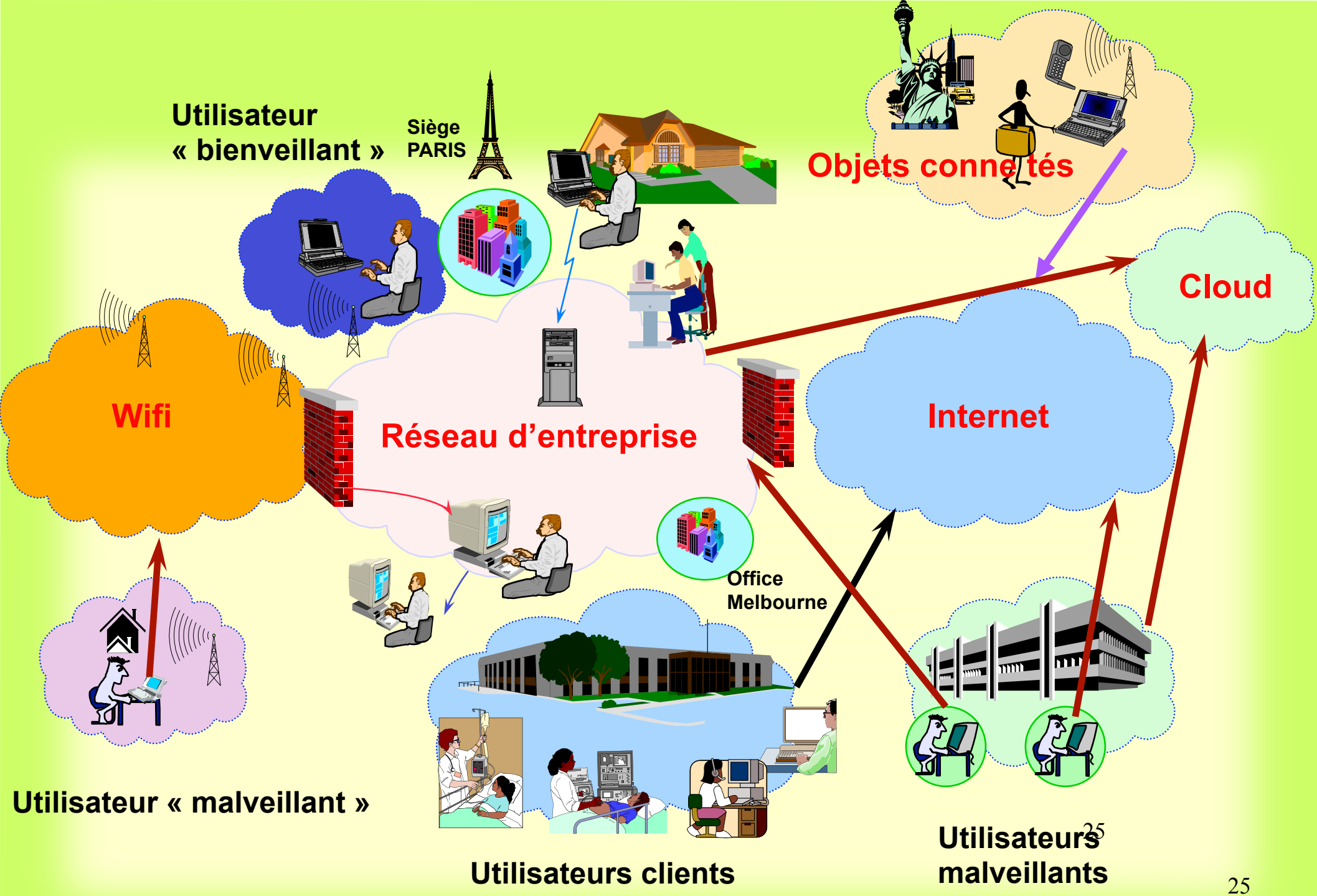
- Introduction to Privacy and Cybersecurity
- Security of Critical Infrastructures (Michael Behringer)
- Security properties (Laurent Gomez)
- DevSecOps (Benjamin Hilaire)
- Android Security (Jeremy Matos)
- Wallets (Louis Raffin)

Plan

- Tour de table☺
- Cybersecurity
  - Definitions and concepts
- Privacy
  - Definitions
  - GDPR
  - Privacy-design concept

Let's discover now some Cybersecurity concepts

What is Cybersecurity for you ?


Utilisateur
« bienveillant »
Siège
PARIS
Objets connectés
Cloud
Wifi
Réseau d'entreprise
Internet
Office
Melbourne
Utilisateur « malveillant »
Utilisateurs clients
Utilisateurs
malveillants

25

Définitions

- **Vulnerability**
- **Threat**
- **Cyber-attack**

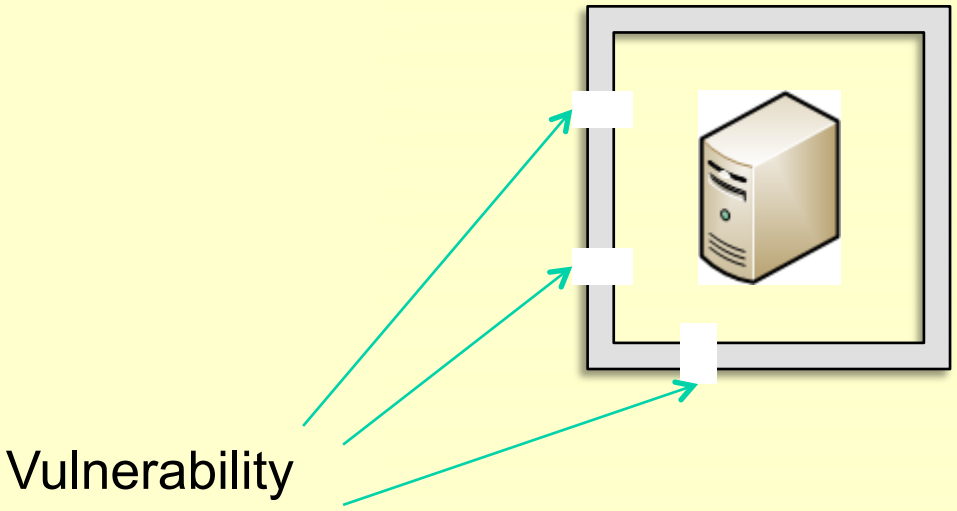
Vulnérability

- **Intrinsic to a**
  - system, machine, network, infrastructure, connected object
- **Known wekanesses/flaws**
  - Can be exploited by hackers
  - Allow the success of an attack
  - to
    - Obtain an access to a non authorized resource
    - Modify (integrity) or access (confidentiality) to a system/data
- **Exploited by**
  - Automatic tools exploiting the vulnerability

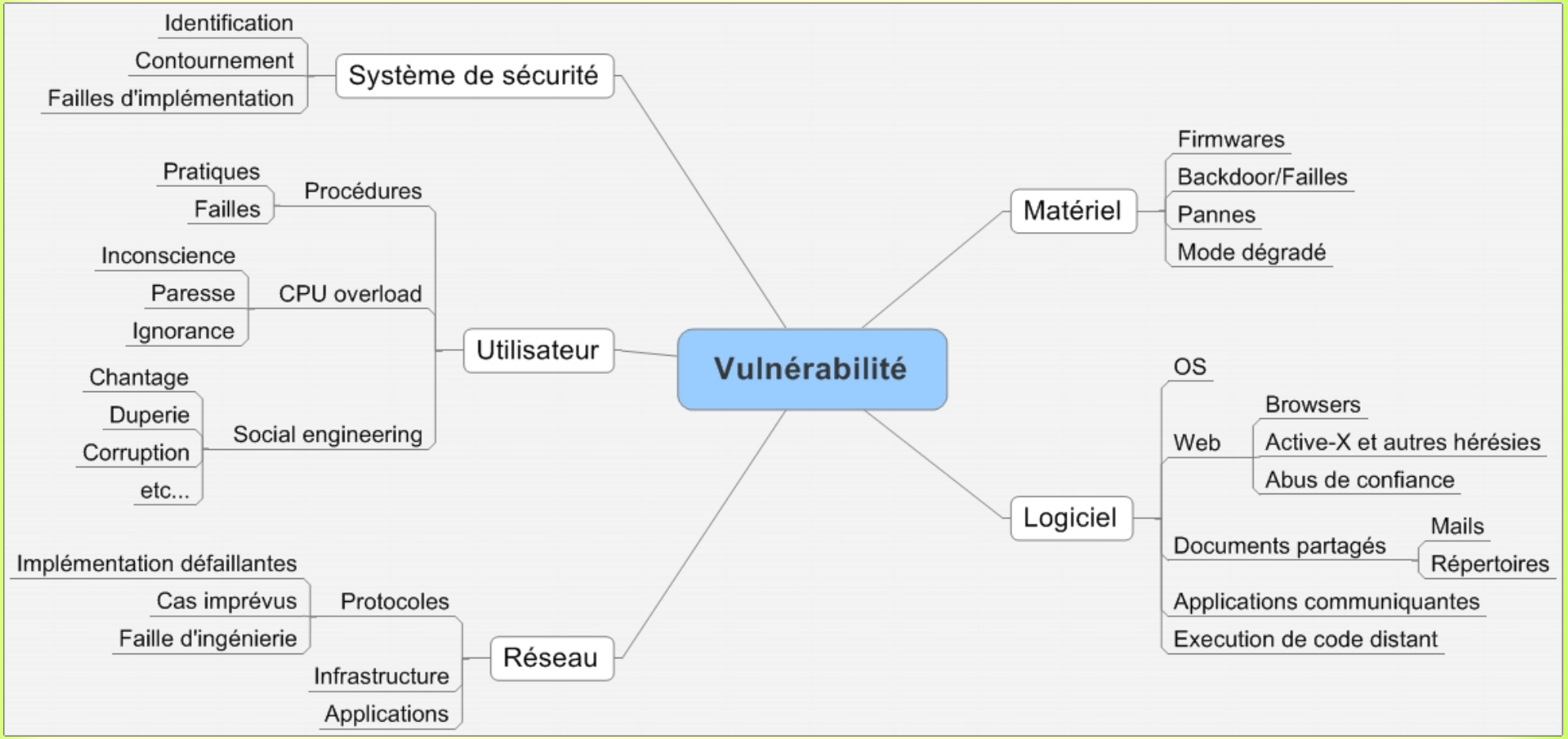
Vulnerability

ANSSI Definition

- **Weakness at any step:** design, implementation, deployment, configuration or use



Vulnerability



*Extrait du cours « The main principals of security »
Stephane Frati & Bernard Sanchez

Vulnerability

- **CVE**
  - **Common Vulnerabilities and Exposure**
  - List of standard identification numbers of known vulnerabilities
  - Reference : CVE-YYYY-NNNN
    - YYYY: Year of publication
    - NNNN: Identifier
  - MITRE: https://cve.mitre.org

Security Incidents & Alerts Management

- **CERT/CSIRT**
  - Computer Emergency Response Team/Computer Security Incident Response Team
  - Principal Role
    - Centralisation + Processing of security incidents
    - Diffusion of alerts on incidents
  - Publish a flaw only after the availability of a patch
  - Exist in all countries
  - CERT-FR
    - https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/

Security Incidents & Alerts Management

- **CERT/CSIRT in France**
  - **Alertes de sécurité**
    - https://www.cert.ssi.gouv.fr/alerte/
  - **Menaces et incidents**
    - https://www.cert.ssi.gouv.fr/cti/
  - Avis de sécurité
  - Indicateurs de compromission
  - Durcissement et recommandations
  - Bulletins d'actualité

Search for the CERT of your country !

Security Incidents & Alerts Management

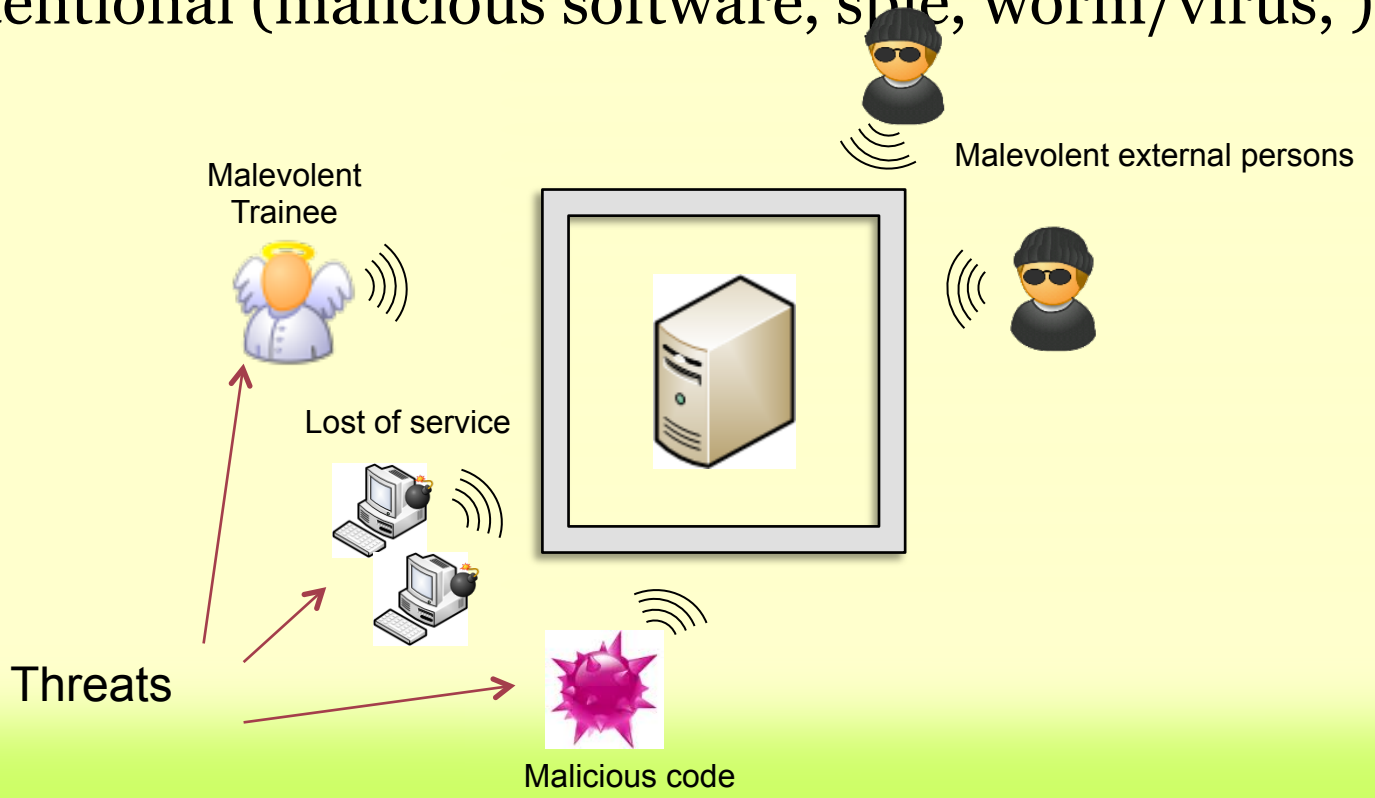
- **Bugtraq**
  - Mailing list that draw up a list of
    - Vulnerabilities and security problems
    - Discussion son these vulnerabilities
    - How to exploit these vulnerabilities
  - Pioneer of **Full disclosure**
    - Complete Divulgation of all the vulnerabilities of software as soon as possible
  - www.securityfocus.com

Threat

- **Extrinsic to**
  - a system, a machine, etc.
  - Can cause a damage to a system, a machine, etc.
- **Everything that can**
  - exploit a vulnerability to cause a damage, access to a non authorized resource, destroy a system,…
- **ANSSI Definition**
  - **Potential cause *of an incident***, that can lead to damages on goods if the threat come true.

Threats

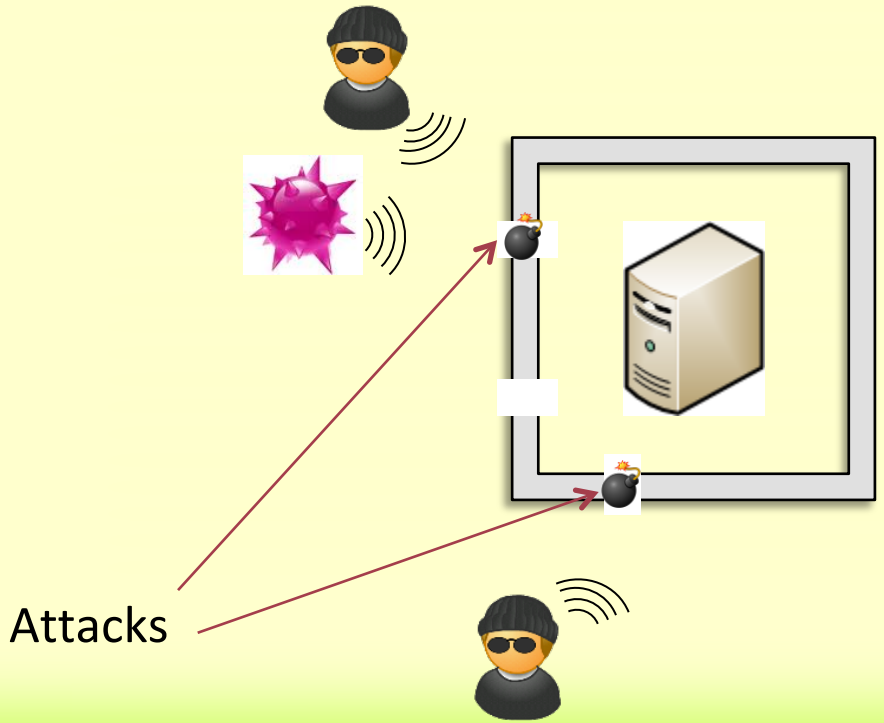
- **Different kinds of threats**
  - Natural (flooding, fire, etc..)
  - Non intentional/ accidental
  - Intentional (malicious software, spie, worm/virus,)



Attacks

ANSSI definition

- **Malicious action** that aims to cause damages to goods.
- It is the **realization of a threat** and requires the **exploitation of a vulnerability.**



Categories of Cyber-attacks

- Cybercrime
- Image Damage (e-reputation)
- Spying
- Sabotage

Cybercrime

- **Target**
  - Users, companies, administrations
- **Objective**
  - Obtain confidential informations to exploit or re-sell them
- **Examples**
  - Phishing
  - Ransomware

Image Damage

- **Target**
  - Companies, administrations, “VIP” persons
- **Objective**
  - Destabilization + damage the image of the victime
  - Replace the contents by ideological, political, etc. messages
- **Examples**
  - Defacement
  - Denial of service

Spying

- **Target**
  - Organisations, Companies,
- **Objective**
  - Spying for different reasons: economical, scientific, etc.
  - Maintain the access as long as possible to obtain strategic information
- **Examples**
  - Watering hole
  - Spearphishing

Sabotage

- **Target**
  - Organisations, companies, etc.
- **Objective**
  - Put the system down
  - By using any kind of attacks

Examples of threats & d'attacks

- Denial of service attacks
- Botnets
- Man-in the middle
- Spoofing
- Virus/Worms

Its your turn:

Go more deeply and search on the Internet ☺

What is Privacy ?

What is privacy for you and What are your experiences with privacy? (Brainstorming)

What is Privacy ? (1/3)

- **Some definitions**
  - "… right to be left alone" [Warren and Brandeis, 1890]
  - "… right not to be annoyed" [Varian, 1996]
  - "control communication of personal data" [Westin 1967]
  - "control of interpersonal boundaries" [Altman 1976]
- **But there are many more** and privacy is a very complex, multi-disciplinary concept and has multiple dimensions…
  - Technical, economic, legal, socio-economic, philosophic,

So, no working definition here …

What is Privacy ? (2/3)

- **Privacy** has **multiple stakeholders perspectives**
  - Users, online businesses, regulators, public authorities, etc.
- **Privacy** for users is highly individual and may depend on
  - Usage context (e.g. user location, application, personal data)
  - Online experience and past privacy violations of a user
  - Cultural background and privacy attitude of users

What is Privacy ? (3/3)

- **Privacy** protection as a challenge for individuals
  - **Takes effort and often technical understanding**
  - Is not directly rewarding (short term) and not perceivable (Privacy Calculus)
  - **Is often demanded by many, but without the willingess to take the effort** (Privacy Paradox)
  - **Can most likely never be outsourced or automated**
  - But can actively be enabled and its effort minimised

Privacy Online vs. Offline

- **Offline Privacy**
  - In the offline world individuals are able to maintain their privacy intuitively
- **Online Privacy**
  - In the online world, privacy
    - Has to be maintained through complex privacy settings or identity management
    - Often cannot be maintained at all by individuals because personal data is collected even without their knowledge

Challenges for Privacy in the Online World

- **The Internet does not forget** or is sometimes not allowed to do so (data retention)
- **The Internet** allows to **easily connect social roles** or **partial identities**, which would have been separated in the offline world
- **Profiling** is **easy** and can be done **automatically**. In contrast, managing personal information is **complex** and has to be done **manually**.

What is difference between Privacy and Security ?

Difference between Privacy and Security*

- **Implement Security** to ensure **Privacy**
- **Use Security** to obtain **Privacy**.
- **Security** is **a process - Privacy** is a **consequence**.
- **Security** is **action - Privacy** is a result of **successful action**.
- **Security** is a **condition - Privacy** is the **prognosis**.
- **Security** is the **strategy - Privacy** is the **outcome.**

*What Is The Difference Between Security and Privacy? Rebecca Herold, CISSP, CISA, FLMI

How to protect Privacy ?

Privacy Protection (1/3)

Legal Data Protection

- EU Regulation : **General Data Protection Regulation (GDPR)**
- Adopted on May 2016 and fully applicable since May 2018
- **Key Elements***
  - ✓ **Increased Territorial Scope:** "*apply to all companies processing personal data of personal subjects residing in EU, regardless the company's location*"
  - ✓ **Penalties:** "*can be fined up to 4% of annual global turnover of the company or €20 Million*"
  - ✓ **Consent**: valid consent to collect data. clear, non ambiguous, easily accessible form.
  - ✓ **Data Protection officer (DPO)**
  - ✓ **Breach notification**: to Supervisory Authority (within 72h)+ Data subject

Privacy Protection (2/3)

Legal Data Protection

- **Key Elements***
  - ✓ **Right to access**
  - ✓ **Right to be forgotten :** right to erasure
  - ✓ **Data Portability**: right to transfer PD + data provided by data controller in a commonly used format
  - ✓ **Accountability**
    - Record data processing activities (data controller and DPO contacts, personal data processed, data recipients, international transfers, **data retention time**).
    - Perform data protection impact assessments (DPIA)
    - Implement right data protection policies
  - ✓ **Privacy by Design and Privacy by Default**
    - **Privacy settings:** set at a high level by default

Privacy Protection (3/3)

Technical Data Protection

- Privacy Enhancing Technology (PET)

  "*Privacy-Enhancing Technology is a system of ICT measures protecting informational privacy by **eliminating** or **minimising** personal data thereby preventing unnecessary or unwanted processing of personal data, **without** the **loss** of the **functionality** of the information system*"[van Blarkom, Borking & Olk, 2003]

  e.g. anonymizers tools

- Security tools (cryptograhy,...)

Privacy by Design and more...

Privacy-by-Design Principles

Privacy by Design Concept

- **What is Privacy By Design?***
  - Defined by Ann Canouvian in the 90's & published in 2009
  - Ensure privacy of data
  - Cannot be assured by « compliance with regulatory framework »
  - Privacy-Enhacing Technologies (PETs) not enough
  - Must be applied to all types of personal data (sensitive data: financia data, medical data, etc.)
  - **7 principles** have been defined

* Privacy by Design – The 7 Foundational Principles – Ann Canouvian

The 7 Foundational Principles (1/4)

1. **Proactive not Reactive; Preventative not Remedial**
   - *Take proactive measures than reactive ones. PbD does not offer any corrective solution. Must be considered in the whole lifecycle of a project from the beginning of its conception. Anticipate privacy issues before happening*
2. **Privacy as the Default Setting**
   - *Default Rules.*
   - *The personal data of users must be protected without their intervention. Implicit data protection.*
   - ***Part of the GDPR***
   - *Responsibility of developers and project managers to apply this principle.*

The 7 Foundational Principles (2/4)

3. Privacy Embedded into Design

- *Data Privacy must be integrated in the design and architecture of IT systems and business practices. It must not be done after thought.*
- *Protection of Data privacy is an essential element of the basic and core functionalities. It is part of the system without having an impact on its functions.*

4. Full Functionality – Positive-Sum, not Zero-Sum

- *Take into account all legitimate interests and objectives using a positive-sum paradigm, i.e "win-win" manner (e.g. in e-health, video-surveillance applications/domain)*
- *Do not use zero-sum approach, where unnecessary trade-offs are made.*
- *Privacy by Design avoids false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.*

The 7 Foundational Principles (3/4)

5. End-to-End Security –Full Life cycle Protection

- *Ensure security of data during its entire lifecycle: data **securely retained** + **securely destroyed** at the end of the process.*
- ***Strong security mechanisms** required from **start to finish** : an end-to-end security of stored data (from collection to destruction)*

6. Visibility and Transparency –Keep it Open

- *Assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification.*
- *The system components and operations concerning privacy **remain visible and transparent**, to **users** as well as **providers**.*
- *Privacy verification create a **trusted environment**.*

The 7 Foundational Principles (4/4)

7. Respect for User Privacy – Keep it User-Centric

- ***Priority to the interests of the user***: *the designers or developers of system and application must give priority to the interests of users concerned by the data processed by the system/application*
- *Strong privacy defaults,*
- *Appropriate notice*
- *Empowering user-friendly options*

Conclusion

- Cybersecurity
- Privacy definitions
- GDPR
- Privacy-By-Design

Thank you, Go raibh maith agat, Merci, Grazie,

Gracias, Obrigado, Danke,

谢谢, ありがとう ございました,

Terima kasih

?