



Introduction à la sécurité

Chapitre 0 Présentation du cours



Pablo Rauzy <pr@up8.edu>
pablo.rauzy.name/teaching/is

Présentation du cours

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.

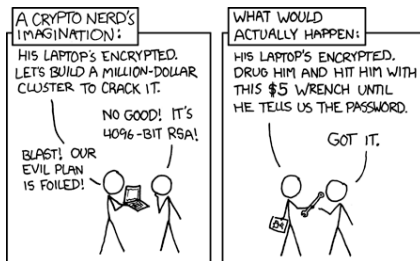
- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.
- ▶ Pourquoi vouloir garantir la sécurité des systèmes informatiques ?

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.
- ▶ Pourquoi vouloir garantir la sécurité des systèmes informatiques ?
 - Protection des personnes.
 - Protection d'intérêts (financiers généralement).

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.
- ▶ Pourquoi vouloir garantir la sécurité des systèmes informatiques ?
 - Protection des personnes.
 - Protection d'intérêts (financiers généralement).
- ▶ La sécurité informatique est donc elle-même un *moyen* et pas une *fin en soi*.

Les moyens de la sécurité informatique

- ▶ Dans ce cours on va principalement s'intéresser aux moyens *techniques*.
- ▶ Cependant, gardez à l'esprit qu'ils ne sont pas suffisant à eux seuls.



Les moyens techniques de la sécurité informatique

- ▶ Les moyens techniques de la sécurité informatique peuvent être catégoriser par *niveaux* qui correspondent à des *disciplines* plus ou moins distinctes :
 - la protection des *données brutes* avec la *cryptologie*,
 - la protection des *systèmes et infrastructures* avec la *sécurité des systèmes d'information*,
 - la protection des *personnes* avec la *privacy*.
- ▶ En pratique, la protection des personnes implique souvent la protection d'un système qui à son tour implique la mise en œuvre de cryptologie.
- ▶ Et il y a bien sûr des champs disciplinaires transverses :
 - la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle,
 - la recherche de vulnérabilité, l'analyse de *malware*,
 - le contrôle d'accès et le contrôle d'usage,
 - l'ingénierie sociale,
 - etc.

► Objectifs :

- Comprendre les bases de la cryptologie.
- Saisir l'importance de se poser la question de la sécurité dès la phase conception d'un projet, par un aperçu en largeur du domaine de la sécurité informatique.
- Acquérir des bases de sécurité par la pratique.

Organisation

- ▶ Module cryptologie :
 - chiffrement par substitution,
 - cryptographie symétrique,
 - cryptographie asymétrique,
 - cryptanalyse classique,
 - canaux auxiliaires.

- ▶ Module sécurité :
 - sécurité système,
 - sécurité réseaux,
 - sécurité web,
 - ingénierie sociale.

- ▶ Module privacy :
 - confidentialité différentielle,
 - contrôle.

Évaluation

- Votre évaluation pour ce cours prendra en compte :
- les TPs,
 - un projet.

Un mot sur les projets tuteurés

- ▶ Premier semestre, état de l'art :
 - comprendre où en est la science sur le sujet,
 - s'approprier la problématique,
 - commencer à esquisser une solution,
 - produire un rapport intermédiaire.
- ▶ Second semestre, implémentation :
 - proposer une solution,
 - mettre en œuvre celle-ci par la programmation,
 - faire une démonstration à la fin de l'année,
 - mettre à jour le rapport avec les résultats obtenus.
- ▶ Les projets tuteurés se font en binôme.
- ▶ Si le domaine de la crypto/sécurité/privacy vous intéresse : contactez-moi !