

TIW4 : SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION GÉNÉRALE

`romuald.thion@univ-lyon1.fr`

<http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4>



Master « Technologies de l'Information et Web »

Outline

- 1 L'unité d'enseignement
- 2 Introduction à la sécurité
- 3 Conclusion

- 1 L'unité d'enseignement
 - Objectifs
- 2 Introduction à la sécurité
- 3 Conclusion

Références

Actualités

- <https://www.cnis-mag.com>
- <https://www.zataz.com/>
- <https://www.pentestit.com>
- <https://www.schneier.com/blog/>
- <https://reflets.info/>
- <https://securelist.com/> (kaspersky)
- <https://ctftime.org/>

Références

Références

- <https://www.ssi.gouv.fr/>
- <https://www.cert.ssi.gouv.fr/>
- <https://www.owasp.org/> et
<https://cheatsheetseries.owasp.org/>
- <https://security.stackexchange.com/> et
<https://crypto.stackexchange.com/>
- <https://www.kali.org/>
- <https://sec.eff.org/>

Références

Ouvrages

- [A Graduate Course in Applied Cryptography](#), Dan Boneh et Victor Shoup (voir les support de cours)
- [Sécurité informatique – cours et exercices corrigés](#), Gildas Avoine, Pascal Junod, Philippe Oechslin, Sylvain Pasini (à la BU)
- [Histoire des codes secrets](#), Simon Singh
- [Silence on the Wire](#) et [The Tangled Web](#), Michal Zalewski
- [The Art of Deception](#), Kevin Mitnick

- 1 L'unité d'enseignement
 - Objectifs
- 2 Introduction à la sécurité
 - Quelques chiffres de la sécurité
 - Aspects juridiques
- 3 Conclusion

Objectifs

Bloc thématiques

- Bases de la cryptographie
- Authentification
- Vulnérabilités web et exploitation
- Gestion des autorisations
- Analyse de risques
- Protection de la vie privée

Compétences

- Reconnaître la sécurité dans le développement (qualité)
- Mettre en place un serveur HTTPS et une authentification sûre
- Reconnaître et réduire les vulnérabilités(web)
- Définir et implémenter une politique de contrôle d'accès

- 1 L'unité d'enseignement
- 2 Introduction à la sécurité
 - Quelques chiffres de la sécurité
 - Aspects juridiques
- 3 Conclusion

- 1 L'unité d'enseignement
 - Objectifs
- 2 Introduction à la sécurité
 - Quelques chiffres de la sécurité
 - Aspects juridiques
- 3 Conclusion

Quelques chiffres de la sécurité

Kaspersky Security Bulletin 2019. Statistics

- 19.8% of user computers were subjected to at least one Malware-class web attack over the year.
- K solutions repelled 975 491 360 attacks launched from online resources located all over the world.
- 273 782 113 unique URLs were recognized as malicious by web antivirus components.
- K's web antivirus detected 24 610 126 unique malicious objects.
- 755 485 computers of unique users were targeted by encryptors.
- 2 259 038 computers of unique users were targeted by miners.
- K solutions blocked attempts to launch malware capable of stealing money via online banking on 766 728 devices.

Quelques chiffres de la sécurité

NortonLifeLock (ex Symantec, racheté par Broadcom inc.)

- Almost 500 Million Consumers* Have Ever Been the Victim of a Cyber Crime ; Nearly 350 Million in the Last Year Alone
- Nearly 46 Million Consumers* Were the Victim of Identity Theft Last Year

There's Nowhere to Hide from the Economics of Cybercrime (MacAfee)

Cybercrime now costs the world almost \$600 billion, or 0.8 percent of global GDP, according to a new report by the Center for Strategic and International Studies (CSIS) and McAfee. Scheduled for release February 21, "The Economic Impact of Cybercrime : No Slowing Down" updates the popular 2014 report, which put global losses at close to \$500 billion, or 0.7% of global income.

Brainstorming

Donner des noms propres, marques, termes techniques, acronymes, etc. de la cyber sécurité

- 1 L'unité d'enseignement
 - Objectifs
- 2 Introduction à la sécurité
 - Quelques chiffres de la sécurité
 - Aspects juridiques
- 3 Conclusion

Art. 323 du Code Pénal

- LIVRE Ier Dispositions générales.
- LIVRE II Des crimes et délits contre les personnes.
- LIVRE III Des crimes et délits contre les biens.
 - TITRE Ier Des appropriations frauduleuses.
 - TITRE II Des autres atteintes aux biens.
 - CHAPITRE Ier Du recel et des infractions assimilées ou voisines.
 - CHAPITRE II Des destructions, dégradations et détériorations.
 - CHAPITRE III Des atteintes aux systèmes de traitement automatisé de données.
 - CHAPITRE IV Du blanchiment.
- LIVRE IV Des crimes et délits contre la nation, l'Etat et la paix publique.

Des atteintes aux STAD

L'article sur lefrance

Infractions « classiques »

- l'escroquerie
- l'usurpation d'identité
- la diffamation
- apologie des crimes et délits
- l'atteinte au secret des correspondances
- l'atteinte à la vie privée (c.f CNIL)

Tout ce qui est illégal offline est illégal offline l'est aussi online

Des atteintes aux STAD

L'article sur legifrance

Infractions « classiques »

- l'escroquerie
- l'usurpation d'identité
- la diffamation
- apologie des crimes et délits
- l'atteinte au secret des correspondances
- l'atteinte à la vie privée (c.f CNIL)

Tout ce qui est illégal offline est illégal offline l'est aussi online

- 1 L'unité d'enseignement
- 2 Introduction à la sécurité
- 3 Conclusion**

Conclusion

My 2 cents

- La sécurité est un compromis : un rapport qualité / prix.
- En constante évolution, sans fin
- Ca peut devenir très technique, dans tous les sens
- Tous les moyens sont bons

Éclatez-vous, c'est fun !

“Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people.”

Kevin D. Mitnick – “The Art of Deception”, p.79

Conclusion

My 2 cents

- La sécurité est un compromis : un rapport qualité / prix.
- En constante évolution, sans fin
- Ca peut devenir très technique, dans tous les sens
- Tous les moyens sont bons

Éclatez-vous, c'est fun !

“Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people.”

Kevin D. Mitnick – “The Art of Deception”, p.79