Master Informatique – parcours SIS
sebastien.duval@loria.fr

Sécurité des Systèmes d'Information

Présentation du cours

2025/2026

Supports basés sur le cours de Laurent Vigneron et sur la formation de l'ANSSI

À propos de moi

Sébastien DUVAL

Maître de Conférences

- Chercheur en Cryptographie (en particulier pour les objets connectés)
- Bureau au LORIA (en face), accès restreint
- En charge de l’exercice Cyber Humanum Est pour la FST

Pour me contacter :

- Avant/après un cours
- Par mail : sebastien.duval@loria.fr

(je réponds généralement sous 48h)

Objectifs du cours

- Situer la problématique de la SSI
- Poser les bases de la SSI
- Permettre d’aborder les UE plus spécialisées
- Focus : identifier ce qui est *fondamentalement* possible, impossible et bientôt possible en SSI

Plan du cours

1. **Notions de base**
2. **Règles d'hygiène informatique**
3. **Aspects réseau et applicatifs**
4. **Cyber-combat**
5. **Panorama des solutions cryptographiques**
6. **Gestion de la sécurité au sein d'une organisation**
7. **Infrastructures de clefs publiques**

Supports de cours sur Arche

Évaluation du cours

- **Examen après Chapitres 1-2 (20%)**
- **Examen après Chapitres 3-4-5 (20%)**
- **Examen final (sur tout) :**
  - **QCM + compréhension : 30%**
  - **rédaction : 30 %**
- **Petits TP/TD (a priori pas notés)**

- **cf. Modalités d’évaluation sur Arche**
- **cf. Auto-tests sur chaque chapitre (pour vous entraîner)**

Auto-tests et votre projet professionnel

- **Les auto-tests servent à vérifier vos connaissances, savoir ce que vous devez retravailler**
- **Je ne récupère pas les notes**
- **Vous pouvez les refaire autant que vous voulez**

Technicien en cybersécurité

Perspectives de carrière :

- Technicien en cybersécurité : savoir appliquer, pas d'évolution de carrière en cybersécurité

Compétences visées :

- Connaissance des fondamentaux (sans compréhension)
- Vocabulaire courant
- Savoir l'utilité de chaque outil

Est-ce que ça s'apprend sur le tas ?

- Partiellement, avec des MOOC
- Partiellement, avec des collègues

Ingénieur en cybersécurité

Perspectives de carrière :

- Ingénieur en cybersécurité : avec évolutions de carrière en sécurité

Compétences visées :

- *Contexte* : en sécu, l'évolution technologique est rapide. Un ingé en cybersécurité doit comprendre les innovations et les mettre en œuvre. Ces innovations sont variées et imprévisibles : il faut comprendre les fondamentaux pour comprendre l'implication des innovations !
- Connaissance et compréhension des fondamentaux
- Savoir trouver l'essentiel d'un article de recherche
- Savoir remettre en question l'état de l'art (car il évolue)

Est-ce que ça s'apprend sur le tas ?

- Non, aucun MOOC et ça évolue trop vite
- Non, peu de formations universitaires de bon niveau (< 10 en France, niveau master)
- Non, besoin de compréhension des fondamentaux académiques – vos collègues n'auront pas les notions et ne seront pas à jour (à vous de les mettre à jour!)

Quelques précisions

- Partiellement basé sur une formation de l'ANSSI (bonne qualité), mais plusieurs chapitres sont nettement plus avancés que leur formation et que tout ce que vous trouverez sur Internet !!!
- L'objectif n'est pas que vous maîtrisiez tout :
  - **Comprenez les principes**
  - Sachez **retrouver les informations** (tip : il y a un bouton pour télécharger les contenus du cours sur Arche)
- Les cours ne seront jamais 100 % à jour (les technologies et modes évoluent vite)
- Les pros ne sont pas à jour non plus !!! Une grande part de la sécurité est du domaine de la recherche, vos collègues ne suivent pas ça : vous débarquerez avec un état de l'art (hors technos) plus à jour, sachez le valoriser !
- N'hésitez pas à **poser des questions** : c'est la dernière année où vous avez accès à des experts académiques, profitez-en !

Quelques précisions

La sécurité informatique est immense, cette UE n'est qu'une introduction.

Seront abordés (rapidement) :

- Raison d'être de la SSI, métiers
- Hygiène informatique
- Sécurité réseau
- Cryptographie (boîte à outils)
- Sécurité organisationnelle
- Certificats de clefs publiques

Ne seront qu'évoqués :

- Contrôle d'accès
- Supervision
- Sécurité Web
- Sécurité du système d'exploitation
- Sécurité électronique
- Sécurité des machines industrielles
- Malwares

Ces sujets sont abordés en détails dans les UE de spécialité !