

Sécurité numérique

Infos pratiques

- > ECTS : 4.5
- > Nombre d'heures : 24.0
- > Période de l'année : Enseignement dixième semestre
- > Méthodes d'enseignement : En présence
- > Forme d'enseignement : Cours magistral
- > Ouvert aux étudiants en échange : Oui
- > Composante : Philo, Info-Comm, Langues, Littératures & Arts du spectacle
- > Code ELP : 4L0ISO1P

Présentation

Ce cours vise à sensibiliser les étudiant·es aux enjeux de la sécurité des systèmes d'information, et leur fournir une large gamme d'outils pour la renforcer. Il abordera plusieurs techniques contribuant à l'authenticité (signature numérique, certification), la confidentialité (chiffrement symétrique et asymétrique) et l'intégrité (somme de contrôle, blockchain, etc.) des données manipulées. Il présentera un certain nombre d'outils implémentant ces techniques, ainsi que leur intégration dans la chaîne de production et de valorisation des données. Il aidera également les étudiant·es à identifier les acteurs susceptibles de participer à la mise en œuvre de stratégies de sécurité, et à réagir avec efficacité lorsqu'une vulnérabilité ou une attaque est découverte.

Objectifs

- comprendre les vulnérabilités et les menaces qui peuvent affecter un projet numérique
- connaître une large gamme de contre-mesure pouvant être mises en œuvre
- définir une stratégie de sécurité numérique en fonction des caractéristiques des données manipulées
- réagir efficacement en cas de découverte d'une vulnérabilité ou d'une attaque

Évaluation

M3C en session unique

- * Régime standard intégral – avec évaluation continue (au moins 2 notes)
 - * Devoir sur table, 2h, 40 %
 - * Présentations et dossiers, 30 %
 - * Participation aux travaux en cours, 30 %

Compétences visées

- Disposer d'une expérience personnelle d'analyse et/ou de production de dispositifs, objets et systèmes informationnels et communicationnels.
- Situer son rôle et sa mission au sein d'une organisation pour s'adapter et prendre des initiatives.
- Respecter les principes d'éthique, de déontologie et de responsabilité environnementale.
- Utiliser les outils numériques de référence et les règles de sécurité informatique pour acquérir, traiter, produire et diffuser de l'information ainsi que pour collaborer en interne et en externe.

Bibliographie

ANSSI & CPME. (2017). *Guide des bonnes pratiques de l'informatique*.

CNIL. (2018). *La sécurité des données personnelles*.

Ressources pédagogiques

Crypto, webdocumentaire de l'ANSSI : <https://www.ssi.gouv.fr/particulier/guide/crypto-le-webdoc/>

Contact(s)

- > **Dario Compagno**
Responsable pédagogique
dcompagno@parisnanterre.fr