Sécurité des systèmes d'information

ECTS : 4

Volume horaire : 24

Description du contenu de l'enseignement :

Ce cours offre une introduction aux **principes de la sécurité des systèmes d'information**, avec un focus sur les outils cryptographiques permettant d'assurer la confidentialité, l'intégrité et l'authenticité des données. Il est organisé autour des grandes thématiques suivantes :

• **Introduction et besoins en sécurité des systèmes d'Informations**(Yann Goetgheluck & Julien Lesca)

Présentation des objectifs fondamentaux (confidentialité, intégrité, disponibilité), distinction vulnérabilités/menaces/risques et du rôle de la cryptographie dans la construction de systèmes sécurisés.

• **Fondamentaux et réglementation** (Yann Goetgheluck)

Triade CIA, frameworks de sécurité (ISO 27001, NIST), cadres réglementaires européens (RGPD, NIS2, DORA) et leurs implications organisationnelles.

• **Cybersécurité opérationnelle** (Yann Goetgheluck)

Équipes Blue/Red/Purple Team, méthodologies de pentesting, typologie des cyberattaquants, et outils techniques (SIEM, EDR, Vulnerability Management).

• **Risk Management et Système de Management de la Sécurité de l'Information**(Yann Goetgheluck)

Analyse de risques qualitative (ISO 27005) et quantitative (FAIR), Threat Modeling (MITRE ATT&CK), mise en place d'un Système de Management de la Sécurité de l'Information avec cycle PDCA et métriques hybrides.

• **Implémentation pratique** (Yann Goetgheluck)

Mapping contrôles ISO 27001 vers solutions techniques, KPIs opérationnels et business (ROI sécurité), ateliers Purple Team et études de cas réels.

• **Chiffrement symétrique : notions fondamentales** (Julien Lesca)

Court historique des algorithmes classiques, mise en évidence de leurs propriétés, de leurs limites et des principaux types d'attaques.

• **Algorithmes symétriques modernes** (Julien Lesca)

Étude de constructions basées sur le schéma de Feistel, notamment**DES** et **3DES**, et introduction aux **modes de fonctionnement** (CBC, OFB, CTR) permettant d'adapter ces algorithmes à différents usages.

• **Chiffrement asymétrique** (Julien Lesca)

Présentation du principe de la cryptographie à clé publique/clé privée et étude de l'algorithme**RSA** comme exemple représentatif.

• **Fonctions de hachage cryptographiques** (Julien Lesca)

Rôle du hachage dans la sécurité et illustration à travers l'algorithme**SHA-3**.

• **Mécanismes d'authentification et d'intégrité** (Julien Lesca)

Étude des **codes d'authentification de message** (HMAC, CMAC) et introduction à la**signature électronique**, avec l'exemple de RSA-PSS.

• **Distribution des clés et certificats** (Julien Lesca)

Présentation des mécanismes permettant de gérer les clés cryptographiques à grande échelle, notamment via les infrastructures de certificats.

Compétence à acquérir :

L'objectif global du cours est de donner aux étudiants une compréhension cohérente et opérationnelle des besoins en sécurité et des principales primitives cryptographiques utilisées pour y répondre.

Bibliographie, lectures recommandées :

- "Cryptography and Network Security: Principles and Practice", W. Stallings, Pearson, 2016.
- S. Al-Dhari, M. Al-Sarti, A. Abdaziz, "Information Security Management System". International Journal of Computer Applications, 158, 29–33, 2017.
- C. Legrenzi, "Informatique, numérique et système d'information : définitions, périmètres, enjeux économiques". Vie & Sciences de L'Entreprise, 200, 49–76, 2016.
- D. Strachan-Morris, "Threat and Risk : What Is the Difference and Why Does It Matter ?", Intelligence & National Security, 27(2), 172–186, 2012
- S. G. Watkins, "ISO/IEC 27001 :2022", IT Governance Publishing Ltd, Ely, Cambridgeshire, Royaume-Uni, 2022.

Document susceptible de mise à jour - 01/04/2026

Université Paris Dauphine - PSL - Place du Maréchal de Lattre de Tassigny - 75775 PARIS Cedex 16