CYB202 - Cybersécurité avancée pour les systèmes et applications

Mis à jour le 25-09-2026

Code : CYB202

Unité d'enseignement de type mixte

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale :
EPN05 - Informatique / Vania CONAN

Contact national :

EPN05 - Informatique

2 rue Conté
75003 Paris
01 40 27 22 58
Swathi RANGANADIN RAJASELVAM
swathi.ranganadin@lecnam.net

Présentation

Prérequis

RSX103, CYB105

Objectifs pédagogiques

L'UE CYB202 adresse la cybersécurité avancée dans les systèmes et applications déployées dans les environnements utilisateurs et industriels. L'UE considère le cycle d'acheminement des données de bout-en-bout : depuis les objets connectés situés auprès des utilisateurs et des infrastructures industriels jusqu'à le Cloud.
Nous traitons particulièrement les problématiques de confiance et solutions associées sur l'ensemble du cycle d'acheminement des données, en considérant deux types d'architectures de confiance :

1. La confiance décentralisée côté utilisateur final au début de la chaine : incluant l'étude de la confiance dans les objets connectés et d'objets connectés industriels, la confiance dans l'accès sans fil WiFi, la confiance dans les services de cryptomonnaies, ainsi que l'investigation numérique Forensic côté utiliser final.
2. La confiance centralisée côté Cloud : incluant la confiance dans les trois infrastructures du Cloud : Infra. du stockage, Infra. du traitement et Infra. des communications.
   CYB202 permettra aux auditeurs de comprendre les stratégies de sécurité et d'appréhender les techniques permettant d'améliorer la protection avancées des données et des systèmes.

L'UE CYB202 cible les services de confidentialité, de disponibilité, et d'authentification.

Compétences

- Appréhender et maitriser les attaques contre les systèmes informatiques ainsi que les mécanismes/politiques de sécurité à mettre en place.
- Mettre en place des mesures techniques pour assurer la sécurité des infrastructures d'objets connectés
- Maitriser les techniques, les standards, et les techniques de confidentialité du WiFi.
- Appréhender les techniques de sécurité du Cloud.
- Comprendre le Forensic et les étapes de l'investigation numérique réalisées par les investigateurs des forces de sécurité
- Maitriser la sécurité des Blockchains, les algorithmes de consensus et les applications des smart contrats.

Programme

Contenu

Introduction à la sécurité des données pour les objets connectés
Contexte et problématique de la sécurité des données dans les systèmes d'objets connectés
Vulnérabilités et risques
Attaques générales et spécifiques
Définition des besoins de sécurisation de bout-en-bout des systèmes d'objets connectés

Cas d'usage de la sécurité des systèmes objets connectés : Sécurité des véhicules connectés
Concepts, architectures et applications
Techniques de communications véhiculaires (issues d'IEEE 802.11p, 1609.x, NIST…)
Définition des besoins de sécurisation de bout en bout
Attaques industrielles
Standards de sécurité (IEEE 1609.2, ETSI 102941…)
Confidentialité avancée et anonymisation des données de la vie privée
Lab : atelier de mise en place d'un V2X sécurisé

Sécurité des données et systèmes dans l’environnement WiFi
Concepts, évolution
Vulnérabilités et modèles de menaces
Authentification et confidentialité avancée
802.1X, PEAP, LEAP, AEP-fast 3
WEP, WPA, WPA2, WPA3
Standards de confidentialité
Lab : améliorer la protection des données dans un environnement WiFi

Confiance centralisée et Cloud
Concepts et architectures
Centres de données : résilience et cybersécurité
Vulnérabilités et attaques
Définition des besoins de sécurisation de bout-en-bout
Modèles de menaces
Autorisation dans le Cloud
Protection des flux privés
Vision du NIST et solutions de sécurité
Lab : atelier sur la sécurisation du Cloud

Confiance distribuée pour les cryptomonnaies et Blockchains
Concepts, architecture
Algorithmes de ménage et algorithmes de consensus
Vulnérabilités et attaques
Sécurité et Smart contrats
Applications sécuritaires des Blockchains
Lab : mise en place et implémentation d’une Blockchain

Forensic
Pourquoi l’investigation Forensic ?
Concepts et étapes de l’investigation Forensic par les forces de Police et Gendarmerie
Méthodes et normes Forensic
Outils Forensic
Analyse des données contenues dans la mémoire vive
Analyse du cache
Réponse de sécurité Forensic aux incidents de sécurité
Métier de l’investigateur Forensic (Police et Gendarmerie)
Lab : atelier sur l'investigation Forensic (sur système Windows)
o Collecter les données volatiles et non volatiles.
o Analyse des données contenues dans la mémoire vive, des fichiers Windows.
o Analyse du cache, cookie et historique de navigation, historique desévénements

Modalités de validation

- Projet(s)

Description des modalités de validation

Validation par Projet (rapport + présentation).