Cybersécurité PHY-MAC

CentraleSupélec
EXED

Ref.: CR01-26

Dans un contexte de numérisation continue et croissante des activités humaines, la sécurité de l'information (SI) devient un enjeu critique de souveraineté qui vise notamment à conserver la maîtrise des systèmes numériques.

La SI repose sur 3 piliers (confidentialité, intégrité et disponibilité) et concerne l'ensemble des systèmes électroniques en réseaux, de la couche physique à la couche applicative du modèle OSI. Cette formation en cybersécurité vise à comprendre et implémenter un ensemble de menaces et de protections sur les couches PHY et MAC, pour les 3 piliers précédemment énoncés.

"Cette formation balaie les menaces courantes qui peuvent affecter un système de communication sur les couches PHY et MAC et propose d'étudier les protections associées. Les fondements théoriques et pratiques des menaces /protections sont détaillés au cours de la formation."

Corentin Fonteneau.
Enseignant-chercheur en traitement du signal et communications numériques à l'INSA Rennes.

À l'issue de cette formation, le participant sera en capacité de :

- **CREER** des menaces sur la disponibilité de la couche phy, Analyser et Adapter des mécanismes de protections.
- **CREER** des menaces sur la confidentialité de la couche phy.
- **CREER** des menaces sur l'intégrité de la couche mac, Appréhender et Développer des mécanismes de protections.
- **ANALYSER** et **UTILISER** les principes fondamentaux de la radio-logicielle

Date d'édition : 11/09/25

Ref.: CR01-26

Cybersécurité PHY-MAC

Synthèse du programme

• Communications en environnements contestés : Brouillage et contre-mesures (1 jour et demi)
• Principe radio-logicielle et plateforme (1/2 jour)
• Menace et protection de l'intégrité de l'information sur la couche MAC (1 jour et demi)
• Reconstruction d'écran : Attaque TEMPEST de la théorie à la pratique (1 jour et demi)

Public concerné

Ingénieurs
Responsables d'équipe qui souhaitent développer leurs connaissances et leurs compétences pratiques en sécurité de l'information sur les couches PHY et MAC pour des applications actuelles.

Pré-requis

• Bases en traitement statistique du signal et en communications numériques.
• Commandes de base en console pour Linux\Ubuntu.
• Langages C/C++ et/ou Python.

• Procédure d'admission à cette formation :
Entretien téléphonique avec le/la chargé/e d'affaires pour comprendre vos attentes et votre projet professionnel en lien avec la formation visée.
Envoi de votre CV et/ou lettre de motivation au/à la chargé/e d'affaires puis transmission au responsable pédagogique du parcours qui étudie votre candidature et valide ou non les prérequis nécessaires à la formation. Retour sous 5 jours ouvrés.
Si votre candidature est validée, vous pouvez procéder à votre inscription via le CPF (si la formation y est éligible), ou via le bulletin d'inscription transmis par le/la chargé/e d'affaires.

Les + de la formation

• Les 3 piliers de la sécurité de l'information sont étudiés
• Une approche multicouche sera proposée
• Développements théoriques illustrés de cas pratiques constitueront la valeur ajoutée de la formation

Contact
Laura Veckens

Lieu
Rennes (35000)

€ (HT)

Dates
Du 05/10/2026 au 09/10/2026

Durée
5 jour(s)
35 heure(s)

QUELQUES CHIFFRES

86/100

Taux de satisfaction globale pour 406 sessions (sur un panel de 2450 répondants sur les 4152 participants en 2024)

89/100

Satisfaction globale relative aux formateurs pour 406 formations (sur un panel de 2450 répondants sur les 4152 participants en 2024)

Date d'édition : 11/09/25

Ref.: CR01-26

Cybersécurité PHY-MAC

Le programme

MODULE 1

COMMUNICATIONS EN ENVIRONNEMENTS CONTESTÉS : BROUILLAGE ET CONTRE-MESURES (1 JOUR ET DEMI)

- Menaces stationnaires au sens large sur la couche PHY et protection associée. (1/2 jour)
  - Modélisation de menaces stationnaires au sens large.
  - Protection du récepteur par filtrage de Wiener.

- Menaces non stationnaires au sens large sur la couche PHY et protection associée. (1/2 jour)
  - Modélisation de menaces non stationnaires au sens large.
  - Protection du récepteur par filtrage de Kalman.

- Implémentation de menaces sur la couche PHY et de protections. (1/2 jour)
  - Implémentation de menaces dans un simulateur de communication.
  - Implémentation d'un filtre de protection au niveau du récepteur.
  - Analyse du gain de performance associé au filtre de protection dans divers scénarios (nature de la menace, taille du filtre, rapport signal à interférence + bruit…).

MODULE 2

PRINCIPE RADIO-LOGICIELLE ET PLATEFORME (1/2 JOUR)

- Comprendre les fondements de la radio logicielle
- Maîtriser les architectures matérielles/logicielles des plateformes SDR.
- Explorer des cas pratiques et outils

MODULE 3

MENACE ET PROTECTION DE L'INTÉGRITÉ DE L'INFORMATION SUR LA COUCHE MAC (1 JOUR ET DEMI)

- Spectrum Sensing (1/2 jour)
  - Comprendre le concept de détection de spectre et son importance dans les réseaux sans fil.
  - Connaître les différentes techniques de détection de spectre.
  - Savoir évaluer les performances des détecteurs.
  - Introduction aux défis pratiques et aux recherches récentes.

- RF fingerprinting (1/2 jour)
  - Comprendre le concept de RF fingerprinting et ses applications.
  - Connaître les fondements physiques et techniques.
  - Explorer les méthodes de collecte et de traitement des signaux.
  - Découvrir les algorithmes d'apprentissage automatique utilisés.

- WiFI-MAC spoofing (1/2 jour)
  - Comprendre le format des trames WiFi (en particulier 802.11) et le concept de spoofing MAC.
  - Savoir configurer un flux GNU Radio pour émettre des signaux WiFi.
  - Générer des trames WiFi avec des adresses MAC modifiées.
  - Mettre en œuvres des algorithmes pour détecter les adresses MAC modifiées.

Date d'édition : 11/09/25

Ref.: CR01-26

Cybersécurité PHY-MAC

MODULE 4

RECONSTRUCTION D'ÉCRAN : ATTAQUE TEMPEST DE LA THÉORIE À LA PRATIQUE (1 JOUR ET DEMI)

- Attaque TEMPEST partie 1 : Introduction et analyse des signaux cibles (1/2 jour)
  - Connaitre le concept de cybersécurité électromagnétique.
  - Comprendre le fonctionnement d'une attaque TEMPEST de recopie d'écran à distance.
  - Analyser les signaux électriques d'une liaison VGA.

- Attaque TEMPEST partie 2 : Mesure radio des émanations compromettantes (1/2 jour)
  - Déterminer les fréquences de fuite électromagnétique.
  - Mesurer les émanations électromagnétiques de la liaison VGA à l'aide de plateformes radio-logicielles.

- Attaque TEMPEST partie 3 : Reconstruction des données (1/2 jour)
  - Traiter les données binaires (enregistrés avec GNU Radio) avec Python.
  - Ecrire le programme Python permettant de reconstruire une image à partir des données (raster).

Date d'édition : 11/09/25

Cybersécurité PHY-MAC

Équipe pédagogique

Responsable Pédagogique

Corentin FONTENEAU
Maître de conférence à l'INSA Rennes.

Intervenants

Amor NAFKHA
Professeur à CentraleSupélec.

Haïfa FARÈS
Maître de conférence à CentraleSupélec.

François SARRAZIN
Professeur à l'Université de Rennes.

Corentin FONTENEAU
Maître de conférence à l'INSA Rennes.

Méthodes pédagogiques

• Apports théoriques illustrés par des exemples concrets.
• Exercices pratiques avec des travaux en sous-groupe.
• Mise en situation concrète au travers d'études de cas issues de projets réels.
• Pédagogie activ.

Moyens Pédagogiques

• CS : Machine virtuelle (VM) et des cartes USRPs B205-mini.
•
• Univ Rennes 1 : Salle "Maxwell" du bâtiment 6 de l'Université pour TPs (oscilloscopes, PCs, radio-logicielles)

Modalités d'évaluation

• Auto-évaluation par quizz tout au long de la formation.
• Questionnaire de satisfaction.
• Délivrance d'une attestation de formation.

Date d'édition : 11/09/25