Semestre 1

Module **Secured Data Structure**		
	TD : 27h	Travail personnel : 43h

Le langage C reste le langage le plus utilisé dans l'IoT (au niveau de l'objet et du réseau).
Ce cours reprend les fondamentaux de la programmation en C pour aborder en détail les bonnes pratiques et les règles de développement sécurisé suivant les recommandations de l'ANSSI.

Ce cours cherche donc à renforcer la démarche « software security by design ».

Objectifs d'apprentissage

- Variables, Expression Arithmétiques
- Tableaux et fonctions
- Types, opérateurs et expressions
- Condition et contrôle des flux de donnée
- Structure des programmes
- Pointeurs et tableaux
- Structures de données
- Bonnes pratiques et développement sécurisé

Compétences visées

A l'issue de ce module l'étudiant aura une bonne compréhension des enjeux liés à la gestion de la mémoire et au développement sécurisé en langage C.

Module **AI on Chip**		
	TD : 27h	Travail personnel : 43h

On ne peut plus aujourd'hui envisager l'écosystème IoT sans aborder l'irruption de l'Intelligence Artificielle en périphérie (edge) de l'écosystème.

Ce module introduit de façon très concrète aux usages de l'IA sur l'edge, et plus particulièrement pour les usages embarqués sur les objets eux-mêmes (sur MCU ou FPGA).

Objectifs d'apprentissage

- Concepts de base
- Python pour Machine Learning et Deep Learning
- Construire des programmes intelligents
- Solution IoT multimédia intelligente
- Découvrir les "structures cachées" par l'apprentissage non supervisé
- Arm Mbed et IoT
- Raspberry Pi
- Xilinx FPGA SocC

Compétences visées

A l'issue de ce module l'étudiant sera à même de choisir le support adéquat à l'implantation d'un algorithme d'IA sur un objet, en fonction de l'usage envisagé pour la solution IoT élaborée.

Module **Cloud & virtualization techniques**		
	TD : 27h	Travail personnel : 43h

Chaque jour de plus en plus de services sont accessibles depuis le cloud.
Ce cours aborde les dernières méthodes permettant de virtualiser le développement et l'installation de programmes dans le cloud.

Le cours repose principalement sur l'environnement Docker.

Objectifs d'apprentissage

- L'utilisation de containers existants permettant d'exécuter des programmes tiers indépendamment de la machine hôte
- La création de containers et leurs compositions afin de contrôler toutes les dépendances nécessaires à l'exécution de ses propres programmes
- La persistance des données afin de contrôler les programmes mais aussi les données qui peuvent y être associées
- Le déploiement des containers en réseau ainsi que leur orchestration, selon les recommandations de l'ANSSI

Compétences visées

Ce cours vise à donner aux étudiants la compréhension des enjeux liés au développement des architectures cloud. Il leur donne les moyens d'exploiter les avantages du Cloud Computing en utilisant les toutes dernières méthodes de virtualisation. Ce cours permet également aux étudiants d'utiliser l'environnement Docker dans le développement d'un projet informatique.

La compréhension globale de ce cours permet également aux étudiants d'appréhender les enjeux de sécurité liés au déploiement de container Docker.

Module **Java/JEE Secure Coding**		
	TD : 27h	Travail personnel : 43h

Le langage Java est très utilisé dans l'IoT (cloud, passerelles…). Quant à JEE et l'architecture client/serveur, ils sont encore très répandus malgré le développement continu du Cloud.

Ce cours reprend les fondamentaux de la programmation en java SE pour aborder en détail les bonnes pratiques et les règles de développement sécurisé suivant les recommandations de l'ANSSI. Il aborde également les derniers Framework JEE et les enjeux de sécurité associés.

Ce cours vise à renforcer la démarche « software security by design » chez l'étudiant.

Objectifs d'apprentissage

Compétences visées

A l'issue de ce module, l'étudiant aura une bonne compréhension du développement sécurisé en langage Java que ce soit sur le plan local ou sur le Web.

Module **Operating Systems**		
CMO : 6h	TD : 21h	Travail personnel : 43h

Ce cours à pour but de donner une vision détaillée du rôle et du fonctionnement d'un système d'exploitation. Le cours est centré sur linux dont l'usage est très majoritaire dans toutes les couches d'un écosystème IoT.

Ce cours débouche sur l'étude des enjeux de sécurité propres à linux (intégrité, techniques de durcissement, traitement des failles matérielles – Meltdown et spectre -, …)

Objectifs d'apprentissage

- OS : objectifs et grandes lignes (abstraction matérielle, exécution de processus, principales architectures, quelques familles et Linux)
- Mémoire (adressage, stack, heap, gestion, concurrence, distribution)
- Modules (principe, architecture, points d'entrée, dépendances, phases d'insertion)
- Processus, tâches et interruptions (systèmes de traitement et calcul vs systèmes embarqués, processus et tâches, IPC, classes d'ordonnancement, interruptions, Multi-CPU, multi-cœurs, gestion de la concurrence, préemption)
- Sous-systèmes et généricité (VFS, PCI, stacks réseau, USB, Industrial IO)
- Droits d'accès et sécurité (contrôle d'accès, capabilities, RBAC, LSM et LSM stacking, intégrité, techniques de durcissement, traitement des failles matérielles Meltdown et Spectre)
- Devices et drivers
- Extensions et dérivés (Temps-réel, Android *NB : l'étude d'Android se poursuit au semestre suivant dans le module Security on Mobile Apps*)

Compétences visées

A l'issue de ce cours l'étudiant sera à même de comprendre en détail le fonctionnement de Linux pour pouvoir tout aussi bien l'utiliser que d'envisager les vulnérabilités du système et les contremesures possibles.

Module **MCU architecture & trust**		
CMO : 6h	TD : 21h	Travail personnel : 43h

Le micro-contrôleur (MCU) est l'élément central d'un objet dans l'écosystème IoT. Ce module vise à donner une bonne compréhension de leur fonctionnement.

De plus, dans l'optique de designer des architecture IoT « secure by design » il convient d'avoir une idée précise des mécanismes de sécurité existant dans l'univers des MCU.

Ce cours aborde particulièrement les micro-contrôleurs de la famille ARM, et d'étudier en détail les solutions de sécurité embarquées (ARM Truszone).

Objectifs d'apprentissage

- CPU et ISA
- Mémoire programme et données
- Accès à la mémoire (flash, RAM, …)
- Registres
- Gestion des exceptions/interruptions
- **ARM Trustzone** :
  hardware/software
  gestion mémoire
  boot sécurisé
  debug…
- MPLAB IDE
- SAM L11 MCU

Compétences visées

A l'issue de ce module, l'étudiant aura une compréhension détaillée du fonctionnement d'un MCU et des mécanismes de protection possibles sur ceux-ci.

L'étudiant sera capable de choisir un MCU (puissance, consommation, sécurité) en fonction de la solution IoT qu'il étudie.

Master Class **Introduction à la cybersécurité**		
CMO : 9h		Travail personnel : 6h

Objectifs d'apprentissage

- Vocabulaire et principes fondamentaux de la cybersécurité
- Typologie des attaques, vulnérabilités, menaces et contre-mesures
- Analyse et gestion de risques
- Acteurs de la cybersécurité
- Sécurité physique

Compétences visées

A l'issue de cette Master Class les étudiant auront une vue générale de l'écosystème de la cybersécurité (acteurs et enjeux)

Master Class **Certification et sécurité des objets connectés**		
CMO : 6h		Travail personnel : 6h

Objectifs d'apprentissage

- Etat de l'art de la certification en sécurité des Objets Connectés (Normes, en France, en UE, principaux acteurs)

Compétences visées

A l'issue de cette Master Class les étudiants auront une connaissance de l'état actuel des normes et certification en sécurité qui pèsent sur le monde des objets connectés.

Semestre 2

Module **Security on Mobile Apps**		
CMO : 6h	TD : 21h	Travail personnel : 43h

Les smartphones et les applications mobiles peuvent être considérés comme faisant parti intégrante des écosystème IoT.

Ce cours se focalise sur le système Android et se divise en deux parties, d'une part les bonnes pratiques pour le développement d'applications mobiles sur Android et d'autre part la sécurité vue depuis l'angle de l'attaquant.

Objectifs d'apprentissage

- Bonnes pratiques pour le développement d'applications mobile
- API et ressources réseau
- Identification et gestion des accès
- Vulnérabilités et exploit sur Android
- Malware et reverse engineering

Compétences visées

A l'issue de ce cours l'étudiant aura une vision de la sécurité des applications mobiles du point de vue défenseur autant qu'attaquant. Il aura donc la capacité de concevoir, planifier et réaliser le développement d'applications mobiles sécurisées.

Module **IoT, Blockchain & Trust**		
CMO : 6h	TD : 21h	Travail personnel : 43h

Ce cours aborde l'utilisation de la blockchain comme élément de confiance dans un écosystème IoT. On y discute également de l'intérêt et de la sécurité d'une architecture décentralisée dans l'IoT en réponse à différents cas d'usage.

Ce cours s'appuie essentiellement sur des applications pratiques permettant aux étudiants d'avoir une vue d'ensemble assez large de la thématique.

Objectifs d'apprentissage

- Protocole de consensus et la blockchain comme élément de confiance
- Eléments de cryptologie
- Les smart contrats
- Transmettre et stocker des données dans la blockchain
- Design et mise en œuvre d'architecture IoT décentralisée avec la blockchain
- Sécurité dans une architecture décentralisée

Compétences visées

A l'issue de ce cours l'étudiant sera capable de comprendre les avantages de l'intégration de la blockchain dans l'IoT en remplaçant le serveur centralisé par des mineurs de blockchain.
Il sera à même de comprendre les principales différences lors du choix d'une blockchain avec ou sans permission pour un cas d'utilisation IoT (sécurité alimentaire, industrie 4.0, etc.) et de mettre en place une architecture IoT décentralisée.

Module **Network Architectures**		
CMO : 12h	TD : 15h	Travail personnel : 43h

Ce module couvre l'architecture générique des réseaux (modèle OSI) dans une approche centrée sur la sécurité.

Objectifs d'apprentissage

- Types et classification des réseaux
- Modèle OSI
- Couche physique et MAC
- Couche transport
- Sécurité (Cryptographie, certificats, pare feu, IDS et IPS, VPN et SSH, DDL et TLS, outils de hack et contremesures)

Compétences visées

A l'issue de ce module l'étudiant aura toutes les connaissances pour aborder les enjeux de sécurité dans les réseaux. Il sera à même d'identifier les failles les plus communes et de proposer des contre-mesures.

Module **Mesh & Lpwan**		
CMO : 6h	TD : 21h	Travail personnel : 43h

Ce cours donne tous les éléments nécessaires (débit, portée, consommation, sécurité) au choix d'une réseau courte ou longue portée dans une architecture IoT. L'accent est mis sur les LPWAN, et notamment Lorawan de part son usage très répandu.

Objectifs d'apprentissage

- Panorama de quelques réseaux spécifiques de l'IoT :
  Zigbee, Bluetooth, Sigfox, LTE-M
- Réseau Lorawan :
  Spécifications
  Authentification et sécurité (principales vulnérabilités, cryptochips, bonnes pratiques)
  Configuration et interférences (spreading factor, puissance de transmission)
  Passerelles et serveurs d'application
  Modélisation et traitement des données (HTTP, MQTT)
  Géolocalisation

Compétences visées

A l'issue de ce module l'étudiant aura une connaissance des différents réseaux courte protée et longue protée en usage dans l'IoT. L'étudiant aura développé une expertise particulière sur le réseau Lorawan.

Module **Digital communications & Cellular networks**		
CMO : 6h	TD : 21h	Travail personnel : 43h

Ce module couvre une grande variété de normes de communications mobiles cellulaires et de dispositifs de communications actuels.

Il traite des exigences de connectivité de base, de la planification, des éléments constitutifs, de l'architecture, de la conception, de la mise en œuvre et de la performance de tous les types de réseaux cellulaires de 2G à 5G.

Tous les cas d'utilisation opérationnels et les sous-systèmes du réseau cellulaire, y compris les appareils mobiles, la connectivité, le réseau radio, le réseau de transmission et le réseau central, sont couverts en mettant l'accent sur les questions pratiques et théoriques et les enjeux de sécurité.

Objectifs d'apprentissage

- Les principes de base des technologies de la voix et des données par paquets
- Le fonctionnement des systèmes radio cellulaires
- Les différents systèmes et normes numériques
- Esquisser les composants, les éléments de réseau, les sous-systèmes et les interfaces des réseaux cellulaires
- Les principes fondamentaux, les services, l'architecture et les procédures élémentaires du GSM
- Le système universel de télécommunications mobiles 3G (UMTS)
- L'évolution à long terme 4G (LTE)
- La technologie 5G, les délais et les applications, y compris le découpage du réseau et l'IoT
- Expliquer les caractéristiques et les scénarios de sécurité des réseaux cellulaires.

Compétences visées

A l'issue de ce cours les étudiants auront une compréhension de la structure et du fonctionnement des réseaux cellulaires dans le but de les utiliser dans une architecture IoT sécurisée. Les étudiants seront en effet sensibilisés aux principales vulnérabilités de ces réseaux avec un accent mis sur la 5G et son usage massif supposé dans les architectures IoT à venir.

Master Class **Fondements de cryptologie**		
*CMO : 6h	TD	Travail personnel : 6h

Objectifs d'apprentissage

- Introduction à la cryptographie et la crypto analyse

Compétences visées

A l'issue de cette Master Class les étudiants auront une idée de la complexité des problèmes de cryptologie ainsi que des enjeux qui lui sont associés.

Semestre 3

Module **IoT Pentesting**		
CMO : 9h	TD : 18h	Travail personnel : 43h

Ce cours sur la sécurité de l'IoT expliquera le concept de l'IoT, la construction d'un écosystème IoT et ses failles de sécurité internes.

Chaque participant se formera sur une carte de vulnérabilité OpenSourced dédiée : le projet DVID (http://dvid.eu).

Ils seront en mesure d'améliorer leurs compétences pour identifier les vulnérabilités et apprendre à les éviter lors du développement ou du piratage (avec l'autorisation correspondante) d'un véritable appareil IoT.

Étant donné que le cours s'appuie sur un projet open-source, les étudiants peuvent développer leur propre formation et recevoir gratuitement toutes les informations publiées par la communauté.

Objectifs d'apprentissage

- Attaques sur le Hardware et les Firmwares
- Interactions au niveau Middleware
- Interactions au niveau du Cloud
- Méthodologie d'audit

Compétences visées

À l'issue du cours, chaque participant sera en mesure d'identifier les vulnérabilités les plus connues de l'IoT, comme le piratage des ordinateurs et des interfaces de débogage, l'analyse des échanges en cours, l'essai de compréhension du protocole utilisé et l'utilisation de quelques astuces amusantes.

Module **IoT Forensics**		
CMO : 9h	TD : 18h	Travail personnel : 43h

Ce cours explique le concept de l'IoT, la construction de l'IoT, les hypothèses et les défis de l'investigation et la meilleure approche pour analyser un système IoT et un environnement IoT (ex. : maison intelligente).

Chaque étudiant aura accès à un environnement de laboratoire hors ligne (à l'aide d'une image Docker) et à un appareil IoT en libre accès : le projet DVID (http://dvid.eu).

Parallèlement à la formation, chaque étudiant explorera le piratage de l'IoT afin de faire parler l'appareil, d'être capable d'instrumenter l'environnement IoT en interagissant avec les systèmes IoT afin de collecter des journaux et d'essayer d'établir une chronologie des événements pour une analyse future.

Étant donné que le cours s'appuie sur un projet open-source, les étudiants peuvent développer leur propre formation et recevoir gratuitement toutes les informations publiées par la communauté.

Objectifs d'apprentissage

- Ecosystème et taxonomie IoT
- Menaces et modèle forensic
- Hacking dans l'écosystème IoT
- Outils et Framework pour le forensic IoT
- Analyse forensic IoT

Compétences visées

Après avoir suivi le cours, chaque étudiant sera en mesure de choisir la meilleure approche technique et organisationnelle pour l'analyse d'un environnement IoT, qu'il s'agisse des informations stockées par les appareils ou de la corrélation des événements provenant de plusieurs appareils IoT (ex. : maison intelligente). Chaque étudiant sera en mesure de mener une enquête et de veiller à ne pas compromettre involontairement les preuves.

Module **IoT Security Architecture**		
CMO : 9h	TD : 21h	Travail personnel : 40h

Ce cours reprend et synthétise tous les éléments d'une défense en profondeur d'une architecture IoT.

Objectifs d'apprentissage

- OWASP 18 IoT Security Threats Report
- Sécurité des objets (Boot sécurisé, mise à jour de firmware, stockage sécurisé modèle ARM PSA)
- Sécurité des passerelles (sniffing – SNORD IDS, dictionnaire d'attaque - Fail2ban, Privilege escalation.)
- Sécurité du Cloud (AWS IoT Key Security Features)
- Pentesting IoT (cycle de vie, vulnérabilités Web et sur applications mobiles, scan réseau et contremesures)
- Threat Modeling (définition d'une solution IoT, design du schéma réseau, modélisation des risques, identification des menaces et proposition de contre-mesures, analyse et rédaction d'une rapport de sécurité)

Compétences visées

A l'issue de ce module l'étudiant doit être capable de créer totalement une solution IoT « secure by design » autant que d'envisager l'audit d'une architecture IoT.

L'étudiant doit pouvoir mettre en évidence les vulnérabilités d'une architecture IoT tout en proposant les contre-mesures nécessaires pour sécuriser celle-ci et rédiger un rapport de sécurité.

Module **Edge AI**		
CMO : 9h	TD : 18h	Travail personnel : 43h

Dans le cadre de l'étude de l'impact de l'intelligence artificielle en périphérie (edge) des écosystèmes, ce module couvre l'implémentation d'algorithmes d'intelligence artificielle (IA) sur une plateforme matérielle reconfigurable basée sur un circuit numérique programmable : Field Programmable Gate Arrays (FPGAs). La méthodologie de conception est basée sur un langage de description de matériel VHSIC (VHDL).

Ce module est destiné aux étudiants avancés qui ont une première expérience des algorithmes d'IA.

Objectifs d'apprentissage
Principaux sujets :
- Aperçu d'un accélérateur matériel général pour les applications d'IA : FPGA, ASIC, GPU
- Outils matériels et logiciels (carte FPGA, Vivado)
- Flux de développement
- Code VHDL
- Contrôleurs de modules périphériques
- Projets : Algorithmes d'IA basés sur FPGA pour les véhicules autonomes ou les robots mobiles

Compétences visées
- Développer des algorithmes d'IA en considérant une implémentation matérielle.
- Convertir un algorithme d'IA en description de circuit numérique
- Simuler une description VHDL pour vérifier que la conception correcte.
- Implémenter des algorithmes d'IA sur une carte FPGA.

Module **Privacy & Security Management**		
CMO : 30h		Travail personnel : 40h

Durant ce cours sont abordés les différents modules d'un SMSI, y compris la politique SMSI, les procédures, la mesure de la performance, l'engagement de la direction, l'audit interne, la revue de la direction et l'amélioration continue.

Après avoir suivi ce cours, les étudiants peuvent se présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27001 Foundation ».

Ce cours montre également les liens entre ISO 27001 et le RGPD.

Objectifs d'apprentissage
- Comprendre les éléments et le fonctionnement d'un Système de management de la sécurité de l'information
- Comprendre la corrélation entre la norme ISO/CEI 27001 et ISO/CEI 27002 ainsi qu'avec d'autres normes (RGPD) et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management de la sécurité de l'information

Compétences visées

A l'issue de ce cours, les étudiants pourront appréhender les éléments fondamentaux pour mettre en œuvre et gérer un Système de Management de la sécurité de l'information, selon la norme ISO 27001.
L'étudiant sera également à même de mettre le RGPD en perspective avec ISO 27001.

Module **Cyber risk and resilience**		
CMO : 18h	TD : 12h	Travail personnel : 40h

Ce cours adresse l'étude et la gestion des risques cyber et envisage également les enjeux de la cyber résilience.

Grâce aux exercices pratiques et aux études de cas, les étudiants vont acquerir les connaissances et les compétences nécessaires pour :

- Réaliser une appréciation optimale des risques liés à la sécurité de l'information
- Gérer les risques dans les temps par la connaissance de leur cycle de vie.
- Envisager des procédures de résilience

Ce cours s'inscrit parfaitement dans le cadre d'un processus de mise en œuvre de la norme ISO/CEI 27001. A l'issue de ce cours les étudiants pourront se présenter à l'examen et faire une demande de certification « PECB Certified EBIOS Risk Manager ».

Objectifs d'apprentissage

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Comprendre les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés
- Acquérir les compétences nécessaires afin de mener une étude EBIOS
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme
- Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS
- Comprendre la nécessité et savoir envisager des solutions de cyber résilience

Compétences visées

A l'issue de ce cours, l'étudiant maîtrisera les concepts et les éléments de management des risques liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la méthode EBIOS.
Il pourra également envisager des mécanismes de cyber résilience associés aux risques identifiés.

Exercice immersif de gestion de cyber crise		
		Travail personnel : 6h

Cet exercice réaliste vise à mettre les étudiants en situation de « confrontation » avec une situation à enjeux, faisant intervenir des aspects émotionnels concrets et un stress réel.

Objectifs d'apprentissage

- Gestion de crise

Compétences visées

A l'issue de cet exercice, les étudiants devraient être parfaitement conscients de l'importance des exercices les plus réaliste possibles dans l'entrainement à la gestion de crise.