Syllabus de la Filière CyberSécurité

ESIEE PARIS

Université Gustave Eiffel

Introduction

ESIEE Paris est une École d'ingénieur en 3 ans (recrutement en classe préparatoire, en licence, en DUT, en BTS) ou 5 ans (recrutement rpsè le bac) spécialisée dans les domaines de l'informatique, de l'électronique, de l'énergie et de l'e-santé. Au cours des deux dernières de sa formation, l'étudiant est invité à choisir une filière parmi les spécialités enseignées au sein de l'école ; la filière Cybersécurité est l'une d'elles. L'objectif du présent document est de décrire l'organisation et les différentes unités d'enseignement de cette filière.

Les années de formation sont notées de E1 à E5, y compris pour les étudiants intégrant l'école en 3ème ou en 4ème année. Pour les 4ème et 5ème années (celles concernant les filières), l'année est divisée en deux semestres, le S1 allant de septembre à janvier et le S2 allant de février à juillet. Le premier semestre de chaque année est lui-même divisé en deux périodes, le P1 de septembre à octobre et le P2 de novembre à janvier. Le second semestre de la première année est aussi divisé en deux périodes, la première (de février à avril) étant dédiée aux cours et la seconde (de mai à juillet) à un stage de 3 mois en entreprise. Les unités d'enseignement ayant lieu sur la première période sont identiées E4/S2. Le second semestre de la deuxième année est intégralement consacré à un stage de 6 mois en entreprise. Les deux stages en entreprise font l'objet d'un rapport et d'une présentation individuels chacun.

Les unités d'enseignement sont regroupées autour de quatre thèmes (Systèmes d'information, Systèmes d'exploitation, Réseaux, et Logiciel et matériel). Les unités d'enseignement des trois premiers thèmes sont obligatoires et spécifiques à la filière Cybersécurité. Les unités d'enseignement du thème « Logiciel et matériel » peuvent être suivies par des étudiants d'autres filières. Elles sont aussi obligatoires pour les étudiants de la filière Cybersécurité.

En 4ème année, les étudiants doivent réaliser en groupe de 4 à 6 un projet d'une durée d'environ 120 heures présentielles sur la période allant de septembre à avril. Ces projets ont pour objectif une activité de développement et/ou de recherche et être proposés soit par les enseignants-chercheurs d'ESIEE Paris, soit par des industriels. Un rapport et une soutenance collectifs sont attendus avant le départ en stage.

Thierry Grandpierre et Éric Renault
Responsables de la filière Cybersécurité à ESIEE Paris

Thème 1

Systèmes d'information

1.1 Normes, Certifications et Gestion des identités

Code module : CYB-4101A
Période : E4 / S1 / P1
Intervenant(s) : Christophe Maudoux
Durée : 30 heures

Objectifs pédagogiques

- Maîtriser la norme ISO 27001 afin de comprendre comment implémenter un SMSI
- Connaître les concepts de base du contrôle d'accès (droits d'accès, comptes, etc.)
- Connaître les modèles de contrôle d'accès les plus représentatifs

Description

Les compétences acquises au cours de ce module sont la maîtrise de la norme ISO 27001 et la capacité à réaliser des analyses de risques cyber avec ISO 27005.

Dans un premier temps, le cours s'attache à présenter les différents normes dans un cadre théorique, puis de nombreuses études de cas sont réalisées afin d'appliquer les normes vues en cours à des cas concrets. Les enseignements sont répartis en 2/3 de cours et 1/3 de travaux pratiques.

Le module est évalué en fin de période sous la forme d'un examen écrit.

Séquencement

Séance	Cours	Pratique
Introduction sur l'ensemble des normes 27000	2 h	
Normes ISO 27005	4 h	
Méthodologie	2 h	
Compréhension des étapes de l'analyse de risques	2 h	
Etude des cas Analyse de risques avec EBIOS		2 h
Normes ISO 27001 et 27002	6 h	
Exercices Mesures de sécurité et KPI		2 h
Rédaction politiques de sécurité	4 h	2 h
Etude de cas ISO 27001		2 h
Préparation à l'examen		2 h
Totaux	**20 h**	**10 h**

Bibliographie

[1] https ://www.ssi.gouv.fr/entreprise/managementdurisque/lamethodeebiosriskmanager/

[2] https ://www.youtube.com/watch ?v=JnrjEqtAElo

oOo

1.2 Sécurité des Systèmes d'Information

Code module : CYB-4201A
Période : E4 / S1 / P2
Intervenant(s) : Sébastien Delcros et Lionel Bour
Durée : 30 heures

Objectifs pédagogiques

— Donner une vision à 360^o des différents aspects composant la sécurité d'un système d'information

— Comprendre les enjeux auxquels sont confrontés les différents décideurs au sein des entreprise

— Fournir des repères méthodologies pour évaluer les risques et concevoir des systèmes sécurisés

Description

Avec ce cours, les étudiants peuvent appréhender les enjeux de la Sécurité du SI dans les entreprises. Il leur permettra de disposer d'une bonne vision d'ensemble du SI, de ses composantes et de leurs spécificités en matière de sécurité, de connaitre les principales menaces et les méthodes d'évaluation du risque, de savoir intégrer la dimension Sécurité dans les travaux de conception d'un système et de connaitre une norme de référence à

laquelle un grand nombre d'entreprises est confrontée : la norme de sécurité PCI-DSS relative aux transactions CB.

Le module est essentiellement composé de séances de cours magistraux au cours desquels des professionnels de la cybersécurité viennent présenter une problématique liée à la sécurité des systèmes et les moyens mis en œuvre afin de les protéger.

L'évaluation du module est réalisé sous la forme d'une étude de cas à réaliser en une heure.

Séquencement

Séance	Cours	Pratique
Qu'est-ce que la sécurité d'un SI	2 h	
Méthodologie pour la conception de systèmes fiables	4 h	
Sécurité des infrastructures (part. 1)	4 h	
Sécurité des infrastructures (part. 2)	4 h	
Sécurité des middleware et des architectures applicatives	4 h	
Sécurité de l'environnement utilisateur	4 h	
Initiation aux aspects réglementaires	4 h	
Méthodologie de défense	4 h	
Totaux	**30 h**	

oOo

1.3 Cyber Défense et Attaque

Code module : CYB-4301A
Période : E4 / S2
Intervenant(s) : Cyril Gayet
Durée : 30 heures

Objectifs pédagogiques

— Comprendre le fonctionnement des cyberattaques
— Mettre en œuvre des exploitations de vulnérabilités

Description

Ce module vise à présenter aux étudiants comment utiliser les principaux outils permettant d'exploiter des vulnérabilités systèmes et applicatives. Les investigations numériques permettent de comprendre le fonctionnement de la mémoire, d'en extraire des contenus et de manipuler des traces réseaux.

Après un rappel sur la sécurité des SI et quelques aspects réglementaires, les séances sont organisées autour de cas concrets d'attaques cyber, que ce soit du côté Blueteam ou Redteam.

L'évaluation du module est réalisée au moyen d'un mini-projet et d'un rapport.

Séquencement

Séance	Cours	Pratique
Mise à niveau SSI et aspects réglementaires	4 h	
Cyberattaque : Découverte et manipulation des techniques d'attaque sur le principe du CTF (*Capture The Flag*)		2 h
Redteam : découverte des outils		4 h
Redteam : premiers CTF		4 h
Redteam : CTF niveau facile		4 h
Redteam : CTF niveau intermédiaire		4 h
Cyberdéfense : Investigation numérique permettant de retrouver les traces d'une attaque et comprendre son fonctionnement		
Blueteam : introduction à l'investigation numérique		4 h
Blueteam : investigations numériques de la mémoire		4 h
Totaux	**4 h**	**26 h**

oOo

1.4 Sécurité Cloud

Code module : CYB-5101A
Période : E5 / S1 / P1
Intervenant(s) : Mawloud Omar
Durée : 30 heures

Objectifs pédagogiques

— Étudier les plateformes de type *cloud*
— Être capable d'administrer leurs différents services de sécurité

Description

Ce module focalise sur la gestion de la sécurité des plateformes de type *cloud*. À titre pédagogique, le contenu est piloté par l'étude de la plateforme d'AWS (*Amazon Web Services*). Elle aborde les services de sécurité les plus répandus, à savoir la gestion d'identités et de clés, l'administration de *clouds* privés virtuels, l'audit et la sécurité de serveurs et d'applications.

Le volume se répartie en 40% pour les cours et 60% pour les travaux pratiques. La partie pratique se fait sur des énoncés de TP très bien orientés en abordant l'administration des services de sécurité par la console, le *shell* CLI d'AWS, et aussi par la programmation à travers les API offerts par AWS.

Séquencement

Séance	Cours	Pratique
Introduction aux architectures du Cloud computing et à AWS	2 h	2 h
Gestion d'identités et de privilèges via le service IAM sous AWS	2 h	2 h
Gestion de clés via le service KMS sous AWS	2 h	2 h
Administration de cloud privé virtuel via le service VPC sous AWS	2 h	3 h
Audit et sécurité des serveurs et des applications sous AWS	4 h	3 h
Etude de Google Cloud Platform/Azure		6 h
Totaux	**12 h**	**18 h**

Bibliographie

[1] Albert Anthony. *Mastering AWS Security : Create and maintain a secure cloud ecosystem*. Packt Publishing Ltd., 2017.

[2] Heartin Kanikathottu. *AWS Security Cookbook : Practical solutions for managing security policies, monitoring, auditing, and compliance with AWS*. Packt Publishing Ltd., 2020.

oOo

1.5 Criminaliste en Cybersécurité & Analyse Post-Mortem

Code module : CYB-5201A
Période : E5 / S1 / P2
Intervenant(s) : Jean-Baptiste Vaillant
Durée : 30 heures

Objectifs pédagogiques

— Être capable d'extraire des traces d'activité sur un poste ou un serveur windows
— Savoir analyser un exécutable malveillant basique et un système de fichiers

Description

Le module Criminaliste Cyber & Analyse Post Mortem vise à apporter aux étudiants le bagage technique et la méthodologie nécessaires à la pratique d'activités de forensique digitale et de gestion de crise cyber. A l'issue de cet enseignements, les étudiants sont capables d'extraire des traces d'activité sur un poste ou un serveur windows à travers les différents artefacts, d'analyser un exécutable malveillant basique, d'analyser un système de fichier, et disposent d'une culture de la menace cyber obtenue à travers une introduction à la "Threat Intelligence" et aux modes opératoires APT (Advanced Persistant Threat : attaques ciblées avancées).

À l'issue des interventions, les étudiants sont confrontés à une mise en situation où ces derniers doivent remonter les traces d'un attaquant sur un environnement d'entreprise factice ayant subi une cyber attaque d'envergure.

L'évaluation est effectuée sur la base d'un rapport de TP.

Séquencement

Séance	Cours	Pratique
Techniques offensives et enjeux de l'environnement Active Directory	4 h	
Sécurité d'un poste de travail et extraction de traces système	3 h	
Analyse d'un système de fichiers compromis ou corrompu	3 h	
Analyse de Malware / Reverse Engineering	3 h	
Analyse de mémoire vive	3 h	
Méthodologie légale de réponse à incident, acquisitions de disque	3 h	
Etude des profils de groupes d'attaquants	3 h	
Les étudiants sont confrontés à un environnement d'entreprise factice compromis et doivent remonter les traces de l'attaquant en extrayant et en analysant les différentes sources d'événements présentées lors du module		8 h
Totaux	**22 h**	**8 h**

Thème 2

Systèmes d'exploitation

2.1 Sécurité Système Exploitation Windows/Linux

Code module : CYB-4101B
Période : E4 / S1 / P1
Intervenant(s) : Nicolas Grenêche
Durée : 30 heures

Objectifs pédagogiques

- Concevoir / Analyser les architectures systèmes sécurisées
- Mettre en œuvre de façon pratique certains mécanismes de protection systèmes
- Manipuler des systèmes d'authentification SSO type Kerberos
- Manipuler une méthode d'isolation de processus type LXC

Description

Dans le cadre de ce module, les étudiants peuvent appréhender les principaux mécanismes de sécurité systèmes des environnements Linux et Windows.

La première partie est consacrée à des cours magistraux illustrés par des manipulations que les étudiants doivent refaire sur leur machine. Ensuite, des TP complètent le cours avec des zooms sur certains points théoriques approfondis pendant les séances. Enfin, un mini-projet est proposé et soutenu durant la dernière demi-journée.

La note du module est celle attribuée pour la réalisation et la présentation du mini-projet.

Séquencement

Séance		Cours	Pratique
Terminologie et rappels		2 h	
Sécurité des processus par DAC		2 h	
Confinement de processus		2 h	
Authentification (AAA)		2 h	
Durcissement d'OS		2 h	
Manipulation de conteneurs			4 h
Test d'intrusion (systeme)			6 h
Authentification Kerberos Windows / Linux			6 h
Mini-projets			4 h
	Totaux	**10 h**	**20 h**

Bibliographie

[1] Robert Love. *Linux Kernel Development.*

[2] *Windows Internals – Part 1 : System architecture, processes, threads, memory management, and more*

[3] Jason Garman. *Kerberos : The Definitive Guide*

oOo

2.2 Sécurité Système Exploitation Smartphones

Code module : CYB-4201B
Période : E4 / S1 / P2
Intervenant(s) : Dominique Ragot
Durée : 30 heures

Objectifs pédagogiques

— Comprendre l'architecture et les composants du système Android
— Étudier les failles du système et réduire leur surface d'attaque
— Les mécanismes permettant de sécuriser les communications sous Android

Description

Ce module est essentiellement composé de cours magistraux présentant les spécificités de la sécurité sur les smartphones, les attaques possibles et les moyens de s'en protéger.

L'évaluation du module s'effectue par l'intermédiaire d'un examen écrit de deux heures en fin de période.

Séquencement

Séance	Cours	Pratique
Android : généralités, architecture et composants	4 h	
Sécurité : terminologie, normes courantes, applicabilité à Android, exemples de failles, éléments de sécurité	2 h	2 h
Applications Android et sécurité : développement, mise à jour, publication, déploiement, interactions système	1,5 h	1,5 h
Mécanismes de sécurité d'Android : permissions, IPC, Binder, Intents, partitions, durcissement, chiffrement, authentifications, gestion de clés, TEE, boot.	4 h	
Etude de faille : Stagefright, détection correction. Mécanismes ALSR et stack-protector, réduction de surface d'attaque.	1 h	3 h
Mise en oeuvre d'Android Studio, application au suivi d'une faille récente (différente chaque année). Cybersécurité et protection de la vie privée	1 h	2 h
Sécurité des communications : Wifi, Bluetooth, 2G/3G/4G, Bluetooth, NFC, USB, GPS. Sécurisations renforcées : 2 facteurs, VPN, chiffrement. Offres de service intégrées, Sécurisations complémentaires à Android : containers, isolation, HSM. Smartphones sécurisés	4 h	
Techniques avancées : Trustzone, Virtualisation. Cyber-attaques. Environnements d'exécution d'applications sécurisées. Utilisation professionnelle, BYOD, CYOD, EMM. Domaines critiques : santé, automobile. Aspects conjoints sécurité et sureté de fonctionnement. Interactions avec IoT. Attaques IoT, Bluetooth et 4G. Solutions dérivées/alternatives à Android	4 h	
Totaux	**21,5 h**	**8,5 h**

oOo

2.3 Sécurité Systèmes Exploitation Virtualisés

Code module : CYB-4301B
Période : E4 / S2
Intervenant(s) : Akos Barrin
Durée : 30 heures

Objectifs pédagogiques

— Comprendre les concepts d'émulation et de virtualisation
— Étudier les failles ayant récemment été découvertes
— Savoir gérer un *pool* de ressources et en connaître les risques

Description

Le module est essentiellement composé de séances de cours. Dans un premier temps, les concepts liés à l'émulation et la virtualisation sont présentés, suivi des problèmes liés à la gestion d'un *pool* de ressources, en particulier en terme de sécurité, et les moyens devant être mis en œuvre afin de les protéger.

L'évaluation du module est réalisée au moyen d'un examen écrit.

Séquencement

Séance	Cours	Pratique
Présentation, révision des concepts d'architectures physique et système d'un ordinateur	2 h	
Présentation et évolutions historiques des notions d'émulation et de virtualisation	4 h	
Premières réflexions sur les risques structurel des concepts de virtualisation	3 h	
Études de risques associées avec les exemples des failles de l'année	3 h	1 h
La gestion des *pools* de ressources et les risques liés	4 h	
Vision globale, comment traiter la virtualisation dans un monde matériel. Exercices pratiques d'études de risques impliquant notions techniques locales et environnementales.		3 h
Mise en avant du facteur humain. de l'importance des politiques de sécurités	4 h	
Remise en question de nos connaissances, de la théorie au contexte d'entreprise	3 h	
Examen	3 h	
Totaux	**26 h**	**4 h**

oOo

2.4 Développement Logiciel Sécurisé

Code module : CYB-5101B
Période : E5 / S1 / P1
Intervenant(s) : Dominique Ragot et Sébastien Delcros
Durée : 30 heures

Objectifs pédagogiques

- Être capable de sécuriser les applications serveur développées en JAVA et en .NET
- Connaître le fonctionnement des bases de données sécurisées
- Appréhender un environnement de développement global (*Software factory*)
- Maîtriser le cycle de vie d'un projet en étudiant les liens avec le management
- Être capable de concevoir des applications sécurisées sur Android

Description

Ce module est composé de deux parties.

La première partie focalise sur le noyau Android. Elle étudie les mécanismes de sécurisation, les principes de sécurisation, le *sandboxing* applicatif, la séparation des applications, les smartphones sécurisés, la messageries sécurisées, les processus de développement sécurisé sur Android, la conception sécurisée, la variabilité matérielle et logicielle d'Android, les outils et la protection des accès.

Il aborde ensuite deux points importants de la cybersécurité :

— Pourquoi sécuriser ? Que ce soit du point de vue i) de l'utilisateur, ii) du fournisseur de services (par exemple une banque), ou iii) du fournisseur de smartphones (réputation) ;

— Comment sécuriser ? Pour cela, le module aborde le principe de la conception avec contraintes de sécurité, le développement, la distribution, les mises à jour, la post-distribution, le retrait, le remplacement et les bonnes pratiques (OWASP, cheklist).

Cette partie étant complétée par l'étude des obligations légales ou réglementaires (RGPD, US DoJ, ...) et des émulations d'attaque sur une base de données Oracle et/ou MySQL avec le cas particulier de l'étude des injections SQL.

Le module est validé par la réalisation d'une étude de cas.

Séquencement

Séance	Cours	Pratique
Sécurisation des applications Android	18 h	
Sécurisation des applications JAVA et .NET	12 h	
Totaux	**30 h**	

oOo

2.5 IA pour la Sécurité

Code module : CYB-5201B
Période : E5 / S1 / P2
Intervenant(s) : Mawloud Omar
Durée : 30 heures

Objectifs pédagogiques

— Connaître les principaux outils d'ingénierie de données et d'intelligence artificielle

— Être capable de mettre en place des solutions de prédiction d'attaques

Description

Ce module aborde les techniques d'apprentissage automatique pour la conception et la mise en place des solutions de cybersécurité. L'unité est répartie entre 40% de cours

et 60% de travaux pratiques. La partie pratique se fait sur des énoncés de TP très bien orientés en abordant plusieurs types d'applications, à savoir la détection de phishing, détection de malwares, détection d'intrusions, et un problème ouvert de cybersécurité. Ces applications sont à réaliser par différentes techniques d'apprentissage sous divers outils tels que Weka et Sklearn de Python.

Séquencement

Séance	Cours	Pratique
Introduction à l'intelligence artificielle	4 h	
Outils d'analyse de données et d'apprentissage automatique	4 h	
Application 1 : détection de phishers par l'apprentissage automatique (Weka)		4 h
Application 2 : détection des malwares par l'apprentissage automatique (Python)		4 h
Apprentissage approfondi	2 h	
Application 3 : détection d'intrusions par l'apprentissage approfondi		4 h
Application 4 : étude d'un problème ouvert de cybersécurité		4 h
Totaux	**12 h**	**18 h**

Bibliographie

[1] Soma Halder and Sinan Ozdemir. *Hands-On Machine Learning for Cybersecurity Safeguard your system by making your machines intelligent using the Python ecosystem*. Packt Publishing Ltd., 2018.

[2] Emmanuel Tsukerman. *Machine Learning for Cybersecurity Cookbook*. Packt Publishing Ltd., 2019.

Thème 3

Réseaux

3.1 Complément de système d'exploitation Linux

Code module : CYB-4102C
Période : E4 / S1 / P1
Intervenant(s) : Éric Renault
Durée : 30 heures

Objectifs pédagogiques

— Aller plus loin dans la compéhension du système d'exploitation Linux
— Compréhension du fonctionnement des éléments fondamentaux du système

Description

Le module est organisé autour de sept séances de quatre heures de cours/TP dont la première partie d'environ une heure consiste en une présentation académique des concepts abordés pendant la séance et la seconde partie est un TP très orienté (un grand nombre de petites questions) permettant à l'étudiant d'expérimenter et de s'approprier directement par la pratique les concepts abordés en début de séance. Les deux dernières heures sont consacrées à une séance de questions sur des points du système que les étudiants voudraient aborder et à la terminaison des TP.

L'ensemble des séances est étalé sur une période de trois semaines maximum afin de favoriser au maximum l'immersion de l'étudiant dans le domaine.

L'évaluation est réalisée sous la forme d'un examem écrit d'une heure.

Séquencement

Séance	Cours	Pratique
Le fonctionnement du système de fichiers Unix. Les notions d'utilisateur, de groupe, de droit d'accès et d'i-noeud sont abordées, ainsi que la différence entre lien physique et symbolique.	1 h	3 h
Les redirections et des tubes ainsi que leur utilisation dans l'interpréteur de commandes.	1 h	3 h
La gestion des processus au niveau utilisateur. L'interpréteur de commandes et les structures (tests, boucles, etc.) présentes. La substitution de commandes. Programmation de *scripts*.	1 h	3 h
Création et gestion des processus en langage C.	1 h	3 h
Création, gestion et utilisation des tubes et des signaux en langage C.	1 h	3 h
Les IPC (*Inter-Process Communication*). Création, utiliation et gestion, en langage C et dans l'interpréteur de commandes.	1 h	3 h
Les appels systèmes sous Unix. Principe de fonctionnement et manipulation. Mécanisme permettant de les intercepter.	1 h	3 h
Finalisation des TP et séance de questions et/ou approfondissement des points abordés pendant le cours.		2 h
Totaux	**7 h**	**23 h**

oOo

3.2 Audit et Sécurité des Réseaux Locaux

Code module : CYB-4201C
Période : E4 / S1 / P2
Intervenant(s) : Nicolas Greneche
Durée : 30 heures

Objectifs pédagogiques

— Concevoir des architectures réseau sécurisée
— Sensibiliser aux méthodes de découverte des services réseaux
— Mettre en place une politique d'instrumentation réseau orientée sécuritée

Description

À l'issue de ce module, les étudiants ont une connaissance approfondie des systèmes de protections réseau (IDS, IPS, Pare-feux), de l'isolation et de la segmentation de réseaux (VLAN). Ils acquièrent aussi une capacité à prendre en main les outils basiques d'attaques réseaux et à gérer les certificats.

La première partie est consacrée à des cours magistraux illustrés par des manipulations que les étudiants doivent refaire sur leur machine. Ensuite, des TP complètent le cours

avec des zooms sur certains points théoriques approfondis pendant les séances. Enfin, un mini-projet est proposé et soutenu durant la dernière demi-journée.

La note du module est celle attribuée pour la réalisation et la présentation du mini-projet.

Séquencement

Séance	Cours	Pratique
Rappels sur les notions essentielles à la sécurité (DNS, ARP, IP etc.)	2 h	
Introduction au Network Security Monitoring (NSM)	2 h	
Analyse de Flux	1 h	
Intrusion Detection System	1 h	
Protection réseau	2 h	
Concevoir des architéctures réseau (toplogie, segmentation et filtrage)	2 h	
Mise en place d'un réseau complet avec mécanismes d'audit et de filtrage		10 h
Introduction au SDN via la mise en place d'un infrastructure Kubernetes		6 h
Mini-projet		4 h
Totaux	**10 h**	**20 h**

Bibliographie

[1] Richard Bejtlich. *The Practice of Network Security Monitoring.*

[2] Kozierok Charles. *The TCP/IP Guide – A Comprehensive, Illustrated Internet Protocols Reference*

oOo

3.3 Audit et Sécurité des Réseaux Opérateurs

Code module : CYB-4301C
Période : E4 / S2
Intervenant(s) : Pascal Foucher
Durée : 30 heures

Objectifs pédagogiques

— Connaître l'architecture des réseaux radio mobile et leurs spécificités techniques

— Mettre en perspective les différentes normes et les services supportés

— Aborder les stratégies de sécurité déployées sur ces réseaux

Description

Le module présente l'architecture des réseaux radio mobile et leurs spécificités techniques (fréquences, modulation, multiplexage). Il met en perspective les différentes normes et les services supportés. Les stratégies de sécurité déployées sur lesdits réseaux sont aussi abordés.

Le module se termine par une épreuve écrite.

Séquencement

Séance	Cours	Pratique
Introduction	4 h	
2G - GSM	4 h	
2,5G - GPRS / EDGE	4 h	
3G - UMTS	4 h	
4G / 4G-LTE / LTE Advanced	4 h	
Stratégies de sécurité dans les réseaux radio mobile	4 h	
Normes et services	4 h	
Examen	2 h	
Totaux	**30 h**	

Bibliographie

[1] André Perez. *Architecture des réseaux de mobiles : GSM/GPRS, UMTS/HSPA, EPS, NGN, IMS*. Lavoisier.

[2] Moray Rumney. *LTE and the Evolution to 4G Wireless : Design and Measurement Challenges*. Wiley.

oOo

3.4 Sécurité IoT : Communications & Systèmes

Code module : CYB-5101C
Période : E5 / S1 / P1
Intervenant(s) : Carlos Pinto
Durée : 30 heures

Objectifs pédagogiques

— Être capable de sécuriser les communications reposants sur les principaux standards actuels

— Être capable de prendre en charge les problèmes de sécurité dans le cycle de vie d'un produit

— Savoir rédiger un rapport d'analyse de risque

Description

Le module commence par la présentation d'un état de l'art des solutions IoT : LoRA, LTE-MTC, SigFox. Il introduit ensuite la définition de ce qu'est un produit et poursuit par l'étude du cycle de développement d'un produit et l'évaluation des produits de sécurité. La méthode EBIOS est ensuite étudiée en vue de la rédaction d'une analyse de risque.

Le cycle de développement de sécurité est le suivant :

1. Management : OBS et WBS,
2. Revue avec ISO15288.1 et ISO15288.2
3. Spécification et traçabilité : outil ReqChecker
4. Analyse fonctionnelle et Dossier de Justification des choix de conception : outil Capella
5. Vulnérabilité commune : CVE
6. Vérification de règle de codage : CppTest, RATS, CppChecker
7. Analyse statique : option de compilation avec GCC, CLANG
8. Preuve formelle : outil Frama-C
9. Test : outil Cunit, Fuzzing AFL

Le module se termine sur la présentation des mécanismes de sécurité des protocoles IoT, ainsi qu'un état de l'art sur SDN et NFV, des mécanismes de sécurité dans le contrôleur SDN et l'orchestrateur NFV.

Séquencement

Séance	Cours	Pratique
État de l'art des solutions IoT : LoRA, LTE-MTC, SigFox	4 h	
Mécanismes de sécurité des protocoles IoT	8 h	
Processus de développement de sécurité	8 h	
Outils de développement : Test Unitaire (cunit), Fuzzing (afl), Frama-C, Jenkins, gcc, clang, Klocwork		10 h
Totaux	**20 h**	**10 h**

oOo

3.5 Sécurité Réseaux Avancés

Code module : CYB-5201C
Période : E5 / S1 / P2
Intervenant(s) : Abdelkader Outtagarts et Christian Hadja
Durée : 30 heures

Objectifs pédagogiques

— Comprendre le principe de fonctionnement de la Blockchain
— Être en capacité de la déployer
— Savoir sécuriser un système virtualisé

Description

Le module est décomposé en deux grandes parties :

1. Blockchain : l'objectif est de non seulement poser les bases théoriques de la Blockchain mais aussi de donner les compétences nécessaires afin que chaque étudiant soit capable de répondre à un besoin ou problème à travers une solution Blockchain qu'il sera capable de mettre en place ;
2. Virtualization : après un rappel des concepts de base sur la sécurité et les différents outils d'audit sécurité, le cours se focalisent sur la sécurité des systèmes virtualisés : containers, orchestrateurs. Les TPs mettrons l'accent sur la sécurité deKubernetes et des containers. Se cours aborde aussi la 5G dans la mesure ou beaucoup de composants de la 5G sont virtualisés et utilisent les containers et des orchestrateurs.

Séquencement

Séance	Cours	Pratique
Blockchain	11 h	4 h
Sécurité des systèmes virtualisés	10 h	5 h
Totaux	**21 h**	**9 h**

Thème 4

Logiciel et matériel

4.1 Cryptographie

Code module : OUAP-4113
Période : E4 / S1 / P1
Intervenant(s) : Laurent Perroton
Durée : 30 heures

Objectifs pédagogiques

— Étudier la sécurité des systèmes d'information à travers les techniques et algorithmes classiques de la cryptographie

Description

Ce module vise à introduire la sécurité des systèmes d'information à travers les techniques et algorithmes classiques de la cryptographie. On s'intéressera notamment aux aspects d'implémentation de ces algorithmes d'un point de vue logiciel mais aussi matériel.

L'évaluation du module est réalisée pra l'intermédiaire de rapports de TP et de devoirs.

Séquencement

Séance	Cours	Pratique
APP : Introduction à la sécurité des systèmes d'information Principes de la Sécurité des Systèmes d'Information Évaluation de la sécurité d'un système		2 h
Chiffrement asymétrique APP : Etude de RSA Aspects mathématiques : arithmétique modulaire Implémentations et failles Attaque par factorisation		4 h
APP : Génération de nombres aléatoires, LFSR Chiffrement symétrique TP : Attaque de DES par force brute APP : AES ; arithmétique dans les corps de Galois Étude de l'algorithme APP : Modes opératoires		10 h
Principe de cryptographie : Authentification, Intégrité Intégrité, fonctions de Hachage, Authentification, Signature	4 h	
Notion de PKI (Public Key Infrastructures) Certificats X509 et notions de PKI	2 h	
Sécurité des réseaux	2 h	
Application Logicielle Application de la boite à outils OpensSSL au chiffrement, hachage, authentification Manipulation des certificats X509 avec OpenSSL, protocole SSL et sécurisation d'un serveur www en SSL		6 h
Totaux	**8 h**	**22 h**

Bibliographie

[1] Bruce Schneier. *Cryptographie appliquée*. Vuibert.

[2] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, October 199.

[3] A. Exertier. *SSI Web site — cryptographie* : http ://intra.esiee.fr/ exertiea/Unites/OV5_SSI/index.html .

oOo

4.2 Architecture des ordinateurs

Code module : OUAP-4217
Période : E4 / S1 / P2
Intervenant(s) : Xavier Renault
Durée : 30 heures

Objectifs pédagogiques

— Adresser la problématique de l'architecture des ordinateurs, et l'impact sur le logiciel
— Comprendre l'impact d'un choix de design matériel sur toute la chaîne du produit

Description

Le module présente l'architecture interne d'un ordinateur, la gestion des périphériques, les principes de la compilation, la génération et l'exécution du code assembleur x86 depuis du code écrit en C, les principes de gestion des caches, de la MMU et des tables d'adressage, les séquences de *boot* d'un ordinateur. Il semsibilise aux attaques cyber sur le matériel (*boot*, canaux auxilliaires) et présente comment mettre en œuvre les outils de *debug* adéquats : debbugger, principe des sondes, etc.

Ce module est organisé sous la forme de cours avec une mise en pratique rapide.

L'évaluation est réalisée sous la forme d'exposés.

Séquencement

Séance	Cours	Pratique
Architecture matérielle des ordinateurs : généralités	3 h	
Principes de compilation	2 h	2 h
Gestion de la mémoire	4 h	
Boot et cybersécurité	1,5 h	1,5 h
Techniques logicielles : *buffer overflow*, canary, *shellcode*...	1 h	2 h
Présentation des étudiants répondant à des problématiques industrielles	8 h	5 h
Totaux	**19,5 h**	**10,5 h**

oOo

4.3 Rétro-ingéniérie

Code module : OUAP-4317
Période : E4 / S2
Intervenant(s) : Carlos Pinto
Durée : 30 heures

Objectifs pédagogiques

— Positionner la menace de rétro-ingénierie dans l'analyse de risque
— Identifier les objectifs de la source de risques
— Faire du *reverse* de logiciel grâce aux outils (gdb, radare2-cutter, ida, ghidra, immunity)
— Lancer des attaques de type strings, surcharge de librairie, ROP, injection de code

Description

L'objectif du module est de former les étudiants à prendre en compte dans les développements la menace de rétro-ingénerie. Pour cela, le module présente la méthodologie d'analyse de risque EBIOS, l'évaluation des produits (CSPN, Critère Commun). Le module traite de la menace de rétro-ingénierie au niveau physique (Radio de composant), au niveau protocolaire (analyse de traffic IP – whireshark) et surtout de la rétro-ingénierie des logiciels.

Sur l'aspect logiciel, le module présente les vulnérabilités les plus communes sur les logiciels (débordement de *buffer* en pile et dans le tas, débordement d'entier, modification des librairies standard, strings) et les exploitations associées (attaques par injection de code, attaques par modification de la GOT, attaques ROP).

Le module est organisé en cours suivi d'exercice de mise en œuvre.

Séquencement

Séance	Cours	Pratique
Introduction, Méthode EBIOS	3 h	
Evaluation Critère Commun, Attaques sur les produits	3 h	
Retro-conception communication sans fil	3 h	3 h
Retro-conception badge Mifare	3 h	4 h
Retro-conception logiciel	3 h	8 h
Totaux	**15 h**	**15 h**

Bibliographie

[1] https ://ghidrasre.org/

[2] https ://cutter.re/

[3] https ://hexrays.com/products/ida/index.shtml

[4] https ://en.wikipedia.org/wiki/Returnoriented_programming

oOo

4.4 Audit de sécurité

Code module : IT-5107E
Période : E5 / S1 / P1
Intervenant(s) : Olivier Chatail
Durée : 30 heures

Objectifs pédagogiques

— Maitriser les concepts et outils fondamentaux de la sécurité

— Comprendre l'ensemble de la chaîne de la sécurité (légal, humain, organisationnel, informatique, réseaux, matériel...)

— Connaître les risques, menaces et vulnérabilités classiques
— Pouvoir proposer des solutions de prévention

Description

Le module commence par un ensemble de définitions (DICP, etc.), et le rôle et les responsabilités d'un audit organisationnel. Il présente ensuite les cadres normatif et juridique de la gouvernance de la sécurité (PSSI).

Ce module aborde ensuite l'analyse de risques, la gestion et le traitement des risques, la méthode EBIOS et les méthodes similaires, la classification des données, la gestion des mesures de sécurité, l'amélioration continue, l'audit technique (concept, métier, types d'audit), les tests d'intrusion, la norme ISO 19011 (programme d'audit et qualités d'un auditeur), l'audit de code et les tests d'intrusion Web, l'introduction aux besoins des TI web, la présentation des vulnérabilités majeures, l'audit d'architecture et les tests d'intrusion en interne. Il permet ensuite d'expliquer, sur la base de codes Java/.NET/PHP, la transition de vulnérabilités traditionnelles à la vulnérabilité logique. Le module se termine sur la présentaion des principes de cloisonnement et les équipements de sécurité (FW, proxies, IDS, SIEM...).

Une application dans le cadre de TP est aussi réalisée avec tests d'intrusion externe et interne (reconnaissance, surface d'attaque, exploitation, post-exploitation), avec l'explication concrète des vulnérabilités (présentation d'audit de code).

L'évaluation du module est réalisée au travers d'un TP noté avec restitution d'un rapport (test d'intrusion), d'un examen partiel (audit organisationnel) et d'un examen final écrit (audit d'Architecture et test d'intrusion en interne).

Séquencement

Séance	Cours	Pratique
Audit	20 h	
Test d'intrusions interne, externes		10 h
Totaux	**20 h**	**10 h**

oOo

4.5 Attaques Matérielles

Code module : IT-5212E
Période : E5 / S1 / P2
Intervenant(s) : Anne Exertier
Durée : 30 heures

Objectifs pédagogiques

— Donner un panorama des attaques matérielles

— Savoir mettre en œuvre certaines de ces attaques afin de comprendre leur fonctionnement

— Savoir s'en prémunir

Description

L'objectif de ce module est d'analyser les risques liées aux attaques matérielles et mettre en œuvre certaines de ces attaques, comme :

1. les attaques par canaux auxiliaires : consommation, temps, JTAG ;
2. les attaques invasives, voire destructrices : injection de fautes, *reverse engineering* matériel.

L'évaluation du module est réalisée sur la base d'un rapport de TP.

Séquencement

Séance	Cours	Pratique
Présentation générale des attaques matérielles	3 h	
Sécurité des FPGA vs CPU	3 h	
Reverse engineering matériel	2 h	6 h
Attaque par le JTAG	2 h	4 h
Attaques par injection de fautes	4 h	
Attaques par canaux auxiliaires	2 h	4 h
Totaux	**16 h**	**14 h**

Thème 5

Autres

5.1 Projet E4

Code module : PRJ-4000
Période : E4
Intervenant(s) : Eva Dokladalova
Durée : 120 heures

Objectifs pédagogiques

— Réaliser en groupe un projet informatique et/ou électronique

Description

La conduite du projet est organisé en quatre étapes :

1. la première semaine, deux jours entiers (20 heures) sont consacrés au démarrage du projet ;
2. pendant les 16 semaines suivantes, une demi-journée (4 heures) est prévue dans l'emploi du temps afin que les étudiants puissent se retrouver et travailler sur le projet ;
3. une semaine entière (35 heures), au mois de mars, est consacrée à la finalisation des travaux et à la rédaction du rapport ;
4. une soutenance (1 heure) permet d'évaluer le travail réalisé.

oOo

5.2 Management, langues et Sciences Humaines

Code module : MSH-*
Période : E4 et E5
Intervenant(s) : —
Durée : Management et Sciences Humaines : 150 heures ; Langues : 150 heures

Objectifs pédagogiques

— Acquérir les savoirs de l'ingénieur (connaissances non scientifiques)

Description

Pour chaque période (trois périodes en E4 et deux en E5), les étudiants doivent :

— choisir un module de 30 heures dans la liste ci-dessous ;

— suivre un module obligatoire de 30 heures en anglais.

Ils peuvent en outre suivre des cours afin d'acquérir ou perfectionner une autre langue étrangère à prendre parmi le chinois, l'allemand, le japonais et l'espagnol.

Liste des modules au choix :

— E4 S1 P1 :
  — Fondement du marketing,
  — Analyse et politique économique,
  — Finance et contrôle de gestion,
  — *Knowledge management* et capacités numériques,
  — *Intercultural Management and Communication* ;
— E4 S1 P2 :
  — Veille technologique,
  — De la technologie au marché,
  — Économie industrielle et analyse sectorielle,
  — Management de l'innovation,
  — Entrepreneuriat et *business plan*,
  — *French Business Culture and Communication* ;
— E4 S2 :
  — Stratégie d'entreprise et développement durable,
  — Droit des affaires,
  — Marketing opérationnel,
  — Les achats 4.0,
  — Économie et environnement,
  — Économie et organisation du système de santé,
  — Gentils flux/méchants flux – potimisation des flux dans l'organisation
  — Penser les modes futures et durables de 2050 avec la prospective ;
— E5 S1 P1 :
  — Droit du travail et gestion des ressources humaines,
  — Management d'équipe et *leadership*,
  — Veille technologique,
  — *Data science* et analyse des réseaux sociaux,

  - Économie de la mondialisation,
  - Entrepreneuriat et *business plan*,
  - Ingéniérie financière et finance de marché ;
- E5 S1 P2 :
  - Simulation de gestion,
  - *Project management & Innovation management.*