Syllabus ESSI[1]

Année 2018-2019 – 31/01/2019

[1] Note : le nombre d'heures de cours et de TP peut varier d'une année à l'autre. Le présent syllabus est celui de l'année scolaire 2018-2019.

LIRE LE SYLLABUS

Chaque module est présenté sous la forme d'un tableau comportant une description des objectifs pédagogiques, une description du contenu et la façon dont il est enseigné, des descriptions des différents sujets enseignés avec le nombre d'heures de cours et de mise en pratique.

La fin du tableau peut proposer une bibliographie (il peut s'agir d'ouvrages à consulter avant, pendant ou après le cours).

Les heures de pratique (ou de mise en pratique) peuvent correspondre à des travaux dirigés, des projets, des études de cas, etc.

Des heures dédiées à la mise en pratiques hors modules sont également prévues à l'emploi du temps (« temps personnel »).

CRYPTOGRAPHIE (132H)

Objectifs pédagogiques

L'objectif de ce module est de donner aux étudiants les outils pour comprendre les enjeux de sécurité liés à l'usage de la cryptographie dans les produits de sécurité. A la fin du module, les étudiants doivent être capables de connaître les principaux mécanismes cryptographiques actuels et les différentes propriétés de sécurité que ces mécanismes permettent d'atteindre. Ils doivent également être capables de comprendre une analyse cryptographique concernant un produit donné.

Description

Ce module présente les nombreux domaines de la cryptographie moderne, que l'on peut regrouper en deux grandes familles : la cryptographie symétrique (ou à clé secrète) et la cryptographie asymétrique (ou à clé publique). Pour chacun de ces domaines, on expose les différents enjeux de sécurité, les problématiques qui en découlent ainsi que les solutions que la cryptographie peut y apporter.

Le module débute par des cours de remise à niveau en mathématiques qui permettent d'appréhender les concepts mis en œuvre par la cryptographie.

L'objectif des cours suivants est d'aborder les grandes familles de primitives et de mécanismes cryptographiques qui existent actuellement. Ces sessions se présentent sous la forme de cours théoriques de 3h ainsi que de séances d'exercices de 3h également, permettant de mettre en application les concepts vus en cours.

Enfin, des présentations plus techniques de cryptanalyse (symétrique, asymétrique et par canaux auxiliaires) exposent les techniques d'attaques actuelles contre certains algorithmes, et apportent une justification aux principes de conception des mécanismes présentés précédemment.

Le module, dans son intégralité, s'étend sur une période de 6 mois.

L'évaluation des étudiants se fait sur la base des épreuves suivantes :

- un examen écrit de mathématiques (coefficient 1), planifié en décembre ;
- un examen écrit (coefficient 1), planifié au mois de décembre, portant sur les principes généraux de la cryptographie symétrique : chiffrement par bloc, modes de chiffrement, fonctions de hachage, chiffrement par flot et authentification de messages …
- un examen écrit (coefficient 1), planifié au mois de mars, portant essentiellement sur la cryptographie asymétrique : chiffrement, signature, échange de clés et authentification, génération d'aléa … Cet examen étant réalisé en fin d'année, quelques questions/exercices de cryptographie symétrique peuvent être ajoutés au sujet, dans le but de voir si les concepts étudiés en début de module restent toujours assimilés.
- un grand oral (coefficient 2) contenant des questions de cryptographie, sous la forme d'un sujet tiré au sort par les élèves, préparé puis exposé à l'oral, ou d'une séance de questions orales lorsqu'un sujet d'une autre matière a été tiré. Le jury de cet oral est composé des professeurs de la formation.

Par ailleurs, tout au long de l'année, les élèves ont la possibilité (s'ils le souhaitent) de rendre, sous forme de devoir écrit, des exercices qui n'ont pas nécessairement pu être traités en séance de pratique. L'assiduité et la qualité des devoirs rendus tout au long de l'année pourront éventuellement être prises en compte dans la notation finale. Enfin deux séances, une de préparation aux examens écrits et une de préparation à l'oral, sont proposées aux étudiants en décembre, puis février.		
Introduction et fondamentaux (60h)	**Théorie**	**Pratique**
Le cours d'**introduction à la cryptographie** permet de définir les différentes notions qui seront approfondies au cours du module.	3h	
De nombreux **cours de mathématiques** sont planifiés tout au long du module : le but est de procéder à une mise à niveau des différents élèves de la promotion. Il s'agit en particulier de voir des notions nécessaires à la compréhension des concepts généraux de la cryptographie. Des thématiques très variées telles que l'algèbre linéaire, l'arithmétique ou encore les probabilités y sont abordées.	54h	Au fil de l'eau
Un cours d'**algorithmique** présente la façon dont sont implémentées sur machine les opérations vues dans le cours de mathématiques (notamment les manipulations de grands entiers ou de polynômes), et explique comment on peut, avant de lancer ces calculs, prédire quelles ressources seront nécessaires (en particulier quel temps durera le calcul).	3h	
Totaux cours/pratique	**60h**	
Cryptographie symétrique (33h)		
Les algorithmes de **chiffrement par bloc** sont des primitives très utilisées dans le domaine de la cryptographie symétrique. Ce cours aborde les principes de conception et les notions de sécurité propres à ces algorithmes, ainsi que les deux exemples les plus utilisés en pratique (DES et AES).	3h	3h
La manière d'employer ces primitives pour assurer la confidentialité d'une donnée est appelée **mode de chiffrement**. Ce cours balaye les principaux modes, en explicitant leur niveau de sécurité et les précautions d'implémentation à prendre en compte pour garantir un bon niveau de robustesse.	3h	3h
Les **fonctions de hachage** sont des primitives utilisées dans un grand nombre de mécanismes et de protocoles. Ce cours décrit les notions de sécurité qui leurs sont propres, et des principes de conception permettant de les atteindre. Les principales fonctions de hachage sont également décrites (SHA-2, SHA-3). La pratique aborde également des notions de cryptanalyse.	3h	3h
Un cours est dédié aux **modes opératoires** permettant d'assurer l'**authenticité** d'une donnée, ainsi qu'aux modes dits combinés permettant de garantir à la fois sa confidentialité et son authenticité.	3h	3h
Les algorithmes de **chiffrement à flot** sont des mécanismes	3h	3h

cryptographiques permettant d'assurer la confidentialité d'une donnée en additionnant le clair avec une valeur secrète. Ce cours décrit les notions de sécurité associées à ces mécanismes, décrit des principes de conception et aborde les techniques de cryptanalyse.		
Le cours de **cryptanalyse symétrique** aborde les principales techniques d'attaque d'algorithmes de chiffrement par bloc : la cryptanalyse différentielle et la cryptanalyse linéaire. En ce sens, il complète les cours sur ces primitives en apportant une justification à certains principes de conception présentés précédemment.	3h	
Totaux cryptographie symétrique	**18h**	**15h**
Cryptographie asymétrique (27h)		
Le cours de **chiffrement asymétrique** expose les concepts de base de de la cryptographie à clé publique, il présente les algorithmes de chiffrement les plus couramment utilisés et les problèmes mathématiques sur lesquels ils reposent.	3h	3h
La confidentialité des données n'est pas la seule problématique de la cryptographie : il faut également garantir l'authenticité de ces données et l'origine de l'émetteur. Une manière d'y parvenir en cryptographie asymétrique est la **signature électronique**. Dans ce cours, on présente différents algorithmes de signature et on donne, pour chacun d'eux, le niveau de sécurité atteint. On aborde également la notion de preuve de sécurité.	3h	3h
De nombreux cryptosystèmes sont définis sur les corps finis. Il existe d'autres espaces mathématiques sur lequels on peut construire des algorithmes de chiffrement et d'authentification : **les courbes elliptiques** en sont un bon exemple. Dans ce cours, on présente cette structure mathématique particulière et on analyse la sécurité de certains problèmes mathématiques difficiles définis sur ces courbes. On présente également les algorithmes cryptographiques les plus classiques que l'on peut construire dessus.	3h	
Le cours **d'échange de clés et d'authentification** présente les différentes méthodes existant permettant à deux intervenants distants de partager une clé commune secrète. On explique notamment comment les phases d'échange de clés et d'authentification mutuelle doivent être imbriquées pour obtenir des garanties fortes de sécurité.	3h	3h
Le cours de **protocoles avancés** présente des mécanismes cryptographiques plus complexes dans le cadre du calcul multiparti, où un certain nombre de participants cherchent à collaborer sans se faire mutuellement confiance. Des outils cryptographiques tels que le partage de secret et la cryptographie distribuée et des applications telles que le vote électronique sont abordés.	3h	
La session de cryptographie asymétrique se clôture par le cours de **cryptanalyse asymétrique**, qui présente des techniques d'attaque de schémas à clé publique (principalement RSA) lorsque les secrets sont de taille plus petite que prévue initialement ou lorsqu'une partie de ces	3h	

secrets est connue de l'attaquant (comme c'est le cas par exemple après certaines attaques par canaux auxiliaires). Des outils mathématiques tels que les fractions continues, les réseaux euclidiens, l'algorithme LLL ou encore l'algorithme de Coppersmith y sont développés.		
Totaux cryptographie asymétrique	**18h**	**9h**
Cours connexes (12h)		
La sécurité des mécanismes cryptographiques repose sur la qualité des valeurs aléatoires utilisées, notamment pour générer les clés. Dans le cours de **génération d'aléa**, on présente les propriétés attendues d'un générateur d'aléa, et les constructions de générateurs d'aléa à l'état de l'art, combinaison de générateurs déterministes et de sources d'aléa physiques ou systémiques.	3h	3h
En pratique, un produit de sécurité repose sur une implémentation d'algorithmes, et les implémentations reposent sur des principes de conception matériels et logiciels qui font fuir de l'information sur les données qu'ils manipulent. C'est le principe des **attaques par canaux auxiliaires**. Dans ce cours, on explique comment la consommation électrique, les ondes électromagnétiques émanant d'un composant lors d'un calcul cryptographique, ou encore le temps d'exécution et même la présence de caches mémoires dans les processeurs, peuvent permettre à l'attaquant de retrouver le secret manipulé.	3h	
Le cours de **cotation cryptographique** permet de discuter d'aspects plus pratiques de la cryptographie, et expose notamment la façon de procéder à l'analyse cryptographique d'un produit de sécurité. On détaille en particulier le type d'information contenu dans le référentiel général de sécurité (les règles ainsi que les recommandations), et on attire l'attention du futur évaluateur sur certains points de vigilance, tels que la génération d'aléa, le stockage des clés ou encore les oracles de *padding* dans les mécanismes de chiffrement.	3h	
Totaux cours connexes	**9h**	**3h**
Total général	**105h**	**27h**

SYSTÈME (174H)

Unix/Linux (111h)

Objectifs pédagogiques

L'objectif de ce module est d'amener les étudiants à comprendre le fonctionnement des éléments constitutifs de base des systèmes d'exploitation (fichiers, processus, etc.), et les enjeux de sécurité associés. Une des finalités est de comprendre et analyser un avis de sécurité concernant une vulnérabilité système.

Description

Le module système a pour objectif de faire comprendre les principes de base d'un système d'exploitation, et d'expliquer les enjeux de sécurité liés à chacune des notions abordées.

La majorité des exemples pris en cours et les mise en pratique concerne les systèmes Unix et Linux en particulier. Un module séparé traite des spécificités du système d'exploitation Windows.

L'approche retenue est de partir des notions les plus abordables et concrètes (shell, fichiers) pour arriver vers les sujets plus complexes et plus bas niveau en fin de module (assembleur, format des exécutables).

Les cours et la pratique sont entrelacés sur une période de 7 mois, allant de début septembre à fin mars.

L'évaluation se fait sur la base des éléments suivants :

- un partiel en décembre (coefficient 1) qui porte sur les premiers modules (shell, fichiers et processus) et dont l'objectif est de vérifier l'assimilation de ces notions.
- un examen en mars (coefficient 1) qui porte sur l'ensemble du programme et vise en général à tester, au-delà des connaissances des notions décrites dans le module, les capacités de raisonnement des étudiants. Cela passe par exemple par l'analyse concrète d'un avis de sécurité récent.
- le grand oral (coefficient 2) évalue en partie le module système, soit au travers du sujet tiré au hasard (car les sujets à traiter par les étudiants peuvent relever du module système), soit dans la partie questions qui suit (puisqu'un enseignant du module système est présent au jury).

Pour information, une colle (un oral blanc) qui ne compte pas dans la note finale, est proposée aux étudiants début décembre.

Cours et pratique	**Cours**	**Pratique**
Le *shell*, qui permet de dresser un aperçu d'un large ensemble de notions, tout en permettant à chacun d'apprivoiser cet outil, essentiel pour le reste du cours.	6h	6h
Les fichiers sont un vaste sujet qui va du fonctionnement d'un système de fichiers sous Unix aux problématiques de synchronisation (accès à une ressource partagée) en passant par l'étude des interfaces disponibles en C (les appels système d'une part et les fonctions de plus haut niveau d'autre part).	12h	12h
Les processus sont un concept essentiel dans la compréhension d'un système d'exploitation. Cette partie du cours traite de la représentation d'un	6h	3h

processus au sein du noyau, d'ordonnancement, et présente là encore les interfaces disponibles en C pour gérer les processus.		
La mémoire est traitée dans un cours long qui présente les mécanismes de gestion sur les architectures classiques (segmentation, pagination).	9h	6h
Les *threads* sont brièvement abordés, notamment pour mettre en avant les problèmes de synchronisation et pour insister sur la notion d'action atomique présenter les problématiques de *race conditions*.	3h	3h
Les *sockets* sont présentés suffisamment tard dans l'année pour que les étudiants aient vu les concepts TCP/IP dans le cours réseau. Ce cours leur permet d'aborder les mêmes concepts, du point de vue du système.	6h	3h
Les signaux (2 créneaux) sont un cours permettant d'illustrer une notion courante, mais complexe, des systèmes d'exploitation. Le caractère asynchrone des signaux les rend délicats à prendre en compte proprement.	6h	3h
L'assembleur est abordé pour présenter en quoi consistent concrètement les binaires exécutés sur un système. Les exemples reposent sur l'architecture x86, le système Linux et les compilateurs C classiques.	6h	
Les exécutables sont enfin présentés en fin de module. Le format ELF est disséqué pour présenter le fonctionnement concret du système, et en particulièrement la manière dont les mesures de sécurité peuvent être appliquées lors de la projection mémoire et de l'édition dynamique de liens.	6h	
OpenBSD : compilation du noyau, étude des appels systèmes et écriture d'un module noyau.		9h
Étude de cas : analyse d'une faille noyau.		3h
Écriture d'un serveur multi-clients.		3h
Totaux	**60h**	**51h**

Bibliographie

Aucune lecture n'est nécessaire préalablement à ce module, mais voici quelques liens utiles pour les étudiants intéressés.

- Les systèmes d'exploitation par Andrew Tanenbaum est un ouvrage de référence. Les premiers chapitres présentent clairement les missions des systèmes d'exploitation, et proposent un historique des architectures et systèmes existants.
- oss-security (http://www.openwall.com/lists/oss-security/) est une liste de diffusion sur laquelle sont publiées des vulnérabilités et des correctifs de sécurité concernant des logiciels libres.
- Smashing Stack For Fun and Profit, l'article historique décrivant l'exploitation d'un dépassement de tampon (http://insecure.org/stf/smashstack.html).

Windows (63h)

Objectifs pédagogiques

L'objectif de ce module est de donner des capacités à appréhender les mécanismes de sécurité mis en œuvre dans les environnements Windows et Active Directory. À la fin du module, les

étudiants doivent connaître les principales thématiques de sécurité des systèmes Windows et des environnements Active Directory. Ils doivent en particulier être en mesure de formuler un avis de sécurité sur un problématique liée à Windows ou des recommandations visant à améliorer le niveau de sécurité.

Description

Le module est séparé en 3 grandes parties :

1. **Sécurité du système d'exploitation Windows (12 cours de 3 heures)**

Cette partie consiste à comprendre le fonctionnement interne d'un système Windows ainsi que les mécanismes de sécurité mis en œuvre sur ces systèmes. Les deux grandes sous-parties sont l'authentification ainsi que le modèle de sécurité.

2. **Sécurité des environnements Active Directory (5 cours de 3 heures)**

Cette partie consiste à décrire le fonctionnement des annuaires Active Directory très souvent mis en œuvre avec des systèmes Windows ainsi que tous les enjeux ou menaces sur ce type d'environnement.

3. **Mise en œuvre (3 cours de 3 heures)**

Cette partie permet aux étudiants de mettre en œuvre les concepts vus dans les deux parties précédentes via la manipulation des principaux outils permettant d'éprouver la sécurité des environnements Windows (type test d'intrusion).

De nombreuses mises en pratique sont effectuées pendant les cours (manipulation d'outils, écriture de scripts, programmation, etc.). De plus, un environnement Active Directory complet (multi-forêts avec DC, RODC et serveurs membres) est mis à disposition des étudiants afin qu'ils puissent pratiquer dessus durant tous les cours du module.

L'évaluation se fait sur la base d'un examen en mars (coefficient 1) qui porte sur l'ensemble du programme et vise à juger les connaissances des notions décrites dans le module.

Cours et pratique	Cours	Pratique
Architecture Architecture générale du système : sous-systèmes Windows, OS/2, Posix Sessions Windows Processus de démarrage	1h	0,5h
Mise à jour Type de mise à jour Microsoft Politique de support Microsoft Windows 10 servicing model : Service Update et Feature Update Serveurs de déploiement : Microsoft Update et WSUS	2h	
Réseau NetBios : NetBIOS Name Service, NetBIOS Datagram Service et NetBIOS Windows Networking (WNet) : Windows Networking et Multiple UNC Provider Redirecteur RDPNP (TS client) Redirecteur WebClient (WebDAV) Redirecteur LanmanWorkstation (SMB) SMB : historique, SMB 1, 2 et 3 Signatures SMB2 et Configuration de la signature SMB2	3h	0,5h

Chiffrement SMB3 et Paramètres de configuration du chiffrement SMB UNC Hardened Access Remote Procedure Call (RPC) Windows Filtering Platform Windows Firewall with Advanced Security Nouveaux protocoles : LLTD et LLMNR		
Authentification Protocole de défi/réponse (NTLMSSP) et attaques associées NetLogon Kerberos Attaques Kerberos : KC, SPN sur compte utilisateur, Pass-the-key, Pass-the-ticket Privilege Attribute Certificate PKINIT	8h	2h
Modèle de sécurité Modèle général du contrôle d'accès Les SID Token Descripteur de sécurité : DACL, SACL, ACE Synopsis du contrôle d'accès Héritage SDDL Primary tokens / Impersonation tokens Restricted SID	8h	2h
Mécanismes de sécurité Structured Exception Handling Data Execution Prevention (DEP) Address Space Layout Randomization (ASLR) Control Flow Guard (CFG) Windows Integrity Mechanism (WIM) User Account Control (UAC) Sécurisation des services Process Mitigation Policy / Mitigation Options / Windows Defender Exploitation Guard	8h	2h
Active Directory Historique : Domaine NT, PDC / BDC, LAN Manager rootDSE LDAP Extended Controls Stockage des données Active Directory (NTDS.DIT) Groupes et utilisateurs principaux Relations d'approbation Authentification Kerberos entre domaine Authentification sélective Contrôle d'accès des objets de l'annuaire Group Policy Object (GPO) PSO (Password Settings Object) SDProp & AdminSDHolder RODC Shadow Principals	12h	3h

Mise en œuvre Manipulation d'outils		9h
Totaux		
Bibliographie		

MANAGEMENT DE LA SECURITE (54H)

Objectifs pédagogiques
L'objectif de ce module est de fournir une vision large des aspects organisationnels, juridiques, normatifs et parfois politiques de la sécurité du numérique. Il sert également d'introduction à la formation en rappelant quelques fondamentaux de la SSI et en fournissant un panorama des menaces pesant sur les systèmes d'information.
Description
Le module est constitué en grande partie de cours/conférences (droits, réglementation, certification, normalisation, lutte contre la cybercriminalité…) et de cours plus approfondis, en particulier sur la l'analyse de risques et l'homologation). L'évaluation des acquis se fait via une étude de cas portant sur une analyse de risque et une homologation via un oral en binôme devant un jury qui représente une autorité d'emploi.

Introduction à la SSI	**Théorie**	**Pratique**
En cours de rédaction	3h	
Totaux cours/pratique	**3h**	
Panorama des menaces		
En cours de rédaction	3h	
Totaux cours/pratique	**3h**	
Droit de la SSI		
En cours de rédaction	3h	
Totaux cours/pratique	**3h**	
Intégration de la SSI dans les projets		
L'objectif du cours est de fournir aux stagiaires l'ensemble des clés de compréhension, les éléments de langage et outils méthodologiques lui permettant d'intégrer les enjeux de la cybersécurité durant tout le cycle de vie d'un projet numérique, et ce dès la phase de cadrage et de faisabilité.	3h	
Totaux cours/pratique	**3h**	
Normalisation de la SSI		

En cours de rédaction	3h	
Totaux cours/pratique	**3h**	
Règlementation nationale SSI		
L'objectif du cours est de fournir aux stagiaires un panorama de la règlementation applicable en France dans le domaine de la SSI. La présentation s'attache à présenter : • la hiérarchie des normes dans le droit français ; • les différentes règlementations du domaine de la confiance numérique ou encore la protection des acteurs critiques de l'État.	3h	
Totaux cours/pratique	**3h**	
Certification de la sécurité des technologies de l'information		
L'objectif du cours est de donner un aperçu des différents référentiels permettant d'évaluer et certifier la sécurité des technologies de l'information. Sont abordés : - les aspects historiques de l'évaluation et de la certification afin de comprendre comment les enjeux (étatiques, commerciaux, techniques…) de cette activité ont évolués à travers le temps. - Un aperçu des Critères Communs (ISO15408). - Un aperçu de la Certification sécurité de premier niveau (CSPN). - Les accords internationaux régissant la reconnaissance des certifications (CCRA, SOGIS, schémas privés). - Un aperçu des schémas d'évaluation alternatifs (PCI, EMVCo…). - Les évolutions à venir de cette activité, en particulier, en Europe. - Les liens existant en France entre certification et qualification.	3h	
Totaux cours/pratique	**3h**	
Qualification et agrément de produits et de services		
L'objectif du cours est de faire découvrir aux stagiaires les critères présidant au choix de produits de sécurité et de services de cybersécurité, savoir comment ces critères peuvent être évalués et découvrir les réponses qu'apportent sur ces sujets les schémas nationaux de qualification et d'agrément.	3h	
Totaux cours/pratique	**3h**	
Lutte contre la cybercriminalité		
L'objectif du cours est de fournir aux stagiaires une vue d'ensemble des phénomènes de cybercriminalité et de l'organisation mise en place pour lutter contre cette criminalité en France. Les principaux contenus portent sur : • les catégories de cyber-infractions, les aspects juridiques et la mesure de cybercriminalité,	3h	

• l'écosystème du cybercrime et les cibles • les types de cyber-attaques (techniques, faille humaine) et autres phénomènes (*blackmarkets*, cartes bancaires…), illustrés au travers d'affaires judiciaires, la compréhension des modes d'action des forces de police (les différents cadres judiciaires, la plainte et les étapes du procès pénal), les services d'enquête compétents en matière de cybercriminalité et la coopération internationale		
Totaux cours/pratique	**3h**	
Analyse de risques		
L'objectif de ce cours est de fournir aux stagiaires les éléments pour pouvoir mener une analyse de risque selon la méthode EBIOS RM. Au travers d'exposés, le stagiaire sera amené à : • acquérir le vocabulaire et les concepts introduits par la méthode ; • comprendre les différents ateliers décrits dans la méthode. Une fois ces éléments présentés, le stagiaire sera invité à les restituer au travers d'une étude de cas.	6h	6h
Totaux cours/pratique	**6h**	**6h**
Homologation		
L'objectif du cours est de fournir aux stagiaires les éléments afin de lui permettre de comprendre la démarche d'homologation et de son inscription dans le paysage règlementaire français. De plus, le stagiaire sera en capacité de pouvoir conduire un processus d'homologation, de la constitution du dossier avec la compréhension de chacune des pièces qui le compose jusqu'à la prise de décision d'homologation, l'argumentaire qui y est associé et les conséquences d'une telle décision.	6h	
Totaux cours/pratique	**6h**	
SMSI		
En cours de rédaction	6h	
Totaux cours/pratique	**6h**	
Gestion de crise		
L'objectif du cours est de fournir aux stagiaires les éléments permettant de comprendre l'organisation de gestion de crise en France et en Europe. Le module s'attache à également donner des éléments de compréhension sur les processus d'étude de la menace, de détection des incidents de sécurité et de réponse aux incidents.	3h	
Totaux cours/pratique	**3h**	

SÉCURITÉ APPLICATIVE (63H)

Bases de données (9h)		
Objectifs pédagogiques		
Description		
Cours et pratique	**Cours**	**Pratique**
Totaux		
Bibliographie		

Programmation C (24h)		
Objectifs pédagogiques		
Les étudiants ESSI peuvent avoir des parcours très différents et un niveau hétérogène en programmation. L'objectif de ce cours est d'effectuer une mise à niveau rapide de l'ensemble de la promotion en programmation afin de pouvoir aborder le plus sereinement possible les travaux pratiques effectués dans d'autres modules (système et Windows, en particulier). Étant donné la nature de ces travaux pratiques, c'est le langage C qui a été retenu comme support. Les difficultés du langage C permettent en outre de mieux appréhender les traits de langages plus évolués. Le cours rappelle les origines du langage, ses particularités par rapports à d'autres langages. Quelques notions sur la compilation et l'édition de lien sont également présentées. La suite du cours porte sur la structure du langage, ses constructions syntaxiques, la gestion de la mémoire et les fonctions d'entrée/sortie. Les concepts présentés sont illustrés de nombreux exemples et mises en pratique. Un accent particulier est mis sur les bonnes pratiques, tant en terme de règles de codage (lisibilité, maintenabilité) que de sécurité des implémentations. La partie pratique du cours est mixée avec la partie théorique et représente environ 50% du volume du module.		
Description		
Les généralités sur le C : origine du langage, normalisation, structure, règles de codage, compilation, édition de lien… La structure du langage : variables, types, opérateurs, structures de contrôle, fonctions, allocation des variables, pointeurs, allocations dynamique, structure et énumérations, entrées/sorties…		
Cours et pratique (TP, projets, études de cas…)	**Cours**	**Pratique**
Programmation C	12	12

Totaux	**12**	**12**
Bibliographie		

Sécurité logicielle (30h)
Objectifs pédagogiques
Une fois assimilé les fondamentaux de la programmation en langage C, les étudiants ESSI abordent le cadre général de la sécurité logicielle et de la programmation sécurisée. L'objectif pédagogique de ce cours est dans un premier temps de comprendre le concept et l'origine des vulnérabilités ainsi que leurs impacts sur la sécurité des données. Autant sur les aspects théoriques que pratiques, ce cours permet ensuite aux étudiants de comprendre les bienfaits de certaines architectures logicielles du point de vue de la sécurité. Le langage C est pris comme langage d'exemple : il est décrit les nombreux pièges de ce langage ainsi que des exemples courants d'erreur de d'implémentation. Tout au long du cours, les étudiants peuvent expérimenter les vulnérabilités au travers de travaux pratiques afin de comprendre l'origine des vulnérabilités et assimiler les protections indiquées en cours (bonnes pratiques de programmation). L'ensemble des exemples est donné sous environnement Windows afin de mettre en pratique les mécanismes de sécurité abordés dans le cours Windows. Enfin, ce cours a pour objectif de décrire comment intégrer la sécurité dans un projet en mode agile.
Description
Le cours commence par décrire le vocabulaire, le contexte et le cycle de vie associés aux vulnérabilités. De nombreux exemples sont donnés pour illustrer des cas réels de vulnérabilités (opensource/closed souce, cas des portes dérobées, etc.). Par la suite, les motivations à la sécurité logicielle (protection des données, RGPD, certification, etc.) sont décrites car ils sont généralement des conditions nécessaires à la mise en œuvre des mécanismes étudiés. Les vulnérabilités sont ensuite classées suivant leur origine : conception, implémentation et configuration/déploiement. Plusieurs exemples sont encore donnés pour décrire parfaitement la difficulté et les contraintes de la discipline. Certains mécanismes de sécurité proactifs sont abordés pour réduire la surface d'exposition des programmes ainsi que la probabilité d'exploitation par un attaquant. Les grandes architectures sécurisées sont décrites en détail ainsi que les mécanismes des systèmes d'exploitation ou du matériel utilisés pour l'implémentation. En particulier, l'architecture bac-à-sable est explicitée pour les environnements Linux & Windows dans le cas du navigateur Internet et du serveur de messagerie. La segmentation logiciel (n-tier) est ensuite abordée pour renforcer la sécurité des applications coté serveur. La sécurité des applications pour l'informatique en nuage (cas AWS) est également décrite. Le cas du langage C est ensuite retenu pour décrire de nombreuses familles de vulnérabilités : certaines propres au langage C, d'autres applicables à de nombreux langages. Plusieurs exemples de vulnérabilités sont issus de véritables applications : elles sont explicitées ainsi que les mesures de sécurité associée. Les principales classes de vulnérabilités sont décrites : promotion numérique, dépassement de mémoire dans la pile/le tas, dépassement d'entier, erreur de format, accès concurrentiel, fuite de données, etc. Par la suite, de nombreuses bonnes pratiques de développement sont dispensées. Elles concernent le langage C (interdiction de certaines fonctions, type de déclaration, etc.), les options du

compilateur (visual C), les fonctions sécurisées. Plusieurs cas d'usage sont explicités afin d'orienter l'étudiant sur des cas pratiques : réinitialiser un mot de passe, filtrer les entrées utilisateur, lire un fichier dans un bac-à-sable, appliquer un système de contrôle d'accès efficace, etc.

Enfin, il est décrit deux contextes de mise en œuvre de la sécurité logicielle : l'encadrement d'un prestataire et la gestion d'une équipe de développement. Dans les deux cas de figure, les pièges et les difficultés à éviter sont explicités afin de rendre compatible un projet logiciel avec les exigences de sécurité vue précédemment. Dans le cas où une méthode de développement agile est mise en œuvre, il est décrit une méthode d'intégration de la sécurité.

Cours et pratique (TP, projets, études de cas…)	**Cours**	**Pratique**
Introduction à la sécurité logicielle (théorie et cas pratique)	3h	30min
Cycle de vie des vulnérabilités	3h	
Classes de vulnérabilités - Etude de cas (exemple d'une vulnérabilité prise dans l'actualité récente)	3h	
Architecture sécurisée des applications	4h	
Cas de la sandbox Chrome, Cas du serveur de messagerie Postfix, Cas d'un serveur Web		2h
Programmation sécurisée dans le cas du langage C	5h	
Exemple du dépassement de mémoire tampon de la pile sous Windows 10 Exemple de dépassement d'entier et de promotion numérique		3h
Exemple de la sécurisation d'une procédure de réinitialisation de mots de passe		30 min
Mécanisme de sécurité sous Linux et Windows	4h	
Sécurité dans les projets	2h	
Un projet en C respectant les pratiques vues en cours est demandé aux élèves.		
Totaux	**24h**	**6h**

Bibliographie

OWASP - https://www.owasp.org/index.php/Main_Page

The CERT C secure coding - https://en.wikipedia.org/wiki/CERT_C_Coding_Standard

The art of software security assessment - https://www.oreilly.com/library/view/the-art-of/0321444426/

RESEAUX (99H)

Principes et sécurité (81h)

Objectifs pédagogiques

À l'issue de ce module, les étudiants doivent avoir compris et être en mesure d'exposer le fonctionnement d'un réseau de communication, de ses protocoles, depuis le niveau réseau jusqu'aux protocoles applicatifs en passant par les protocoles de routage et de ses différents constituants, qu'il s'agisse d'un réseau distant (WAN), d'un réseau local (LAN) et bien sûr, du cas particulier de l'Internet. Tous ces aspects sont également vus sous l'angle de la sécurité (des applications, des communications, des protocoles…).

Description

Le module réseau a pour objectif d'exposer les principes des réseaux, et d'expliquer les enjeux de sécurité liés à chacune des notions abordées.

Sa pédagogie s'articule autour de deux grands axes :

- l'enseignement des principes ;
- les cours spécialisés.

L'enseignement des principes se déroule sur 12 cours de 3 heures dans lesquels les étudiants apprennent les prémisses du réseau, le fonctionnement en couches et les principes auxquels il répond. Deux cours avec mise en pratique, font un focus sur la sécurité durant cet enseignement. Il se déroule de septembre à décembre.

Les cours spécialisés s'appuient sur les enseignements dispensés dans l'enseignement des principes. Ils se concentrent sur des présentations de protocoles, technologies ou encore de concepts, parfois accompagnés de travaux pratiques.

Cet enseignement entre janvier et avril, mois du départ en stage des étudiants.

L'évaluation des acquis se fait de la façon suivante :

- un partiel en décembre, de coefficient un, qui porte sur les principes. Il s'agit d'un examen écrit d'une durée de 3h00 ;
- un partiel en mars, de coefficient un, qui porte sur les cours spécialisés. Il s'agit d'un examen écrit d'une durée de 3h00 ;
- un « grand oral », de coefficient deux. L'étudiant doit préparer et présenter un exposé sur une question tirée au hasard et portant sur un des trois modules suivants : réseau, cryptographie ou système. Il est ensuite interrogé sur les deux autres modules par les examinateurs.

Cours et TP	Cours	Pratique
L'enseignement des principes traite du modèle en couche, le fonctionnement de chacune d'entre elles et enfin des protocoles de routage permettant d'établir les communications entre différents équipements d'un réseau. Cet enseignement est complété par des travaux pratiques sur une journée au sein de Télécom Sud Paris.	24h	12h
TP SMTP. Ce protocole utilisé quotidiennement sur Internet peut être fragile. Des mesures de sécurité ont été prises mais leur fonctionnement n'est pas toujours bien compris ou connu.	1h	2h

DNS. Ce protocole continuellement utilisé par les ordinateurs est souvent méconnu ou mal compris. Sa création date des débuts de l'Internet et a dû faire face à des mises à jour de sécurité présentées dans ce cours.	3h	
Architectures sécurisées et pare-feux. Ce cours se concentre sur la présentation du fonctionnement d'un pare-feu et des différentes architectures réseau qui peuvent être réalisés, ainsi que leur conséquence du point de vue de la sécurité.	3h	
Systèmes industriels. Ces systèmes sont encore mal connus de beaucoup de professionnels alors qu'ils sont au cœur des usages quotidiens. De plus, ils sont souvent assimilés à tort aux SCADA. Ce cours suivi d'un TP permet de comprendre les enjeux et les risques liés à de tels systèmes.	3h	3h
IPv6. Ce protocole qui succède à IPv4 a vu le jour il y a plus de 20 ans. Les paradigmes d'Ipv4 et certaines faiblesses ont été revus et corrigés par cette nouvelle mouture. Néanmoins, il apporte aussi son lot de problèmes qui sont abordés dans cet enseignement	3h	3h
TLS. Ce protocole apporte une amélioration significative du point de vue de la sécurité sur Internet. Souvent associé au cadenas vert dans le navigateur, ce cours vise à en expliquer et faire comprendre son fonctionnement ainsi que ses usages.	3h	3h
Opérateurs. Ce cours a pour vocation d'expliquer et faire comprendre aux étudiants le fonctionnement de l'Internet, ses acteurs et leur interdépendance.	3h	
IPsec. Ce protocole de communications sécurisées vise à apporter de nombreuses garanties aux échanges. Au cours de cet enseignement, les fondamentaux de ce protocole sont vus, ainsi que les points d'attention à prendre en compte lors de sa mise en œuvre.	3h	
Développement web. Les applications web constituent l'essentiel des usages des particuliers mais aussi de nombreux employés vis-à-vis de l'Internet. Dans ce cours, sont vus les erreurs communes lors du développement web, et les bonnes pratiques à mettre en œuvre sur ce sujet. Un TP en fin de cours permet de mettre en pratique les enseignements reçus.	9h	3h
Totaux	**55h**	**26h**
Bibliographie		
Aucune lecture n'est nécessaire préalablement à ce module		

Sécurité des réseaux sans fil (18h)
Objectifs pédagogiques
Ce module permet de présenter les différents types de réseaux sans fils, leurs architectures, leurs usages ainsi que les risques associés, les contre-mesures disponibles et les limites de ces dernières.
Description
Ce module est un stage 11a (cf. formation continue du CFSSI) auquel les étudiants ESSI

participent. Il est organisé sous forme d'exposés théoriques et de démonstrations.		
Cours et TP	Cours	Pratique
Wifi (IEEE 802.11) : les diverses normes, les architectures de réseaux, les évolutions, les vulnérabilités et parades. Sécurisation d'un réseau Wifi : organisation, déploiement, configurations, serveurs d'authentification (Radius), protocoles de sécurité, politique de sécurité. Divers : Bluetooth, RFID, géo-positionnement, réseaux mobiles.	18h	
Totaux	**18h**	
Bibliographie		

APPLICATIONS DE LA SECURITE (135H)

Tempest (3h)		
Objectifs pédagogiques		
Après une introduction générale à la sécurité électromagnétique, ce module présente la menace TEMPEST et la démarche de protection dictée par la réglementation nationale. La menace TEMPEST est liée à l'interception et l'exploitation de signaux parasites électromagnétique en vue de compromettre les informations traitées par un système d'information.		
Description		
Les thèmes de la confidentialité et de la résilience sont deux enjeux majeurs de la sécurité des systèmes d'information. La susceptibilité des équipements vis-à-vis des interférences électromagnétiques intentionnelles ainsi que la corrélation potentielle entre le bruit généré par un système électronique et les informations traitées par celui-ci induisent un risque de compromission qu'il convient de considérer dans les analyses de risques. Au cours de l'intervention proposée le thème particulier de l'interaction entre la SSI et la compatibilité électromagnétique est présenté, suivi d'un panorama de l'évolution des moyens d'acquisition radiofréquence. La démarche de protection et la mise en œuvre des moyens de protections sont finalement abordés.		
Cours et pratique	**Théorie**	**Pratique**
Mise en contexte, introduction aux signaux compromettants et aux agressions électromagnétique. Évolutions des outils d'analyse RF puis démarche de sécurisation électromagnétique.	3h	
Totaux	3h	
Bibliographie		
II 300, DIR485, DIR495, REP490		

Logiciels malveillants-*Malware* (6h)
Objectifs pédagogiques
Ce module permet de préciser le fonctionnement et les impacts des logiciels malveillants ainsi que les méthodes pour s'en prémunir.
Description
Le module présente tout d'abord une définition des logiciels malveillants ainsi que les différentes catégories régulièrement rencontrées. Les méthodes de réalisation et de protection contre l'analyse sont également détaillées au travers d'exemples. Les logiciels et techniques permettant de lutter contre les codes malveillants sont également présentés en précisant les limites techniques ou organisationnelles qu'ils posent.

La seconde partie du cours présente quelques outils *opensource* utilisé pour traiter les logiciels malveillants : rétro-conception, analyse automatique (bac-à-sable), stockage, partage et corrélation. Plusieurs exemples issus de l'expérience du CERT-FR sont donnés pour illustrer le cours.		
Cours et pratique	**Théorie**	**Pratique**
Présentation théorique des codes malveillants : typologie, fonctionnement, antivirus, méthodes de détection.	3h	
Manipulation de certains outils *opensource* pour traiter les codes malveillants		3h
Totaux	3h	3h
Bibliographie		

Détection d'incidents (18h)		
Objectifs pédagogiques		
Description		
Cours et pratique	**Théorie**	**Pratique**
Totaux		
Bibliographie		

Infrastructures de gestion des clés (9h)		
Objectifs pédagogiques		
Description		
Cours et pratique	**Théorie**	**Pratique**

Totaux		
Bibliographie		

Architecture SSI (9h)		
Objectifs pédagogiques		
Ce module vise à sensibiliser aux questions d'architecture des produits de sécurité (essentiellement cryptographiques) et d'architecture des systèmes de gestion de ces produits, en analysant les conséquences de certains choix de conception.		
Description		
Ce module est constitué de 2 cours théoriques, sous forme de retours d'expérience sur différentes équipements cryptographiques gouvernementaux.		
Cours et pratique	**Théorie**	**Pratique**
Gammes d'équipements cryptographiques (ressource, stockage sécurisé, chiffrement réseau…) et autres produits (problématique du multi-niveau), principes d'architectures des produits (coupure, sécurité locale), principes d'architectures des systèmes de gestion, principes d'architectures de clés cryptographiques, illustrations sur la base de différents systèmes (RECRU, TEOREM, ECHINOPS, CRYPSIS…).	6h	
Totaux	**9h**	
Bibliographie		
Aucune lecture n'est nécessaire préalablement à ce module. Les connaissances requises (concepts de base sur la mise en œuvre de la cryptographie notamment) sont acquises au travers des autres modules de la formation.		

Principe et organisation des audits en SSI (42h)
Objectifs pédagogiques
L'objectif de ce module est d'acquérir des compétences théoriques et pratiques sur les méthodes d'audits en sécurité.
Description
Dans une première partie du module permettent d'aborder les aspects théoriques du domaine : - une introduction aux méthodes d'audit technique de la sécurité d'un système d'information (expertise sécurité).

- L'apprentissage d'une méthode d'audit générique ainsi que des procédures.
- Fourniture des listes techniques de points à vérifier pour les différents domaines.

Les compétences méthodologiques et pratiques obtenues en fin de stage permettent de superviser la réalisation d'un audit technique, et d'organiser et choisir différentes prestations d'audit (type de prestation, contour retenu, etc.). Cette première est un stage 8a (cf. formation continue du CFSSI) auquel les étudiants ESSI participent.

Dans une deuxième partie, les étudiants appliquent la méthodologie d'audit ainsi que des méthodes plus détaillées pour différents domaines afin de réaliser concrètement un audit technique de sécurité des systèmes d'information.

Les compétences méthodologiques et pratiques obtenues en fin de stage doivent permettre de mener de façon autonome un audit technique élémentaire.

Cette seconde partie est un stage 8b (cf. formation continue du CFSSI) auquel les étudiants ESSI participent.

Cours et pratique	**Théorie**	**Pratique**
Première partie, stage 8a : - Méthodologie générale des audits en SSI. - Approche organisationnelle. - Analyse de la sécurité physique et logique d'un système d'information (y compris les autocommutateurs téléphoniques par exemple).	12h	
Deuxième partie, stage 8b : - Techniques et procédures particulières : découverte d'un réseau, analyse de sécurisation de systèmes d'exploitation Windows et Linux (Debian), d'applications (messagerie, serveur internet, etc.). - Outils spécifiques : scanneurs de vulnérabilités, outils de vérification de la force de mots de passe, etc.		30h
Totaux	**12h**	**30h**

Bibliographie

Pratique de la sécurité des systèmes d'information (30h)

Objectifs pédagogiques

Apprendre à monter une infrastructure réseau sécurisée : mise en place d'une zone démilitarisée (DMZ), configuration de pare-feu, des services réseaux (DNS, messagerie) et mise en place de mécanismes de protection cryptographique (TLS, S/MIME, IPsec).

Former les administrateurs système aux techniques récentes de sécurité dans un environnement hétérogène (Linux, OpenBSD et Windows).

Description

Ce module est un stage 7b (cf. formation continue du CFSSI) auquel les étudiants ESSI participent.

Les étudiants travaillent en binôme dans le cadre de travaux pratiques.

Cours et pratique	**Théorie**	**Pratique**
Installation d'un pare-feu Linux (installation et configuration Linux, recompilation noyau, configuration iptables). Mise en place de services dans une DMZ sous OpenBSD (installation et présentation d'OpenBSD, serveur DNS avec NSD et Unbound, SMTP avec Postfix, IMAP avec Cyrus). Gestion d'une IGC (ou PKI) pour sécuriser les échanges de mails avec S/MIME et les connexions clients/serveurs avec TLS. Mise en œuvre de tunnels IPsec entre des passerelles Linux et entre un poste nomade Windows et une passerelle Linux.		30h
Totaux		**30h**

Bibliographie

Projet bibliographique (6h)

Objectifs pédagogiques

Le projet bibliographique a pour objet de mettre les étudiants dans une situation où ils ont à exposer à un décideur (le jury), une problématique de sécurité (par exemple, une attaque et ses conséquences).

Dans sa note, le jury, qui peut poser des questions, doit prendre en compte la clarté de l'exposé, la compréhension des enjeux, des aspects technique, du contexte, et éventuellement des aspects économique.

Tous les étudiants assistent aux exposés de leurs collègues.

Description

Plusieurs sujets sont proposés aux étudiants qui disposent d'une quinzaine de jours pour les étudier et préparer leur exposé.

Cours et pratique	**Théorie**	**Pratique**
Présentations		6h
Totaux		**6h**

Bibliographie

Protocoles d'authentification (12h)

Objectifs pédagogiques

Comprendre le fonctionnement de systèmes d'authentification, leurs forces et leurs faiblesses. Être capable de mettre en œuvre ces systèmes et d'exploiter leurs faiblesses.

Description

Ce module est organisé en quatre parties :

- mots de passe et mécanismes d'authentification : fonctionnalités des gestionnaires des mots de passe, méthodes de stockage des mots de passe (par un système Linux, par un système Windows, par une application), attaques sur les mots de passe, mots de passe à usage unique (HTOP, TOTP) ;
- protocoles courants et authentification : systèmes d'authentification en environnement Web (HTTP Basic, HTTP Digest, HTTPS, authentification applicative), cadriciel SASL ;
- protocoles et serveurs d'authentification : serveur et protocole LDAP, serveur RADIUS ;
- authentification d'accès au réseau : norme 802.1X, protocole EAP.

Cours et pratique	**Théorie**	**Pratique**
Protocoles d'authentification	6	6
Totaux	**6**	**6**

Bibliographie

Prestations de service en sécurité (3h)

Objectifs pédagogiques

L'objectif de ce module est de donner des informations sur les principales prestations de service dans le domaine de la sécurité (test de pénétration, accompagnement 27001, évaluation et expertises de produits, assistance à maitrise d'ouvrage, analyses de risques, audits, etc.) et de donner des éléments permettant de négocier ces prestations avec les sociétés de service et d'ingénierie.

Description

Conférence d'un prestataire de service.

Exemple d'intervention :

- Expliquer ce que sont les ESN
- Expliquer les différents types d'interventions (conseil, expertise, AMO...) dans le domaine de la sécurité.de coûts associés. Exemple :
  - un audit technique (type PASSI).
  - un audit organisationnel (type PASSI).
  - une mise en conformité ISO27001 (AMO)
  - une prestation de SOC (ou une prestation abonnée)
  - une prestation de conseil de haut niveau

- etc.
- Modes de contractualisation et coûts de l'homme jour et illustrations en fonction des profils et des prestations.

Cours et pratique	**Théorie**	**Pratique**
Conférence	3h	
Totaux	**3h**	
Bibliographie		

DIVERS (99H)

LaTex (3h)		
Objectifs pédagogiques		
LaTex fait partie de la famille des outils de formatage et de création de documents en *batch*, utilisant un langage de commande (ou macro-commandes) et un processeur qui les interprète pour générer le document prêt à imprimer. Il est très utilisé dans les publications scientifiques, en particulier, pour ses facilités à coder des équations mathématiques. L'objectif de ce module est de faciliter la prise en main de ce langage et des outils associés.		
Description		
Ce module est un cours s'appuyant sur de nombreux exemples.		
Cours et pratique	**Théorie**	**Pratique**
Cours et illustrations	3h	
Totaux	**3h**	
Bibliographie		
Le cours est donné par l'auteur de l'ouvrage « LaTeX pour l'impatient ».		

Prise de parole en public (12h)		
Objectifs pédagogiques		
Les objectifs de ce module sont : - d'identifier les principales clés de la réussite d'une prise de parole en public ; - de savoir préparer une intervention sur le fonds et sur la forme ; - de connaître et appliquer les techniques d'une communication orale attractive et efficace ; - de gérer l'interaction avec le groupe ; - d'améliorer de façon durable la prise de parole en public.		
Description		
La méthode d'enseignement passe par : - un questionnaire d'identification des attentes ; - des mises en situation ; - des conseils pratiques du formateur ; - des livrets pédagogiques et d'exercices.		
Cours et pratique	**Théorie**	**Pratique**
Cours et mise en pratique	9h	3h
Totaux	**9h**	**3h**

Bibliographie
Sans objet

Soutien (12h)		
Objectifs pédagogiques		
L'objectif est ce module est de permettre de revoir certains points mal compris par la promotion à l'aide d'un intervenant différent de celui qui a fait le cours. 12h sont réservés à cet effet dans l'emploi du temps. Les points à revoir sont définis par les étudiants.		
Description		
Reprise de cours ou de TP par un intervenant différent du titulaire du cours.		
Cours et pratique	**Théorie**	**Pratique**
Soutien	12h	
Bibliographie		
Sans objet		

Temps personnel (72h)		
Objectifs pédagogiques		
Permettre la mise en pratique des différents cours.		
Description		
Les heures de temps personnels sont destinées à la réalisation des différents exercices et travaux pratiques qui sont donnés par les intervenants lors de leurs interventions.		
Cours et pratique	**Théorie**	**Pratique**
Essentiellement, mise en pratique.		72h
Bibliographie		