SYSTEMES D'INFORMATION SECURISES

Professeur responsable : Christophe Bidan

SIS

COURS	TD/BE	TOTAL	EXAMENS	Intitulé
13h30	**6 BE et 4 TD (24h)**	**37h30**	Atelier (1/2h)	**Fondements**
-	3 TD (4h30)			*Connaissance de la menace*
3h	2 BE (6h)			*Programmation*
-	1 BE (3h)			*Réseau*
3h	1 TD (1h30)			*Sûreté de fonctionnement*
4,5h	2 BE (6h)			*Développement formel et certification logiciel*
3h	1 BE (3h)			*Unix sécurisé*
21 h	**4 BE (12 h)**	**33h**	Ecrit (2h)	**Cryptographie pour ingénieur**
9h	1 BE (3h)			*Principes fondamentaux de la cryptographie.*
6h	3 BE (9h)			*Protocoles cryptographiques.*
6h	-			*Cryptographie avancée*
25h30	**7 BE et 1 TD (22h30)**	**48h**	Atelier (1/2h)	**Prévention et détection des intrusions et logiciels malveillants**
3h	-			*Politique de sécurité*
7h30	2 BE (6h)			*Virus et malware*
13h30	2 BE (6h)			*Détection d'intrusions (IDS)*
-	1 TD et 1 BE (4h30)			*Buffer overflow*
1h30	2 BE (6h)			*Authentification et contrôle d'accès réseau*
21h	**-**	**21h**	Atelier (1/2h)	**Propriété intellectuelle et vie privée**
3h	-			*Aspect juridique de la protection des données*
9h	-			*Protection de la propriété intellectuelle*
9h	-			*Protection de la vie privée*
19h30	**1 BE (3h)**	**22h30**	Atelier (1/2h)	**Ingénierie de la SSI**
-	1 BE (3h)			*Test de la sécurité*
3h	-			*Evaluation et certification de la sécurité*
16h30	-			*Etudes de cas*
TOTAL COURS	**TOTAL TD/BE**	**TOTAL C+BE/TD**	**Exams**	
100h30	**61h30**	**162h**	**4h**	

BULLETIN D'APPRÉCIATION DE TROISIÈME ANNÉE

Majeure
SIS
2016 - 2017

Il est établi à partir des examens et travaux évalués soit sous la forme de notes affectées de coefficients pondérateurs, soit directement en niveau (travail de fin d'études).

Ces coefficients pondérateurs correspondent au nombre de crédits ECTS attribués à l'activité correspondante.
Ils permettent d'établir, dans chaque rubrique, une note moyenne d'après laquelle est déterminé le niveau ECTS d'appréciation (A à F).
Les aptitudes en langues sont appréciées dans une grille d'évaluation linguistique de 0 à 4 (du débutant au quasi bilingue).

L'obtention du diplôme **d'Ingénieur de l'École Supérieure d'Électricité** nécessite :

- un niveau au moins satisfaisant (D à A) dans les cinq premières rubriques et
- un niveau minimal égal à **2,5 en anglais** (il s'agit d'une obligation de résultat qui n'implique aucune obligation de suivre des cours d'anglais).

RUBRIQUES	EXAMENS ET TRAVAUX		Crédits ECTS
MAJEURE	Fondements, prévention et détection des intrusions et logiciels malveillants	Atelier	4
	Cryptographie pour ingénieur	EE	4
	Propriété intellectuelle et vie privée, Ingénierie de la SSI	Atelier	4
			12
ÉTUDES ET PROJET	Étude de laboratoire	EL	3
	Projet ou étude industrielle	PRO	9
			12
PARCOURS	6 mineures à choisir		**12**
TRAVAIL DE FIN D'ÉTUDES	Stage en entreprise ou dans un laboratoire de recherche		**20**
SEMINAIRE			**2**
LANGUES			**2**

EE : examen écrit
EO : examen oral individuel ou exposé oral (en trinôme ou individuel)
PRO : projet ou contrat d'étude industrielle
EL : réalisations et comptes rendus des études de laboratoire
Atelier : exposé devant l'ensemble de la promotion (présence obligatoire)

La majeure « Systèmes d'Information Sécurisés » permet aux étudiants d'enrichir leur curriculum vitæ par un apport de compétences en sécurité informatique, domaine aujourd'hui fortement recherché dans l'industrie. En effet, toute entreprise, quelle que soit sa taille, dépend à présent si étroitement de son système d'information que la sécurité de ce système est devenue pour elle un enjeu vital. La majeure SIS apporte les clés nécessaires au succès de la sécurisation du système d'information, via une formation équilibrée (théorique et pratique) couvant cryptologie, prévention et détection des intrusions et logiciels malveillants, sûreté de fonctionnement et ingénierie de la sécurité.

1. Cours et travaux dirigés

Fondements

13h30 C / 24h TD / 1 ORAL sous forme d'atelier / 4 crédit ECTS / SISFON

Cours magistraux : Guillaume Hiet (3h), Guillaume Piolle (3h), Nicolas Prigent (4,5h), Valérie Viet Triem Tong (4,5h), Eric Totel (3h)

L'objectif de ce cours est en premier lieu d'apporter aux étudiants les connaissances indispensables à la compréhension d'autres cours de la majeure ainsi qu'à la réalisation des études de laboratoire. Ainsi des concepts importants en programmation et en réseau sont présentés (ou rappelés). De même, les bases de la sûreté de fonctionnement, discipline connexe à la SSI, sont expliquées. Ce module introduit par ailleurs des concepts fondamentaux en sécurité, à commencer par la connaissance de la menace, ou encore, les modèles de sécurité dans un système d'exploitation réel (Unix). Enfin, l'importance d'une approche formelle de développement pour garantir un certain niveau de sécurité est illustrée au travers des exemples de COQ, B et Isabelle/HOL.

Connaissance de la menace : attaques Web, virus (4,5h de TD - G. Hiet)
Programmation : Java avancé (1,5h de cours - E. Totel, 1 BE - G. Piolle), langage d'assemblage (1,5h de cours et 1 BE - G. Hiet)
Réseau : rappels (1 BE - G. Piolle)
Sureté de fonctionnement : introduction (3h de cours et 1 TD - E. Totel)
Unix sécurisé : AppArmor, SElinux, GrSecurity (3h de cours et 1 BE - G. Hiet)
Développement formel et certification de logiciel : challenge de programmation (1 BE – V. Viet Triem Tong), méthodes formelles (4,5h de cours et 1 BE - V. Viet Triem Tong)

Bibliographie

Le langage C, Norme ANSI, 2ème édition. Kernighan and Ritchie. DUNOD.

Le Langage C++, 2ème édition. Bjarne Stroustrup. Addison Wesley.

Security Power Tools, Bryan Burns et al, O'Reilly, ISBN 0-596-00963-1

Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, James Foster, Syngress, ISBN 1-597-49074-1

SELinux by Example: Using Security Enhanced Linux, Frank Mayer, Karl MacMillan, David Caplan, Prentice Hall, 0-131-96369-4

SELinux, First Edition, Bill McCarty, O'Reilly, ISBN 0-596-00716-7

Cryptographie pour ingénieur

21h C / 12h TD / 1 ÉCRIT / 3 crédits ECTS / SISCRY

Cours magistraux : Pierre-Alain Fouque (6h), Christophe Bidan (15h)

Les objectifs de ce module sont multiples. En premier lieu, il s'agit de donner les principes fondamentaux de la cryptographie moderne, en mettant l'accent sur l'utilisation concrète de ces principes, ainsi que leurs limites. Ensuite, sont introduits les protocoles cryptographiques, ainsi que les attaques classiques auxquels ils sont sujets, justifiant le besoin de preuve de protocoles. Finalement, les dernières avancées en cryptographie sont présentées. Un TL lié à SSL permet d'illustrer la cryptographie asymétrique par la pratique. Il est introduit par un TD dédié.

Principes fondamentaux de cryptographie (3h de cours de C. Bidan, 6h de cours de P.A. Fouque et 1 BE de V. Viet Triem Tong)
Cryptographie symétrique, cryptographie asymétrique, fonctions de hachage, choix des algorithmes, standards, taille des clés, limites de la cryptographie, ...

Protocoles cryptographiques (6h de cours, C. Bidan et 3 BE, C. Bidan)
Authentification, certification, échange de clés, attaques classiques, preuves à apport nul de connaissance, ...

Cryptographie avancée (6h de cours, C. Bidan)
Signature de groupe, cryptographie homomorphe, ...

Bibliographie

Menezes, A.J., Vanstone, S.A., Oorschot, P.C. Handbook of applied cryptography. 1st. CRC Press, Inc. 1996 (www.cacr.math.uwaterloo.ca/hac/)

Schneier, B. Applied cryptography (2nd ed.): protocols, algorithms, and source code in C. 1995. ISBN 0-471-11709-9. John Wiley & Sons.

Goubault-Larrecq J. Sécurité, modélisation et analyse de protocoles cryptographiques. La revue de la sûreté de fonctionnement, 20, 2002

Prévention et détection des intrusions et logiciels malveillants

25h30 C / 22h30 TD / 1 ORAL sous forme d'Atelier / 4 crédits ECTS / SISDIM

Cours magistraux : Jean-Marie Borello (6h), Guillaume Hiet (3h), Eric Totel (3h), Valérie Viet Triem Tong (3h), Frédéric Tronel (3h)

Les approches de sécurité classiques sont des approches préventives qui visent à empêcher les violations des propriétés de sécurité. Si les approches préventives sont indispensables, elles ne sont cependant pas suffisantes. En effet, des failles permettent de contourner les mécanismes préventifs. La sécurité réactive s'intéresse en conséquence à des techniques permettant de détecter les tentatives de violation des propriétés de sécurité et de superviser la sécurité des systèmes d'information. Cette forme de sécurité est complémentaire de la prévention et constitue une seconde ligne de défense dans la protection des systèmes.

L'objectif de ce module est de présenter les classes de menaces (virus, vers, exploit), d'introduire les outils préventifs permettant de se protéger a priori de ces menaces (authentification, firewall, IPS), ainsi que les outils réactifs permettant de se prémunir contre les attaques (IDS, anti-virus). La mise en place de ces outils de sécurité commençant par la définition d'une politique de sécurité, le module débute par une introduction aux modèles de sécurité classique : HRU, BLP, Biba, RBAC.

Enfin, un TL, préparé par un BE, permettra de réaliser un buffer overflow afin de bien comprendre le fonctionnement de ce type d'attaque.

Politiques de sécurité : HRU, Bell-LaPadula, Biba, RBAC, OrBAC (3h de cours - G. Piolle)
Détection d'intrusions :

- Systèmes de détection d'intrusions classiques (3h de cours et 1 BE – G. Hiet),
- Approches alternatives pour la détection d'intrusions (3h de cours – V. Viet Triem Tong, 4,5h de cours – E. Totel, 1,5h de cours – G. Hiet),
- Coopération entre approches et corrélation d'alertes (1,5h de cours – E. Totel & G. hiet, 1 BE – G. Hiet)

Virus et malware : Virologie (6h de cours et 2 BE - J-M Borello), Analyse de Malware (1,5h de cours – V. Viet Triem Tong)
Buffer overflow : préparation au TL (1 TD et 1 BE – G. Hiet)
Authentification et contrôle d'accès réseau : 802.1X (1 BE - G. Piolle), Firewall (1,5h de cours et 1 BE firewall - G. Hiet)

Bibliographie

Éric Filiol. Les virus informatiques : techniques virales et antivirales avancées. Springer, 2007.

Éric Filiol. Les virus informatiques : théorie, pratique et applications. Springer, 2003.

McHugh J. Intrusion and intrusion detection. International Journal of Information Security, Vol. 1(1):14-35, 2001

Kerry J. Cox and Christopher Gerg. *Managing Security with Snort & IDS Tools*. O'Reilly. 2004.

Kruegel C., Valeur F., Vigna G. Intrusion detection and correlation: Challenges and solutions. Springer Advances in Information Security, Vol. 14, ISBN: 978-0-387-23398-7, 2005.

Propriété intellectuelle et vie privée

21h C / 1 ORAL sous forme d'atelier / 3 crédit ECTS / SISIS

Cours magistraux : Guillaume Piolle (9h), Caroline Fontaine (9h), Tristan Allard (3h)

L'objectif de ce cours est d'une part de présenter les aspects liés à la protection de la propriété intellectuelle, en illustrant cela à travers la protection des données multimédias, et d'autre part, les problématiques relevant de la protection de la vie privée et des données personnelles. Le contexte juridique et le cadre réglementaire seront également abordés.

Aspect juridique de la protection des données : propriété intellectuelle, données personnelles et autres cadres réglementaires (3h de cours – G. Piolle)

Partie 1 – protection de la propriété intellectuelle

- Tatouage numérique (protection pérenne des données après déchiffrement) – 3h de cours, C. Fontaine.
- Codes anti-collusion (traçage des utilisateurs malhonnêtes) – 3h de cours, C. Fontaine.
- Protocoles de distribution de contenus (combinaison de traçabilité et de respect de la vie privée) – 3h de cours, C. Fontaine

Partie 2 – protection de la vie privée et des données personnelles

- Privacy by design et principes de conception (minimisation, souveraineté, protection au long du cycle de vie…) – 3h de cours, G. Piolle
- Protection de la vie privée dans les bases de données (anonymat, réidentification, assainissement, private information retrieval…) – 3h de cours, T. Allard
- Protection des communications (outils et infrastructures garantissant confidentialité, intégrité, anonymat, répudiabilité…) – 3h de cours, G. Piolle

Bibliographie

N/A.

Ingénierie de la SSI

16h30 C / 3h TD / 1 ORAL sous forme d'atelier / 3 crédit ECTS / SISIS

Cours magistraux : Thierry Bedoin (1h30), Sébastien Husson (1h30), Eric Bornette (1h30), Julie Chuzel (3h), Etienne Lafore (3h), Ludovic Pietre-Cambacedes (3h), Franz Regul (3h), Guillaume Hiet (3h)

L'objectif de ce cours est d'une part d'illustrer comment les concepts théoriques et les outils pratiques étudiés par ailleurs dans la majeure s'exploitent dans des cas concrets pour bâtir des systèmes d'information sécurisés (études de cas, aspects techniques et aspects organisationnels), d'autre part de montrer comment la sécurité d'un tel système sécurisé donné peut et doit être évaluée (test, certification). Un TL et son BE préparatoire sont dédiés au pentest.

Evaluation de la sécurité : 3h de cours de J. Chuzel et 1 BE de G. Hiet
Exemples de réseaux et de systèmes d'information sécurisés :

- Banque de France : 3h de cours - T. Bedoin, S. Husson
- Société Générale : 3h de cours – F. Regul
- EDF : 3h de cours - L. Pietre-Cambacedes
- WaveStone : 3h de cours – E. Lafore
- Analyse de risque : 1,5h de cours - E. Bornette

Bibliographie

N/A.

2. Travaux de laboratoire et projet

Travaux de laboratoire

Durant les deux premiers mois de la formation, les étudiants conduisent, par groupe de 3, trois études courtes d'une durée de 20 heures chacune. Durant ces études, les étudiants doivent faire preuve d'initiative personnelle dans la conduite de leur travail. Les études proposées illustrent des aspects important de la sécurité informatique, déjà abordés en cours. Ils portent sur les thèmes suivants :

1. SSL (Java), C. Bidan
2. Buffer overflow (C), G. Hiet
3. Pen testing, G. Hiet

Projet ou étude industrielle

Le projet où l'étude industrielle porte sur un sujet en lien avec les thèmes de la majeure et est réalisée sous la supervision d'un enseignant-chercheur. Les sujets de projet sont souvent liés aux travaux en cours dans l'équipe « Confidentialité, Intégrité, Disponibilité et REpartition » (CIDRE). Les études industrielles, sont quant à elle réalisées, comme leur nom l'indique, en partenariat avec un industriel sur un sujet qui l'intéresse. Dans un cas comme dans l'autre, la coopération, avec l'équipe de recherche ou avec l'industrie, constitue un aspect important de ce travail. D'un volume de 225h réparties sur l'année scolaire, le projet ou l'étude représente une part importante de la majeure SIS et constitue un « couronnement » de la formation reçue à Supélec, puisqu'il s'agit, pour la première fois, d'y mettre en pratique sur un cas réel le savoir, savoir-faire et savoir-être acquis à l'école. Certains étudiants poursuivent par un stage sur le même sujet.