

SYSTEMES D'INFORMATION SECURISES

Professeur responsable : Ludovic Mé

SIS

COURS	TD/BE	TOTAL	EXAMENS	Intitulé
15h 4,5h 3h 3h 1,5h 1,5 h 1,5h	7 BE (21h) 4 BE (12h) - 1 BE (3h) 1 BE (3h) 1 BE (3 h) -	36h	Exposé 1 (1/2h)	Fondements <i>Compléments langage de programmation</i> <i>Politiques de sécurité</i> <i>Certification de logiciel avec COQ</i> <i>Développement formel en B</i> <i>Unix sécurisé</i> <i>Virtualisation</i>
21 h	3 BE (9 h)	30h	Ecrit 1 (2h)	Cryptographie pour ingénieur
18h 4,5h - 1,5h 3 h 9h	5 BE (15h) - 1 BE (3h) 1 BE (3h) 1 BE (3 h) 2 BE (6 h)	33h	Exposé 2 (1/2h)	Prévention et détection des intrusions et maliciels <i>Connaissance de la menace</i> <i>Authentification 802.1x</i> <i>Firewalling</i> <i>Virologie (anti-virus)</i> <i>Détection d'intrusions (IDS)</i>
10,5h	2 TD (3 h)	13,5h	Oral 1 (1/2h)	Sûreté de fonctionnement
10,5h	1 TD (1,5 h)	12h	Oral 1 (1/2h)	Protection des contenus multimédia
33h 24h 3h 3h 3h	2 BE (6h) - 2 BE (3h) - -	39h	Exposé 3 (1/2h)	Ingénierie de la SSI <i>Etudes de cas</i> <i>Audit technique et test de la sécurité</i> <i>Evaluation et certification de la SSI</i> <i>Respect de la vie privée</i>
TOTAL COURS 108h	TOTAL TD/BE 55,5h	TOTAL C+BE/TD 163,5h	Exams 4h	

BULLETIN D'APPRÉCIATION DE TROISIÈME ANNÉE

majeure
SIS
2012

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	EXP 1	1
	Cryptographie pour ingénieur	EE 1	3
	Prévention et détection des intrusions et maliciels	EXP 2	3
	Sûreté de fonctionnement	EO 1	2
	Protection des contenus	EO 1	
	Ingénierie de la SSI	EXP 3	<u>3</u>
		12	
ÉTUDES ET PROJET	Étude de laboratoire	EL	3
	Projet ou étude industrielle	PRO	<u>9</u>
		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

PRO : projet ou contrat d'étude industrielle

EO : examen oral individuel ou exposé oral (en trinôme ou individuel)

EL : réalisations et comptes rendus des études de laboratoire

La majeure « Systèmes d'Information Sécurisés » permet aux étudiants d'enrichir leur curriculum vitae 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) couvrant cryptologie, prévention et détection des intrusions et maliciels, sûreté de fonctionnement, protection des contenus multimédia, et ingénierie de la sécurité.

1.Cours et travaux dirigés

Fondements

15h C / 21h TD / 1 ORAL / 1 crédit ECTS / SISFON

Guillaume Hiet (1,5h), Guillaume Piolle (3h), Nicolas Prigent (4,5h), Frédéric Tronel (1,5h), Valérie Viet Triem Tong (4,5h)

L'objectif de ce cours est en premier lieu d'apporter aux étudiants les compléments indispensables à la compréhension d'autres cours de la majeure ainsi qu'à la réalisation des études de laboratoire. Par ailleurs, ce cours introduit des concepts fondamentaux en sécurité. Ainsi, sont présentées les grandes approches (politique de sécurité) ayant été proposées pour gérer la confidentialité et l'intégrité des informations au niveau du système d'information, sans tenir compte du recours éventuel additionnel à la cryptographie : HRU, BLP, Biba, RBAC. La déclinaison de ces modèles dans un système d'exploitation réel (Unix) est aussi présentée. La virtualisation des machines, élément fondamental de la sécurité actuelle, est décrite. Enfin, l'importance d'une approche formelle de développement pour garantir un certain niveau de sécurité est illustrée au travers des exemples de COQ et B.

Connaissance de base (4,5h de cours de N.Prigent et 4 BE par les encadrants de TL) :

java avancé, Python, Visual Basic

Politiques de sécurité (3h, G.Piolle)

HRU, Bell-LaPadula, Biba, RBAC, OrBAC

Assistance à la preuve avec Coq (3h de cours et 1 BE, V.Viet Triem Tong)

Méthode B (1,5 h de cours et 1 BE, V.Viet Triem Tong)

Unix sécurisé (1,5h de cours et 1 BE, G.Hiet)

AppArmor, SELinux, GrSecurity

Virtualisation (1,5h de cours, F.Tronel)

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 / 9h TD / 1 ÉCRIT / 3 crédits ECTS / SISCRY

Christophe Bidan (10,5h), Marc Joye (7,5h), Valérie Viet Triem Tong (3h)

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. La partie suivante traite précisément de cet aspect preuve de protocoles cryptographiques, et détaillant plus particulièrement l'approche à base de model-checking. Finalement, l'utilisation des protocoles cryptographiques est présentée dans le contexte de groupes d'utilisateur.

Principes fondamentaux de cryptographie (3h de cours de M.Joye et 1 BE de V.Viet Triem Tong)

Cryptographie symétrique, cryptographie asymétrique, fonctions de hachage, ...

Cryptographie appliquée (4h30 de cours, M.Joye)

Cryptographies symétrique et asymétrique, choix des algorithmes, standards, taille des clés, limites de la cryptographie, ...

Protocoles cryptographiques (4h30 de cours et 2 BE, C.Bidan)

Authentification, certification, échange de clés, attaques classiques, preuves à apport nul de connaissance, ...

Preuve des protocoles cryptographique (3h de cours, V.Viet Triem Tong)

Modèle formel, preuve de propriétés par model-checking, validation.

Protocoles appliqués / Cas d'étude (6h de cours, C.Bidan)

Cryptographie à seuil, authentification de groupe, chiffrement de groupe, signature de groupe, certification de groupe, ...

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 maliciels

18h C / 15h TD / 1 ORAL / 3 crédits ECTS / SISDIM

Christophe Bidan (4,5h), Eric Filiol (3h), Ludovic Mé (9h), Frédéric Tronel (1,5h)

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), comment on tente de s'en protéger au travers de la mise en place d'outils préventifs aptes à les bloquer (firewall, IPS) ou réactifs (IDS, anti-virus). En outre, l'authentification réseau sera étudiée.

Connaissance de la menace (4,5h de cours, C.Bidan)

Attaques Web, buffer overflow, virus

BE Authentification 802.1x (1BE, G.Piolle)

Firewalling (1,5h de cours et 1 BE, F.Tronel)

Virologie (3h de cours et 1 BE, E.Filiol)

Systèmes de détection d'intrusions classiques (3h de cours de L.Mé) et 1 BE de G.Hiet)

Architecture fonctionnelle d'un outil de détection d'intrusion : présentation des différents éléments de cette architecture et de leurs caractéristiques. Acquisition de données de sécurité aux niveaux réseau, OS et application. Etude des modèles classiques pour la détection d'intrusions : approches comportementales et par signatures, limites de ces approches (faux positifs, faux négatifs, techniques d'évasion). Cas de l'IDS SNORT.

Approches alternatives pour la détection d'intrusions (3h de cours, L.Mé)

Exemples de solutions potentielles : détection paramétrée par la politique, approche comportementale à modèle implicite, etc.

Coopération entre approches et corrélation d'alertes (3h de cours de L.Mé et 1 BE de G.Hiet)

Grandes fonctions de la corrélation ; corrélation implicite et explicite ; prise en compte du contexte ; supervision globale de la sécurité (« veille-alerte-réponse »).

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.

Sûreté de fonctionnement

10,5h C / 3h TD / 1 ORAL / 1 crédit ECTS / SISSF

Eric Totel (4,5h), Frederic Tronel (6h)

Ce cours aborde le problème de la disponibilité qui est l'un des attributs majeurs de la sûreté de fonctionnement. L'accent est mis sur la conception et l'utilisation de mécanismes de redondance en présence de fautes transitoires qui peuvent être de nature accidentelle ou intentionnelle. L'essentiel du cours est consacré à l'étude des solutions logicielles permettant d'assurer la disponibilité d'un service critique accédé par des entités extérieures. Les mécanismes de tolérance aux fautes sont analysés aussi bien du point de vue de leurs architectures globales que du point de vue des problèmes algorithmiques fondamentaux qu'ils nécessitent de résoudre.

Définitions et architectures des solutions (4,5h de cours et 1,5h de TD, E.Total)

Après un rappel des concepts liés à la sûreté de fonctionnement et plus particulièrement à la notion de disponibilité, nous considérons tour à tour les fautes accidentelles (pannes matérielles et erreurs de conception) puis les fautes intentionnelles (comportements arbitraires) en présentant des mécanismes assurant la tolérance aux défaillances (détection, recouvrement, masquages) puis des mécanismes de détection (diversification fonctionnelle) et de tolérance aux intrusions (fragmentation-redondance-dissémination).

Calculabilité dans des environnements asynchrones non fiables (6h et 1,5h de TD, F.Tronel)

Les solutions décrites se heurtent toutes à des problèmes de maintien de la cohérence entre des copies distribuées. Pour résoudre ces problèmes, il faut, en particulier, apporter auparavant des solutions à divers problèmes d'accord. Outre le fait de présenter des solutions algorithmiques mettant en œuvre des paradigmes classiques (réutilisables dans d'autres contextes applicatifs), notre objectif est de mettre en lumière les résultats d'impossibilité associés à ce type de problème et les stratégies adoptées pour les contourner (accroître les hypothèses ou affaiblir la spécification du problème). Une étude des fautes arbitraires transitoires sera l'occasion d'identifier les relations qui peuvent exister entre des mécanismes assurant la disponibilité et des mécanismes de recouvrement.

Bibliographie

Laprie J.-C et al. Guide de la sûreté de fonctionnement. Cépaduès - Éditions, 1995.

Nancy A. Lynch. Distributed Algorithms. Morgan Kaufmann Publishers, 1996.

Sape Mullender, Distributed Systems - Second edition, Addison-Wesley, 1998.

Protection des contenus multimédia

10,5h C / 1,5h TD / 1 ORAL / 1 crédit ECTS / SISPC

Mohamed Karroumi (6h), Caroline Fontaine (4,5h)

Ce cours aborde les outils permettant de gérer la diffusion de documents numériques, que ce soit pour contrôler l'accès à ces derniers, faciliter la gestion et la protection des droits d'auteur qui leurs sont associés, lutter contre les fraudes par des techniques de traçage.

Protection de contenus (2h de cours, C.Fontaine)

Cette partie introductive traite du concept de protection de copie, des techniques de base pour la protection de contenus, des techniques utilisées en accès conditionnel, des tendances actuelles (cinéma numérique, superdistribution, ...), de la standardisation. Des exemples concrets de systèmes de protection de contenus (Cinéma Numérique, DTCP, SmartRight...) seront présentés.

DRM (3h de cours, M.Karroumi)

Cette partie approfondit théorie et pratique des trois couches composant le modèle actuel de tout système DRM : l'expression des droits (XrML et ODRL), l'application des droits et la protection du contenu. Les systèmes OMA DRM et Marlin seront plus particulièrement étudiés. Enfin, les différentes approches de l'interopérabilité des DRM seront étudiées (Coral, DVB, DMP).

Tatouage numérique (2,5h de cours et 1 TD, C.Fontaine)

Il s'agit d'une introduction à la problématique du tatouage, qui vise à cacher une information dans un signal, par exemple pour identifier le propriétaire de celui-ci. Cette présentation ne s'appuie pas sur des connaissances de traitement du signal ; l'objectif est de faire découvrir les principes liés à ce type de protection, de plus en plus actuel comme complément aux techniques purement cryptographiques.

Traçage de traîtres (3h de cours, M.Karroumi)

Cette dernière partie présente les différentes techniques qui permettent de diffuser du contenu chiffré à n'importe quel sous-groupe d'utilisateurs choisis parmi un grand nombre ainsi que les techniques visant à repérer les utilisateurs pirates (responsables d'une fuite de contenu ou de clés) afin de permettre leur révocation. L'exemple pratique d'AACS (protection de contenus sur DVD Haute Définition) sera présenté. On abordera également ce problème sous l'angle du tatouage, expliquant comment ces mêmes techniques trouvent leur intérêt dans le contexte du traçage de documents multimédia via des données cachées dans le medium lui-même et pas seulement dans les procédés de chiffrement.

Bibliographie

Davoine F., Pateux S. Tatouage de documents audiovisuels numériques. Hermès-Lavoisier, 2004.

Furht B., Kirowski D. Multimedia security handbook. CRC Press, 2004.

Ingénierie de la SSI

33h C / 6h TD / 1 ORAL / 4 crédit ECTS / SISIS

Thierry Bedoin (3h), Pascal Benard (3h), Eric Bornette (1,5h), Pascal Chour (4,5h), Yves Deswarte (3h), Jean-Marie Fraygefond (3h), Siegfried Günther (3h), Jean-Claude Pailles (3h), Ludovic Pietre-Cambacedes (3h), Jean-Marie Ulmann (3h), Franck Veysset (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 (audit, évaluation, certification). Enfin, un éclairage est apporté sur le nécessaire respect de la vie privée, y compris dans des contextes sécurisés.

Etudes de cas (24h de cours)

Exemples de réseaux et de systèmes d'information sécurisés (T.Bedoin, S.Günther, J-M.Ulmann), ISO 27000 (P.Benard), sécurité des infrastructures critiques (L.Pietre-Cambacedes), carte à puce (P.Chour), informatique de confiance (J-C.Pailles), analyse de risque (E.Bornette), rôle des CERT (F.Veysset)

Audit, test (3h de cours de J-M. Fraygefond et 2 BE de J-M.Fraygefond et C.Bidan))

Evaluation de la sécurité (3h de cours, P.Chour)

Respect de la vie privée (3h de cours, Y.Deswarte)

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, quatre 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 portent sur les thèmes suivants :

1. Application de monitoring de machines (java/RMI), G.Piolle
2. Application base de données (VB et/ou python/SQL), N.Prigent
3. Buffer overflow (C), G.Hiet
4. SSL (C++), C.Bidan

Projet ou étude industrielle

Le projet où l'étude industrielle porte sur un sujet en lien avec les thèmes de l'option et est réalisée sous la supervision d'un enseignant-chercheur. Les sujets de projet sont souvent liés au travaux en cours dans l'équipe « Sécurité des Systèmes d'Information et des Réseaux » de Supélec. 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 entre novembre et mars, le projet ou l'étude représente une part importante de l'option 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.