TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

# SYLLABUS

INP ENSEEIHT – INSA Toulouse - ENAC

# TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

## Aspects pédagogiques

La formation sera dès la première année adressée à un public diversifié, venant de la formaiton initiale et de la formation continue. Au niveau de la formation initiale les étudiants arrivent d'écoles d'ingénieurs et de parcours différents. Plus précisément il y aura potentiellement des élèves venant des formations :

- informatique et réseaux de l'INSA Toulouse ;
- automatique et électronique de l'INSA Toulouse ;
- génie mathématique et modélisation de l'INSA Toulouse ;
- sciences et ingénierie de la navigation aérienne de l'ENAC ;
- télécommunications et réseaux de l'INP-ENSEEIHT ;
- informatique mathématiques et applications de l'INP-ENSEEIHT ;
- et des élèves de divers départements d'autres écoles de l'INP, des Mines d'Albi, et du Centre Universitaire Jean-François Champollion.

Pour s'adapter à un public aussi diversifié nous intégrerons dans la formation diverses techniques pédagogiques..

**Autoformation :** les étudiants disposent d'une salle à l'année avec des ordinateurs récents et haut de gamme et de nombreux éléments actifs dernier cri (switchs, routeurs, ASAs, etc.). De nombreuses références sont données aux étudiants pour permettre de ser remettre à niveau et d'approfondir leurs connaissances en auto-formation.

**Projets :** dès le démarrage de l'année scolaire les étudiants seront regroupés équipes avec des profils variés au niveau des compétences d'entrée (électronique, réseau, système, programmation, mathématiques). L'évaluation sera en grande partie par projets, où les équipes seront en concurrence.

**Challenges :** il est habituel dans les formations en sécurité de participer aux challenges en ligne nationaux ou internationaux. Un des principaux objectifs que nous nous sommes donnés est la participation à ces challenges. De nombreuses ressources en ligne sont disponibles pour préparer ces challenges et nous avons déjà donné des pointeurs vers ces ressources aux étudiants qui ont déjà déposé leur dossier de candidature. Nous avons également des challenges que nous avons développé nous mêmes. Ces *challenges* seront structurés sous la forme d'une suite de défis qui permettent aux étudiants de pénétrer au fur et à mesure au cœur d'un système d'informations ou d'un réseau vulnérable. Cette méthode d'apprentissage active permet aux étudiants de mieux cerner les stratégies d'attaque que des personnes malveillantes peuvent adopter lors d'une attaque informatique. Elle présente alors l'avantage de leur faire réaliser les enjeux, défis et difficultés de leur futur métier.

**Conférences :** un ensemble de conférences est mis en place pour permettre à des intervenants industriels et gouvernementaux d'illustrer les concepts théoriques vus lors des différents enseignements. Cette forme d'apprentissage permet aux étudiants 1) d'être sensibilisé aux implications de la mise en place de la sécurité informatique au sein d'une entreprise et au sein d'un état, et 2) de mettre en perspective leurs acquis vis-à-vis des problématiques concrètes rencontrées dans le monde industriel ou gouvernemental.

# Structure générale de la formation

**1er semestre :**
- 400h d'enseignements.
- dont 100h de TP et 60h Compétences professionnalisantes (Anglais, Conférences)

380h distribués sur 4 modules plus 20h d'Anglais :
- 80h Module d'Entrée : Bases de la Sécurité
- 95h Module Réseau
- 105h Module Logiciel / Système / Matériel
- 100h Module de Sortie : Cas pratiques

**2ème semestre :** Projet long (rapport et soutenance en Anglais), certifications, stage de 6 mois

**Calendrier :**
- Rentrée : fin septembre
- Fin premier semestre : fin janvier
- Début stage : mars
- Fin stage : septembre

**Répartition des modules dans l'année :**
- Module d'Entrée : trois semaines à partir de la rentrée, temps complet
- Module de Sortie : jeudis matin (conférences) et trois semaines complètes en janvier
- Module Réseau : lundis et mardis de mi-octobre à début janvier
- Module Logiciel / Système / Matériel : mercredis et vendredis de mi-octobre à fin décembre

TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

# Module d'Entrée : Bases de la Sécurité

INP ENSEEIHT – INSA Toulouse - ENAC

Fiche Enseignement

# Rappels et harmonisation en systèmes d'exploitation
# 6 créneaux de 1h45 (10h30)

| OBJECTIFS |
|---|
| L'objectif de ce cours est de mettre l'ensemble des étudiants à niveau sur les principaux concepts fondamentaux des systèmes informatiques, en particulier ceux qui sont utiles pour les différents enseignements de sécurité par la suite. Les principaux points abordés concernent les architectures matérielles des ordinateurs, les concepts fondamentaux des systèmes opératoires (espace noyau, espace utilisateur, processus et les mécanismes d'ordonnancement associés, etc).<br><br>A l'issue de cet enseignement, l'étudiant sera capable de décrire le fonctionnement des éléments importants d'un système d'information. Sur cette base, il sera capable d'analyser ces éléments pour déterminer leur impact sur la sécurité du système. |

| DEROULEMENT | | |
|---|---|---|
| **Promo** | **Durée** | **Contenu** |
| Entière | 2 créneaux | **Architecture des ordinateurs**<br>✓ Structure du processeur (instruction, MMU, contrôleur mémoire, registres, modes ,etc)<br>✓ Structure des buns internes (pcie, etc)<br>✓ Accès aux composants depuis le processeur (MMIO, PIO, requêtes PCIE) |
| Entière | 4 créneaux | **Système d'exploitation**<br>✓ Les processus<br>✓ Techniques d'ordonnancement<br>✓ Gestion des appels systèmes |

| INTERVENANTS |
|---|
| Stéphane Duverger – Airbus Groupe Innovation |

Fiche Enseignement

# Rappels et harmonisation en réseau
# 6 créneaux de 1h45 (10h30)

| OBJECTIFS |
|---|
| L'objectif de ce cours est de mettre l'ensemble des étudiants à niveau sur les principaux concepts fondamentaux des réseaux d'ordinateurs, en se focalisant sur les concepts des réseaux IP.<br>Les principaux points abordés concernent les couches MAC, réseaux et transports (tels que DHCP, ARP, IP ou TCP), mais également certains protocoles applicatifs particulièrement sensibles du plan de gestion (tels que les protocoles d'annuaires avec le DNS ou le routage avec RIP ou BGP).<br><br>A l'issue de cet enseignement, l'étudiant sera capable de décrire les principes fondamentaux de la constructions des protocoles réseaux, sera capable d'analyser des traces réseaux et sera en mesure de comprendre l'encapsulation des flux. Il sera en mesure de proposer l'utilisation de certains protocoles et services en fonction des besoins. En particulier, il sera en mesure de comprendre les principaux éléments des protocoles réseaux qui peuvent avoir des impacts sur la sécurité. |

| DEROULEMENT | | |
|---|---|---|
| **Promo** | **Durée** | **Contenu** |
| Entière | 2 créneaux | Rappels sur l'architecture IP, le modele OSI et les différentes couches associées |
| Entière | 2 créneaux | Présentation plus détaillée des couches du modèle OSI les plus concernées par les problèmes de sécurité : la couche 2 (protocole ARP notamment) et la couche 3 (protocole IP, la fragmentation, les options), la couche 4 (protocole TCP notamment) |
| Entière | 1 créneau | Présentation des protocoles du plan de gestion |
| Entière | 1 créneau | Présentation des principaux protocoles de routage tels que RIP ou BGP |

| INTERVENANTS |
|---|
| Emmanuel Chaput – INP-ENSEEIHT |

Fiche Enseignement

# Rappels et harmonisation en programmation C et assembleur 9 créneaux de 1h45 (15h75)

OBJECTIFS

L'objectif de ce cours est de mettre l'ensemble des étudiants à niveau sur les principaux concepts fondamentaux de la programmation. Les langages orientés bas-niveaux seront privilégiés car ce sont ceux qui seront le plus abordés lors de l'analyse de problèmes de sécurité. Les langages abordés seront donc le langage C et l'assembleur, en particulier sur architecture x86.

A l'issue de ce cours, l'étudiant maîtrisera les techniques de base de la programmation avec le langage C et assembleur. Il sera capable de concevoir des programmes en utilisant ces techniques. Il sera capable d'analyser précisément un programme écrit avec ces langages pour en comprendre son fonctionnement. Il sera également capable de comprendre le fonctionnement de programmes écrits dans des langages différents.

DEROULEMENT

| **Promo** | **Durée** | **Contenu** |
|---|---|---|
| Entière | 3 créneaux | **Le Langage d'assemblage x86, ARM**<br>✓ Rappels de l'architecture des processeurs x86/ARM<br>✓ Présentation des jeux d'instructions x86/ARM<br>✓ Chaînes de compilation |
| Entière | 6 créneaux | **Le langage C**<br>✓ Le langage C et ses principales caractéristiques<br>✓ Gestion de la mémoire, statique et dynamique<br>✓ Utilisation généralisée des pointeurs, arithmétique des pointeurs<br>✓ Structures de données et pointeurs<br>✓ Les différents espaces d'adressage en fonction des sections de mémoire (code, pile, DATA, BSS, tas)<br>✓ Les entrées/sorties |

INTERVENANTS

Vincent Nicomette – INSA Toulouse
Eric Alata – INSA Toulouse

Fiche Enseignement

# Définitions et techniques de base en sécurité et *safety*
# 4 créneaux de 1h45 + 1h d'examen (8h)

| OBJECTIFS |
|---|
| Ce cours présentera la terminologie et les bases fondamentales de la sécurité et de la tolérance aux fautes.<br><br>A l'issue de ce cours, l'étudiant saura :<br>✓ différencier les domaines de la sécurité (sécurity et safety) ;<br>✓ distinguer et utiliser correctement les termes correspondant : aux propriétés de sécurité de l'information et des systèmes ; et aux techniques apportant la sécurité<br>✓ appréhender la sécurité dans sa globalité en allant au-delà des questions techniques et en prenant en compte les aspects organisationnels ;<br>✓ modéliser les différents types d'attaquant ;<br>✓ reconnaître les grands outils et éléments architecturaux apportant de la sécurité dans un réseau comme dans un système ;<br>✓ décrire les différentes approches pour authentifier un utilisateur et autoriser des actions sur un système informatique. |

DEROULEMENT

| **Promo** | **Durée** | **Contenu** |
|---|---|---|
| Entière | 1 créneau | Définitions principales de la sécurité (CID, AAA, tolérance aux fautes, politiques de sécurité, évaluation, classification des attaques) |
| Entière | 1 créneau | Tolérance aux fautes |
| Entière | 2 créneaux | Éléments architecturaux (pare-feu, IDS, Antivirus) |

| INTERVENANTS |
|---|
| Carlos Aguilar – INP-ENSEEIHT<br>Jean-Charles Fabre – INP-ENSEEIHT<br>Etienne Capgras – Solucom |

Fiche Enseignement

# Cryptographie
# 19 créneaux de 1h45 + 2h d'examen (35h15)

OBJECTIFS

Ce cours présente dans un premier temps les bases de la complexité pour la cryptographie et la notion d'aléa. Ensuite la cryptographie symétrique et asymétrique ainsi que les attaques habituelles sont décrites. Enfin les standards modernes et quelques notions de cryptographie avancée sont introduits. Tout ce cours alternera l'introduction aux techniques cryptographique et définitions de sécurité et notions d'attaque (qui n'ont un sens que face à des techniques cryptographiques).

A l'issue de ce cours, l'étudiant saura :

- ✓ distinguer les différents outils cryptographiques, comprendre ce qu'ils peuvent apporter à la sécurité et ce qu'ils ne peuvent pas ;
- ✓ appliquer les bonnes pratiques, et comprendre les dangers d'une utilisation inappropriée ;
- ✓ utiliser les termes techniques de la cryptographie et rechercher les propriétés qui peuvent apporter des contributions à des problèmes complexes de sécurité ;
- ✓ trouver les standards internationaux de la cryptographie, comprendre leur contenu et mettre en place une utilisation d'un outil cryptographique respectant les standards ;
- ✓ identifier les dangers classiques (homme du milieu, attaques par canaux cachés) et utiliser des modèles d'attaquant larges pour définir si une nouvelle utilisation d'un outil cryptographique est sûre ou pas ;
- ✓ réaliser des déploiements à l'aide d'outils réels de haut niveau (PKI, VPN, IPSec) ou de bas niveau (openss) en choisissant les algorithmes, les niveaux de sécurité, les modes de fonctionnement de façon raisonnée.

DEROULEMENT

| **Promo** | **Durée** | **Contenu** |
|---|---|---|
| Entière | 3 créneaux | **Introduction et notions de base**<br>✓ Introduction (apports et limites de la cryptographie) et fonctions de base (générateurs pseudo-aléatoires, fonctions de hachage)<br>✓ Notions de complexité (temps exponentiel, polynomial, notion d'avantage, distingueurs, avantage d'un attaquant) |
| Entière | 3 créneaux | **La cryptographie symétrique**<br>✓ Techniques (Vernam, chiffrement à flots, chiffrement par blocs, intégrité et chiffrement authentifié, problèmes de la gestion de clés)<br>✓ Attaques (distinction de force brute vs dictionnaires, notion de bits de sécurité et de cryptosystème faible, durée de vie d'une clé, mécanismes de dérivation) |
| Entière | 7 créneaux | **La cryptographie asymétrique**<br>✓ Techniques (le chiffrement à clé publique et l'échange de clés, la cryptographie hybride, notion de clés de session, la signature, l'horodatage)<br>✓ Attaques (factorisation, logarithme discret, mauvais paramétrages historiques, homme du milieu, oracles de déchiffrement) et les définitions de sécurité (sens unique, attaques par clairs choisis, par chiffrés choisis)<br>✓ Les certificats numériques et les PKI<br>✓ Les attaques par canaux cachés (analyse de courant, |

| | | |
|---|---|---|
| | | de temps) et les contres classiques (protections physiques, randomisation, algorithmes en temps constant) |
| Entière | 6 créneaux | **Standards cryptographiques et notions avancées**<br>✓ Les standards cryptographiques du NIST (SP 800) et de fait (TLS, IKE) et la notion d'association de sécurité.<br>✓ La cryptographie avancée (chiffrement basé sur l'identité, cryptographie à boîte blanche, chiffrement homomorphe, signatures de groupe et d'anneau, chiffrement sur des attributs, chiffrement fonctionnel) |

| INTERVENANTS |
|---|
| Carlos Aguilar – INP-ENSEEIHT |

TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

# Module Logiciel/Système/Matériel

INP ENSEEIHT – INSA Toulouse - ENAC

Fiche Enseignement

# Vulnérabilités logicielles
# 11 créneaux de 1h45 + 2h d'examen (21h15)

## OBJECTIFS

L'objectif de ce cours est de présenter aux étudiants différents types de vulnérabilités logicielles que l'on rencontre fréquemment, en particulier dans les programmes écrits en langage C, langage qui sera le support pour ce cours. Les contre-mesures usuelles protections mémoires permettant de se protéger de ce type de vulnérabilités sont également proposées.

A l'issue de cet enseignement, l'étudiant saura analyser un programme et juger de son niveau de sécurité en considérant les vulnérabilités logicielles présentées dans cet enseignement. Il sera capable d'identifier les tests à réaliser pour mettre en évidence l'existence d'une vulnérabilité logicielle. Il sera également capable de comparer différentes contre-mesures, d'identifier le plus adapté pour corriger une vulnérabilité et de le mettre en œuvre.

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 1 créneau | ✓ Rappels de l'appels de fonction sur architecture x86 (frame de pile, sauvegarde de l'adresse de retour, passage de paramètres, stockage des variables locales) et du fonctionnement des bibliothèques partagées |
| Entière | 2 créneaux | ✓ Débordement de tampon dans la pile, principe d'exploitation, exemples |
| Entière | 2 créneaux | ✓ Attaque de type return-into-libc, en cas de protection en exécution de la pile et sa généralisation avec les attaques de type ROP (*Return Oriented Programming*) |
| Entière | 1 créneau | ✓ Débordements de tampon dans d'autres sections de mémoire des processus : le tas et sa gestion, DATA, BSS |
| Entière | 1 créneau | ✓ Exploitation des vulnérabilités logicielles liées à l'utilisation des chaînes de caractères : les chaînes de format |
| Entière | 1 créneau | ✓ Exploitation des vulnérabillités logicielles liées à la manipulation des entiers : *Integer overflow* |
| Entière | 1 créneau | ✓ Les risques liées à l'utilisation de programmes SUID, en particulier SUID-root ; les précautions à prendre pour coder ce type de programme |
| Entière | 1 créneau | ✓ Identification des vulnérabilités par analyse statique de code |
| Entière | 1 créneau | ✓ Les contre-mesures techniques pour faire face à ces différentes vulnérabilités (les mécanismes de protection usuels des compilateurs, les canary, la randomization de l'espace d'adressage (ASLR), etc) |

## INTERVENANTS

Eric Alata – INSA Toulouse
Vincent Nicomette – INSA Toulouse
Benoit Morgan – LAAS/CNRS

Fiche Enseignement

# Techniques virales
# 6 créneaux de 1h45 + 1h d'examen (11h30)

| **OBJECTIFS** |
|---|
| L'objectif de ce cours est de présenter aux étudiants la théorie liée aux vers et virus. Une première partie est consacrée à l'étude des algorithmes utilisés par les vers et virus pour infecter les systèmes informatique et se répandre. Cette connaissance est nécessaire pour appréhender les protections conctre ces malveillances. Ces protections font l'objet de la seconde partie qui se consacre plus particulièrement sur les anti-virus avec les méthodes qu'ils utilisent pour la détection des vers et virus.<br>A l'issue de ce cours, l'étudiant saura apprécier les enjeux de la protection virale, décrire les différents types d'infection informatique, analyser les techniques virales et antivirales et éagir en cas d'infection. |

| **DEROULEMENT** | | |
|---|---|---|
| **Promo** | **Durée** | **Contenu** |
| Entière | 2 créneaux | **Présentation des virus et vers**<br>✓ Historique<br>✓ Infections informatiques (définition et taxonomie)<br>✓ Virus et vers (automates génériques, diagramme fonctionnel et stratégies anti-détection) |
| Entière | 2 créneaux | **Présentation des anti-virus**<br>✓ Théorème de Cohen<br>✓ Techniques statiques de détection<br>✓ Techniques dynamiques de détection<br>✓ Effic**acité et conduite a tenir** |
| Entière | 2 créneaux | **Expérimentations**<br>✓ écriture d'un virus en shell bash<br>✓ *autorun* d'un script malveillant sur clé USB |

| **INTERVENANTS** |
|---|
| Sébastien Leriche – ENAC |

Fiche Enseignement

# Développement Logiciel Sécurisé
# 9 créneaux de 1h45 et 1h d'examen (16h45)

## OBJECTIFS

L'objectif de ce cours est de présenter un ensemble de bonnes pratiques pour développer du logiciel de façon sécurisée. Ces bonnes pratiques sont illustrées avec le système OpenBSD qui est reconnu pour avoir adopté des méthodes de développement rigoureuses. Une présentation des méthodes formelles pour la détection de vulnérabilités sera également réalisée.

A l'issue de cet enseignement, l'étudiant doit être capable de comprendre les enjeux du développement logiciel sécurisé, en connaître les principales méthodes et être capable de proposer l'utilisation de ces méthodes en fonction du logiciel qui est développé, de sa fonction et du contexte dans lequel il est utilisé.

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 6 créneaux | Preuves formelles et sécurité |
| Entière | 1 créneau | Programmation défensive utilisée dans le projet OpenBSD : principes du moinde privilége dans le codage de fonctions sensibles (exemple de strlcpy), principes du moindre privilège dans les programmes SUID, utilisation d'API plus sûres |
| Entière | 2 créneaux | Analyse statique |

## INTERVENANTS

David Delmas – Airbus
Matthieu Herrb – LAAS-CNRS
Yamine Aït-Ameur – INP-ENSEEIHT
Marc Pantel – INP-ENSEEIHT

Fiche Enseignement

# Protection des systèmes d'exploitation
# 10 créneaux de 1h45 et 2h d'examen (19h30)

## OBJECTIFS

L'objectif de ce cours est de présenter les principaux mécanismes de protection qui existant aujourd'hui dans les noyaux de systèmes d'exploitation. Ce cours aborde également un certain nombre d'attaques permettant d'exploiter des vulnérabilités des noyaux de système eux-mêmes. Il se base sur les noyaux de système Linux et Windows. Il fournit également un panorama des outils et techniques disponibles pour protéger les données contenues dans les systèmes de fichiers et dans la mémoire. La plupart de ces techniques reposent sur des méthodes de chiffrement et sur des contrôles d'accès.

A l'issu de ce cours, l'étudiant devra être capable d'identifier les propriétés de sécurité à préserver concernant les données manipulées dans un système pour ainsi déterminer de les protections les plus adaptées à mettre en œuvre. L'étudiant sera également capable d'analyser un système d'exploitation pour identifier les menaces et les vulnérabilités qui peuvent l'affecter. Il sera capable de décrire les conséquences liées à l'exploitation de ces vulnérabilités. Il sera capable d'exposer les différents mécanismes de protection pour contenir ces menaces. Il sera capable de choisir et d'implémenter le mécanisme le plus adapté au système en train d'être étudié.

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 1 créneau | Rappels sur les éléments d'architecture x86 (rings, gestion mémoire, I/O, …) |
| Entière | 5 créneaux | **Etudes des noyaux Linux et Windows du point de vue de la sécurité**<br>✓ Mécanismes noyau de protection de l'espace utilisateur<br>✓ Attaques sur le noyau depuis l'espace utilisateur (via abus de privileges, ...)<br>✓ Protection du noyau face à des attaques depuis l'espace utilisateur<br>✓ Ouverture sur la protection du noyau face aux attaques de composants matériels |
| Entière | 3 créneaux | **Etude de la sécurité des données dans un système**<br>✓ Présentation des systèmes de fichiers<br>✓ Protection des fichiers (droits d'accès, chiffrement)<br>✓ Gestion des droits vis-à-vis des accès mémoire<br>✓ Protection mémoire |

## INTERVENANTS

Eric Lacombe – Airbus
Alexandre Gazet – Quarkslab
Sébastien Renaud – Quarkslab
Eric Alata – INSA
Vincent Nicomette – INSA

Fiche Enseignement

# Attaques matérielles et sécurisation du matériel
# 11 créneaux de 1h45 + 2h d'examen (21h15)

| OBJECTIFS |
|---|
| L'objectif de ce cours est de présenter les principales attaques réalisées depuis le matériel ainsi que les contre-mesures associées. Un balayage des composants d'un système sera réalisé en identifiant l'utilité et les risques associés à la présence de chacun de ces composants. Certains de ces risques seront illustrés par des attaques récentes, soit en reconfigurant les composants concernés, soit en réalisant une étude matérielle et physique de ces composants. Aussi, des contre-mesures seront présentées avec les dernières avancées en terme de protection matérielle réalisées par les fondeurs de processeurs et de chipset.<br>A l'issue de ce cours, l'étudiant devra être capable d'obtenir une vue globale des échanges entre les composants matériels d'un système d'information, en considérant aussi bien les composants logiciels et réseaux que matériels. Il sera capable de comprendre le fonctionnement d'une attaque sur le matériel, de la décrire et d'expliquer les mécanismes de protection associés. Il sera également capable d'identifier les composants critiques d'un système, d'analyser les vulnérabilités pouvant cibler ces composants, de déterminer les contre-mesures permettant de les protéger et de mettre en œuvre ces contre-mesures. |

| DEROULEMENT | | |
|---|---|---|
| **Promo** | **Durée** | **Contenu** |
| Entière | 7 créneaux | **Composants matériels des systèmes d'information pour la sécurité**<br>✓ Panorama des composants matériels présents dans un système informatique<br>✓ Utilisation de ces composants pour améliorer la sécurité (virtualisation, TPM, IO-MMU)<br>✓ Création d'une chaîne de confiance au démarrage basée sur l'utilisation de matériels de confiance<br>✓ Présentation de projets de recherche utilisant le matériel comme support pour la sécurité<br>✓ Mise en pratique de ces concepts par le développement d'une solution de sécurité sur architecture Intel |
| Entière | 4 créneaux | **Attaques et sécurisations matérielles**<br>✓ Rappels fondamentaux de microélectronique et d'architecture matérielle<br>✓ Canaux auxiliaires (SPA, DPA, ...)<br>✓ Contre mesures matérielles et algorithmiques<br>✓ Démonstration d'une attaque Bellcore sur un processeur grand public |

| INTERVENANTS |
|---|
| Eric Alata – INSA Toulouse<br>Rémy Daudigny – Thales (Cesti)<br>Stéphane Duverger – Airbus Group Innovation |

Fiche Enseignement

# Reverse Engineering
# 5 créneaux de 1h45 + 1h d'examen (9h45)

## OBJECTIFS

L'objectif de ce cours est de présenter aux étudiants les activités autour de la rétro-conception de logiciels (*reverse engineering)*. Dans un premier temps, la chaîne de compilation est présentée avec les modèles utilisés par les compilateurs pour générer le code machine. Dans un second temps, des stratégies sont présentées pour inverser ce processus pour premettre de mieux comprendre certaines parties d'un code logiciel. Pour finir, les contre-mesures à la rétro-conception sont présentées pour rendre cette activités plus difficile.

A l'issue de cet enseignement, l'étudiant sera capable d'analyser précisément et de décrire globalement le fonctionnement d'un programme en se basant uniquement sur le code assembleur. Il sera capable d'appliquer les acquis des enseignements liés à l'étude des vulnérabilités pour identifier des vulnérabilités dans ces programmes. Il sera capable de justifier l'existence des vulnérabilités en mettant en œuvre une preuve de concept de l'exploitation.

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 1 créneau | **Chaîne de compilation**<br>✓ Introduction aux techniques de compilation<br>✓ Analyse de graphes de controles et de donnees |
| Entière | 5 créneaux | **Techniques de rétro conception logicielle**<br>✓ Introduction à la rétro-ingénierie: méthodologie et outils<br>✓ Découverte et prise en main des outils: désassembleurs, débuggers et de leurs languages de scripting<br>✓ Application à l'analyse de code malveillant et/ou à l'exploitation de vulnérabilité<br>✓ Initiation à l'outil IDA |

## INTERVENANTS

Eric Alata – INSA Toulouse
Alexandre Gazet – Quarkslab
Jean-Baptiste Bedrune – Quarkslab

TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

# Module Réseau

INP ENSEEIHT – INSA Toulouse - ENAC

Fiche Enseignement

# Attaques et sécurisation des couches OSI
# 11 créneaux de 1h45 + 2h d'examen (21h15)

## OBJECTIFS

Ce cours présente les principales attaques et contre-mesures sur les couches OSI en commençant par les attaques sur le lien physique et en allant vers les attaques applicatives sur les protocoles indispensables au bon fonctionnement d'un réseau.

À la fin de ce cours l'étudiant saura :

- ✓ Reconnaître et mettre en place les attaques réseau classiques dans le cadre d'un test d'intrusion
- ✓ Identifier et mettre en place les mécanismes de protection contre ces attaques
- ✓ Informer sur les dangers inhérents à un réseau informatique et connaître les limites des protections que l'on peut obtenir à un coût raisonnable
- ✓ Informer sur les apports des grandes infrastructures de sécurité DNS, et BGP mises en place par l'ICANN
- ✓ Utiliser et mettre en place ces infrastructures

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 2 créneaux | Attaques sur les couches 1-4 (écoute, usurpation et inondation MAC, empoisonnement ARP, usurpation IP, fragmentation IP, usurpation TCP, vol de session TCP) |
| Entière | 1 créneau | Contres sur les couches 1-4 (commutation, port security, tables ARP, IDS spécifiques). |
| Entière | 4 créneaux | Attaques sur la couche 7 (usurpation DNS classique et à la Kaminsky, détournement des routes RIP et BGP), et défense (DNSSEC, RPKI) |
| Entière | 4 créneaux | Dénis de service : principes (distribution, exploitation de bugs), inondations (amplification par smurf ou fragmentation, amplification DNS, SYN flood), malformations (ping of death, Teardrop), perturbations (TCP reset), détection d'anomalies et attaques de type dénis de service distribué (DDOS), architectures de botnets, sécurité proactive |

## INTERVENANTS

Carlos Aguilar – INP-ENSEEIHT
Philippe Owezarski – LAAS-CNRS

Fiche Enseignement

# Sécurité des réseaux non-filaires
# 7 créneaux de 1h45 et 1h d'examen (13h15)

## OBJECTIFS

Cet enseignement présente la sécurisation des réseaux cellulaires de GSM à LTE ainsi que les attaques et la sécurisation des réseaux WiFi.

À la fin de ce cours l'étudiant saura dans le domaine du WiFi :

- ✓ Choisir une solution de sécurité adaptée pour un point d'accès
- ✓ Comprendre et choisir les multiples options disponibles pour chaque solution
- ✓ Mettre en avant les apports en sécurité et limites de la solution choisie
- ✓ Réaliser un test d'intrusion sur un point d'accès

À la fin de ce cours l'étudiant saura dans le domaine des réseaux cellulaires :

- ✓ Différentier les objectifs de sécurité dans les différents réseaux cellulaires
- ✓ Décrire les mécanismes d'authentification et d'échange de clés et comparer les apports en sécurité de chacun
- ✓ Décrire les attaques possibles dans le cadre de chaque technologies
- ✓ Reconnaître les éléments architecturaux de la sécurité dans un réseau d'opérateurs

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 4 créneaux | WiFi sécurisations (portails captifs, WPA1\|2, 802.1X, EAP) et dangers (usurpations MAC et IP, tunnels, failles WPA) |
| Entière | 3 créneaux | Réseaux cellulaires (évolution de la sécurisation dans GSM / GPRS / EDGE / UMTS / LTE) |

## INTERVENANTS

Isabelle Kraemer – Orange
Carlos Aguilar – INP-ENSEEIHT

Fiche Enseignement

# Sécurisation des protocoles
# 5 créneaux de 1h45 et 1h d'examen (9h45)

## OBJECTIFS

Ce cours met en avant les nombreux protocoles fragiles utilisés de nos jours et décrit les bonnes pratiques pour concevoir des protocoles sûr a posteriori et des techniques pour sécuriser des protocoles fragiles a posteriori par l'utilisation de tunnels.

À la fin de ce cours l'étudiant saura :

- ✓ Reconnaître les protocoles fragiles mis en place habituellement dans un réseau informatique
- ✓ Sécuriser les protocoles fragiles par l'utilisation de tunnels pour les applications où ceci sera nécessaire
- ✓ Utiliser SSH et les fonctions associées (transfers de fichiers, proxys, etc.)
- ✓ Décrire les bonnes pratiques pour la définition d'un protocole sécurisé

## DEROULEMENT

| **Promo** | **Durée** | **Contenu** |
|---|---|---|
| Entière | 1 créneau | Protocoles fragiles (protocoles en r, NFS, X, FTP, etc.), sécurisation a priori (authentification, confidentialité, intégrité) et a posteriori (utilisation d'un tunnel) |
| Entière | 2 créneaux | SSH : description (mise en place et sécurisation de la connexion), utilisation normale (shell, transfer de fichiers), et pour la sécurisation d'autres protocoles (tunnels, proxy SOCKS, sécurisation de X) |
| Entière | 2 créneaux | Mise en pratique : utilisation basique de SSH, mise en place de tunnels, d'un proxy SOCKS, sécurisation de X et attaques par un utilisateur root distant |

## INTERVENANTS

Carlos Aguilar – INP-ENSEEIHT

Fiche Enseignement

# Composants fondamentaux d'une architecture de sécurité
# 10 créneaux de 1h45 et 2h d'examen (19h30)

## OBJECTIFS

Cet cours présente les éléments architecturaux indispensables à la sécurisation d'un réseau : Firewalls, NIDS, IPsec, VPN et outils de gestion des identités.

À la fin de ce cours l'étudiant saura :

- ✓ Distinguer les différents types de pare-feux ainsi que leurs capacités et limitations
- ✓ Définir et auditer une architecture de filtrage adaptée à un réseau informatique donné
- ✓ Choisir pour un tunnel IPsec les protocoles à utiliser, les modes de fonctionnement et un plan de routage adapté pour les passerelles associées
- ✓ Faire le design complet d'une architecture de sécurité pour un réseau complexe incluant la gestion des identités et de l'authentification

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 2 créneaux | **Firewalls** : classes (sans états, avec états, applicatif, personnel) ; architectures (routeur filtrant, bastion, zones démilitarisées) ; limites (fragmentation, tunnels, authentification par IP) |
| Entière | 2 créneaux | **IPsec** : principes sur les tunnels (niveaux 2 et 3), protocoles (AH, ESP) et modes (transport et tunnel) de IPsec, négiciations (IKE, TLS), routage et utilisations classiques (lien AP-AS dans 802.1X, antqennes/site central, roaming) |
| Entière | 1 créneau | **Solutions VPN** : OpenVPN, Cisco VPN, les solutions VPN SSL |
| Entière | 2 créneaux | **NIDS** : outils classiques (Snort, Suricata, IDS spécialisés), la prévention (bans firewall, etc.), les sondes et SIEM |
| Entière | 2 créneaux | **IAM** : Outils de gestion de l'identite et de l'authentification |

## INTERVENANTS

Carlos Aguilar – INP-ENSEEIHT
Etienne Capgras – Solucom
Rodolphe Ortalo – CARSAT

Fiche Enseignement

# Bureau d'étude en réseau
# 20 créneaux de 1h45 (35h)

## OBJECTIFS

Ce bureau d'étude a pour but de mettre en pratique les divers enseignements du module réseau.

À la fin de ce cours l'étudiant saura :

- ✓ Mettre en place et auditer un tel tunnel IPsec
- ✓ Mettre en place ou auditer un VPN créé sur du IPsec manuellement ou en utilisant les outils tout-en-un du marché
- ✓ Mettre en place et auditer un système de détection d'intrusion éventuellement distribué avec des options de prévention
- ✓ Mettre en place une architecture de logs avec un système centralisé de gestion des événements

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 3 créneaux | **Mise en pratique d'une architecture de logs + SIEM** |
| Entière | 4 créneaux | **Mise en pratique Attaques ARP + IDS/IPS** |
| Entière | 4 créneaux | **Mise en pratique Firewalls** (mise en place, contournement sans états, contournements SSH/SOCKS/DNSTOTCP) |
| Entière | 8 créneaux | **Mise en pratique sur ASA Cisco** (Firewall, VPN, IDS) |

## INTERVENANTS

Carlos Aguilar – INP-ENSEEIHT
Nicolas Larrieu – ENAC
Vincent Nicomette – INSA Toulouse
Etienne Capgras – Solucom

TLS-SEC : La Formation en Sécurité des Systèmes d'Information de Toulouse Ingénierie

# Module de Sortie : Cas Pratiques d'Application

INP ENSEEIHT – INSA Toulouse - ENAC

Fiche Enseignement

# Conférences en Gouvernance de la sécurité
# 17 créneaux de 1h45 et 3h d'examen (32h45)

## OBJECTIFS

Cette série de conférences présentera divers aspects de la sécurité dans le monde de l'entreprise avec un intérêt particulier pour les question légales, humaines et organisationnelles.

A la fin du cours l'étudiant saura **:**

- ✓ Identifier les principaux éléments juridiques liés à la SSI
- ✓ Reconnaître et définir les principaux acteurs chargés de la sécurité à l'intérieur et autour d'une entreprise, ainsi que les difficultés associées.
- ✓ Identifier les enjeux et les parties prenantes, au sein d'une organisation, pour définir et élaborer les briques de base d'une démarche de gouvernance de la sécurité.
- ✓ Apprécier les besoins en sécurisation à satisfaire et les objectifs de sécurité à atteindre pour mettre en place des exigences de sécurité d'ordres juridique / organisation / technique, aux niveaux des mesures de prévention / protection / récupération.
- ✓ Structurer et organiser les catégories de risques-types existant en matière de sécurité et caractériser et apprécier l'efficacité des modes et mesures de traitement des risques (réduction/augmentation, évitement/rejet, partage/transfert, maintien/accepta-tion).
- ✓ Apprécier et appliquer les concepts régissant une politique de sécurité spécifique à des secteurs d'activité de sensibilité particulière (santé, social, médical, sociétal) et/ou nécessitant de satisfaire des enjeux élevés en matière de continuité d'activité.
- ✓ Appliquer les concepts des politiques de sécurité et les différents documents associés dans une entreprise ou dans les cadres réglementaires usuels (PSSI E, guides officiels, etc.).
- ✓ Manipuler et ordonner les principaux modèles de sécurité formels associés aux systèmes logiciels des plus hauts niveaux de sécurité ; et apprécier les propriétés de sécurité associées.
- ✓ Identifier et caractériser les principales techniques d'évaluation de la sécurité (les approches qualitatives industrielles et certaines travaux de recherche).
- ✓ Apprécier comment défendre un système d'information orienté système industriel comme celui de la navigation Aérienne, contre des intentions potentiellement hostiles utilisant les systèmes de traitement de données.
- ✓ Apprécier et appliquer les concepts régissant une politique de sécurité spécifique à la problématique des systèmes d'information hybrides (industriels)

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 3 créneaux | **Ecosystème de la cybersécurité (**ANSSI, Thalès CESTI, CERT-IST) |
| Entière | 1 créneau | **Dimension Juridique** |
| Entière | 4 créneaux | **Management de la SSI et appréciation des risques**<br>✓ Management et organisation<br>✓ Politiques de sécurité administratives et Logiques |
| Entière | 3 créneaux | **Politiques de Sécurité, Critères Communs et Évaluation** |
| Entière | 5 créneaux | **Le cas de l'aviation civile**<br>✓ SSI et Navigation Aérienne<br>✓ Gouvernance de la sûreté Aviation Civile |
| Entière | 1 créneau | **Le cas des systèmes bancaires** |

## INTERVENANTS

Gilles Trouessin - ACCESSS-IF
Rodolphe Ortalo - CARSAT Midi-Pyrénées
Ladislas Hajnal - ENAC/SINA/INF/ LSI
Mathieu Gualino – ENAC
José Araujo – ANSSI
Remy Daudigny – Thalès (CESTI)
Philippe Bourgeois – CERT-IST
Jean-Philippe Constant – Lyra Networks

Fiche Enseignement

# La sécurité dans l'aérospatiale
# 10 créneaux de 1h45 et 2h d'examen (19h30)

## OBJECTIFS

**Sécurisation des communications satellitaires**

L'objectif de cette partie du cours est de présenter les différentes techniques utilisées de nos jours pour sécuriser les communications sol/air dans le contexte satellitaire. Nous présenterons les problématiques liées aux différents types de mission et les standards utilisés. Une attention particulière sera portée à la sécurisation des transmissions par étalement de spectre (TRANSSEC).

**Architecture ATM et protocoles sécurisés pour les communications aéronautiques**

L'objectif de cette partie du cours est d'introduire les principes du réseau informatique pour la gestion du trafic aérien (ATM). L'axe de présentation choisit est d'illustrer les points communs et les différences avec les réseaux industriels actuels. Dans un deuxième temps la notion de cohabitation entre approche « safety » et « security » pour l'ATM sera abordé.

En effet, au jour d'aujourd'hui les référentiels "security" qui sont utilisés en aéronautique pour les systèmes embarqués s'appuient sur les référentiels "safety" existant. Les ingénieurs identifient en plus des incidents safety classiques des menaces et attaques qui peuvent impacter la "security" du système et qui vont se traduire par des incidents "safety". Il s'agit de faire de la "secuirty for safety". Ce référentiel « safety » n'est néanmoins pas suffisant pour mener une analyse complète, les spécialistes "security" rajoute donc en parallèle d'autres analyses basées sur des référentiels extérieurs "security" dérivés du domaine de la sécurité des systèmes d'informations (SSI) : exemple de la norme ISO 27005. La deuxième partie du cours traitera donc des travaux actuels en matière de définition d'une norme commune pour la gestion de la sécurité du SI ATM.

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 2 créneaux | **Sécurisation des communications satellitaires**<br>✓ Chiffrement<br>✓ Authentification<br>✓ TRANSSEC |
| Entière | 5 créneaux | **Architecture ATM et protocoles sécurisés pour les communications aéronautiques**<br>✓ Introduction du concept de réseau industriel<br>✓ Limites sécuritaire des réseaux industriels actuels<br>✓ Complexité du réseau ATM actuel<br>✓ Détection d'intrusion pour les réseaux ATM actuels<br>✓ Gestion security vs safety dans l'ATM |
| Entière | 3 créneaux | **Présentation sur les retours d'expérience d'Airbus** |

## INTERVENANTS

Nicolas Larrieu – ENAC
Conférencier – Airbus
Conférencier – Thalès Aliena Space

Fiche Enseignement

# Intrusion

# 15 créneaux de 1h45 (26h15)

## OBJECTIFS

Tout d'abord le cours présentera un panorama des attaques qui exploitent les technologies employées pour la conception de sites web et fournit des éléments pour protéger ces systèmes. Le cours se poursuivra en présentant aux étudiants les risques auxquels ils devront faire face et en leur faisant réaliser que le comportement d'utilisateurs légitimes peut être exploité par des attaquants pour cibler les systèmes.

Ensuite, l'étudiant sera confronté à plusieurs challenges, qui lui permettront concrètement de se placer dans la peau d'un attaquant et d'exploiter des vulnérabilités de différentes natures : 1) un premier challenge illustrant les techniques d'intrusion dans un réseau ; 2) un second challenge centré sur la mise en oeuvre des techniques d'intrusions et d'élévation de privilèges sur un système informatique ; et 3) un cours/TP traitant de la réaction en cas d'incident avec une mise en pratique de techniques d'investigation numérique sur un système, après intrusion.

A l'issue de ce cours l'étudiant saura lister et quantifier les vulnérabilités inhérentes aux architectures système et réseau et sera sensibilisé aux grandes techniques d'intrusion

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 5 créneaux | **Sécurité des Applications Web**<br>✓ Présentation des attaques et vulnérabilités sur le web<br>✓ Mécanismes de défense côté navigateur et serveur<br>✓ Présentation de projets de recherche sur la détection<br>✓ Mise en pratique des attaques et des protections |
| Entière | 8 créneaux | **Techniques d'intrusion réseau et système**<br>✓ Stratégies d'intrusion (recueil d'informations, exploitation de vulnérabilités, pivot, cryptanalyse, reverse engineering)<br>✓ Les outils d'intrusion (Nmap, Metasploit, Craqueurs de mots de passe, pivots ssh, proxychains, debugger, compilateur) |
| Entière | 2 créneaux | **Analyse forensics**<br>✓ Traitement des incidents, continuité, investigation numérique |

## ORGANISATION

Ladislas HAJNAL – ENAC
Nicolas Larrieu – ENAC
Eric Atala – INSA Toulouse
Vincent Nicomette – INSA Toulouse

Fiche Enseignement

# Protection de la vie privée
# 6 créneaux de 1h45 et 1h d'examen (11h30)

## OBJECTIFS

Ce cours présentera les bases légales, les enjeux, et les principaux outils de la protection de la vie privée.

Plus précisément, l'objectif de ce cours est :

- ✓ De présenter les enjeux de la protection de la vie privée dans les systèmes d'information ;
- ✓ De caractériser l'ensemble de la problématique liée à la protection des données à caractère personnel ;
- ✓ D'illustrer cette problématique dans certains cas particuliers assez sensibles, en faisant la distinction entre *Security* et *Privacy*, et aussi entre RSSI et CIL (futur DPO), ou encore entre une analyse de risques en SSI et analyse d'impact sur le respect de la vie privée (ou *Privacy Impact Analysis*) ;
- ✓ De matérialiser certaines solutions techniques déployées dans certains domaines d'activité bien spécifiques, à travers les techniques d'anonymisation et/ou de pseudonymisation (par exemple : ré-utilisation de données de santé anonymisées, ou de géolocalisation) ;
- ✓ De décrire les techniques d'attaque contre l'anonymisation ;
- ✓ De présenter les principaux outils techniques de la protection de la vie privée.

## DEROULEMENT

| Promo | Durée | Contenu |
|---|---|---|
| Entière | 2 créneaux | **Management de la vie privée**<br>✓ Rappels sur la loi *Informatique & Libertés*<br>✓ Convergences et divergences entre des démarches destinées à la sécurisation de l'information et des approches visant à la protection des données à caractère personnel,<br>✓ Démarche et concepts autour de la protection des données à caractère personnel : enjeux et exigences |
| Entière | 2 créneaux | **Geoprivacy**<br>✓ Sensibilisation aux dangers de la géolocalisation<br>✓ Principes des protections mises en place<br>✓ Attaques contre l'anonymisation |
| Entière | 2 créneaux | **Outils techniques**<br>✓ Techniques cryptographiques (argent électronique, autorisations anonymes, chiffrement homomorphe)<br>✓ Techniques de communication (TOR, mixmaster) |

## ORGANISATION

Carlos Aguilar – INP-ENSEEIHT
Gilles Trouessin – ACCESSS-IF
Marc-Olivier Killijian – LAAS-CNRS