TLS-SEC

Syllabus

UE 1 : Bases de la sécurité (79 h) Responsable. V. Nicomette

Matière 1 : Rappels et harmonisation en systèmes d'exploitation

L'objectif de ce cours est une mise à niveau sur les principaux concepts fondamentaux des systèmes informatiques, en particulier ceux qui sont utiles pour les différents enseignements de sécurité. 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 …).

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.

Matière 2 : Rappels et harmonisation en réseau

L'objectif de ce cours est une mise à niveau sur les principaux concepts fondamentaux des réseaux d'ordinateurs, en se focalisant sur les concepts des réseaux IP. 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).

A l'issue de cet enseignement, l'étudiant sera capable de décrire les principes fondamentaux de la construction des protocoles réseaux, 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.

Matière 3 : Rappels et harmonisation en programmation C et assembleur

L'objectif de ce cours est une mise à niveau sur les principaux concepts fondamentaux de la programmation. Les langages orientés bas-niveaux seront privilégiés car ce sont ceux qui seront les 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.

Matière 4 : Définitions et techniques de base en sécurité et safety

L'objectif de ce cours est de présenter la terminologie et les bases fondamentales de la sécurité et de la tolérance aux fautes. A l'issue de ce cours, l'étudiant saura :

- Différencier les domaines de la sécurité (security et safety)
- Distinguer et utiliser correctement les termes correspondants : aux propriétés de sécurité de l'information et des systèmes ; et aux techniques apportant la sécurité

- Appréhender la sécurité dans sa globalité en allant au-delà des questions techniques et en prenant en compte les aspects organisationnels
- Modéliser les différents types d'attaquant
- Reconnaître les grands outils et éléments architecturaux apportant de la sécurité dans un réseau comme dans un système
- Décrire les différentes approches pour authentifier un utilisateur et autoriser des actions sur un système informatique.

Matière 5 : Cryptographie

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 cryptographiques 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.

UE 2 Module Sécurité du logiciel (50.25 h). Responsable. V. Nicomette

Matière 1 : Vulnérabilités logicielles

L'objectif de ce cours est de présenter 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.

Matière 2 : Virus et techniques virales

Objectifs : L'objectif de ce cours est de présenter 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 contre 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 par la détection des vers et virus.

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 réagir en cas d'infection.

Matière 3 : Développement Logiciel Sécurisé

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 par 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.

UE 3 Module Sécurité système et matérielle, rétro-conception (59.25 h). Responsable. V. Nicomette

Matière 1 : Protection des systèmes d'exploitation

L'objectif de ce cours est de présenter les principaux mécanismes de protection qui existent aujourd'hui dans les noyaux de systèmes d'exploitation. Ce cours aborde également un certain nombre d'attaques permettant d'exploiter les vulnérabilités des noyaux de systèmes 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'issue 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 les protections le 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 et d'exposer les différents mécanismes de protection pour contenir ces menaces. Il sera enfin capable de choisir et d'implémenter le mécanisme le plus adapté au système en train d'être étudié.

Matière 2 : Attaques matérielles, composants matériels pour la sécurité

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.

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. l sera capable de comprendre le fonctionnement d'une attaque sur le matériel, de la décrire et d'expliquer les mécanismes de protection associés. Il sear également capable d'identifier les composants critiques d'un système, d'analyser les vulnérabilités pouvant cibler ces composantes, des déterminer les contre-mesures permettant de les protéger et de mettre en oeuvre ces contre-mesures.

Matière 3 : Reverse Engineering

L'objectif de ce cours est de présenter 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 permettre de mieux comprendre certaines parties d'un code logiciel. Pour finir, les contre-mesures à la rétro-conception sont présentées pour rendre cette activité 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.

UE 4: Module Sécurité des réseaux et de leurs protocoles (44.25 h) Responsable J. Fasson

Matière 1 : Attaques et sécurisation des couches OSI

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.

A 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 sur l'ICANN
- Utiliser et mettre en place ces infrastructures

Matière 2 : Sécurité des réseaux non-filaires

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

A 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 actions 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

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

- Différencier 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 technologie
- Reconnaître les éléments architecturaux de la sécurité dans un réseau d'opérateurs.

Matière 3 : Sécurisation des protocoles

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

A 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 (transferts de fichiers, proxys, etc ..)
- Décrire les bonnes pratiques pour la définition d’un protocole sécurisé

UE 5: Module Architectures réseaux sécurisées (56.25 h) Responsable J. Fasson

Matière 1 : Composants fondamentaux d'une architecture sécurisée

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

A 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

Matière 2 : Bureau d'étude

Ce BE a pour but de mettre en pratique les divers enseignements du module réseau. A la fin de ce bureau d'étude, l'étudiant aura réaliser l'ensemble des manipulations suivantes :

- 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
- Comprendre les vulnérabilités des réseaux IPV6 et mettre en place des mécanismes de protection
- Comprendre les principes fondamentaux des vulnérabilités Web et mettre en place les mécanismes de protection adaptés
- Manipuler des ASA Cisco, matériels spécifiquement conçus pour la protection des réseaux

UE 6 : Sécurité des systèmes embarqués critiques (35,5 h) Responsable P. Queinnec

Matière 1 : La sécurité dans l'aérospatiale

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 « security 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.

Matière 2 : Challenge

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. 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 vient également complété cette matière.

UE 7 : Gouvernance et Ecosystème (45,5 h) Responsable V. Nicomette

Cette UE est optionnelle pour les étudiants ingénieurs. Elle permet d'obtenir en double diplôme le master Réseaux et Télécommunication (parcours SSIR Sécurité des Systèmes d'Information et des Réseaux)

Matière 1 : Gouvernance de la sécurité

Ce cours présente divers aspects de la sécurité dans le monde de l'entreprise avec un intérêt particulier pour les questions locales, humaines et organisationnelles

A la fin de ce 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 sien 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 de modes et mesures de traitement des risques (réduction/augmentation, évitement/rejet, partage/transfert, maintien/acceptation).
- Appliquer les concepts des politiques de sécurité et des 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 certains 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).

Matière 2 : Ecosystème de la sécurité

Cette matière est composée d'un ensemble de conférences permettant aux étudiants 1) de découvrir les principaux acteurs composant l'ecosystème de la sécurité et 2) d'appofondir certains aspects de la sécurité informatique.

Concernant les principaux acteurs composant l'ecosystème de la sécurité, différentes interventions sont programmées, par un représentant de l'ANSSI, un représentant du CERT-IST, le FSD (Fonctionnaire

Sécurité Défense) de l'INSA notamment. Par ailleurs, certaines thématiques importants de la sécurité sont ici approfondies, comme la sécurité dans le milieu médical, le milieu bancaire. Ces thématiques peuvent varier en fonction des années.

UE 8 : Conférences/Anglais (vie privée) (43 h) Responsable V. Nicomette

Cette UE est composée d'un ensemble de conférences sur la sécurité qui permettant aux étudiants de découvrir des facettes particulières de la sécurité au travers de brèves interventions. Chaque conférence fait l'objet d'un ou de 2 créneaux de cours au maximum. Le contenu de ces conférences peut varier en fonction des annéees, puisque nous souhjaitons proposer aux étudiants des thématiques importantes qui sodnt au coeur de l'actualité scientifique de la sécurité informatique. Par exemple, certains conférences sont liés à des métiers spécifiques de la sécurité et à ce titre des interventions sont faites par la Marine Nationale, la DGSI, par le CERT Eurocontrol. D'autres conférences permettent de découvrir des aspects importants de la sécurité , comme la protection de la vie privée (et notamment la RGPD), la présentation des aspects juridiques relatifs à la sécurité ou la présentation des principaux OIV et des problématiques de la sécurité qui leur sont relatives.

UE 9: Stage et Soutenance. Responsable P. Queinnec

Les étudiants en formation ingénieur effectuent un stage durant le second semestre. Ce stage s’achève par la production d’un rapport de satge et d’une soutenance devant un jury chargé d’évaluer ce stage.