INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

5e ANNEE PTP TOULOUSE SECURITE_SEMESTRE 9

Présentation

Description

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

DOMAINE TOULOUSE SECURITE

ECTS
30 crédits

Volume horaire
196h

Présentation

Description

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Bases de la sécurité

ECTS

Volume horaire
43.75h

Présentation

Description

-Rappels et Harmonisation en architecture des ordinateurs (structure du processeur, structure des bus internes) et en système d'exploitation (processus, techniques d'ordonnancement, gestion des appels systèmes)
- Rappels et Harmonisation en réseau (l'architecure IP, le modèle OSI, protocole ARP, protocole IP, la fragmentation, les options, le protocole TCP, les protocoles du plan de gestion, RIP, BGP)
- Rappels et Harmonisation en programmation C (gestion de la mémoire, pointeurs, structures de données,
entrées/sorties) et en assembleur (jeux d'instructions x86, chaînes de compilation)
- Définitions et techniques de bases de la Sécurité et Safety, éléments architecturaux, sensibilisation à la menace, techniques d'authentification, autorisation
- Cryptographie (introduction et notions de base, cryptographie symétrique, cryptographie asymétrique, standards cryptographiques et notions avancées)

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les principaux concepts des systèmes d'exploitation, des réseaux TCP/IP, de la programmation en langage C et en assembleur. Il s'agit ici d'une mise a niveau de tous ces domaines scientifiques, pour être sûr que les étudiants aient les bases fondamentales pour suivre l'ensemble de la formation
- Les principaux concepts de la sûreté de fonctionnement
- Les principaux concepts de la cryptographie

L'étudiant devra être capable de :

- décrire le fonctionnement des éléments importants d'un système d'information.
- décrire les principes fondamentaux de la construction des protocoles réseaux, d¿analyser des traces réseaux et de comprendre l¿encapsulation des flux
- utiliser les techniques de base de la programmation avec le langage C et assembleur. Il sera capable de concevoir des programmes en utilisant ces techniques.
- différencier les domaines de la sécurité (sécurity et safety) et utiliser correctement le vocabulaire associé
- distinguer les différents outils cryptographiques, comprendre ce qu'ils peuvent apporter à la sécurité et ce qu'ils ne peuvent pas
- trouver les standards internationaux de la cryptographie, comprendre leur contenu et mettre en place une utilisation d'un outil cryptographique respectant les standards ;
- réaliser des déploiements à l'aide d'outils réels de haut niveau (PKI, VPN, IPSec) ou de bas niveau (openssl) en choisissant les algorithmes, les niveaux de sécurité, les modes de fonctionnement de façon raisonnée

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Sécurité du logiciel

ECTS

Volume horaire
26.25h

Présentation

Description

Panorama des vulnérabilités logicielles : débordement dans la pile, return-into-libc, débordement dans le tas, DATA, BSS, chaînes de caractères, entiers ;
- Les risques et précautions liées à l'utilisation de programmes SUID ;
- 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) ;
- Historique des virus et des vers ;
- Présentation des anti-virus (théorème de Cohen), des techniques de détection et de leur efficacité et de la conduite à tenir ;
- Expérimentations de techniques de détection des vers et virus ;
- Bonnes pratiques, langages restreints et cycles de développement et validation du code ;
- Programmation défensive, principes du moindre privilège dans les programmes SUID, utilisation d'API plus sûres ;
- Preuves formelles.

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les différents types de vulnérabilités logicielles que l'on rencontre fréquemment, en particulier dans les programmes écrits en langage C ;
- Les contre-mesures usuelles de protections mémoires permettant de se protéger de ces différents types de vulnérabilités ;
- La théorie liée aux vers et virus, en particulier les algorithmes utilisés par les vers et virus pour infecter les systèmes informatique et se répandre, les protections contre ces malveillances et le fonctionnement des antivirus et des méthodes qu'ils emploient ;
- Les bonnes pratiques pour développer du logiciel de façon sécurisée.
- Les méthodes formelles permettant le développement de logiciel sécurisés

L'étudiant devra être capable de :

- Développer des logiciels en tenant compte des risques liés aux vulnérabilités logicielles ;
- Employer les méthodes formelles pour la détection de vulnérabilités logicielles ;
- 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

Pré-requis nécéssaires

De bonnes compétences en programmation en langage C et assembleur ;
- Un minimum de connaissances sur le fonctionnement des OS ;

- Des bases en algèbre et sur l¿utilisation de la théorie des automates

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Sécurité système et matérielle, rétro conception

ECTS

Volume horaire
17.5h

Présentation

Description

.Études des noyaux Linux et Windows du point de vue de la sécurité :
- Mécanismes noyau de protection de l'espace utilisateur
- Attaques sur le noyau depuis l'espace utilisateur (via abus de privilèges, ...)
- Protection du noyau face à des attaques depuis l'espace utilisateur
- Ouverture sur la protection du noyau face aux attaques de composants matériels

. Composants matériels des systèmes d'information pour la sécurité :
- Panorama des composants matériels présents dans un système informatique
- Utilisation de ces composants pour améliorer la sécurité (virtualisation, TPM, IO-MMU)
- Création d'une chaîne de confiance au démarrage basée sur l'utilisation de matériels de confiance
- Présentation de projets de recherche utilisant le matériel comme support pour la sécurité
- Mise en pratique de ces concepts par le développement d'une solution de sécurité sur architecture Intel

. Attaques et sécurisations matérielles :
- Rappels fondamentaux de microélectronique et d'architecture matérielle
- Canaux auxiliaires (SPA, DPA, ...)
- Contre mesures matérielles et algorithmiques
- Démonstration d'une attaque Bellcore sur un processeur grand public

. Chaîne de compilation
- Introduction aux techniques de compilation
- Analyse de graphes de contrôles et de données

. Techniques de rétro conception logicielle
- Introduction à la rétro-ingénierie: méthodologie et outils
- Découverte et prise en main des outils: désassembleurs, débuggers et de leurs langages de scripting
- Application à l'analyse de code malveillant et/ou à l'exploitation de vulnérabilité
- Initiation à l'outil IDA

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les principaux mécanismes de protection qui existent aujourd'hui dans les noyaux de systèmes d'exploitation ;
- Les principales attaques réalisées depuis le matériel ainsi que les contre-mesures associées ;
- Le fonctionnement des principaux composants matériels pour la sécurité tels que les hyperviseur et les IOMMU ;
- L'intérêt des dernières avancées en terme de protection matérielle réalisées par les fondeurs de processeurs et de chipset ;
- Le fonctionnement des attaques matériels et

physiques principales qui ciblent les systèmes informatiques ;
- La rétro-conception de logiciels (reverse engineering) tout en étant capable d'expliquer la la chaîne de compilation avec les modèles utilisés par les compilateurs pour générer le code machine ;
- Les stratégies pour rendre la rétro-conception de logiciels plus difficile à réaliser.

L'étudiant devra être capable de :

- Identifier les composants logiciels les plus adaptés pour protéger un système d'exploitation vis-à-vis des attaques logicielles ;
- Identifier les menaces provenant des couches basses et les vecteurs d'attaques à considérer dans un système ;
- D'obtenir une vue globale des échanges entre le composants matériels d'un système pour identifier les composants critiques et déterminer les contre-mesures a intégrer dans le système d'exploitation ;
- Identifier les menaces sur les composants physiques d'un système ;
- De réaliser une rétro-conception de maliciels pour en comprendre le fonctionnement voire créer des signatures
pour les détecter

Pré-requis nécéssaires

De bonnes compétences en programmation en langage C et assembleur ;

- Un minimum de connaissances sur le fonctionnement des OS ;
- Des bases en algèbre et sur l¿utilisation de la théorie des automates.

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Sécurité des réseaux et de leurs protocoles

ECTS

Volume horaire
22.75h

Présentation

Description

Attaques sur les couches 1-5 (écoute, usurpation et inondation MAC, empoisonnement ARP, usurpation IP, fragmentation IP, usurpation TCP, vol de session TCP)
- Contres mesures sur les couches 1-5 (commutation, port security, tables ARP, IDS spécifiques)
- Attaques sur la couche 7 (usurpation DNS, détournement des routes RIP et BGP), et défenses associées (DNSSEC,RPKI)
- Dénis de service
- Sécurisation WiFi (portails captifs, WPA1|2, 802.1X, EAP) et menaces (usurpations MAC et IP, tunnels, failles WPA)
- Réseaux cellulaires (évolution de la sécurisation dans GSM / GPRS / EDGE / UMTS / LTE)
- Protocoles fragiles (protocoles rsh, rcp, NFS, X, FTP, etc.), sécurisation a priori (authentification, confidentialité, intégrité) et a posteriori (utilisation d'un tunnel)
- SSH : description (mise en place et sécurisation de la connexion), utilisation standard (shell, transfer de fichiers), utilisation pour la sécurisation d'autres protocoles (tunnels, proxy SOCKS, sécurisation de X)
- 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

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts):

- Les principaux concepts de la sécurité des réseaux filaires, les principales attaques ciblant ces réseaux et les mécanismes de protection associés
- Les principaux concepts de la sécurité des réseaux non filaires (Wifi, GSM, GPRS, LTE, UMTS)
- Les principales faiblesses des protocoles réseaux fragiles et comment les sécuriser.

L'étudiant devra être capable de :

- 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 ; utiliser et mettre en place des infrastructures de défense
- Choisir une solution de sécurité adaptée pour un pointenti d'accès Wifi ; réaliser un test d'intrusion sur un point d'accès Wifi
- 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 technologie ; reconnaître les éléments architecturaux de la sécurité dans un réseau d'opérateurs
- Reconnaître les protocoles fragiles mis en place habituellement dans un réseau informatique ; sécuriser ces protocoles fragiles par l'utilisation de tunnels pour les applications lorsque ceci est nécessaire ; utiliser SSH et les fonctions associées (transferts de fichiers, proxys, etc.) ; décrire les bonnes pratiques pour la définition d'un protocole sécurisé

Pré-requis nécéssaires

De bonnes compétences dans l'informatique en général et dans la compréhension des protocoles réseaux qui régissent l'Internet (TCP/IP, protocoles de routage a minima) . En particulier, toute la terminologie doit être connue et les principes fondamentaux de la cryptographie doivent être acquis

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Architectures réseaux sécurisées

ECTS

Volume horaire
24.5h

Présentation

Description

- Firewalls : classes (sans états, avec états, applicatif, personnel) ; architectures (routeur filtrant, bastion, zones démilitarisées) ; limites (fragmentation, tunnels, authentification par IP)
- 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, antennes/site central, roaming)
- Solutions VPN : OpenVPN, Cisco VPN, les solutions VPN SSL
- NIDS : outils classiques (Snort, Suricata, IDS spécialisés), la prévention (bans firewall, etc.), les sondes et SIEM
- Mise en pratique Attaques ARP + IDS/IPS
- Mise en pratique Firewalls (mise en place, contournement sans états, contournements SSH/SOCKS/DNSTOTCP)
- Mise en pratique sur ASA Cisco (Firewall, VPN, IDS)

- Sécurité des Applications Web
  - Présentation des attaques et vulnérabilités sur le web
  - Mécanismes de défense côté navigateur et serveur
  - Présentation de projets de recherche sur la détection
  - Mise en pratique des attaques et des protections

- Techniques d'intrusion réseau et système
  - Stratégies d'intrusion (recueil d'informations, exploitation de vulnérabilités, pivot, cryptanalyse, reverse engineering)
  - Les outils d'intrusion (Nmap, Metasploit, Craqueurs de mots de passe, pivots ssh, proxychains, debugger, compilateur)

- Analyse forensics
  - Traitement des incidents, continuité, investigation numérique

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les principaux concepts associés à la conception et l'implémentation d'architectures réseaux sécurisées
- Les outils et techniques principaux permettant cette sécurisation et leur utilisation en fonction des différents contextes ainsi que des objectifs correspondants.
- Les vulnérabilités inhérentes aux architectures système et réseau et les grandes techniques d'intrusion ;
- Le fonctionnement des principales vulnérabilités du web.

L'étudiant devra être capable de :

- 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

- 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
- Faire le design complet d'une architecture de sécurité pour un réseau complexe

- Identifier les limites et avantages de différentes solutions de détection d'intrusion ;
- Positionner les sondes de détection d'intrusion de manière efficace ;
- Analyse les évènements collectés par les sondes et corréler ces évènements pour identifier une menace réelle.
- Identifier les vulnérabilités dans les architectures web et proposer des solutions pour réaliser une protection efficace

Pré-requis nécéssaires

Une bonne connaissance des architectures Web, de la cryptographie et des réseaux.

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Sécurité des systèmes embarqués critiques

ECTS

Volume horaire
19.25h

Présentation

Description

- Sécurisation des communications satellitaires (chiffrement, authentification, TRANSSEC)
- Architecture ATM et protocoles sécurisés pour les communications aéronautiques
  - Introduction du concept de réseau industriel
  - Limites sécuritaire des réseaux industriels actuels
  - Complexité du réseau ATM actuel
  - Détection d'intrusion pour les réseaux ATM actuels
  - Gestion security vs safety dans l'ATM

- Réalisation d'une analyse de sécurité en boite noire d'un système embarqué critique : identification de vulnérabilités et exploitation de ces vulnérabilités dans un contexte de système embarqué, potentiellement très différent d'un système IT classique

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les différentes techniques utilisées de nos jours pour sécuriser les communications sol/air dans le contexte satellitaire ;
- Les problématiques liées aux différents types de mission et les standards utilisés ;
- Les moyens pour la sécurisation des transmissions par étalement de spectre (TRANSSEC) ;
- Les principes du réseau informatique pour la gestion du trafic aérien (ATM) et les problématiques de sécurité associées ;
- Les principes et les problématiques de la gestion de la sécurité dans le contexte de la DGAC.

L'étudiant devra être capable de :
- Effectuer des choix pertinents vis-à-vis de la sécurité pour architecturer les moyens de communication sol/air ;
- Réaliser une analyse en boite noire d'un système embarqué critique

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

SHSJ

ECTS

Volume horaire
42h

Présentation

Description

Cette UE est composée d'un ensemble de conférences sur la sécurité qui permettent aux étudiants de découvrir des facettes particulières de la sécurité au travers de brèves interventions.

Chaque conférence fait l'objet d'un ou de deux créneaux de cours au maximum. Le contenu de ces conférences peut varier en fonction des années, puisque nous souhaitons proposer aux étudiants des thématiques importantes qui sont au cœur de l'actualité scientifique de la sécurité informatique.

Par exemple, certaines conférences sont liées 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 le 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.

Évaluation

L'évaluation des acquis d'apprentissage est réalisée en continu tout le long du semestre. En fonction des enseignements, elle peut prendre différentes formes : examen écrit, oral, compte-rendu, rapport écrit, évaluation par les pairs...

Infos pratiques

Lieu(x)

Toulouse

Informations non contractuelles