1EL6000 - Réseaux et Sécurité

Responsables : **Pierre WILKE**

Langues d'enseignement : **ANGLAIS , FRANCAIS**

Type de cours : **Electif 1A**

Campus où le cours est proposé : **CAMPUS DE PARIS - SACLAY**

Nombre d'heures d'études élèves (HEE) : **60**

Nombre d'heures présentielles d'enseignement (HPE) : **30**

Année académique : **2024-2025**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

Ce cours de SPI a pour but de donner aux élèves ingénieurs de CentraleSupélec une connaissance de base en réseau et de les sensibiliser à la sécurité informatique.
Pour le réseau, l'accent sera mis sur la compréhension de l'ensemble des différents mécanismes mis en œuvre pour permettre aux utilisateurs que nous sommes de naviguer sur le web ou d'utiliser les services Internet. Ainsi, seront introduites les différentes couches réseau, en partant du physique jusqu'à l'applicatif, mais aussi les services réseau additionnels, tels que le DNS (Domain Name System). La pratique en TD et TP permettra aux étudiants de se confronter à la mise en œuvre technique des différentes notions abordées, dans des situations et systèmes réalistes.
Concernant la sécurité informatique, les cours permettront d'introduire les concepts fondamentaux et de présenter succinctement quelques mécanismes de sécurité. Ces cours seront complétés par des TP qui illustreront les risques de sécurité et des exemples de contre-mesures pouvant être déployées.

Période(s) du cours (n° de séquence ou hors séquence) :

SG1 et SG3

Prérequis :

- Systèmes d'information et programmation
- Pratique de base de la programmation en langage Python

Plan détaillé du cours (contenu) :

Partie 1 : Réseau - Couches basses

- Couche physique / Accès réseau (Ethernet)
- Protocole de résolution d'adresse (ARP - Address Resolution Protocol), adressage MAC (Media Access Control)

Partie 2 : Réseau – Couches intermédiaires

- Protocole et adressage IP
- Routage IP et protocoles de routage

- Protocoles de transport (TCP et UDP)
- TD1 : Analyse de trames réseau (Wireshark)
- TD2 : Spécification d'un protocole de communication
- TP1 : Manipulation d'équipements réseau (commutateurs / routeurs)
- Travail personnel : BGP (Border Gateway Protocol), peering, migration de IPv4 vers IPv6, contrôle de congestion, contrôle de flux, qualité de service…

Partie 3 : Réseau – Services et Couches applicatives

- Résolution de noms de domaines (DNS – Domain Name System)
- Protocole HTTP et technologies du Web
- TD3 : Implémentation du protocole spécifié en TD2 en Python (programmation sockets)
- Travail personnel : protocoles d'email (IMAP, POP, SMTP), service d'annuaires (LDAP)…

Partie 4 : Sécurité informatique

- Introduction à la sécurité, concepts fondamentaux
- Aspects juridiques et sociétaux
- Introduction à la cryptographie et aux protocoles cryptographiques
- Introduction aux logiciels malveillants (malware)
- TP2 : Virtual Private Network (OpenVPN)
- TP3 : Sécurité des applications Web
- Travail personnel : IPSec, DNSSEC, TLS, Sécurité de la messagerie instantanée…

Déroulement, organisation du cours :

Réseau – Couches basses : CM (1h30)
Réseau – Couches intermédiaires : CM (3h), TD (6h), TP (3h), travail personnel (9h)
Réseau – Services et couches applicatives : CM (3h), TD (3h), travail personnel (9h)
Sécurité informatique : CM (3h), TP (6h), travail personnel (10h)
Examen écrit (2h)

Les occurrences 1.2 et 1.4 sont enseignées en français
L'occurrence 1.3 est enseignée en anglais

Organisation de l'évaluation :

L'évaluation sera la moyenne d'un examen écrit (CF) en fin de session d'une durée de 2h et de l'évaluation des TPs 1 et 2 (évaluation obligatoire, EO)
- 50% pour l'examen final examen écrit (QCM) sans document
- 25% TP1
- 25% TP2

Les notes de TP participent toujours à la note finale, peu importe qu'elles l'améliorent ou qu'elles la fassent baisser.

Moyens :

- Équipe enseignante : membres de l'équipe CIDRE (Rennes), enseignants du campus Paris-Saclay (départements informatique et télécommunications) ;
- La plupart des TD et TP requièrent l'utilisation d'un ordinateur portable personnel ;
- Logiciels utilisés : Wireshark, Python, VirtualBox, OpenVPN (tous libres / open source) ;
- Certaines sessions de travaux pratiques mettent en oeuvre du matériel réseau spécifique ;
- Certains cours magistraux pourront être faits en visio-conférence depuis Rennes.

Acquis d'apprentissage visés dans le cours :

À l'issue de cet enseignement, les étudiants seront capables de :

- Connaître les concepts, protocoles et mécanismes des réseaux informatiques sur TCP/IP ;
- Analyser l'activité réseau générée par une application web ;
- Connaître les principales familles de schémas cryptographiques ;
- Connaître des techniques utilisées par les logiciels malveillants ;
- Mettre en place et administrer des réseaux informatiques commutés et interconnectés ;
- Concevoir et implémenter un protocole de communication applicatif ;
- Mettre en place et configurer un réseau privé virtuel (VPN) ;
- Détecter et analyser certaines vulnérabilités liées aux applications web.

Description des compétences acquises à l'issue du cours :

- C1.1 - Examine a problem in full breadth and depth, within and beyond its immediate parameters, thus understanding it as a whole. This whole weaves the scientific, economic and social dimensions of the problem.Examine a problem in full breadth and depth, within and beyond its immediate parameters, thus understanding it as a whole. This whole weaves the scientific, economic and social dimensions of the problem
- C1.4 - Design, detail and corroborate a whole or part of a complex system
- C2.1 - Thoroughly master a domain or discipline based on the fundamental sciences or the engineering sciences.

Bibliographie :

Transparents du cours mis à disposition au format électronique
Livres :

- J.F. Kurose and K.W. Ross, Computer Networking: A Top-Down Approach, 7th ed. Eyrolles. Pearson. ISBN : 978-0133594140
- Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition. Wiley. ISBN : 978-0470068526 (accessible en ligne sur https://www.cl.cam.ac.uk/~rja14/book.html)

MOOC :

- Stanford Online: Introduction to Computer Networking (https://lagunita.stanford.edu/courses/Engineering/Networking-SP/SelfPaced/about)
- Coursera / Université du Maryland : spécialisation Cybersécurité (https://www.coursera.org/specializations/cyber-security)
- Cisco Networking Academy: modules CCNA1 et CCNA2 (https://netacad.centralesupelec.fr/)