Internet et sécurité

ECTS

Volume horaire
62.75h

Présentation

Description

- Partie Interconnexion de réseaux :
o Le cours présente tout dabord les technologies classiques d'interconnexion de réseaux locaux dans l'Internet (répéteur, pont, routeur), et détaille en particulier le routage dans l'Internet (algorithme mis en œuvre au niveau IP et protocoles RIP, OSPF, BGP) et ses évolutions (subnetting et routage sans classe - CIDR). Les protocoles ARP, proxy ARP, ICMP et DHCP sont également introduits.
o Le cours présente ensuite les concepts et les techniques associés à la gestion de réseaux locaux virtuels (VLAN) et de réseaux privés virtuels (VPN) et à la gestion des adresses IP privées dans lInternet (proxy applicatif, NAT).
o Les deux principaux protocoles de Transport de l'Internet (TCP, UDP) sont détaillés dans une troisième partie.
o Les évolutions de lInternet vers la prise en compte des besoins en multicast, en qualité de service (QoS) et en mobilité sont finalement introduites et la gestion du multicast dans sa version primitive est détaillée.
o Des TP d'administration de réseaux Ethernet et IP sur PC Linux et matériel CISCO illustrent le cours.

- Partie Algorithmique répartie :
o Temps causal (horloges logiques et vectorielles)
o Synchronisation par phases (application au routage optimal) et par vagues (construction distribuée d'un arbre de recouvrement)
o Choix distribué (application au problème de l'élection)
o Exclusion mutuelle distribuée
o Détection de la terminaison
o Gestion des données distribuées (illustration de la théorie des Quorums)

- Partie Sécurité :
o Principes de la sécurité informatique : propriétés (confidentialité, intégrité, disponibilité), l'authentification, l'autorisation, les politiques de sécurité, l'audit, la détection d'intrusion, l'évaluation
o Classification des attaques : virus, vers, chevaux de Troie, etc.
o Vulnérabilités des réseaux : étude des vulnérabilités principales des couches 2,3 et 4 de l'OSI (arp spoofing, arp flooding, ip spoofing, attaques sur la fragmentation IP, TCP hijacking, etc.),
o Vulnérabilités applicatives : focus sur les débordements de buffer en mémoire.

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :
- Partie Interconnexion de réseaux et de l'Internet :
o les concepts et les techniques de base pour interconnecter des réseaux locaux dans l'Internet : répéteur, pont, routeur,
o les concepts et les techniques avancées pour interconnecter des LAN dans l'Internet : routage, subnetting, CIDR, VLAN, VPN, proxy applicatif, NAT,
o les principaux protocoles de l'architecture de l'Internet TCP/IP : UDP, TCP, IP, ARP/proxy ARP, ICMP, DHCP (Note : les protocoles de routage RIP, OSPF et BGP sont introduits a minima).

Informations non contractuelles

- Partie Algorithmique répartie :
o les caractéristiques principales des systèmes répartis (asynchronisme, répartition du contrôle et des données, absence de connaissance commune, dynamisme, ...),
o les problèmes qui leurs sont spécifiques et la difficulté de leur solution répartie (exclusion mutuelle, gestion des données partagées, choix réparti, diffusion, détection de la terminaison, ...),
o quelques outils algorithmiques génériques permettant de les résoudre : causalité, récursivité et itération réparties, structures topologiques spécifiques.

- Partie Sécurité :
o les principes de la sécurité informatique aux travers des propriétés qui la caractérisent mais aussi la classification des principales menaces et des mécanismes de défense
o les principales vulnérabilités des réseaux informatiques, en particulier du réseau Internet ainsi que les mécanismes de défense associés
o les principales vulnérabilités applicatives ainsi que certains mécanismes de défense associés

L'étudiant devra être capable de :
- Partie Interconnexion de réseaux et de l¿Internet :
o d'effectuer des choix d'architecture matérielle permettant de prendre en compte les besoins et les contraintes associés à une interconnexion de réseaux locaux,
o d'effectuer des choix de plans d¿adressage et de routage simples,
o de mettre en œuvre (administrer) des réseaux Ethernet et IP dans les contextes d'nterconnexion de base abordés dans le cours.

- Partie Algorithmique répartie :
o de résoudre des problèmes génériques liés à la mise en œuvre de systèmes répartis,
o de manipuler les outils les plus généraux permettant de les aborder.

- Partie Sécurité :
o d'étudier un réseau d'entreprise et ses applications de façon à identifier les principales vulnérabilités, tant du point de vue applicatif que du point de vue réseau, de proposer les solutions adéquates pour améliorer la sécurité de l'ensemble

Pré-requis nécéssaires

Cours d'introduction aux réseaux informatiques (3MIC)
Cours de programmation distribuée dans les réseaux (API socket) (3MIC)

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