le cnam
Nouvelle-Aquitaine

Fiche récapitulative

UTC505 | Introduction à la cyberstructure de l'internet : réseaux et sécurité

30
Total d'heures d'enseignement

3
Crédits ECTS

Date non définie
Début des cours prévu

Programme

Sujets traités pour la partie Réseaux (2/3 du volume de l'enseignement) :
Diviser pour régner / Modèles en couches OSI vs Internet / Encapsulation

Découverte de l'architecture de communication en couches : du modèle OSI à l'architecture Internet ;
L'outil d'analyse de traces Wireshark pour comprendre l'encapsulation et l'articulation entre les couches.

Les autoroutes de l'information : nids de poules et travaux en tous genres / Couche Physique/

Concepts et problèmes de la transmission de données
Erreurs de transmission, et le contrôle d'erreur

Collectivisme ou Libre entreprise? à la recherche d'un modèle efficace / Couche Liaison, sous-couche MAC /

Ponts, Commutation et Arbre Couvrant-STP.
VLAN

Carrefours, itinéraires et destinations / Couche Réseau /

Protocole IP.
Adressage IPv4 sans classe (CIDR, Classless Inter-Domain Routing) : adresse d'interface, adresse de réseau, masques, broadcast sur sous-réseau.
Tables de routage (plan de données et commutation/forwarding) et acheminement de datagrammes dans un réseau IP.
D'IPv4 à IPv6 : le point de vue du datagramme et des adresses IPv6
Algorithme du plus court chemin de Dijkstra pour le routage dynamique

Une lettre ou un appel ? / Couche Transport /

Transport de données entre un client et un serveur
Mode connecté TCP : ouverture de connexion, transfert de données, fermeture de connexion, contrôle de flux et fenêtre glissante

Quelques protocoles de la couche application

Introduction aux protocoles dédiés aux applications : HTTP, DNS

Sujets traités pour la partie Sécurité (1/3 du volume de l'enseignement) :

Introduction à la sécurité

Bonnes pratiques de sécurité personnelle
Droit du numérique
Côté entreprises : normes et règlementation : RGPD, SOx, PCI DSS, OIV, ISO 27000

Menaces

Études de cas : Stuxnet, TV5Monde, Banque du Bangladesh, EternalBlue/WannaCry/NotPetya, Carbanak/Cobalt, fraude au président (Pathé), SolarWinds.
Rançongiciels : Colonial Pipeline, HSE, Kaseya VSA
Processus d'attaque : MITRE ATT&CK Framework, Unified Kill Chain, menaces persistantes avancées (APT)

Mesures de sécurité

Vulnérabilités : failles 0-day, échelle de sévérité, CVE MITRE, score CVSS
Processus de déploiement des correctifs de sécurité. Séparation des environnements.
Scan de vulnérabilités, durcissement de configuration, vérification de la conformité technique
Modélisation des menaces
Sécurité du code pour les développements logiciels : débordement de tampon ou d'entiers, MITRE CWE. Bonnes pratiques de développement et d'amélioration de la qualité du code. Fuzzing, tests d'intrusion, exercices red/blue team.
Impacts : bilan d'impact sur l'activité (BIA), temps et point de rétablissement (RTO et RPO), Data Protection/Privacy Impact Assessment (D)PIA, plans de reprise (PRA), de continuité (PCA), d'urgence et de poursuite d'activité (PUPA)
Gestion des risques informatiques : ISO 27000, méthodologies EBIOS et MEHARI
Organisation de la sécurité : SOC, surveillance des événements de sécurité (SEM)
Sensibilisation des utilisateurs à la sécurité informatique
Sécurité des authentifications : biométrie, mots de passe, possession. Authentification forte multi-facteurs.
Défense en profondeur, modèle du château fort, dépérimétrisation de l'infrastructure informatique et réseaux ?zéro trust'.

Primitives cryptographiques

Propriétés de sécurité, de contrôle d'accès et de sûreté de fonctionnement
Approches historiques : codage, stéganographie, chiffrement
Principe de Kerckhoffs
Taxinomie des techniques de cryptanalyse : KPA, CPA, CCA. Exemple d'attaque sur la carte à puce via l'horloge.
Niveau de sécurité
Analyse des fréquences (Al-Kindi). Indice de coïncidence de Friedman
Algorithmes historiques : César, Vigenère, Playfair, ADFGVX, Enigma.
Sécurité inconditionnelle de l'algorithme du masque à usage unique (chiffre de Vernam)
Principe des chiffres symétriques (en continu ou par blocs) et à clé publique.
Cryptosystèmes hybrides. Infrastructures de clés publiques et autorités de certification.

Suivant l'enseignant, le cours peut démarrer par la partie sécurité ou par la partie réseaux, il y a des articulations dans les deux cas. Pour la partie réseaux, en général on commence par le modèle ISO, puis on peut décrire en commençant par la couche application en allant vers la couche physique, ou le contraire. A paris, on démarre souvent après le modèle en couches et l'encapsulation, mais pas toujours, par la couche Réseau et IP car c'est la clef de voute de l'Internet.

L'enseignant est libre aussi de proposer des extensions optionnelles au cours qui ne comptent pas pour l'examen mais qui peuvent intéresser une partie du public. A Paris, le cours s'appuie sur différents types de ressources : supports de cours, exercices corrigés : vus en séance, à faire soi-même ou pour s'auto-évaluer, animations power point et vidéos. Les vidéos du cours sont complétées par des vidéos de youtubeurs du domaine qui complètent le contenu du cours sur certains thèmes et peuvent répondre à la curiosité des auditeurs souhaitant se spécialiser en réseaux ou en cybersécurité. Le cours se découpe en 5 séquences Réseaux et 5 séquences Sécurité. Ces séquences se subdivisent elles-mêmes en séances. Le nombre de séances par séquence est variable. Les contenus par séquence sont divisés en partie principale et en parties optionnelles. Les parties optionnelles sont identifiables par l'expression « pour aller plus loin » ou plus clairement par « optionnel ». Les contenus optionnels sont offerts aux curieux soit pour creuser le sujet du cours, soit pour préparer aux unités d'enseignement qui suivent comme RSX101 ou RSX102. Il est rappelé que les contenus optionnels ne font pas l'objet de questions à l'examen. Tous les contenus sont consultables jusqu'au 30 septembre de l'année académique en cours, ils sont tous sur l'espace numérique de formation (ENF) que ça soit pour les inscrits en présentiel ou à distance. Toutes et tous disposent des mêmes contenus. L'ENF contient aussi des sujets d'examens parfois corrigés et sont en libre

accès aux inscrits à UTC505.

Objectifs : aptitudes et compétences

Objectifs :

L'objectif de l'UE est d'introduire le domaine des réseaux à travers l'exemple de l'Internet, de décrire ses principaux ingrédients et les concepts clefs de son fonctionnement, et de présenter les propriétés de sécurité qui sont générales et pas seulement liées aux réseaux.

Compétences :

L'UE UTC505 dès sa conception avait une visée théorique comme l'a explicitement demandé la Commission du Titre de l'Ingénieur. Le Cnam, en particulier, l'équipe IRSM, a respecté cette exigence. Cette UE apporte donc d'abord des connaissances dans le domaine des réseaux et de la sécurité. Les compétences découlent des exercices et des cours qui s'inspirent de situations réelles ou proches de la réalité.

Connaissances associées aux concepts, protocoles, architectures du Modèle en couche OSI ou Internet. L'auditeur pourra, à l'issue du cours, évaluer les principales contraintes réseaux et leur impact sur une application de type client/serveur,
L'auditeur sera en mesure de participer à la définition des principaux éléments d'un cahier des charges fonctionnel à destination d'une maîtrise d'ouvrage dont l'objectif est d'urbaniser une application ou un système d'information distribués.
L'auditeur disposera de repères pour évaluer fonctionnellement une livraison d'équipements réseaux, et mettre en place une procédure de recette de ceux-ci dans un cadre applicatif.

Savoirs : Protocoles et normes télécoms, Protocoles de l'Internet, Technologies clefs des réseaux de données, Règles de sécurité Informatique et Télécoms, CyberSécurité, Architectures réseau, Réseaux de données et télécoms.

Prérequis

Pas de pré-requis nécessaire dans l'absolu, mais avoir obtenu une UE comme NFA009 peut aider à exploiter plus pleinement le contenu du cours. Il faut bien sûr une culture de base en systèmes d'exploitation, en programmation et en mathématiques telle que demandée dans un DUT informatique. UTC505 est un pré-requis de RSX101, RSX102 et RSX112. Ces UE poursuivent le programme de UTC505 et ne le refont pas.

Délais d'accès

Le délai d'accès à la formation correspond à la durée entre votre inscription et la date du premier cours de votre formation.

- UE du 1er semestre et UE annuelle : inscription entre mai et octobre
- UE du 2e semestre : inscription de mai jusqu'à mi-mars

Exemple : Je m'inscris le 21 juin à FPG003 (Projet personnel et professionnel : auto-orientation pédagogique). Le premier cours a lieu le 21 octobre. Le délai d'accès est donc de 4 mois.

Planning

Légende:

Cours en présentiel

Cours 100% à distance

Mixte: cours en présentiel et à distance

Modalités	Lieux	Disponibilités	Prochaines sessions *	Tarif indicatif
	En ligne	Semestre 1	Prévue en 2025-2026	De 0 à 600 €
	En ligne	Semestre 2	Prévue en 2025-2026	De 0 à 600 €
	En ligne	Semestre 1	Prévue en 2026-2027	De 0 à 600 €
	En ligne	Semestre 2	Prévue en 2026-2027	De 0 à 600 €
	En ligne	Semestre 1	Prévue en 2027-2028	De 0 à 600 €

	En ligne	Semestre 2	Prévue en 2027-2028	De 0 à 600 €

*Selon les UEs, il est possible de s'inscrire après le début des cours. Votre demande sera étudiée pour finaliser votre inscription.

Modalités

Modalités pédagogiques :

Pédagogie qui combine apports académiques, études de cas basées sur des pratiques professionnelles et expérience des élèves. Équipe pédagogique constituée pour partie de professionnels. Un espace numérique de formation (ENF) est utilisé tout au long du cursus.

Modalités de validation :

Un examen de 3h00 qui se découpe en une partie sécurité (1/3) et une partie réseaux (2/3).
Pour valider cette UE, vous devez obtenir une note minimale de 10/20

Tarif

Mon employeur finance	600 €
Pôle Emploi finance	300 €
Je finance avec le co-financement Région	Salarié : 78 €
Je finance avec le co-financement Région	Demandeur d'emploi : 62,40 €

Plusieurs dispositifs de financement sont possibles en fonction de votre statut et peuvent financer jusqu'à 100% de votre formation.

Salarié : Faites financer votre formation par votre employeur

Demandeur d'emploi : Faites financer votre formation par Pôle emploi

Votre formation est éligible au CPF ? Financez-la avec votre CPF

Si aucun dispositif de financement ne peut être mobilisé, nous proposons à l'élève une prise en charge partielle de la Région Nouvelle-Aquitaine avec un reste à charge. Ce reste à charge correspond au tarif réduit et est à destination des salariés ou demandeurs d'emploi.

Pour plus de renseignements, consultez la page Financer mon projet formationopen_in_new ou contactez nos conseillers pour vous accompagner pas à pas dans vos démarches.

Passerelles : lien entre certifications

- LG025B41 - Bloc Informatique : Fondements des systèmes informatiques et des réseaux
- CRN0801A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Systèmes et réseaux
- CRN0802A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Systèmes d'information (SI)
- CRN0803A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques : Cybersécurité
- CYC9101A - Diplôme d'ingénieur Architecture et ingénierie des systèmes et des logiciels (AISL)
- CYC9104A - Diplôme d'ingénieur Informatique, réseaux, systèmes et multimédia (IRSM)
- CYC9105A - Diplôme d'ingénieur Informatique : Systèmes d'information
- CYC9106A - Diplôme d'ingénieur Cybersécurité
- LG02501A - Licence 3 Informatique générale

Avis des auditeurs

Les dernières réponses à l'enquête d'appréciation de cet enseignement :

↓ Fiche synthétique au format PDF

Taux de réussite

Les dernières informations concernant le taux de réussite des unités dcenseignement composant les diplômes

↓ Taux de réussite