INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES	S6

Pourquoi cette UE ?

Un système informatique communique avec le monde extérieur. Il est ainsi nécessaire d’acquérir les compétences et connaissances pour sécuriser des serveurs et vérifier l'application des mesures de protection.

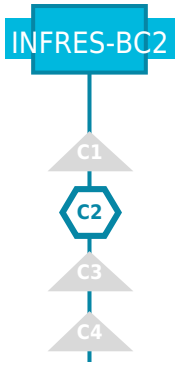
Eléménts constitutifs de l'UE

	coefficient
INFRES_6_3-1 Réseaux et protocoles - 2 - SR	**2**
INFRES_6_3-2 Réseaux et protocoles - 2 - DL	**1**
INFRES_6_3-3 Cryptographie	**2**
INFRES_6_3-4 Gestion du cycle de vie des certificats	**1**

Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
78	27	3

Alignement curriculaire

Parmi les compétences visées par la formation, lesquelles sont développées dans cette UE ?



INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-1 Réseaux et protocoles - 2 - SR	**S6**

Contexte et enjeux de l'enseignement

Les réseaux, avec l’énergie et l’hébergement des Datacenters, sont les briques fondamentales des architectures IT des Cloud Service Providers, accessibles via Internet. Les protocoles de routage sont les mécanismes au cœur des réseaux et comprendre ces architectures réseaux orientées applications, sécurisées dès la conception est décisive.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Cours réseaux

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	23
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	10

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

Après avoir rappelé les fondements du réseau IP (adressage, acheminement et routage des datagrammes IP), le concept de virtualisation réseau (VLAN, VBF, VRF), on rappelle les types de protocoles de routage entre IGP et EGP (BGP) et on approfondit OSPF dans le cadre des réseaux de grandes dimensions. On introduit BGP comme protocole de routage inter AS qui permet l’accès sur Internet, l’appairage aux Cloud Service Provider et on étudie ses caractéristiques si particulières de fiabilité et de mis

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

TP de mise en place d'un réseau de systèmes autonomes géré par BGP

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

QCM
TP

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-1 Réseaux et protocoles - 2 - SR	**S6**

Plan de cours

- Briques constitutives d’un réseau datagramme IP : Adressage, Acheminement et Routage
- Un peu de virtualisation réseaux : VLAN, VRF, VBF
- Adressage IP privé et public : le NAT (Network Address Translation) et ses utilisations
- Qu’est-ce qu’un « bon » protocole de routage dynamique ?
- Notion de système autonome, mécanismes de routage à états de liaison, distance vecteur (et vecteurs de chemin)
- Exemple de protocole IGP : OSPF
- Qu’attend-on d’un routage inter système autonome
- Internet et la loi d’échelle
- Exemple de protocole EGBàBGP
- Métriques BGP et mise en œuvre
- Policy Routing BGP
- Cas des AS de transit de grandes tailles : Confédération BGP, Route Reflector
- Etude de cas : réurbanisation d’un LAN DC orienté application
- Etude de cas : urbanisation d’une Landing Zone Azure
- Technologies de tunnels réseaux : GRE, IPSEC, LSP MPLS, VxLAN

Ressources et références

Cours réseaux

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-2 Réseaux et protocoles - 2 - DL	**S6**

Contexte et enjeux de l'enseignement

La maîtrise des applications réseau est essentielle dans un monde interconnecté où la communication de données est omniprésente. Cet enseignement s'inscrit dans un contexte où la résilience, la performance et la sécurité des échanges sont des préoccupations majeures. Il répond aux besoins industriels en ingénieurs capables de concevoir des solutions communicantes, robustes et évolutives. Les élèves seront confrontés à des problématiques réelles telles que l'interopérabilité, la scalabilité ou la gestion des erreurs. Cette compétence est transverse, au carrefour des systèmes, des réseaux et du développement logiciel.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Cours réseaux et développement en langage C

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	23
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	9

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Concevoir l'architecture d'une application réseau.
- Implémenter des échanges client-serveur via sockets.
- Utiliser des protocoles applicatifs (HTTP, FTP, etc.).
- Intégrer la sécurité des communications.
- Diagnostiquer et corriger les problèmes réseau dans une application

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

TP sur le protocole de routage dynamique OSPF
Projet de conception d'un protocole de routage dynamique avec validation et remise de rapports de tests de performance

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Évaluation : validation du projet et rapport de tests

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-2 Réseaux et protocoles - 2 - DL	**S6**

Plan de cours

- Présentation du protocole de routage dynamique OSPF
- Présentation du projet de développement d'un protocole de routage dynamique en remplacement d'OSPF
- Encadrement des projets
- Validation des projets

Ressources et références

Les supports pédagogiques sont disponibles en ligne sous Campus.

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-3 Cryptographie	**S6**

Contexte et enjeux de l'enseignement

Dans un monde de plus en plus interconnecté, la protection des données, la confidentialité des échanges et l'intégrité des systèmes numériques sont devenues des enjeux cruciaux. La cryptographie constitue le socle technique garantissant ces propriétés, tant dans les communications que dans le stockage et les traitements décentralisés. L'élève ingénieur doit comprendre comment concevoir, analyser et mettre en œuvre des primitives cryptographiques sûres, mais aussi comment prouver mathématiquement leur sécurité. Cet enseignement prépare à appréhender des systèmes critiques tels que les paiements électroniques, les réseaux sécurisés, les blockchains et les identités numériques. Une attention particulière est portée à la rigueur des preuves, à la résistance aux attaques et à l'implémentation sûre dans des environnements contraints.

Prise en compte des dimensions socio-environnementales

Prérequis

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	18
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Expliquer les principes fondamentaux de la cryptographie moderne.
- Concevoir des protocoles cryptographiques simples et sûrs.
- Analyser la sécurité d'un système à l'aide de preuves formelles.
- Identifier les vulnérabilités cryptographiques courantes.
- Implémenter des primitives de manière correcte et résistante aux attaques.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours
TP de mise en place de certificats

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

QCM
Rapport

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-3 Cryptographie	**S6**

Plan de cours

- Fondements mathématiques : rappels sur les structures algébriques (groupes, anneaux, corps), complexité calculatoire, fonctions à sens unique, et hypothèses de sécurité.
- Primitives cryptographiques : chiffrement symétrique (AES, modes opératoires), chiffrement asymétrique (RSA, Diffie-Hellman, courbes elliptiques), fonctions de hachage, MAC, signatures numériques.
- Modèles et preuves de sécurité : définition de la sécurité (IND-CPA, IND-CCA, EUF-CMA…), modèles d'attaques, cadres formels pour prouver la robustesse des constructions cryptographiques.
- Protocoles cryptographiques : protocoles d'authentification, échanges de clés, canaux chiffrés, signatures aveugles, preuves à divulgation nulle de connaissance.
- Implémentation sécurisée et cas d'usage : bonnes pratiques de développement, contre-mesures aux attaques par canaux auxiliaires, étude de cas (TLS, chiffrement disque, messageries sécurisées, blockchain, etc.).

Ressources et références

Deprecated: htmlspecialchars(): Passing null to parameter #1 ($string) of type string is deprecated in **C:\Developpement\syllabus\public_html\views\syllabus_template.php** on line **297**

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-4 Gestion du cycle de vie des certificats	**S6**

Contexte et enjeux de l'enseignement

Dans un environnement numérique où la sécurité des communications, l'identité des équipements et la confiance dans les échanges sont essentielles, la gestion du cycle de vie des certificats constitue un pilier fondamental. De la génération à la révocation, en passant par le déploiement et le renouvellement, chaque étape doit être maîtrisée pour garantir la continuité des services et la sécurité des infrastructures. Cet enseignement prépare les élèves à concevoir et maintenir des systèmes de gestion de certificats robustes, adaptés aux exigences industrielles, réglementaires et techniques. Il aborde également les défis liés à l'automatisation, à l'intégration dans les systèmes distribués et aux politiques de sécurité.

Prise en compte des dimensions socio-environnementales

Prérequis

Utilisation basique du système Linux.

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	11
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	8

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Expliquer le rôle et les principes des certificats numériques.
- Déployer une autorité de certification et ses composants associés.
- Gérer le cycle de vie complet des certificats dans un SI.
- Automatiser l'émission et le renouvellement de certificats.
- Identifier et résoudre les incidents liés aux certificats.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours
TP de déploiement et gestion de certificat sur un environnement Windows

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

QCM
TP évalué

INFRES_6_3 Architecture et Sécurité du Système d'information	INFRES
INFRES_6_3-4 Gestion du cycle de vie des certificats	**S6**

Plan de cours

- Écosystème PKI et architecture d’une autorité de certification
- Modèles hiérarchiques et distribués
- Fonctionnement d’une CA racine et intermédiaire
- Infrastructure matérielle et logicielle associée
- Cycle de vie d’un certificat
- Génération de clés, demandes de certificats (CSR)
- Délivrance, publication, renouvellement et révocation
- Listes de révocation (CRL), OCSP, durée de vie et rotation
- Automatisation et intégration dans les systèmes d’information
- Protocoles ACME, SCEP, EST
- Intégration avec les serveurs web, systèmes internes, IoT
- Sécurité des processus automatisés
- Surveillance, gestion des incidents et conformité
- Détection des pannes liées aux certificats
- Bonnes pratiques de surveillance et d’alerte
- Audits, conformité réglementaire (eIDAS, RGPD, etc.)

Ressources et références

Les supports pédagogiques sont disponibles en ligne sous Campus + QCM en ligne sur Campus sur la base de la séance précédente et préparatoire à la séance suivante.