INSA VALOR

SÉCURITÉ NUMÉRIQUE

98,8%
de clients satisfaits*

* enquête réalisée auprès de nos clients en septembre 2024

CODE : 5391

NOUVEAUTE

PROTECTION DES DONNÉES : CRYPTOGRAPHIE POUR LA CYBERSÉCURITÉ

COMPÉTENCE PRINCIPALE VISÉE

- Maîtrise des fondements mathématiques et de la mise en œuvre des solutions de cryptographie permettant d'offrir les services de sécurité (confidentialité, intégrité, authentification, non-répudiation, etc.)

OBJECTIFS PÉDAGOGIQUES

- Maîtriser la mise en œuvre des mécanismes pour offrir les services de confidentialité, d'intégrité et d'authentification
- Connaître les principaux algorithmes de chiffrement à clé secrète et à clé publique
- Appréhender la cryptanalyse et les attaques connues
- Maitriser la vision globale des enjeux liés à la protection des données

PUBLIC

- Responsables sécurité
- DSI : Développeurs, Chefs de projets, Ingénieurs techniques
- Toute personne impliquée dans les systèmes d'information ou souhaitant acquérir des connaissances en cryptographie pour garantir les différents services de sécurité

PRÉREQUIS

- Des connaissances générales en mathématiques et en algorithmique sont souhaitables afin de tirer pleinement profit de la formation.

CONTENU

PARTIE 1 : CRYPTOGRAPHIE

Introduction :

- Terminologie et vocabulaire
- Historique et acteurs à connaître
- Services de sécurité fournis par la cryptographie
- Menaces et vulnérabilités
- Concepts mathématiques de base

Cryptographie symétrique :

- Cryptographie symétrique Vs cryptographie asymétrique
- Cryptographie symétrique par flux (RC4, A5/1, etc.)
- Cryptographie symétrique par bloc (DES, AES, etc.)
- Étude détaillée de l'algorithme AES
- Avantages et limites de la cryptographie symétrique

Cryptographie asymétrique :

- Principe et Fondements de la cryptographie asymétrique
- Cryptographie basée sur le problème de factorisation : étude détaillée de l'algorithme RSA
- Cryptographie basée sur le logarithme discret : Cryptographie sur les courbes elliptiques
- Taille des clés, recommandations et justifications

Travaux pratiques :

- Mise en place de solutions de cryptographie AES et RSA: fonctionnement, chiffrement, déchiffrement et attaques.
- Prise en main de OpenSSL: chiffrement et déchiffrement

SESSIONS

VILLEURBANNE : du 24/06/2025 au 26/06/2025
Frais pédagogiques individuels : 2 310 € H.T.

* Repas inclus

L'ouverture de la session est conditionnée par un nombre minimum de participants.

DURÉE

3 jours (21 heures)

ÉQUIPE PÉDAGOGIQUE

Enseignant/chercheur INSA Lyon du département Telecoms / Laboratoire CITI. Spécialiste en sécurité, réseaux, IoT et évaluation de performances.

RENSEIGNEMENTS ET INSCRIPTION

Tel : +33 (0)4 72 43 83 93
Fax : +33 (0)4 72 44 34 24
mail : formation@insavalor.fr
Préinscription sur formation.insavalor.fr

Accueil des personnes en situation de handicap nécessitant un besoin spécifique d'accompagnement : nous contacter à l'inscription

PARTIE 2 : HACHAGE ET SIGNATURE NUMERIQUE

Fonctions de hachage

- Concept et cas d'utilisation
- Propriétés mathématiques et fondement algorithmique
- Hachage simple (Unkeyed) et sécurisé (Keyed)
- Sécurité et longueur du hachage
- Attaques contre les fonction de hachage (focus sur l'attaque de collisions)
- Étude de quelques algorithmes MD5, SHA-1, SHA-256
- Applications : Stockage des mots de passe.

Scellements et signatures numériques :

- Scellement Vs Signature numérique
- Code d'Authentification de Message (HMAC, CBC-MAC, etc.)
- Signatures numériques : principe et fonctionnement
- Les algorithmes de signature numérique
- Applications : Intégrité et authentification dans les protocoles de communications
- Applications : Signature électronique des documents

Travaux pratiques :

- Calculs d'empreintes et de signatures avec OpenSSL
- Stockage des mots de passe : Mise en place de plusieurs solutions, comparaison et évaluation.

PARTIE 3 : CLES ET PKI

Gestion de clés cryptographiques et plateforme à clés publiques (PKI) :

- Principe de distribution/pré-distribution/échange de clés symétriques/asymétriques
- Gestion de clés symétriques et problèmes associés
- Gestion de clés asymétriques et problèmes associés
- Attaque de l'homme du milieu / Algorithme Diffie-Hellman
- Certification des clés publiques
- Norme X.509
- Modèles d'infrastructures de gestion de clés publiques
- Étude détaillée du modèle à base d'autorités de certification
- Exemple d'application : étude du protocole TLS
- Étude d'autres modèles : DANE, PGP, modèles à base de blockchain

Travaux pratiques :

- Mise en place d'autorité de certification avec OpenSSL,
- création et signature de certificats, révocation, renouvellement, etc.

MOYENS ET MÉTHODE PÉDAGOGIQUE

Cours - Travaux Pratiques - Exercices - Etude de cas et Echanges avec un expert du domaine

Un support de cours sera remis à chacun des participants.

ÉVALUATION ET RÉSULTATS

Évaluation des acquis de la formation

Evaluation des acquis des apprenants réalisée en lors de la formation par des exercices, des travaux pratiques et un questionnaire ouvert contextualisé.

Taux de réussite

90.5% des apprenants ont acquis la compétence principale visée

Résultat obtenu pour 155 participants évalués ayant suivi une formation dans la thématique sur les 5 dernières années

Évaluation de la satisfaction

Evaluation du ressenti des participants en fin de formation (Niveau 1 KIRKPATRICK)

Résultats de l'évaluation

Le niveau de satisfaction globale est évalué à 4.3/5 par les participants.

Evaluations réalisées auprès des 192 participants ayant suivi une formation dans la thématique sur les 5 dernières années

Actualisée le 07/11/2024