DOMAINE : Systèmes d'Information Industriels - MES - Historians / **SOUS-DOMAINE :** Urbanisation des SI Industriels

ACTION DE FORMATION
CRYPTOGRAPHIE POUR LA CYBERSECURITE (PROTECTION DES DONNEES)

RÉF. CYBR-04

DURÉE : 3,00 jours- 21,00 h.

PUBLIC VISÉ (FONCTIONS & SERVICES)

Responsables Sécurité DSI : Développeurs, Chefs de projets, Ingénieurs techniques et toute personne impliquée dans les systèmes d'information ou souhaitant acquérir des connaissances en cryptographie pour garantir les différents services de sécurité.
issus des services : Informatique, Informatique de Gestion, Informatique industrielle ; DSI, Systèmes, IT

PRÉREQUIS

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

OBJECTIFS DE L'ACTION DE FORMATION ET COMPÉTENCES ACQUISES

- 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.

À l'issue de la formation, les stagiaires seront capables de mettre en œuvre des solutions de cryptographie permettant d'offrir les services de sécurité de confidentialité, d'intégrité, d'authentification, de non-répudiation, etc.

MÉTHODE ET MATÉRIEL PÉDAGOGIQUE

Pédagogie active basée l'alternance d'exposés généraux théoriques, d'échanges avec l'expert du domaine, d'exercices pratiques et études de cas.

INTERVENANT

Expert du domaine, Spécialiste en sécurité, réseaux, IoT et évaluation de performances.

COMMENTAIRES COMPLEMENTAIRES EVENTUELS

Nous vous invitons à prendre contact en cas de participation de personnes en situation de handicap.

DOCUMENTATION STAGIAIRE

Une documentation sera remise à chaque participant.

SPC Formation
204 route de Vourles - Parc Inopolis - 69230 Saint-Genis-Laval - France
Tél : +33 4 72 67 12 34 - E-mail : formation@groupe-spc.com
Web : www.groupe-spc.com/fr/formation
RCS Lyon B 391 572 567 - NAF 8559A - Id. TVA FR 86 391 572 567
SARL au capital de 10.000 euros
Organisme de formation enregistré sous le n° 82 69 04028 69 auprès du préfet de la Région Auvergne-Rhône-Alpes.
Membre les acteurs de la compétence (Fédération de la Formation Professionnelle)

CONTENU DE LA FORMATION

PARTIE 1 - CRYPTOGRAPHIE

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

II - 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

III - 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

IV - 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

PARTIE 2 : HACHAGE ET SIGNATURE NUMERIQUE

I - 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 fonctions de hachage (focus sur l'attaque de collisions)
- Étude de quelques algorithmes MD5, SHA-1, SHA-256
- Applications : Stockage des mots de passe.

II - 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

III - 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

I - 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

II - Travaux pratiques
- Mise en place d'autorité de certification avec OpenSSL,
- Création et signature de certificats, révocation, renouvellement, etc.

ÉVALUATION DE L'ACTION DE FORMATION

-Évaluation des acquis des apprenants réalisée en fin de formation
-Évaluation du ressenti des participants en fin de formation (Niveau 1 KIRKPATRICK)

SPC Formation
204 route de Vourles - Parc Inopolis - 69230 Saint-Genis-Laval - France
Tél : +33 4 72 67 12 34 - E-mail : formation@groupe-spc.com
Web : www.groupe-spc.com/fr/formation
RCS Lyon B 391 572 567 - NAF 8559A - Id. TVA FR 86 391 572 567
SARL au capital de 10.000 euros
Organisme de formation enregistré sous le n° 82 69 04028 69 auprès du préfet de la Région Auvergne-Rhône-Alpes.
Membre les acteurs de la compétence (Fédération de la Formation Professionnelle)