FC9CS14 Nous consulter 2 jour(s)

Comprendre la cryptographie et son utilité dans le monde numérique

OBJECTIFS

- Décrire les bases théorique et pratique des techniques de cryptographie pour répondre aux risques et enjeux de protection des données et des applications sensibles.
- Maîtriser les bases de la cryptographie, les problématiques techniques, les contraintes.

PROGRAMME

Contexte

- Exemples d'attaques et fraudes récentes
- Identités, protection des données personnelles, anonymat, Privacy
- Contexte normatif et réglementation autour de la cryptographie
- Écosystème
- Cryptographie et biométrie

Introduction à la cryptographie et exemples classiques

- Authentification, chiffrement, hachage, One-Time Password, signature, etc.
- Techniques symétriques à clés secrètes : niveau de confiance, avantages et contraintes
- Algorithmes de chiffrement DES, AES, etc.

- Fonctions de hachage SHA-1, SHA256, SHA3, etc.

- Gestion, taille et sécurisation des clés

- Recommandations pratiques lors d'un déploiement

- Études de cas et d'exemples concrets : implémentation et limites dans les réseaux mobiles 2G, 3G, 4G, etc., retours d'expériences.

- Techniques asymétriques à clés publiques : avantages et contraintes

- Algorithmes RSA, DH, courbes elliptiques

- Gestion, taille et sécurisation des clés, recommandations

- Certificat numérique, autorité de certification, PKI, contraintes

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Toute personne souhaitant comprendre la problématique de la cryptographie dans un objectif de protection des données, ou étant impliquée dans la mise en place de solutions de sécurité : responsable de systèmes d'information, techniciens et administrateurs réseaux, responsables d'entreprises, ingénieurs, etc.

Une connaissance de base des principes de sécurité des données, des services ou des réseaux peut s'avérer un avantage pour tirer le meilleur profit de cette formation.

COORDINATEURS

Thierry BARITAUD

Responsable Sécurité des Services et Réseaux à la Division Innovation d'Orange.

Jean-François MISARSKY

Responsable d'une équipe, au sein des Orange Labs, travaillant dans le domaine de la Cybersécurité, de la protection des données personnelles, de la conception de services innovants et sûrs.

MODALITES PEDAGOGIQUES

Démonstrations et études de cas.

de déploiement

- Études de cas et d'exemples concrets : messagerie sécurisée, SSL, monde bancaire, EMV, etc.

Nouvelles techniques et solutions innovantes

- Cryptographie avancée : nouveaux algorithmes et applications
  - Zero-Knowledge
  - Anonymat révocable, enchères électroniques
  - Vote électronique : études des solutions déployées en France
- Cryptographie à bas coût : théorie et pratique
  - Contraintes en environnement IoT (Lightweight Cryptography)
  - Exemples d'applications : Ticketing, etc.
- Cryptographie quantique et post quantique, ordinateur quantique
  - Théorie, mythe et réalité, contraintes de déploiement
- Chiffrement homomorphe : principes et apports
  - Exemple : utilisation en environnement Cloud
- Blockchain
  - Théorie, applications, conseils
  - Exemples: crypto-monnaie, etc.
- Nouvelles perspectives