G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Principes et mise en œuvre des PKI

But de la formation

- Apprendre les technologies et les normes (initiation à la cryptographie)
- Apprendre les différentes architectures
- Apprendre les problématiques d'intégration (organisation d'une PKI, formats de certificats, points d'achoppement)
- Apprendre les aspects organisationnels et certifications
- Apprendre les aspects juridiques (signature électronique, clés de recouvrement, utilisation, export / usage international)

Pré-requis

- Formation universitaire de base ou Ingénieur en informatique
- Pas de connaissance de la cryptographie ni des certificats requis
- Constitue un plus : utilisation de la ligne de commande, notion d'API bases de réseau IP

Type de public

- Architectes,
- Chefs de projets,
- Responsables sécurité/RSSI avec une orientation technique,
- Développeurs seniors,
- Administrateurs système et réseau senior.

Moyens pédagogiques

- Support de cours au format papier en français
- Ordinateurs portables et 'tokens' cryptographiques mis à disposition par HS2 pour les exercices
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Sanction de la formation

- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec échanges interactiff et travaux pratiques

Durée

21 heures (3 jours).

Programme

Journée 1 : Mise en contexte

- Bases de cryptographie:
  - Notions de dimensionnement et vocabulaire de base
  - Mécanismes, 1.1.3 Combinaisons de mécanismes,
  - Problèmes de gestion de clés
  - Sources de recommanda on: ANSSI, ENISA, EuroCrypt, NIST
- Implémentation de la cryptographie:
  - Bibliothèques logicielles,
  - Formats courants
  - Usages courants et gestion associée
  - Chiffrement de fichiers et disques
  - Chiffrement de messagerie
  - Authentification
  - Chiffrement des flux
- Grands axes d'attaques et défenses
- Exercices OpenSSL d'utilisation des primitives cryptographiques
- Cadre général : Historique

Journée 2 : PKI et organisation

- Matériel cryptographique
  - Différents types d'implémentation matérielles
  - Certification Critères Communs
  - Certification FIPS 140-2
- Structure de PKI
  - Certificats X509
  - Rôles : sujet, vérificateur, certificateur, enregistrement, révocation
  - Architectures organisationnelles courantes
  - Cinéma ques dans PKIX
  - Hiérarchies d'autorités
  - Vérification récursive d'une signature
- Cadre légal et réglementaire
  - Droit de la cryptologie
  - Droit de la signature électronique
  - Référentiel général de sécurité
- Certification d'autorité
  - ETSI TS-102-042 et TS-101-456, certification RGS
  - Exigences pour les inclusions dans les navigateurs et logiciels courants
  - Evolution des pratiques
  - Exercice : Opération d'une infrastructure de gestion de clés avec Gnomint jusqu'à authentification TLS réciproque

Journée 3: Implémentation de PKI et perspectives

- Suite des exercices de gestion d'IGC et ajout d'une génération de certificat sur token USB
- Mise en oeuvre de PKI
  - Différents types d'implémentation d'IGC rencontrées couramment
  - Types d'acteurs du marché
  - Recommandation pour l'intégration
  - Attaques sur les PKI
  - Problème des PKI SSL/TLS
  - Remédiations mise en oeuvre pour TLS
- Infrastructures de gestion de clés non X509
  - GPG
  - SSH
  - R/PKI
- Prospective
  - Evolution de la cryptographie: les évolutions réelles, et phénomènes médiatiques
  - Distribution de clés par canal quantique (QKD)
  - Cryptographie Homomorphique
  - Cryptographie-post quantique
  - Gestion des clés symétriques
  - Tendances et conclusion