Formation « Principes et mise en œuvre des PKI »

Réf : SECUPKI

La cybersécurité repose sur une brique de base indispensable : la cryptographie. La cryptographie repose sur des conventions secrètes, des clés secrètes en cryptographie symétrique, des bi-clés : clé privée et clé publique en cryptographie asymétrique. La PKI est ce qui permet de gérer ces clés cryptographiques asymétriques et de leurs certificats. Les PKI sont indispensables à la construction de services de confiance comme la mise en place d'identités numériques, la signature électronique, le chiffrement des échanges, etc.

Objectifs

- Apprendre les technologies et les normes (initiation à la cryptographie)
- Apprendre les différentes architectures et les moyens de les sécuriser
- Comprendre les besoins métier concernant les certificats
- Acquérir les connaissances et compétences nécessaire afin de fournir un support haut-niveau aux métiers
- 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, séquestre)

Durée & horaires

- 5 jours soit 35 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 15 participants

Public visé

- Architectes
- Chefs de projets
- Responsable sécurité/RSSI avec une orientation technique
- Développeurs séniors
- Administrateurs système et réseau senior

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, bases de réseau IP
- Connaissance de Windows et de Linux ubuntu souhaitable

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours 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

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**
- **Evaluation de pré-formation envoyée avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUPKI par**
- **HS2.**

Programme

Jour 1 : Technique & cryptographie

- Primitives cryptographiques la synthèse
  - Histoire de la cryptographie
  - Mécanismes cryptographiques symétriques et asymétriques, condensé
  - Objectifs de sécurité :
    - Authentification, confidentialité, intégrité
  - Assemblages courants :
    - Signature, MAC message d'authentification, association hybride symétrique & asymétrique, clé de session, vecteur d'initialisation
  - Attaques cryptographiques :
    - De la force brute à la cryptanalyse quantique
  - Attaques « man in the middle », attaques sur la gestion des clés
    - Gestion des clés et des secrets :
    - Conteneur matériel TPM, HSM, Secure Keys
    - Conteneur logiciel cryptoAPI, API cryptoki
    - Recommandations ANSSI/NIST/ECRYPT
  - Le besoin d'une infrastructure à clés publiques

Implémentations techniques de la cryptographie

- Le certificat X509 : objectif, format, limitations et usages
- Intégration de tokens et cartes à puce : PKCS #11, Java JCE, Ms CryptoAPI
- Usages de la cryptographie :
  - Authentification, intégration dans les domaines Windows
  - Réseaux privés virtuels VPN
  - SSL/TLS : principes et attaques
  - Signature électronique : principes, usages et normes
  - Horodatage
  - Chiffrement de messagerie avec S/MIME
  - Chiffrement de disques : BitLocker, EFS

Mise en œuvre des Infrastructures à clés publiques (PKI)

- Architecture et intégration
  - Architecture PKI-X :
    - Autorité de certification racine, Autorité de certification secondaire, Autorité d'enregistrement, Autorité de validation

- Architectures communes : déclinaisons des rôles, sécurisation
- Définition d'une politique de certification et d'une politique de sécurité
- Mise en place du modèle de confiance

- Mise en œuvre
  - Génération de clés, émission des certificats, liste de révocation
  - Séquestre de clés, Définition de l'agent de récupération des clés
  - Diffusion des clés
- Répondeurs OCSP, Agrafage OCSP

- Aspects Organisationnels : Processus clés, contrôles

Mise en œuvre d'une Infrastructures à clés publiques

- Présentation de la PKI EJBCA
- Présentation de Microsoft Active Directory Certificate Services
- Présentation de l'architecture des produits
- Installation et configuration de l'autorité de confiance racine autonome avec le produit EJBCA sous Linux Ubuntu
- Installation et configuration de l'autorité de confiance secondaire avec le produit Microsoft ADCS
- Demande de certificats via le portail EJBCA
- Demande de certificats Microsoft pour un ordinateur via la console MMC
- Gestion de la révocation
- Publication dans l'annuaire Active Directory

Aspects légaux et perspectives

- Aspects juridiques
  - Signature électronique : valeur juridique, cadre...
  - Réglementations d'usage : limitations, escrow (tiers de confiance)

Travaux Pratiques

Les exercices pratiques seront exécutés avec le produit EJBCA sous Linux pour la partie autorité de certification racine autonome et avec Microsoft Active Directory Certificate Services (ADCS) sous Windows 2019 Server pour la partie autorité de certification secondaire.
Les travaux pratiques, les démonstrations, et les vidéos de ce cours vous permettront d'apprendre à déployer une autorité de certification racine, une autorité de certification secondaire, de générer des certificats pour vos serveurs, vos utilisateurs. Vous serez à même de mettre en œuvre la publication et la révocation de vos certificats, de définir une politique de certification et de sécurité.