Cryptographie Appliquée

UFR d'informatique, électronique, électrotechnique, automatique (IEEA)
Université de Lille – sciences et technologies

Université de Lille 1 SCIENCES ET TECHNOLOGIES

Formation continue

http://formation-continue.univ-lille1.fr

www.facebook.com/Formation.continue.Lille.1

OBJECTIFS

À l'issue de la formation, vous aurez acquis les connaissances nécessaires pour savoir :

- proposer une solution cryptographique à un problème de sécurité informatique et plus précisément à un problème d'authentification, de confidentialité et d'intégrité des données ;
- utiliser des outils cryptographiques conventionnels, tels que :
  - la cryptographie symétrique (notamment AES) ;
  - la cryptographie asymétrique (notamment RSA et ECC) ;
- réaliser des solutions logicielles cryptographiques à l'aide d'outils de base (openssl).

PUBLIC

Tout informaticien professionnel et notamment les concepteurs de solutions logiciels et les administrateurs de systèmes informatiques

PRÉ-REQUIS

- Il est nécessaire d'avoir de solides notions d'informatique, notamment en termes de programmation, d'algorithmique et en termes d'infrastructure matérielle.
- Des connaissances en scripting (bash, perl, python…) faciliteront le suivi des manipulations.

CONTENUS

- Vue d'ensemble des technologies cryptographiques
  - cryptographie symétrique (clefs secretes - AES)
  - cryptographie asymétrique (paire de clefs public/privé - RSA/ECC)
  - Problématique de production de clefs cryptographiques
  - hachage (sha) et hachage cryptographique (PBKDF2, Scrypt)
  - notion d'autorité de confiance et de certificat
- Utilisation de technologies cryptographiques
  - chiffrement / déchiffrement simples
  - techniques de challenge / réponses
  - techniques de signature numérique
  - solutions cryptographiques à multiples ayant-droit/autorités
- Réalisations pratiques utilisant openssl

MODALITÉS PÉDAGOGIQUES

Démonstrations et discussions sur les éléments cryptographiques, suivis d'expérimentations et de manipulations en travaux pratiques. Les enseignements sont ensuite utilisés en Travaux Dirigés (sur machine) pour répondre à des problèmes cryptographiques concrets.

MATÉRIELS UTILISÉS

- Station de travail conventionnelle (PC)
- Système d'exploitation type Unix (Linux, mac os x ou windows 10)
- Librairie open source openssl (version à jour)
- Scripting shell, perl ou python pour les expérimentations/travaux dirigés

CONTACT

SABINE MARQUIS

03 20 33 72 37
sabine.marquis@univ-lille1.fr

Service formation continue
et alternance
Bâtiment B8
Cité scientifique
Rue Guglielmo Marconi
59655 Villeneuve d'Ascq Cedex

DURÉE - DATES

24 heures, 3 jours
8h30-12h30 14h-18h

9, 10, 11 mai 2017

TARIF

1 728 €

LIEU DE LA FORMATION

Bâtiment M5
Salle TIIR, B03, aile B
Av. Paul Langevin
Cité scientifique
Villeneuve d'Ascq

RESPONSABLE PÉDAGOGIQUE

GILLES GRIMAUD
Professeur des universités
Département informatique, IEEA
Cité scientifique
Villeneuve d'Ascq