

UE Security architectures



Niveau d'étude
Bac +5



ECTS
6 crédits



Crédits ECTS
Echange
6.0



Composante
UFR IM2AG
(informatique,
mathématiques
et
mathématiques
appliquées)



Période de
l'année
Automne (sept.
à dec./janv.)

- > **Langue(s) d'enseignement:** Anglais
- > **Méthodes d'enseignement:** En présence
- > **Forme d'enseignement :** Cours magistral
- > **Ouvert aux étudiants en échange:** Oui
- > **Crédits ECTS Echange:** 6.0
- > **Code d'export Apogée:** GBX9SY02

Présentation

Description

1. Introduction



- Motivation/Diffie-Hellman ; MitM ; Kerberos ;
- Electronic Signatures ; DSS ; RSA-PSS ;
- References : RFC/PKCS/FIPS

2. Key Management.

- PKI elements, functions ; Certificates, ASN.1, X509, CRL ;
- Trust models
- PKIX : Administration ; migration ; OCSP, SCVP, Novomodo;
- Cross-certification ; Bridge ;
- Embedded Model : Certificates Browsers/OS; pinning, EV certs, notaries, bulletin board ;
- PGP + GnuPG ; Spooky/Sudsy ; IBE; CBE ;

3. Authentication by PKI

- fips-196 and variants

- Key transport
- Authenticated Diffie-Hellman (SIGMA)
- TLS (handshake)
- 4.  Cybersecurity of industrial IT
 - Electronic Signature and industrial PKI
 - Certification and Security Policies
 - PKI deployment in industry
 - Attacks against certification authorities and similar services
 - Evaluation Criteria and regulations (common criteria ; RGS ; e-IDAS)
- 5.  Application Security
 - Transactions: EMV ; SET ; 3D-Secure ; bitcoin
 - Messaging: E-mail, S/MIME ; OTR
 - Web: https
- 6. Threats
 - Introduction / Concepts / Threat Landscape
 - Network Architecture - Threats / Protection Layer 1 to 7
- 7. Communication Security
 - VPN: TLS, IPsec
 - Firewall / proxying
 - Wireless Security
 - IPv6
 - Routing: DNS / DNSSec ; TOR
 - Canal: TLS ; IPsec
- 8. OS Security
 - hardening
 - SeLinux, AppArmor, GRSec
 - HIDS

Heures d'enseignement

CM	CM	48h
TP	TP	30h

Pré-requis recommandés

Classic symmetric or asymmetric cryptosystems (RSA, AES, El Gamal).

Période : Semestre 9

Bibliographie

- J-G. Dumas, P. Lafourcade et P. Redon. *Architectures PKI et communications sécurisées*. Dunod, 2015.
- Brian Komar. *Windows Server 2008 PKI and Certificate Security*. Microsoft Press, 2008.

- Carlisle Adams and Steve Lloyd. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional; 2nd edition 2002.
- C. Cachat et D. Carella. *PKI Open source: déploiement et administration*. O'Reilly 2003.
- Thierry Autret, Laurent Bellefin et Marie-Laure Oble-Laffaire. *Sécuriser ses échanges électroniques avec une PKI: Solutions techniques et aspects juridiques*. Eyrolles 2002.
- *Enjeux de la sécurité multimédia*, T. Ebrahimi, F. Leprevost, and B. Warusfeld, éditeurs, Hermès 2006.
- *Cryptographie et sécurité des systèmes et réseaux*, T. Ebrahimi, F. Leprevost, and B. Warusfeld, éditeurs, Hermès 2006.
- B. Schneier. *Secrets and Lies*. John Wiley & Sons, 2000.
- A. J. Menezes, P. C. van Orschoff et S. A. Vanstone.  *Handbook of Applied Cryptography*. CRC Press 1997.
- W. Stallings. *Sécurité des Réseaux: applications et standards*. Vuibert 2002.
- J. A. Buchmann, E. Karatsiolis et A. Wiesmaier. *Introduction to Public Key Infrastructures*. Springer 2013.
- A. Karamanian, S. Tenneti et F. Dessart. *PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks*. Cisco Press 2011.
- J-G. Dumas, J-L. Roch, É. Tannier et S. Varrette. *Théorie des codes: compression, cryptage, correction*. Dunod 2007.
- J-G. Dumas, J-L. Roch, É. Tannier et S. Varrette. *Foundations of Coding: compression, encryption, error-correction*. 2012.

Infos pratiques

Contacts

Responsable pédagogique

Jean-Guillaume Dumas

✉ Jean-Guillaume.Dumas@grenoble-inp.fr

Lieu(x) ville

> Grenoble

Campus

> Grenoble - Domaine universitaire