Cryptography (CS110)

24 Hours

Outline

The Cryptography course teaches best practice and deep understanding of how to distinguish between symmetric and asymmetric encryption. There will be presented various types of ciphers.

The course will deal with the advantage, disadvantage and best practice of cryptographic implementation. In addition, the students will receive deep understanding of well-known encryption implementation protocols such as

NTLM, Kerberos, IPSEC, SSL. After the course, the student will have the appropriate capabilities to design, implement and analyze cryptographic solutions.

Objectives

The course will provide strong fundamentals in cryptographic area, including deep understanding of SSL/TLS, IPSEC and Kerberos protocols. The students will be able to design and implement cryptographic solutions based on the deep knowledge that will be provided during the lessons.

Target Audience

Developers, IT Managers, Security managers

Prerequisites

Advantage: Knowledge in network (TCP/IP)

Contents

- Cyber security overview
- CIA principles

- Introduction to cryptography
  - History
  - Examples

- Basic ciphers
- The security model
- Modern cryptography
- Symmetric ciphers : block ciphers (DES, 3DES, AES),Stream ciphers (RC4)
- Cryptographic hash functions : MD5, SHA-1, SHA-2, SHA-3

- Asymmetric cryptography
  - Diffie-Hellman key exchange
  - IKE
  - Encryption
  - Digital signature

- PKI infrastructure
  - Certificates
  - CA
  - Revocation (CRL, OCSP)

- SSL/TLS protocol implementation

- IPsec protocol implementation
  - ESP, AH protocols

- SSH protocol implementation
- NTLM
- Kerberos protocol authentication implementation
- Cryptographic attacks
- Qualys SSL Labs practice
- Wireshark practice