Cryptography

Intermediate Level

2 day Course

AppSec Labs Ltd.
info@appsec-labs.com | https://appsec-labs.com | 23 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

Cryptography: Intermediate level 2-Day Course

Seminar description

Cryptography is the cornerstone of security, used as the building block upon which important security operations are based, such as encryption, data integrity validation, hashing, secure random number generation, authentication, and so on.

In this seminar, we will extend our knowledge base over the cryptography domain, helping us to implement security features in our applications while utilizing crypto services for our own customized usage.

Target audience

- Designers, architects and developers
- Security teams

Course prerequisites

In order to be able to perform the hands-on labs, student must bring:

- Laptop/PC with 64-bit Windows OS
- .NET Framework v4.5.2 installed
- Visual Studio with minimum version 10.0.40219.1

Seminar topics

Day 1

Introduction to cryptography – 1:30 hours

- Definitions
- From classical to modern cryptography
- Shift Cipher (Caesar Cipher)
- Affine Cipher
- Substitution Cipher
- Transposition Cipher
- Enigma
- Through DES to AES and RSA
- Crypto attacks
- Brute force
- Cryptanalysis
- MitM
- Replay attacks
- Reflection attacks
- Cryptanalysis
- What cryptanalysis is
- Why is it important to use strong ciphers only
- Stream VS. Block ciphers
- Initialization vector (IV)
- Mode of operation– CBC, CFB, and why you should never use ECB
- Hash functions – MD5, SHA-1, SHA-2 (SHA-256 and SHA-512) and SHA-3

Hands-on Lab: Data Confidentiality – 0:45 hours

- Manual Cryptanalysis – Decrypting cipher text

Data at Rest – 2:15 hrs.

- Protecting data confidentiality with Symmetric encryption – DES, 3DES, AES
- Protecting the data saved in a data store
- Sensitive information disclosure
- Man in the middle
- Using hashes for password storage
- Adding complexity by using a Salt
- Protecting the data against tampering
- Reviewing data integrity requirements
- Difference between the confidentiality and integrity
- Message Authentication Codes (MAC) and HMAC
- Detecting Changes Using Hash functions

Hands-on Lab: Protecting Data at Rest – 1:30 hrs.

- Protecting data confidentiality with AES
- Protecting data integrity with Hash
- Protecting data integrity with HMAC

Day 2

Data in Motion – 2:15 hrs.

- Protecting data confidentiality with Asymmetric encryption
- Protecting the data against tampering
- Digital Signatures
- Cryptography based authentication
- Identify one side or both sides (mutual authentication)
- Challenge based authentication
- Protecting the data in network communication
- Potential threats
- SSL - The protocol, flow, flaws and mitigations
- Message Level Security vs Transport Level Security

Hands-on Lab: Protecting Data in Motion – 0:45 hrs.

- Protecting data confidentiality with Asymmetric
- Protecting data integrity with Digital Signature

Key management – 1:45 hrs.

- Secure creation of encryption keys
- Secure generation of random numbers
- Password Derived Key
- Diffie-Hellman key exchange
- Secure Key storage
- DPAPI (Data Protection API)
- X509 Certificates
- The Certificate store
- PKI (Public Key Infrastructure)
- SSL/Certificate Pinning

Hands-on Lab: Secure Key Management – 1:15 hrs.

- Generating certificates using makecert
- Using DPAPI
- Generating encryption keys using password-based key derivation functions