.NET Cryptography

1-day seminar

Syllabus

AppSec Labs Ltd.
info@appsec-labs.com | https://appsec-labs.com | 10 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

.NET Cryptography
1-Day Seminar

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'll 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

Members of the software development team:

- .NET developers
- Designers & architects

Prerequisites

Before attending this seminar, students should be familiar with:

- Basic knowledge of the .NET framework

Seminar topics

Introduction to cryptography

- Definitions
- From classical to modern cryptography
- Crypto attacks
- Cryptanalysis
- Stream VS. Block ciphers
- Initialization vector (IV)
- Mode of operation– CBC, CFB, and why you should never use ECB

.NET cryptography

- The System.Security.Cryptography namespace
- Protecting data confidentiality with Symmetric encryption – DES, 3DES, AES
- Protecting data confidentiality with Asymmetric (public-private key) encryption
- Hash functions – SHA-1, SHA-2 (SHA-256 and SHA-512) and why use should never use MD5
- Secure generation of random numbers
- Protecting the data in network communication
- Protecting the data saved in a data store
- Cryptography based authentication

Data integrity

- Protecting the data against tampering
- Using hashes for password storage
- Adding complexity by using a Salt
- Message Authentication Codes (MAC)
- Digital Signatures

Key management

- Secure creation of encryption keys
- Key storage
- DPAPI (Data Protection API)
- Password Derived Key
- X509 Certificates
- The Certificate store
- PKI (Public Key Infrastructure)