Building Secure Applications

Course No. 1704 **Duration:** 2 Days

Course Overview:
Although application security is a relative old subject, most of the focus in the 90's was focused on securing the network infrastructure (e.g. firewalls, VPNs etc.), as well as the servers OS (e.g. patch management systems). However, in the last years focus has been shifted from the network and the infrastructure to the application layer. This is due to the fact that the infrastructure (i.e. network and OS) security has improved significantly while applications have remained vulnerable. Thus, the application layer has become the main target of attacks. In addition, it is well understood today, that secure applications means high-quality and more safe applications.
In the course we will learn the different aspects of application security including authentication, authorization, auditing, confidentiality, and data-integrity, as well as the different technologies addressing these requirements. We will study the risk analysis model and understand how to use it to analyze the risk of the threat associated with vulnerabilities in the application.
In addition, we will learn how to build secure applications, starting from including the security in the application development life cycle, continuing in secure coding practices, and security testing tools.

Who should attend?
- Application developers
- Software System Engineers
- Development Engineers
- System Architects
- Information Security Experts

Prerequisites:
Experience and comprehension of application development

Course Content:

1. Confidentiality and Data-Integrity
- Overview of the requirements
- Overview of Cryptology
  - Symmetric encryption
  - Asymmetric encryption
  - Digital signatures
  - Digital certificates
- How encryption and hash function are used to address these requirements
- XML-Encryption (for web services)
- XML-Digital signatures (for web services)

2. Authentication
- Overview of the requirements
- The different technologies used for user authentication
  - Passwords including Password Management
  - Challenge-Response authentication and Challenge-Response tokens
  - One-Time Passwords (OTP) and OTP tokens
  - Smart-cards and Public-Key technology
  - Biometric authentications
  - SAML (for web services)

3. Authorization and Access-Control
- Overview of the requirements
- Implementation of authorization mechanisms in the application layer
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role Based Access Control (RBAC)

4. Auditing & Logging
- Overview of the requirements
- Central logging
- Auditing and log analysis

5. Integrating security into the application development life cycle
- Security in the design stage
- Secure coding
- Security testing

6. Risk analysis and Threat Modeling

7. Application coding vulnerabilities

8. Secure coding best practices
- In Java (J2EE)
- In .NET

9. Security features of application frameworks
- J2EE
- NET

10. Summary