IT Systems Identity and Access Management

Why Attend

- We are living in the age of the Internet of Things (IoT) which provides seamless integration and ease of access between various objects regardless of their physical proximity. The IoT is spreading across different vertical domains such as healthcare systems, government services, banks and telecommunications, just to name a few. We are no longer only vulnerable to attacks against valuable enterprises' digital content but also to life threatening attacks, terrorist attacks, espionage attacks, etc. The need for providing identity assurance and stringent access control, as a result, is of utmost importance. This course covers the fundamental principles and architecture framework for an end-to-end IT identity and access management system. This includes identity assurance, authentication, authorization, accountability, auditability, Single Sign-On (SSO) and identity federation. It also discusses practical case studies such as e-passport, mobile banking, e-government services, EMV systems and other selected cases.

Course Methodology

- This course is highly interactive and includes group discussions, case studies and syndicate work. It also includes practical exercises and role playing that allow all participants to use the knowledge they gained to demonstrate their skills in identity and access management.

Course Objectives

By the end of the course, participants will be able to:

- Illustrate the identity and access management architecture framework and discuss the security risks associated with its various deployment options
- Discuss the different mechanisms for establishing strong authentication (e.g. OTP, certificate based authentication, device authentication, etc)
- Explain the principles of key public infrastructure and certification authorities, and demonstrate their value in mitigating the security risks facing modern societies
- Explain the most well-known access control mechanisms and the roles of oauth, OATH, SAML and OpenID standards in the IAM domain and apply the concepts of (federated) SSO
- Demonstrate the building of IAM using selected industrial tools and practical case studies (e.g. e-passport and boarder gate, mobile-banking, EMV scheme, and e-movement services)

Target Audience

- This course has been designed for IT professionals such as IT Strategic Planners, Project Managers, Security Managers, Security Architects and Risk Managers.Although the course is technical in nature, complex concepts are discussed at an abstract level to fit the needs of participants from various technical backgrounds.

Target Competencies

- Information security management
- Impelementing public key infrastructure
- Identification and authentication management
- Identity Access Management (IAM)

Introduction and principles of information security:

- Identity and access management (IAM) overview
- Attributes of information security:
- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Accountability
- Auditability
- Symmetric and asymmetric cryptography
- Hashing and digital signature
- Key management

Public Key Infrastructure (PKI)

- Architecture: certification and registration authority
- Life cycle management
- Types of certificates and usage patterns
- Encryption
- Digital signature
- Client certificate
- SSL server certificate
- Attribute based certificate
- Case studies (e.g. email protection, mobile banking, and document signing)

Identification and authentication

- Identification, verification and authentication overview
- Mechanisms of identification and authentication
- One time password
- Biometric
- Digital signature
- Smartcard
- Soft/hard tokens
- Mobile device
- Risk based authentication
- Step-up authentication
- Single-sign on and federated single-sign-on
- OATH, OpenID, BorwserID, and SAML
- Architecture framework and industrial tools
- Trusted computing role in identity assurance
- Security risks associated with the discussed mechanisms

Access control

- Principles of authorization
- Access control schemes
- OAuth protocol
- Enterprise rights management and digital rights management
- Privileged account management
- Governance and compliance

IAM framework and use cases

- IAM architecture framework
- IAM echo system
- IAM and cloud computing
- Illustrative use cases
- Border control
- E-passport
- National ID
- E-banking
- E-health system
- EMV scheme