

Fundamentals Of Security

Security Concepts, Crypto, Certs, Identity, Trust, Attack Patterns, ISO2700x, Reviews, Processes

The entire software user base - specifiers, management, users, developers, administrators – all demand security and all have a role in delivering it. The goal of this course is to teach participants a common core set of fundamentals that is the first step in achieving this. Security should be treated as part of the expected skill set of every software professional. They need a fundamental understanding of security issues, before considering how to address them in the apps they develop and deploy (or better, as an integral part of the design). Security considerations must be part of software decision making, though they should not

overwhelm it. Most software pros already have some awareness of security issues – this course builds on this basic knowledge and ensures the entire dev and infrastructure teams have a heightened and consistent appreciation of security concepts, along with a deep understanding of the core security standards.

This course focuses on the fundamental concepts and standards behind security. It is independent of any operating system or software environments Those attending will be well placed afterwards to think about optimum implementation strategies for their platforms.

Contents of One-Day Training Course	
<p>Target Audience Software developers and IT. professionals who need a good grounding in all the important security concepts</p> <p>Prerequisites Experience of working on software projects, including development, deployment and ongoing service provision.</p> <p>No previous security programming or infrastructure experience is required, though any such knowledge would be beneficial.</p>	<p>Security Services Message integrity Authentication Non-repudiation Proof of submission/delivery Confidentiality Privacy Anonymity</p> <p>Security Concepts Network authentication, authorization, auditing, ciphers, key exchange, hashing, salting, least privilege, default lockdown-mode, canonicalization, leaks, buffer overflows, attacks (dictionary, mitm)</p> <p>Cryptography Symmetric and asymmetric crypto Latest crypto standards AES and SHA-3 Elliptic Curve Cryptography Comparison of performance & robustness Problems with older specs [des/md5]</p> <p>Digital Certificates Public Key Infrastructure (PKI) Revocation and CRL Attributes, certificate fields</p> <p>Identity Identity management Identity and federation Limiting dispersal of identity</p> <p>Trust Services Offloading work to trusted third parties Whom to trust, how, and to what extent? Trust server</p> <p>Common Attack Patterns Social engineering Web app attacks and insider attacks Human factors</p> <p>ISO 2700x International standards for identifying, documenting and countering threats The proposed ISO 2700x series Purpose of ISO 27001 Information Security Management Systems</p> <p>Security Reviews Conducting security reviews Security threats – from inside and outside Building a threat model</p> <p>A Security Development Process Integral part of how we write software Best practices as part of dev process Ongoing influence</p> <p>A Security Infrastructure Process Security policy in the enterprise Secure deployment and operations Advisories – CERT, vendor-specific</p> <p>Design Patterns for Security How to correctly design security features into your software systems</p> <p>Security and ... Project Storage, backups, networking, WiFi, user interface, identity, kernel, etc. Designing a secure programmable infrastructure for a sample system</p>