

Cyber Security: What you Need to Know to Protect Your Corporate Assets

Duration

2 days

Instructor

Kal Toth

Class Limit

20 students

Prerequisite

None

Price

On-site:

Please contact SPC for pricing (contact information on page 2)

Public Training:

\$995 (2 days)

*Discount available for early registration

Materials Provided

- Student manual containing the course slides
- Student handouts with class exercises and class studies

Whether it has to do with personal privacy or corporate information, it is safe to say that ignoring information security is at your peril. Although information security has been relatively well understood by security practitioners for many years, corporations, software product companies and even financial institutions have been surprisingly slow at taking appropriate information security measures and have more often than not treated information security as “nice-to-have” or a luxury.

This is no-longer true of course. Events of the last two years have rudely awakened the unaware. It would appear that the business case for implementing sound security architectures and mechanisms should be more readily formulated and enunciated. Those armed with some technology know-how probably agree that firewalls, demilitarized zones, intrusion detection, security nets and message filters are necessary to keep hackers, spies, viruses and SPAM from accessing or misusing our vital information assets.

However, security does not come free and poorly chosen or improperly deployed security will “look good” but may leave holes that a “wily-hacker” can easily detect and covertly exploit. The question of what security to put in place and how much security is enough requires a sound understanding of the security threats, risks, policies, privacy legislation, models, mechanisms, procedures and best implementation practices.

Intended Audience

This seminar is specifically designed for software and systems engineers and information technology managers. The sessions first introduce them to the motivations, challenges, definitions and models of the information security discipline. They are then progressively introduced to current and emerging security architectures, the underlying mechanisms and protocols, and finally the implementation challenges of constructing such systems. Upon completion of this seminar, the attendee should be to begin to analyze feasible alternatives for their own organization and develop information security implementation plans designed to protect their sensitive corporate, customer and employee data.



TRAINING

Cyber Security

Instructor

Kal Toth is an Associate Professor in the Department of Computer Science at Oregon State University. His areas of experience and research interests are in the fields of software engineering and information security, especially as they relate to e-commerce, mobile devices and distributed systems. He is currently conducting research on a web-enabled consumer-centered authentication and assertion architecture based on the so-called "Persona Concept".

Prior to joining academia in 1999, over a 15 year period, Kal led several development and consulting teams focused on security product development and security evaluation of on-line systems supporting national security and consumer privacy data and applications. He also conducted several analysis and design studies of gateways and interfaces for trusted computing projects.

Kal has a Ph.D. in Computer Systems Engineering from Carleton University and is a P.Eng (British Columbia) with a Software Engineering designation.

For more information on this or other SPC Springboard courses, please visit www.spcspringboard.com or e-mail SPC at info@spc.ca

Software Productivity Center
Suite 460—1122 Mainland Street
Vancouver, BC V8M 4T8
www.spc.ca

Toll Free:	Fax:
1.877.548.1948	604.689.0141
Vancouver:	Toronto:
604.662.8181	416.885.0512

Outline

Motivation, Models, Definitions

- Security Risks, Vulnerabilities, Challenges And Pitfalls
- Definitions: Security, Privacy, Trust, Misuse, Crime, Fraud, Confidentiality, Availability, Integrity And Non-Repudiation
- Computer Security & Privacy Issues (Canada, US, Europe)
- Information Security Model: Administrative, Personnel, Physical, Communications, Network, Computer, Software and Electromagnetic Aspects.

Security Architectures

- Security Network Architectures: Private Nets, Virtual Private Nets (VPNs), Extranets
- Electronic Data Interchange (EDI) And Electronic Funds Transfer (EFT)
- Electronic Payment Processing / Payment Gateways
- Key Management: Public Key Infrastructure (PKI); Pretty Good Privacy (PGP); Secure Electronic Transaction Standard (SET)
- Emerging Security Architectures: MS Passport and Liberty Alliance

Security Mechanisms and Protocols

- Standard Host and Web Access Control and Authentication Mechanisms
- Encryption and Digital Signatures: How They Work
- Secure Socket Layer (SSL) Protocol
- Other Security Mechanisms: Biometrics, Smart Cards, Anti-Virus
- The Emerging Secure Assertion Markup Language (SAML)

Implementation Challenges

- Information Security Components: Cryptos, Routers, Firewalls, Trusted Software
- Security In Wireless Networks and Connections
- Software Development Implications: Specs, Designs, Processes, Tools
- Development and Maintenance Issues: Security Test, Penetration Testing, Security Audit

