

Course Description: The movement towards Web Services and Service Oriented architecture (SOA) paradigms requires new security paradigms to deal with new risks posed by these architectures. This session takes a pragmatic approach towards identifying Web Services security risks and selecting and applying countermeasures to the application, code, web servers, databases, application, and identity servers and related software.

Many enterprises are currently developing new Web Services and/or adding and acquiring Web Services functionality into existing applications -- now is the time to build security into the system!

Who Should Attend: This course is for those people who want to understand the real risks in SOA, WebServices, and XML.

Prerequisites: Students should have a basic understanding of SOA, web services, and XML. In addition, students will benefit more from the course if they have completed a basic course in web application security.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Architect security services in Web Services and SOA
- Understand how an attacker looks at Web Services
- Use best practices

Course Outline:

Web Services attack patterns

Common XML attack patterns

Data and XML security using WS-Security, SAML, XML Encryption and XML Digital Signature

Identifying services and federation with SAML and Liberty

Hardening Web Services servers

Input validation for Web Services

Integrating Web Services securely with backend resources and applications using WS-Trust

Secure Exception handling in Web Services

Understanding the impact of Web 2.0 technologies like Ajax, and REST on distributed systems security