

Tutorial Session 3

Web Services Security and Privacy

Patrick C. K. Hung

*Faculty of Business and Information Technology
University of Ontario Institute of
Technology (UOIT), Canada*

Casey K. Fung

*Network Centric Operations
Boeing Phantom Works, USA*

Abstract

Web services are becoming widely deployed to implement the automation of business processes such as supply chain management, inventory tracking, and healthcare management, just to name a few. A Web service is a new breed of web application that supports interoperable application-to-application interaction over a network based on a set of XML standards. This new architecture and new set of protocols brings a new set of security challenges such as confidentiality, integrity, anonymity, authentication, authorization and availability. As security has become an essential component for all information systems, several security solutions for Web services data have been proposed such as WS-Security, SAML and XACML. To enable privacy protection for Web service consumers across multiple domains and services, the World Wide Web Consortium (W3C) published a document called “Web Services Architecture (WSA) Requirements” that defines some specific privacy requirements for Web services as a future research topic.

This tutorial will discuss security risks and issues in Web services for supporting business processes. This talk will also briefly address the common practices and related tools/procedures for addressing those security risks. In addition, this tutorial will discuss privacy issues in WSA and related privacy access control issues in this context.

Furthermore, this tutorial will also introduce the concept of survivability in the context of Web services. Survivability is defined as the capability of a Web service to fulfill its mission in a timely manner, even in the presence of attacks, failures, or accidents.

About the Presenters

Patrick C. K. Hung is an Assistant Professor at the Faculty of Business and Information Technology in UOIT and an Adjunct Assistant Professor at the Department of Electrical and Computer Engineering in University of Waterloo. Patrick is currently collaborating with Boeing Phantom Works (Seattle, USA) and Bell Canada on security- and privacy-related research projects, and he has filed two US patent applications on “Mobile Network Dynamic Workflow Exception Handling System.” In addition, Patrick is also cooperating on Web services composition research projects with Southeast University in China. He was a Research Scientist with Commonwealth Scientific and Industrial Research Organization (Canberra, Australia) and a Visiting Assistant Professor at the Department of Computer Science in the Hong Kong University of Science and Technology. Patrick has been serving as a panelist of the Small Business Innovation Research and Small Business Technology Transfer programs of the National Science Foundation (NSF) in the States since 2000. He is an executive committee member of the IEEE Computer Society’s Technical Steering Committee for Services Computing, a steering member of EDOC Enterprise Computing Conference and an associate editor/editorial board member/guest editor in several international

journals. He is the Program Co-Chair of the 9th IEEE EDOC 2005, the General Chair of the 10th IEEE EDOC 2006 and the Program Committee Vice-Chair of the 2006 IEEE SCC 2006 and 2007. In addition, he also designed and organized the 2006 International Conference on Privacy, Security and Trust (PST 2006) in Canada.

Dr. Casey K. Fung is Principal Research Engineer in Boeing Phantom Work. He is principal investigator for Survivable Mobile Ad Hoc Network and other quality of service research projects. Casey was the lead inventor of a methodology for the development of mobile ad hoc systems that are resilient to attacks, failures, or accident. In the area of survivability of MANET, he has filed two patents and published three papers in collaboration with Prof. Patrick Hung. This methodology is being used to develop a prototype survivable MANET in Boeing. This research is valuable to network centric systems because a distributed system developed under this process will be able to adapt dynamically to exceptional behaviors through the regeneration of workflow specification. Technologies involved include attack tree analysis, transaction logic, Prolog engine, formal workflow language, and workflow engine. He was Affiliate Assistant Professor at University of Washington, Seattle. He obtained B.S. in Electrical Engineering from Ohio University, M.S. and Ph.D. in Computer and Information Science from Ohio State University, Columbus.