

ICWS 2006 **Tutorial 6**

Security in SOA and Web Services

Elisa Bertino and Lorenzo Martino
Department of Computer Sciences
Purdue University

Abstract:

Security is today a relevant requirement for any distributed application, and in particular for those enabled by the Web such as e-health, e-commerce, and e-learning. It is thus crucial that the use of Web services, stand-alone or composed, provide strong security guarantees. Web services security encompasses several requirements that can be described along the well known security dimensions, that is: integrity, whereby a message must remain unaltered during transmission; confidentiality, whereby the contents of a message cannot be viewed while in transit, except by authorized services; availability, whereby a message is promptly delivered to the intended recipient, thus ensuring that legitimate users receive the services they are entitled to. Moreover, each Web service must protect its own resources against unauthorized access. This in turn requires suitable means for: identification, whereby the recipient of a message must be able to identify the sender; authentication, whereby the recipient of a message needs to verify the claimed identity of the sender; authorization, whereby the recipient of a message needs to apply access control policies to determine whether the sender has the right to use the required resources.

In the tutorial we will first discuss the main security requirements underlying the interactions between clients and Web services and among the Web services themselves. Then we will describe how such security requirements are addressed by standards for Web services security recently developed or under development by various standardization bodies. Standards that are covered include: WSS, that encompasses a large number of components addressing various security aspects; XACML, that is related to access control and has been recently extended with a profile for Web services access control; WS-Federation, Liberty Alliance and Shibboleth, that address the important problem of identity management in federated organizations. Issues related to the use of these standards are discussed. Then, research approaches to the problem of Web service security will be surveyed, including negotiation-based access control for Web services, and access control for conversation-based Web services.

About the Presenters:

Elisa Bertino is professor of at the Computer at the Department of Computer Sciences, Purdue University and Research Director of CERIAS. Her main research interests cover many areas in the fields of information security and database systems. Her research combines both theoretical and practical aspects, addressing as well applications in a number of domains, such as medicine and humanities. She is co-editor in chief of *VLDB Journal* and she is currently a member of the editorial boards of several international journals, including *ACM Transactions on Information and System Security*, *IEEE Internet Computing*, *IEEE Security&Privacy*, and *Acta Informatica*. She is the author of many articles which appeared in International Journals and Conference Proceedings.

Lorenzo Martino is currently a Visiting Professor at the Department of Computer and Information Technology in Purdue University.