Journal of Information Security Research Volume 2 Number 2 June 2011

Contents

Editorial

One of the most growing domains in the distributed computing is the web services and it has far reaching applications in the near future. As the domain is growing at a faster rate, the concern for computing research is the security issues. *Hikmat Farhat* and *Khalil Challita* in their paper on *"A Security Architecture for Web Services"* built an architecture that includes the components such as authentication, authorization and a defense against denial of service attacks. This model was built on existing standards such as SOAP, WSS and XACML. Further, the authors have provided a detailed implementation with performance evaluation using the open source Apache tools.

One of the crucial challenges in XML management is how to define an XML access control model to handle update operations that include insertion, deletion, and modification, the authors *Meghdad Mirabi, Hamidah Ibrahim, Leila Fathi, Nur Izura Udzir* and *Ali Mamat* argue in their paper on "*An XML Access Control Model Considering Update Operations"*. Hence, to offset this problem they have proposed an XML access control model to support update privileges. They have updated operations supported by their proposed XML access control model based on the different default and conflict resolution policies .

A current technology in the mobile computing is the machine-to-machine (M2M) communications. The mobile computing systems need to ensure secure and reliable means of data communication. *Hao Wang* and *William Emmanuel Yu* in their paper on *"Comparison Between PKI (RSA-AES) and AEAD (AES-EAX PSK) Cryptography Systems For Use in SMS-based Secure Transmissions*" compared two cryptographic mechanisms, the RSA-AES and the AES-EAX PSK which provide end-to-end security for SMS-based transmission. They have implemented these two mechanisms assuming the constraints of standard SMS network and measured their performance in terms of transaction time. Their study indicated that in terms of processing time, the Authenticated Encryption and Associate Data (AEAD) modes represented by EAX performed better even when the digital signature of the Public Key Infrastructure (PKI) mode represented by RSA was not included.

Virtualization threats are common in many applications and in the log files the threats are identified by *Dennis C. Guster, Olivia F. Lee* and *Dustin C. Rogers* who presented their resulsts in the paper on *"Pitfalls of Devising a Security Policy in Virtualized Hosts"*. They suggest solutions to mitigate those security vulnerabilities. The solutions offered in their empirical study have been implemented on a network with over 200 hosts, 40 of which are virtualized.

Web services have potential features such as the composablity, interoperablity and autonomous nature. which means that a single web service interaction could involve services written in several different languages provided by several different service providers as *Michael Ruth* and *Curtis Rayford, Jr.* view in their paper on "*A Privacy-Aware, Decentralized, End-to-End, CFG-based Regression Test Selection Framework for Web Services using only Local Information"*. They have proposed a framework which is unique as it does not require service providers to expose private and sensitive implementation details in order to participate in the regression testing framework. They have documented a case study to highlight the approach and an empirical study to evaluate the cost-effectiveness of the approach.

The papers in this issue represent significant research in Information Security Research.

Editors