Int. J. Inf. Secur. (2012) 11:213
DOI 10.1007/s10207-012-0168-3

SPECIAL ISSUE PAPER

Message from the guest editors

Irfan Ahmed · Martin Naedele · Bradley Schatz · Ryoichi Sasaki · Andrew West

Published online: 21 June 2012

Supervisory control and data acquisition (SCADA) and industrial control systems monitor and control a wide range of industrial and infrastructure processes such as manufacturing production lines, water treatment, fuel production and electricity distribution. Such systems are usually built using a variety of commodity computer and networking components and are becoming increasingly interconnected with corporate and other Internet-visible networks. As a result, they face significant threats from internal and external actors. For example, the now famous Stuxnet (which is a Windows-specific computer worm containing a rootkit and four zero-day attacks) was specifically written to attack SCADA systems that alone caused multi-million dollars damages in 2010. 2011 and 2012 have seen additional increases in vulnerability disclosures in SCADA and industrial control systems, further increasing the urgency of finding effective and cost-efficient security measures.

The critical requirement for high availability in SCADA and industrial control systems, along with the use of bespoke, resource constrained computing devices, legacy operating systems and proprietary software applications creates special challenges for the applicability of traditional information security solutions. Thus, research focusing on devising security solutions that are applicable in the control systems context is imperative, as evidenced by the increased focus on the problem by governments worldwide.

This special section of the international journal of information security contains articles on SCADA and control system security. As a result of the call for papers, totally 11 papers were submitted to the special section. Each paper received at least two reviews based on which three papers were short listed and sent to the experts in the field to ensure their quality. Finally, two papers were selected for the issue. The papers were evaluated based on the originality, quality and relevance to the issue.

In the paper ‘An open virtual testbed for industrial control system security research’, Morris and Reaves describe a virtual control system simulator and testbed for conducting hardware in the loop experiments on intrusion detection systems for control systems. Such research is foundational to evaluating research in new mitigation strategies and systems effects.

In the paper ‘A log mining approach for process monitoring in SCADA’, Hadziosmanovic et al. describe the results of applying a pattern mining approach to detecting malicious actions from the process event logs of a control system.

We would like to thank our external reviewers for their hard work during the review process, as well as Javier Lopez and the other editors-in-chief of this journal for making this special section possible.

I. Ahmed (✉)
Computer Science Department, University of New Orleans,
New Orleans, LA, USA
e-mail: iahmed4@uno.edu

M. Naedele
Industrial Software Systems, ABB Corporate Research,
Baden, Switzerland
e-mail: martin.naedele@ch.abb.com

B. Schatz
Schatz Forensic, Queensland University of Technology, Brisbane,
Australia
e-mail: b.schatz@qut.edu.au

R. Sasaki
Tokyo Denki University, Tokyo, Japan
e-mail: sasaki@im.dendai.ac.jp

A. West
Invensys Operations Management, Brisbane, Australia
e-mail: andrew.west@ieee.org