3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)

University of Applied Sciences Ingolstadt, Germany

17 - 18 September 2015

Editors

Dr. Helge Janicke

Dr Kevin Jones

Abstract

The 3rd International Symposium for Industrial Control System & SCADA Cyber Security Research (ICS-CSR) brings together researchers with an interest in the security of industrial control systems in the light of their increasing exposure to cyber-space. ICS-CSR is a research conference aimed at high-quality academic research in the cyber security of industrial control system from the hardware, system and human-factor perspectives.

Sponsors

Full Synopsis

The 3rd International Symposium for Industrial Control System & SCADA Cyber Security Research (ICS-CSR) brings together researchers with an interest in the security of industrial control systems in the light of their increasing exposure to cyber-space. ICS-CSR is a research conference aimed at high-quality academic research in the cyber security of industrial control system from the hardware, system and human-factor perspectives.

The papers in this proceedings cover a wide spectrum of ICS cyber security issues and range from automated asset identification over Intrusion Detection to Active Defence using large scale honeypots. Other technical contributions include the extraction of vulnerabilities from ICS designs and the analysis of microgrid cyber security. This year, other topics are covered that address the response to incidents in ICS and SCADA systems as well as their forensically sound investigation. www.ics-csr.com

Editors

This conference was edited by:

Dr. Helge Janicke is a Reader in Computer Science at De Montfort University, Leicester (UK). He is heading the Software Technology Research Laboratory and the Cyber Security Centre. His research interests are in particular the cyber security of industrial control systems, access control and policy-based system management. He is chairing the International Symposium on ICS and SCADA Cyber Security Research and has published widely in this area of research.

Dr Kevin Jones is Head of the Airbus Group Innovations Cyber Operations team and is responsible for research and state of the art cyber security solutions in support of the Airbus Group (Airbus, Airbus Helicopters, Airbus Defence & Space, and Airbus HQ). He holds a BSc in Computer Science and MSc in Distributed Systems Integration from De Montfort University, Leicester (UK), where he also obtained his PhD (A Trust Based Approach to Mobile Multi-Agent System Security) in 2010. He has many years experience in consultancy to aid organisations in achieving accreditation to ISO27001 standard on Information Security Management and currently acts as an executive consultant to the Airbus Group on matters of cyber (information) security across multiple domains and platforms. Kevin is a recognised expert in cyber security of ICS/SCADA/OT systems and is active within the research community where he holds a number of patents and whose research interests include Risk Assessments, Security Architectures, Cyber Forensics and Cyber Operations. He is a Member of the IEEE, BCS, ISACA, and ISC2 and accredited as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and ISO27001 Lead Auditor.

Papers:

Laurens Lemaire, Jan Vossaert, Joachim Jansen & Vincent Naessens Extracting Vulnerabilities in Industrial Control Systems using a Knowledge-Based System
<http://dx.doi.org/10.14236/ewic/ICSCSR2015.1>

Roman Schlegel, Sebastian Obermeier & Johannes Schneider Assessing the Security of IEC 62351
<http://dx.doi.org/10.14236/ewic/ICSCSR2015.2>

Alexandru Vlad Serbanescu, Sebastian Obermeier & Der-Yeuan Yu ICS Threat Analysis Using a Large-Scale Honeynet <http://dx.doi.org/10.14236/ewic/ICSCSR2015.3>

Tingting Li & Chris Hankin A Model-based Approach to Interdependency between Safety and Security in ICS <http://dx.doi.org/10.14236/ewic/ICSCSR2015.4>

Peter Eden, Andrew Blyth, Pete Burnap, Kevin Jones & Kristan Stoddart A Forensic Taxonomy of SCADA Systems and Approach to Incident Response <http://dx.doi.org/10.14236/ewic/ICSCSR2015.5>

Ivo Friedberg, David Laverty, Kieran McLaughlin & Paul Smith A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation <http://dx.doi.org/10.14236/ewic/ICSCSR2015.6>

Manuel Cheminod, Luca Durante, Lucia Seno & Adriano Valenzano Analysis of Exploitable Vulnerability Sequences in Industrial Networked Systems: A Proof of Concepts
<http://dx.doi.org/10.14236/ewic/ICSCSR2015.7>

Adam Wedgbury & Kevin Jones Automated Asset Discovery in Industrial Control Systems - Exploring the Problem <http://dx.doi.org/10.14236/ewic/ICSCSR2015.8>

Giuseppe Settanni, Florian Skopik, Helmut Kaufmann, Tobias Gebhardt, Klaus Theuerkauf, Konstantin Boettinger, Mark Carolan, Damien Conroy & Pia Olli A Blueprint for a Pan-European Cyber Incident Analysis System <http://dx.doi.org/10.14236/ewic/ICSCSR2015.9>

Johannes Schneider, Sebastian Obermeier & Roman Schlegel Cyber Security Maintenance for SCADA Systems <http://dx.doi.org/10.14236/ewic/ICSCSR2015.10>

Ying He & Helge Janicke Towards Agile Industrial Control Systems Incident Response
<http://dx.doi.org/10.14236/ewic/ICSCSR2015.11>

Christoph Lang-Muhr, Matthias Schrattenholzer & Paul Tavalato Multi-Layer Agent-Based Simulation of Network Behaviour in Advanced Metering Infrastructures
<http://dx.doi.org/10.14236/ewic/ICSCSR2015.12>

Grigoris Tzokatzidou, Leandros Maglaras & Helge Janicke Insecure by Design: Using Human Interface Devices to exploit SCADA systems <http://dx.doi.org/10.14236/ewic/ICSCSR2015.13>

Cordell C. Davidson, Joel Dawson, Paul Carsten, Mark Yampolskiy & Todd R. Andel Investigating

the Applicability of a Moving Target Defense for SCADA systems
<http://dx.doi.org/10.14236/ewic/ICSCSR2015.14>

Paul Carsten, Todd R. Andel, Mark Yampolskiy, Jeffrey T. McDonald & Samuel Russ A System to
Recognize Intruders in Controller Area Network (CAN) <http://dx.doi.org/10.14236/ewic/ICSCSR2015.15>