Journal of Universal Computer Science, vol. 24, no. 5 (2018), 554-555
submitted: 16/5/18, accepted: 20/5/18, appeared: 28/5/18 © J.UCS

Technical and Social Aspects of Critical Infrastructure Security

J.UCS Special Issue

Jörg Keller
(Faculty of Mathematics and Computer Science, FernUniversität in Hagen, Germany
joerg.keller@fernuni-hagen.de)

Igor Bernik
(Faculty of Criminal Justice and Security, University of Maribor, Slovenia
igor.bernik@fvv.uni-mb.si**)**

Wojciech Mazurczyk
(Faculty of Electronics and Information Technology
Warsaw University of Technology, Poland
wmazurcz@elka.pw.edu.pl)

Critical infrastructure comprises various sensitive information which represent tremendous values. Their compromise could affect critical infrastructure and the results could potentially be catastrophic for people and the environment. Therefore, critical infrastructure systems need to be protected from cyber attacks. In recent years, cyber attackers have proven that they are becoming more motivated, they have various intentions, capabilities, knowledge, funding and tactics. Do we really know what are cyber attackers looking for, what types of information could be considered sensitive, their responsible personnel and how do we protect them?

Critical infrastructure has several sectors whose assets, systems, physical and virtual networks are considered so vital to a country that their destruction or incapacitation would have a debilitating effect on security, economic security, public health or any combination thereof. Critical infrastructure includes the communications sector, the chemical sector, the commercial facilities sector, the critical manufacturing sector, the defense industrial base sector, the emergency services sector, energy sector, the financial services sector, the food and agriculture sector, the government facilities sector, the healthcare sector, the information technology sector, the transportation systems sector, the water and wastewater systems sector, and the nuclear reactors, materials and waste sector.

Today, all critical infrastructure sectors rely heavily on IT for operations. The critical infrastructure security however remains a major challenge. As shown by the latest global ransomware attacks, both social and technical shortcomings play important roles in achieving adequate levels of critical infrastructure (in)security. For example, targeted attacks exploiting social shortcomings may be used to first penetrate into a critical infrastructure system, and then spread like wildfire by exploiting its technical shortcomings.

The special issue targets security of all types of critical infrastructure, and addresses both social and technical aspects of ensuring critical infrastructure security. The call for papers for this special issue was distributed over relevant mailing lists, call-for-paper distribution websites, personal and university websites, and on the homepage of the journal. In addition to submissions of new articles, extended versions of accepted papers from the Central European Cybersecurity Conference – CECC 2017 have been invited for submission under the condition of providing at least 50% new content. The submissions were peer-reviewed by experts in the domain.

Based on the reviews and our own judgment, six articles were selected for publication in this special issue, that represent the breadth of the field. Ralf Kreidel, Steffen Wendzel, Sebastian Zilien, Eric S. Conner and Georg Haas present a testbed for the evaluation of algorithms to detect covert channels in networks, which aims to support experimental work in this field. S. Prabavathy, K. Sundarakantham and S. Mercy Shalinie investigate a security system that targets the use of Internet-of-Things (IoT) sensors in critical infrastructure, and hence uses fog computing instead of a centralized solution to detect attacks. Loganathan Yamuna Devi and Kaliannan Thilagavathy present and analyze a privacy-preserving protocol to check integrity of critical infrastructure data that have been outsourced into a cloud. Barbara Bobowska, Michał Choraś and Michał Woźniak analyze data streams to prevent critical infrastructure from attacks on the application layer. Simon Vrhovec and Blaž Markelj investigate how information of hospital employees on the consequences of data breaches and information security conformance influences the use of mobile devices to access medical data in hospitals. Anže Mihelič and Simon Vrhovec discuss a controversial topic: are offensive measures, i.e. attacking the attacker, adequate to fight an attack on a critical infrastructure?

We would like to express our thankfulness to Christian Gütl (Managing Editor) and Dana Kaiser (Head of Editorial Team) for permitting us to organize this special issue under the umbrella of the Journal of Universal Computer Science. We also like to thank all reviewers who facilitated the review process, namely Miroslav Bača, Igor Bernik, Krzysztof Cabaj, Luca Caviglione, Michal Choras, Tobias Eggendorfer, Bela Genge, Christian Hummert, Jörg Keller, Maciej Korczynski, Jean-Francois Lalande, Olaf Maennel, Jorge T. Martins, Blaž Markelj, Wojciech Mazurczyk, Roman Messmer, Kai Simon, Mark Strembeck, Simon Vrhovec, Damian Weber, Steffen Wendzel, and Dirk Westhoff. Last but not least, we like to thank all authors for submitting their work to this special issue.

Jörg Keller
Igor Bernik
Wojciech Mazurczyk
(Guest Editors)