Workshop on Novel Approaches in Risk and Security Management for Critical Infrastructures

AIT Austrian Institute of Technology GmbH
Donau-City-Strasse 1, 1220 Vienna - Austria
19th and 20th September, 2017

HyRiM MITIGATE Sauron SPARKS SMART GRID PROTECTION AGAINST CYBER ATTACKS AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Imprint

Workshop on Novel Approaches in
Risk and Security Management for Critical Infrastructures

Vienna, 19th and 20th September, 2017

Publisher, media owner and content:
AIT Austrian Institute of Technology GmbH
Donau-City-Strasse 1
1220 Vienna
Austria

Printed by Repa Copy
Graphic Design and Layout: Friederich Kupzog

Table of Contents

Welcome Message

Critical infrastructures have increasingly moved into the focus of cyber criminals and hacktivists over the last years. They have become the target of phishing emails, ransomware attacks and highly sophisticated advanced persistent threats. Since a failure within critical infrastructures might have huge impacts on the economy, environment, population and society, a comprehensive and well-integrated risk and security management has become of particular importance to those organizations. Nevertheless, current frameworks and methodologies often do not meet the specific needs of critical infrastructures and their highly interconnected cyber-physical systems.

In this workshop, new methodologies, concepts and tools towards the security and risk assessment for critical infrastructures will be presented. Being developed in four EU projects (HyRiM, SPARKS, MITIGATE and SAURON), these approaches reflect leading-edge research activities on critical infrastructure protection. The contributions cover innovative concepts for identification and analysis of attacker behaviour and potential threats, the assessment of cascading effects in infrastructure networks, the influence of the human factor on security and the protection of physical perimeter. An additional focus of the workshop will be current legislation and standardization initiatives. Furthermore, live demonstrations will be prepared to showcase the implementation of these concepts in realistic use case scenarios.

I hope the workshop will positively impact your future work on this topic and will result in fruitful discussions over the two days.

Stefan Schauer
Austrian Institute of Technology GmbH
Center for Digital Safety and Security

Speakers

Mohammed Amine Abid, University of Passau – Dr. Mohammed Amine is currently a Postdoc Fellow in the chair of Computer Networks and Communications at the University Of Passau, Germany. From 2012 to 2016, he was appointed as an assistant professor at the National School of Computer Science (ENSI: http://www.ensi.rnu.tn) in Tunisia. He received his M.Sc. and Ph.D. degrees both in Computer science, in the area of networks and distributed systems, from the National School of Computer Science, in 2009 and 2012 respectively. His research and teaching interests focus on risk management, physical and cyber security, privacy preserving, energy systems and smart grid, mobile ad hoc and wireless sensor networks. Particularly, he works on QoS management in wireless networks, location-based routing, RPL and precision agriculture, M2M, IoT, autonomous flying machines, performance evaluation and protocol optimization and specification. He also served as an invited professor in several Engineering schools in Tunisia (Tunisia Polytechnic Engineering School (EPT), Higher School of Digital Economy (ESEN), etc.).
Website: http://www.fim.uni-passau.de/en/computer-networks/staff-and-guests/dr-mohamed-amine-abid/

Ali Alshawish, University of Passau – Ali Alshawish is a research associate and a Ph.D. candidate in the Computer Networks and Computer Communications Group, Faculty of Computer Science at the University of Passau, Germany. His research interests include network security, computer networks, privacy preserving using encryption, energy systems, surveillance technologies, and critical infrastructure protection. His current research focuses on risk management for utility networks. He holds a master's degree in Computer Science and Automation from the Ilmenau University of Technology, Germany. He is currently a member of the Institute of IT-Security and Security Law (ISL) and involved in the EU-project "HyRiM".
Website: http://www.fim.uni-passau.de/en/computer-networks/staff-and-guests/ali-alshawish/

Stefan Beyer, S2 Grupo - Dr. Stefan Beyer is Head of Research and Development at S2 Grupo, a leading European Cyber Security company and CERT operator. He obtained his PhD in Computer Science from Manchester University (United Kingdom) in 2004 and his BSc in Computer Science in 2001 from the same university. He has more than 10 years of experience in leading international research projects and is particularly specialised in transferring research results into industry. He was the Director of the Internet and Ubiquitous Computing research group at Instituto Tecnológico de Infromática (Valencia,

Spain) before joining S2 Grupo.
Website: https://s2grupo.es/es/inicio/

Santiago Cáceres, ETRA I+D – Santiago Cáceres, PMP, has been involved for more than ten years as senior project manager and analyst at the Technology Department of ETRA Research and development in several European projects in the areas of ICT and Security. His main interests are the protection of critical infrastructures and the use of secure technologies in the Smart City. He is Electronic Engineer – communications networking specialization - from the Polytechnic University of Valencia (Spain). He has worked in the past in LE-Technichs (Slovenia), the Technical University of Prague (Czech Republic) and in Generalitat Valenciana (the public administration of Valencia, SPAIN).
Website: http://www.etra.es/en/

Rafael Company, Valenciaport Foundation – is Environmental, Chemical and Biology Senior by the University of Valencia (1995). He has a large experience as responsible for the Environmental, Safety and Security International Projects on European Ports. Furthermore, he did a Master on Environmental Sciences degree specialised on Chemical Engineering. Rafael is involved in several European Projects since 2003 when he joined to the Port of Valencia, coordinating the assigned activities in different projects mainly related to environmental protection and port security as well as creating different port networks. In this way, he participates as speaker in International Forums, Congresses and Conferences around the world. Currently, Rafael is security project manager at the Valenciaport Foundation, a R+D area of Valenciaport. Moreover, Rafael is General Secretary and Technical Director of the European Economic Association EUROPHAR, a group formed by Port Authorities, Institutions and private organizations. Last but not least, Rafael is the SAURON project coordinator.
Website: https://www.valenciaport.com/en/

Christos Douligeris, University of Piraeus Research Center – Christos Douligeris, currently a professor at the department of Informatics, University of Piraeus, Greece held positions with the Department of Electrical and Computer Engineering at the University of Miami. He was an associate member of the Hellenic Authority for Information and Communication Assurance and Privacy and the President and CEO Hellenic Electronic Governance for Social Security SA. Dr. Douligeris has published extensively in the networking scientific literature and he

has participated in many research and development projects. He is the co-editor of a book on ‘‘Network Security’’ published by IEEE Press/ John Wiley and he is on the editorial boards of several scientific journals as well as on the technical program committees of major international conferences. He has been involved extensively in curriculum development both in the USA and Greece. His latest work has focused on the use of big data and artificial intelligence techniques in several areas, mainly in Telecommunications Planning and Management and in Security Analysis of Port Information Systems. Moreover, he has been working in data analytic techniques in Learning and Education and Emergency Response Operations. Prof. Douligeris has been the technical project manager of DAEDALUS, a MedEnpi funded project that dealt with the matching of skills between employers and potential employees through the development of an ICT platform. The Daedalus consortium consisted of partners from Greece, Cyprus, Palestine, Lebanon, Tunisia, Egypt and Italy. Prof. Douligeris has been instrumental in the signing of MOUs between his lab and major companies operating in Greece, like COSMOTE, Vodafone and Nokia, that allow the continuous interaction, training, transfer of knowledge and hiring of university students and graduates in the respective companies.
Home Page: http://www.unipi.gr/unipi/en/

Armend Duzha, Maggioli Group– Armend Duzha is an EU Project Manager at Maggioli Group, Special Projects. He received his M.Sc. in Economics and Market Policy (2013) and B.A. in Business Administration and Management (2011) from the University of Bologna. His main responsibilities include, but are not limited to the design, coordination and management, monitoring, controlling and reporting of the multiple R&D projects co-funded by the European Union under the various Frameworks and Programmes (e.g., Horizon 2020, Ambient Assisted Living, Interreg MED, Interreg CE, Interreg ADRION, ENI CBC MED, Erasmus+ etc.). In particular, he is/has been actively involved in the following EU projects: e-Health/e-Inclusion field (indicative projects include CarerSupport AAL), Cyber Risk Assessment and Management field (indicative projects include MITIGATE H2020), Cloud Computing field (indicative projects include UNICORN H2020, ARCADIA H2020). Mr. Duzha is also involved in the dissemination and exploitation planning and operations of the EU funded projects. He represents Maggioli in EU project reviews, international consortia, conferences and workshops and participates in a number of events organized in Italy and abroad. He has excellent communication and mediation skills, and the ability to deal well with people in many different contexts, which he has gained through his participation in multinational consortia.
Website: http://www.maggioli.com/

Ralf Fiedler, Fraunhofer CML – Ralf Fiedler is group manager at the Fraunhofer Center for Maritime Logistics and Service for the group "Ports and Transport Markets" since 2011. After having worked for Swedish and British transport and logistic research organizations, Mr. Fiedler joined in the Logistics Initiative Hamburg for the federal state Schleswig-Holstein in 2008. For 20 years, Ralf Fiedler has worked on intermodal and maritime issues within transport and logistics in a large variety of projects for public customers, such as for the European Commission since the 4th framework programme, and for private customers. Reference studies include, among others, the current German federal transport plan 2030, intermodal transport projects in the Baltic Sea region, port policy and port competitive studies and location analyzes as well as studies about the transport demand for RoRo services and Motorways of the Sea.
Website: https://www.cml.fraunhofer.de/

Ivo Friedberg, AIT – Ivo Friedberg finished his master's studies of Software Engineering & Internet Computing at Vienna University of Technology in 2014.He is currently pursuing his PhD degree with the Austrian Institute of Technology and Queens University Belfast on resilience of Smart Grids under cyber-attacks. His research interests lie in intrusion response, machine learning, resilience and cyber-physical control systems.
Website: http://www.ait.ac.at/

Antonios Gouglidis, Lancaster University – Antonios Gouglidis is a Senior Research Associate at Lancaster University, and currently involved in the EU funded project HyRiM. In the past, he worked in the industry as a software engineer, and in the public sector as an educator. He received his PhD in Applied Informatics from University of Macedonia, Greece; MSc in Mathematics from Aristotle University, Greece; MSc in Computer Science from Lancaster University, UK; and, BSc in IT Engineering from the Alexander Technological Educational Institute of Thessaloniki, Greece. His research interests include security, resilience, access control, and formal methods.
Website: http://www.lancaster.ac.uk/scc/about-us/people/antonios-gouglidis

Sandra König, AIT Austrian Institute of Technology – Sandra König is a researcher in AITs Center for Digital Safety & Security. She received her Bachelor and Master in Mathematics with a focus on Statistics at ETH Zurich and her PhD with distinction in Technical Mathematics at Alpen Adria University Klagenfurt. Working for AIT since 2014, her main focus lies on probabilistic models of risk as well as game theoretic analysis. Currently she is involved in several national and international projects including the EU founded project HyRiM.
Website: http://www.ait.ac.at

Sylvia Mayer, Federal Ministry of the Interior - Sylvia Mayer began her career after finishing an engineering-focused secondary school in the Austrian police. She completed the study of law in 2011 and the study of strategic security management in 2017. Since 2012, she works for the Federal Agency for State Protection and Counter Terrorism in the Ministry of the Interior, where she was charged with setting up a unit on the protection of critical infrastructure. Since autumn 2013, she leads this organizational unit and is also responsible for the national implementation of the directive on network and information security in an inter-ministerial cooperation.
Website: http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/ski/start.aspx

Laurens Naudts, KU Leuven – Laurens Naudts is a legal researcher at KU Leuven CiTiP - imec and has been involved in several EU-funded projects, such as iLINC, OpenScienceLink, Fidelity, Preemptive and, currently, VICTORIA. Recently finalised, the Preemptive project aimed to provide an innovative solution for the prevention of cyber-attacks targeted towards utility networks. Laurens' main research interest is to focus on the interrelationship between algorithms, algorithmic classification, the principle of equality, privacy and data protection.
Website: https://www.kuleuven.be/wieiswie/en/person/00097793

Michalis Pavlidis, University of Brighton – Dr Michalis Pavlidis is a Senior Lecturer in Information Systems Security at the School of Computing, Engineering and Mathematics at the University of Brighton UK, since 2014. He is also a member of the Secure and Dependable Software Systems (SenSe) research cluster. He holds a PhD in software engineering and was awarded a PhD scholarship

from the Engineering and Physical Sciences Research Council (EPSRC) and British Telecom (BT). His main research focuses on the engineering of trustworthy information systems. His research interests are in the area of requirements engineering and more particularly in trust, security, and privacy engineering. He is currently participating in the H2020 VisiOn and MITIGATE projects investigating privacy challenges in public administration services and security challenges in maritime supply chains.
Website: http://www.sense-brighton.eu/our-team/pavlidis/

Israel Perez, Universitat Politècnica de València – Israel Pérez received both his M.Sc. in Computer Engineering and his Ph.D. in Telecommunications Engineering (Dr.Ing.) from the Universitat Politècnica de València in 2000 and 2009, respectively. He has been enrolled in the Communications Department since 2004, where he Works as a senior researcher in the Distributed Real-time Systems Laboratory. He has been actively involved in national and international research and development projects, mainly for government agencies, defence and European Commission EU-FP6, EU-FP7 and Horizon 2020. His areas of interest include real time systems, command and control systems, cyber security and tactical communications.
Website: http://www.upv.es/

Stefan Rass, Universität Klagenfurt – graduated with a double master degree in mathematics and computer science from the Alpen-Adria Universität Klagenfurt (AAU) in 2005. He received a PhD degree in mathematics in 2009, and habilitated on applied computer science and system security in 2014. His research interests include applied system security, as well as complexity theory, statistics, decision theory and game-theory. He authored numerous papers related to security and applied statistics and decision theory in security. Closely related to the project is his (co-authored) book Cryptography for Security and Privacy in Cloud Computing, published by Artech House. He participated in various nationally and internationally funded research projects. Currently, he is an associate professor at the AAU, teaching courses on theoretical computer science, complexity theory, security and cryptography.
Website: https://www.aau.at/en/

Anna Sarri, ENISA – Anna Sarri joined ENISA in 2014 as an Officer in NIS. Her work is evolving around studies related to National Cyber Security Strategies (NCSS), Critical Information Infrastructure Protection (CIIP) and studies that provide guidelines and support to the European Commission and the EU Member States regarding the implementation of the Directive on network and information security. In the past, she worked for more than ten years in the telecoms sector holding several positions, such as IT Security engineer, service provision officer and technical team leader. She holds a B.Sc. in Computing and a M.Sc. in Information Security and Computer Crime from the University of South Wales in the UK.
Website: https://www.enisa.europa.eu

Stefan Schauer, AIT Austrian Institute of Technology – Stefan Schauer is an experienced researcher in AIT's Center for Digital Safety & Security. He studied Computer Science at the University of Klagenfurt and received his PhD in Theoretical Physics, working on Quantum Cryptography, at the Technical University Vienna. Since 2005 he is working for the AIT in several projects related to the fields of classical security and risk management. Currently, his main focus lies in the field of risk management and risk assessment as well as security architectures for critical infrastructures. In this context, he is interested in risk assessment using game theoretic approaches and the identification and handling of threats coming from the human factor. He is coordinating the FP7 project "Hybrid Risk Management for Utility Networks" (HYRIM).
Website: http://www.ait.ac.at

Paul Smith, AIT Austrian Institute of Technology - Paul Smith is a Senior Scientist in the Center for Digital Safety and Security at AIT, Austrian Institute of Technology. Previous to this appointment he was a Senior Research Associate at Lancaster University, UK. He received his PhD in September 2003 and graduated in 1999 with an honours degree in Computing from Lancaster. Paul's research interests are focused on the security and resilience of critical information infrastructures. He has participated in a number of international research projects in this area, and has published articles on numerous aspects that relate to this core interest.
Website: http://www.ait.ac.at

Invited Talks

Risk Assessment for Cyber-physical Smart Grid Systems

The SPARKS Project Approach

Paul Smith[1] and Martin Hutle[2]

[1]Center for Digital Safety & Security
AIT Austrian Institute of Technology
paul.smith@ait.ac.at

[2]Fraunhofer AISEC
martin.hutle@aisec.fraunhofer.de

Abstract – Risk assessment is the basis for securing the smart grid. Although many methods for risk assessment exist, they do not fully address the specific requirements that arise from the very nature of the system under consideration. In the SPARKS project, we developed a smart-grid-specific risk management cycle, based on existing standards and new technologies, and combined it with supporting tools.

1. Introduction

The smart grid is a typical representative of a networked cyber-physical system (CPS). An adequate risk assessment methodology for the smart grid needs to consider the nature of such a system. The infrastructure of the smart grid is highly heterogeneous, in terms of technology, ownership, and functionality. It is an interconnected system, composed of data networks, electrical and administrative dependencies. This implies the need to consider multi-stage cyber-attacks (such an attack was also a demonstration case in the SPARKS project) and complex scenarios of combined attacks. Finally, the primary attack goals target the physical part of the system – the electrical grid.

A typical risk assessment process starts with the identification of assets and defines their protection needs. The overall risk is defined as the combination of the impact of an attack and the likelihood that such an attack could happen. The latter is determined by an analysis of threats, vulnerability and attacker motivation and capabilities. Both, impact and likelihood are usually determined independently and then used together to assess the overall risk and to prioritise protection measures.

In the SPARKS risk assessment methodology [1], we adopted such a process. In particular, we took the ISO 27005 framework and defined a set of building blocks that can be used to populate the different steps of the framework.

The remaining sections of this paper discuss these steps of the SPARKS risk assessment methodology.

2. Assets and Security Objectives

In security and risk assessment for systems that are purely information technology, such as database systems or web-services, assets reside potentially in all parts of the system. In contrast, in the smart grid the most important assets – those that are responsible for the operation of the grid – are usually located at the edge between the cyber part and the physical part.

Another difference is related to the priority of security objectives. While for pure IT systems, confidentiality of the information assets is one of the core security objectives, in cyber-physical systems and in particular, in the smart grid, integrity often has highest priority, as it is the basis for functional safety. For fail-stop systems, system safety is even guaranteed without availability of the information asset.

Considering these two aspects allows us to distinguish two kinds of assets: primary assets whose violation of integrity directly impairs the physical process, and secondary assets whose manipulation indirectly could lead to manipulation of the primary asset.

As assessing and protecting assets comes with expenses, exactly those assets that are needed for the underlying business case should be considered. Identifying this set is a difficult and fault-prone task. To address this, in the SPARKS project we use a model-based approach to identify primary assets and their dependencies from secondary assets. The modelling is based on the Smart Grid Architecture Model (SGAM) [2]. We employ a precise language to formulate the elements on the different SGAM layers. A tool – implemented as a plugin for Enterprise Architect – serves as a graphical user interface to model the system. The model cannot only be used for identifying assets, but also for assessing threats and vulnerabilities, and for deriving countermeasures.

3. Handling the Complexity of Threat Analysis

The networked nature of the system under consideration leads to a large number of assets, threats and attack scenarios. Multi-stage attacks allow an attacker, e.g., to get a foothold in some office network, use weaknesses to compromise the automation network, and then use

automation protocols to manipulate the state of an actuator. Complex combined attacks use the combination of effects at different parts of the smart grid to achieve some adverse effect. An example is the attack on the Ukraine power grid in late 2015, where the primary attack on the automation system was combined with DoS-Attacks on the phone system and firmware manipulation to prevent recovery.

Standard risk assessment techniques like ETSI TVRA [3] look for threats for each individual asset, and ignore these interdependencies. They are not able to capture those attacks or e.g. countermeasures based on zoning and isolation. Attack trees [4] allow the representation of complex scenarios but become – when drawn manually – quickly intractable, as the number of attack vectors in such networks potentially grows exponentially. Tools-based approaches suffer significantly less from these drawbacks, as they allow an implicit representation of the attack graph, including threats and propagation paths.

In the SPARKS project, we use ontology reasoning [5] to deduce attack paths. Therefore, an ontology language was defined that can be used to export a knowledge model of the system from the SGAM system description in Enterprise Architect. Queries to the knowledgebase can then be used to extract attack paths and the associated threats.

A key feature is the reusability of created models. This is important for a periodic analysis as it is suggested, e.g., by [6]. The approach can be extended in a straightforward way to include vulnerabilities (e.g., from vulnerability databases) to the analysis.

4. Impact Analysis

The impact analysis comprises two steps: the identification of consequences and the actual assessment of those consequences.

In the smart grid, the view on the impact depends on the stakeholder under consideration. Not all types of consequences are relevant for a specific stakeholder. Figure 1 shows a mapping of various consequence categories to different stakeholders.

Category	PM	P	ICTP	ESCO	TSO	DSO
Economic		●		●	●	●
Safety	●					●
Quality of Supply				●	●	●
Infrastructures	●					
Regulatory	●		●	●	●	●
Reputational		●	●	●	●	●
Data Protection and Privacy		●	●	●	●	●
Equipment		●	●		●	●
Population	●					

Figure 1: Mapping of relevant consequence categories to stakeholders: policy makers (PM), producers (P), ICT equipment producers (ICTP), energy service companies (ESCO), transmission system operators (TSO), distribution system operators (DSO)

For each consequence category, a set of consequences and associated metrics can be given that characterize the different aspects of the impact category. Combining these metrics with Figure 1 allows the deduction of stakeholder specific impact tables. For example, in the SPARKS project, we deduced impact tables for our demonstration sites, a microgrid and a medium-size distribution system operator.

For the actual identification of consequences, we consider the following possibilities:

- *Expert Analysis* where a group of domain experts explore the potential consequences of a cybersecurity incident, e.g., in brainstorming sessions.
- *Safety and Security Analysis* employs adapted methods from the safety domain, such as event tree analysis, FMVEA, system theoretic process analysis (STPA), or Bayesian networks.
- *System analysis* uses mathematical equations, often differential equations, to model the electrical system and looks for analytical solutions to these equations.
- *Simulation* also relies on a mathematical description of the electrical grid but assesses the impact using tools such as GridLAB-D. This allows solutions for systems that are too complex for an analytical solution. In addition, it allows the combination with data network simulation (co-simulation) and for including real hardware in the simulation (hardware-in-the-loop).

In the SPARKS project, we carried out a system analysis to assess the resilience of a PV inverter installation when a certain number of inverters operate maliciously. We used co-simulation for assessing the impact of manipulated market information on the medium voltage grid. In addition, we used simulation with hardware in the loop to assess the manipulation of the voltage control in low voltage grids.

5. Risk Treatment

Although for risk mitigation there are many standards, best practices, and other catalogues for countermeasures and security recommendations, their linkage to the actual existing threats is mainly neglected for existing risk management cycles. In many standards, a set of high-level recommendations is made that are based solely on the final risk level. This completely neglects the results of a thorough threat analysis that has been performed, and might lead to the implementation of inappropriate countermeasures.

Therefore, for the SPARKS risk management process, we propose to use Semantic Threat Graphs (STGs) [7] as a tool to precisely determine the necessary countermeasures for the identified threats. STGs relate semantic information about security configuration with threats, vulnerabilities and countermeasures. Given the attack graph from the threat analysis, we start with a source node of this graph, which represents a high-level threat, and construct an STG for this node.

STGs are represented in terms of ontologies, which leads to a high re-usability of previously compiled graphs and gives access to a large number of implementation tools. Moreover, this formalization allows tool-based querying, and results in the necessary countermeasures being determined from a technologically precise perspective. By not implementing all available countermeasures but only those that are strictly necessary, costs can be reduced or the impact of security measures on the functionality of the system can be minimized.

Acknowledgements

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608224.

References

[1] Langer L, Smith P, Hutle M, Schaeffer-Filho A (2016) Analysing cyber-physical attacks to a Smart Grid: A voltage control use case. In: PSCC 2016: 1-7.

[2] https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf.

[3] ETSI (2010) Intelligent transport systems (ITS); security; threat, vulnerability and risk analysis (TVRA) ETSI TR 102 893, European Telecommunications Standards Institute.

[4] Schneier, B (1999). Attack Trees. Dr Dobb's Journal, 24/12.

[5] Wolf J, Wieczorek F, Schiller F, Hansch G, Wiedermann N, Hutle M (2016) Adaptive Modelling for Security Analysis of Networked Control Systems. In: ICS-CSR 2016.

[6] VDI/VDE 2182 “IT-security for industrial automation”.

[7] Foley S N, Fitzgerald W M (2009) An Approach to Security Policy Configuration Using Semantic Threat Graphs. DBSec 2009: 33-48.

The MITIGATE Methodology

An Overview

Christos Douligeris

Department of Informatics
University of Piraeus
cdoulig@unipi.gr

Abstract – This presentation overviews the main goals and methodology of the MITIGATE (Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrastructurEs) project, which introduces, integrates, validates (in real pilot operations), evaluates and commercializes a risk management system for port infrastructures, which will be able to deal with port critical information infrastructures (CIIs) and Information and Communication Technologies (ICT) systems, as well as their impact on dynamic maritime supply chains. MITIGATE pays attention to the collaboration of various stakeholders in the identification, assessment and mitigation of risks associated with cyber-security assets and international supply chain processes. This collaborative approach is able to boost transparency in risk handling by the various stakeholders, while it will also generate unique evidence about risk assessment and mitigation. The collaborative approach of the project is empowered by an open simulation environment enabling stakeholders to simulate risks and take relevant risk mitigation actions. This Open Simulation Environment enables the participants to model, design, execute and analyze attack-oriented simulation experiments using novel simulation processes. Particular emphasis is paid on the estimation of the cascading effects, as well as on the prediction of future risks

1. Introduction

Modern port infrastructures tend to be highly dependent on the operation of complex, dynamic Information and Communication Technologies (ICT) -based maritime supply chains. Maritime supply chains comprise globally distributed, interconnected set of organizations including port authorities, ministries, maritime companies, ship industries, customs agencies, maritime/ insurance companies, other transport Critical Infrastructures (CIs) (e.g. airports), other Critical

Information Infrastructures (CIIs) (e.g. transport networks , energy networks, telco networks), people, processes, services and products.

For over a decade significant efforts have been allocated in the introduction of risk management and assurance methodologies for CIs [1]. Most of these risk management methodologies focus on the identification and classification of threats, the identification of the various vulnerabilities and ultimately the evaluation of the potential impact of threats and vulnerabilities (e.g., [2], [3]). These methodologies feature differences in terms of the stakeholders that they address (e.g., policy makers, decision makers, asset managers, CI operators, solution integrators), but also in terms of the assets that they support and the level of accuracy that can handle. However, the interconnection of these actors and organizations relies typically on an interconnected web of transportation infrastructures and pathways, information technology, as well as cyber and energy networks and they are not appropriate for dealing with contemporary dynamic ICT based dynamic maritime supply chains, due to the fact that they are: overly focused on physical-security aspects and pay limited attention to CIIs and they do not adequately take into account security processes associated with international supply chains, which are nowadays ICT enabled and therefore severely dependent on intentional and unintentional compromise of CIIs. This is reflected in the fact that up to now we have seen only limited/partial implementations of relevant standards (such as ISO 28000). These limitations have also been acknowledged in reports, standards and regulations produced by prominent security stakeholders [4].

As a result, most of the actors involved in the maritime supply chain use varied and nonstandard practices to guarantee the credibility and the effectiveness of the full system development life cycle including design/development, acquisition of custom or commercial off-the-shelf (COTS) products, delivery, integration, operations, and disposal/retirement. During the last couple of years, we have witnessed the emergence of early initiatives that attempt to deal with the risks and vulnerabilities of the port CII ecosystem, both in terms of the number of stakeholders and in terms of the complexity and interdependencies of the CII assets involved. For example, the S-PORT project on ports' CIIs cyber risk assessment has provided a collaborative environment for the security management of the Port Information and Telecommunication systems [5], [6]. Moreover, other EU wide activities towards a holistic risk management framework for port security have recently emerged under the CIPS (e.g., the CYSM (Collaborative Cyber/Physical Security Management System) project - http://www.cysm.eu/) and FP7 programmes (SUPPORT (Security UPgrade for PORTs, (http://www.support-project.eu)). Nevertheless, the risk assessment methodologies studied in these projects are limited to the ports' CII domain and do not consider or predict cross-sectoral, cross-border threats from the port's supply chains. Likewise, tools and techniques for risk assessment take into account and implement general-purpose (cyber) security standards (such as ISO27001) and do not imple-

ment standards (such as ISO28000) which emphasize on security processes associated with international supply chains.

2. The MITIGATE Goals

The main goal of MITIGATE (http://mitigate.europrojects.net/) is to realize a radical shift in risk management methodologies for the maritime sector towards a collaborative evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA) approach that alleviates the limitations of state-of-the-art risk management frameworks. To this end, the project will integrate, validate and commercially exploit an effective, collaborative, standards-based risk management (RM) system for port's CIIs, which shall consider all threats arising from the global supply chain, including threats associated with port CIIs interdependencies and associated cascading effects. The project's RM system will enable port operators to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from the global ports' supply chain. In this way, port operators will be able to predict potential security incidents, but also to mitigate and minimize the consequences of divergent security threats and their cascading effects in the most cost-effective way i.e. based on evidence associated with simulation scenarios and security assurance models. MITIGATE will comprise simulation models, which will enable the production of timely, accurate, objective, reliable, relevant and high quality evidence, information, indicators and factors. The latter will empower a first-of-a-kind analysis and assessment of multi-dimensional risks, which is not nowadays possible.

In order to realize this goal the project sets the following specific objectives, shown also in Figure 1:

- To elicit, understand and analyze risk management requirements for port infrastructures, with particular emphasis on requirements associated with the dynamic nature of international ICT based maritime supply chains.
- To introduce and promote a rigorous, rational approach to risk management, which will produce high quality scientific and experimental based proofs and findings, (including simulation results, indicators and recommendations) in order to assist ports operators to evaluate and mitigate their risks.
- To optimize the Maritime Supply Chain governance system through enabling a variety of agents (e.g., maritime stakeholders, companies) to collaborate and share information, experience and expertise associated with port risks. MITIGATE will also provide tools and techniques for the configuration of this governance system, with

particular emphasis on parameters and processes that have to be configured in order to appropriate customize MITIGATE to the needs of different ports.

- To create an Open Simulation Environment that will promote the involvement and collaboration of the necessary maritime entities in the design and execution of various risk assessment simulation experiments towards creating high quality research evidence.
- To integrate appropriate monitoring and forecasting procedures to aid ports operators to predict and represent combined attacks/threats paths and patterns and to measure their effectiveness and applicability..
- To validate the operation of the MITIGATE system and of the accompanying tools in the scope of realistic scenarios/conditions comprising real-life infrastructures and end-users.
- To develop credible business models and business plans for the commercial roll-out of the MITIGATE framework (and accompanying tools) and to validate the business models based on feedback from all the envisaged business actors (both within and outside the consortium).
- To leverage, use and implement existing security standards (including ISPS, ISOS27001, ISO27005, ISO28000), and to contribute its risk management approach and system to the NIS* public-private platform (Network Information Security Platform).
- To elicit and document best practices for risk identification, assessment, classification, simulation and resolution, which will be appropriately structured in a knowledge base in order to facilitate the execution of relevant services of the MITIGATE framework.

3. The MITIGATE risk management system

In this section, we present the overall architecture of MITIGATE along with a fine-grained componentization scheme. As mentioned before, MITIGATE will provide a set of functional features such as collaborative risk assessment, visualization, simulation and open intelligence analytics. All these features rely on discrete components that implement the aforementioned functionality. However, these components have to collaborate to each other since the end-most functionalities of MITIGATE will be achieved through the synergy of these individual components. Therefore, beyond the elaboration of the high level architecture, it is necessary to identify the component interdependencies. .Furthermore, since most of the components rely on existing software artefacts it is extremely essential to identify the complementarity or any potential conceptual mismatch regarding the data structures that the various component interactions may raise. Since the aim of MITIGATE is to come up with a unified environment

where all aforementioned services are offered seamlessly it is extremely important to identify the interactions between the various services.

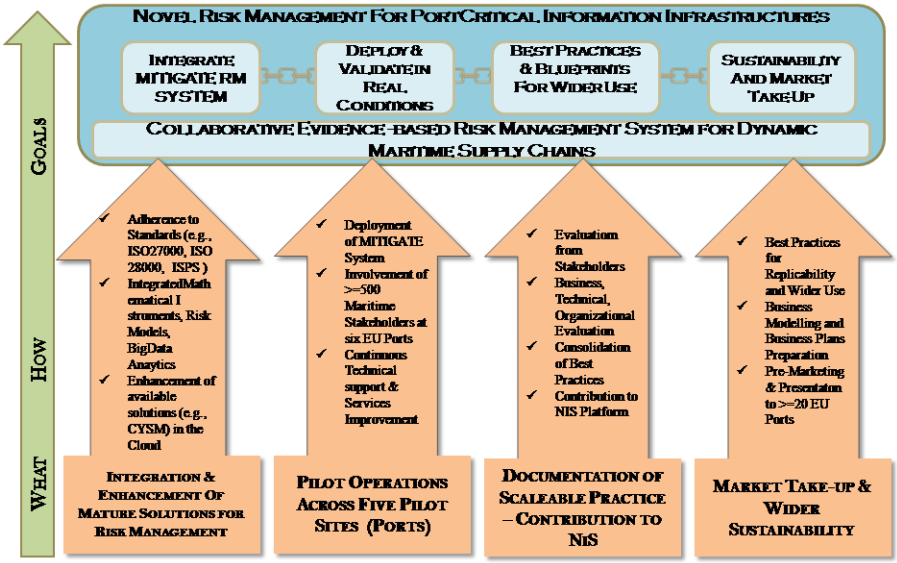

Figure 1: Overview of MITIGATE's main objectives and goals relative to the corresponding activities

We present the high level architecture and then we briefly discuss the functional components that comprise the architecture. Given the nature of MITIGATE, a specific set of services need to be developed and integrated in a seamless manner. Such services include assessment of risk in a collaborative manner among organizations, advanced simulation and visualization of potential attacks and advanced reports from open intelligence analysis services. In order to achieve the goal of developing a unified system, a high level architecture has been defined. This architecture is presented on Figure 2.

As it is depicted, there are seven main components that comprise the MITIGATE system: a) the Asset Modelling & Visualization, b) the Supply Chain Service Modelling, c) the Simulation & Game Theory, d) the Collaborative Risk Assessment, e) the Open Intelligence and Big-Data Analytics, f) the Notification and Reporting, g) the Administration and h) the Access Control and Privacy Component (which is not depicted on Figure 2).

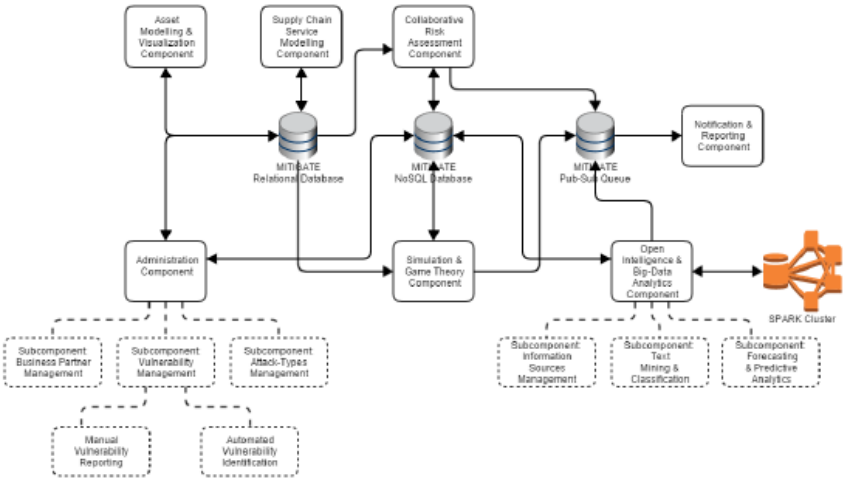

Figure 2: The MITIGATE high level architecture

The Asset Modelling & Visualization component allows security analysts to declare their assets along with the cyber relationships. This declaration is serialized in a strict format which has been introduced by the project and is called "Asset Cartography". The creation of a valid asset cartography within the frame of an organization is the first step towards the realization of a collaborative risk assessment. Each organization that participates in a supply chain service will use this component in order to create its own cartography. The cartography will be automatically linked to available vulnerabilities and attack-types that are relevant to the individual assets that are declared.

The Supply Chain Service Modelling component allows users to model the supply chain services that are performed by their organizations. More specifically, supply chain services consist of various business processes that are performed in a synergetic way among different business partners. Each business partner has a predefined role in the supply chain service which requires the 'participation' of specific cyber assets. Towards these lines, this component relies on the output of the Asset Modelling component since it allows to map assets that are already defined in the asset cartography of each organization with the processes that these assets are involved. This 'mapping' plays a significant role during the calculation of risks.

The Simulation & Game Theory component has a twofold goal. On the one hand it is responsible for the discovery of attack paths given a specific asset cartography and a specific supply chain service and on the other hand it is responsible to propose the best defensive strategy

regarding the protection of a specific asset based on game theoretical principles. Both of these features provide significant added value to the final solution.

The Collaborative Risk Assessment component is responsible to guide the security analyst in order to perform the appropriate steps that are required for the conduction of a risk assessment for a specific supply chain service. More specifically, MITIGATE has introduced a detailed multi-step processes in order to calculate SCS risks. These steps have to be executed in a guided way in order to stay in-line with the defined methodology. This component offers all the supportive features that are required for an error-free execution of the methodology.

The Open Intelligence and Big-Data Analytics component is responsible to provide near real-time notifications regarding potential vulnerabilities that are related to the assets that exist in the asset cartography of one organization. These notifications will be generated based on the text-processing of open sources.

The Notification and Reporting component is responsible to provide push notifications to the security analyst regarding any type of messages that are published in the pub/sub queue. Since MITIGATE involves many time-consuming operations (e.g. the conduction of a vulnerability assessment, the calculation of risks, the processing of open information sources) every time that such an operation is completed a specific message is placed in a predefined topic of the pub/sub queue.

The Administration component is responsible for the management and the consistency of the various 'enumerations' that are required by all the other components. Such enumerations include mainly vulnerabilities, attack-types and business partners. This component also implements the semi-automated update of these enumerations from open sources.

The Access Control and Privacy component provides security guarantees in a horizontal manner to all the other components. More specifically, since the information that is provided and processed (e,g, asset cartography, attack paths, risk calculations etc) is extremely sensitive, the specific component undertakes the responsibility of implementing the appropriate authentication, authorization and encryption schemes that are required in order to protect MITIGATE services and data end-to-end.

Finally, it should be noted that the architecture is complemented by a persistency layer, which consists of two types of databases; one relational and one NoSQL and a pub/sub system.

Acknowledgements

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653212, project MITIGATE. This presentation

is a collective work of the participants of the project who are hereby thanked for their contributions to the MITIGATE deliverables.

References

[1] G. Giannopoulos, R. Filippini, M. Schimmer, «Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art», Joint Research Center Publication, JRC 70046, EUR 25286 EN, ISBN 978-92-79-23839-0, ISSN 1831-9424, doi: 10.2788/22260, Luxembourg: Publications Office of the European Union, 2012. International Standardization Organization, *ISO 31000: Risk Management – Principles and Guidelines*. Geneva, Switzerland, 2009.

[2] J. P. G. Sterbenz, D. Hutchison, E. K. Etinkaya, A. Jabbar, J. P. Rohrer, M. Schoeler et al., (2010) Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks, Vol 54, pp. 1245-1265.

[3] I.A. Herrera, R.Woltjer, Comparing a multi linear (STEP) and systemic (FRAM) method for accident analysis, Reliability Engineering and System Safety 95 (2010) 1269-1275. [2] J. P. G. Sterbenz, D. Hutchison, E. K. Etinkaya, A. Jabbar, J. P. Rohrer, M. Schoeler et al., (2010) Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks, Vol 54, pp. 1245-1265.

[4] European Network and Information Security Agency, «Analysis of Cyber Security Aspects in the Maritime Sector», November 2011. [2] J. P. G. Sterbenz, D. Hutchison, E. K. Etinkaya, A. Jabbar, J. P. Rohrer, M. Schoeler et al., (2010) Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks, Vol 54, pp. 1245-1265.

[5] N. Polemi, T. Ntouskas: Open Issues and Proposals in the IT Security Management of Commercial Ports: The S-PORT National Case. SEC 2012: 567-572

[6] T. Ntouskas, N. Polemi: Collaborative Security Management Services for Port Information Systems. DCNET/ICE-B/OPTICS 2012: 305-308

A Hybrid Risk Management Process for Interconnected Infrastructures

Stefan Schauer

Center for Digital Safety & Security
AIT Austrian Institute of Technology GmbH
stefan.schauer@ait.ac.at

Abstract – Critical infrastructures together with their utility networks play a crucial role in the societal and individual day-to-day life. Thus, the estimation of potential threats and security issues as well as a proper assessment of the respective risks is a core duty of utility providers. Despite the fact that utility providers operate several networks (e.g., communication, control and utility networks), most of today's risk management tools only focus on one of these networks. In this article, we will give an overview of a novel risk management process specifically designed for estimating threats and assessing risks in highly interconnected networks. Based on the internationally accepted standard for risk management, ISO 31000, our risk management process integrates various methodologies and tools supporting the different steps of the process from risk identification up to risk treatment. At the heart of this process, a novel game-theoretic framework for risk minimization and risk treatment is applied. This approach is specifically designed to take the information coming from the various tools into account and model the complex interplay between the heterogeneous networks, systems and operators within a utility provider. It operates on qualitative and semi-quantitative information as well as empirical data and uses distribution-valued payoffs to account for the unpredictable effects occurring in this highly uncertain environment.

1. Introduction

Utility networks are critical infrastructures consisting of physical and cyber-based systems. The organizations operating these networks are providing essential services for the society, e.g., the electrical power production and distribution, water and gas supply as well as telecommunication services. A failure within a critical infrastructure might have huge societal impact, as shown for example in [1] [2].

These infrastructures are heavily relying on Information and Communication Technology (ICT) as well as Supervisory Control and Data Acquisition (SCADA) systems for providing

their services. As it has been shown in recent events [3] [4], ICT and SCADA systems are potential targets of cyber-security threats and may have vulnerabilities that attackers could exploit. Therefore, protecting and assuring the availability and security is of the utmost importance for normal societal and business continuity.

In this context, risk management is a core duty in critical infrastructures. Current risk management frameworks [5] [6] [7] [8] are mostly a matter of best practices, often focusing on one specific topic (e.g., the ICT area, SCADA systems or the physical utility layer). In particular, the aforementioned network-centric structure within utility providers builds upon a high integration and a heavy interrelation between the different networks (cf. Figure 1). Hence, an incident within one network might affect not only the network itself but might also have cascading effects on several other networks. Standard risk management frameworks are often not designed to identify and assess these cascading effects, thus leaving them underestimated or even undetected.

2. The HyRiM Project

In the course of the FP7 project HyRiM ("Hybrid Risk Management for Utility Networks") [9], we are focusing on these sensitive interconnection points between the different networks operated by a utility provider. The main goal is to define a novel risk management approach for identifying, assessing and categorizing security risks and their cascading effects in interconnected utility infrastructure networks. In more detail, we are focusing on three major networks operated by utility providers, i.e., (cf. also Figure 1)

- the utility's *physical network infrastructure*, consisting of, e.g., gas pipes, water pipes or power lines
- the utility's *control network* including SCADA systems used to access and maintain specific nodes in the utility network
- the *ICT network*, collecting data from the SCADA network and containing the organization's business logic

Additionally, we are also including the human factor and the social interrelations (i.e., the *social network*) between employees, wherever possible. In other words, we are choosing a holistic or "hybrid" view on these networks, laying a strong emphasis on the interrelations between them. Hence, we refer to our approach as "*Hybrid Risk Management*" and to the respective risk measures as "*Hybrid Risk Metrics*".

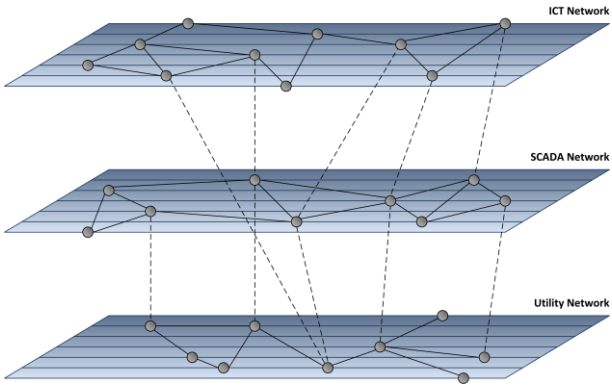

Figure 1: Interconnected networks operated by a utility provider.

When looking at the risk measures we develop in HyRiM, we are focusing on a qualitative approach to avoid the illusion of "hard facts" based on subjective numerical risk estimates provided by humans. Nevertheless, simulation tools based on well-defined mathematical frameworks like percolation and co-simulation are provided, which support the qualitative analysis with quantitative results.

Hence, our risk management process unifies the advantages of quantitative assessment with the ease and efficiency of a qualitative analysis and supports a qualitative assessment with a sound quantitative mathematical underpinning. The aim is to provide utility network operators with a risk management framework supporting qualitative risk assessment based on numerical (quantitative) techniques. In this way, the HyRiM project takes an explicit step towards considering security in the given context of utility networks based on a sound and well-understood mathematical foundation, ultimately supporting utility network operators with a specially tailored solution for the application at hand.

3. The HyRiM Process

The Hybrid Risk Management (HyRiM) Process we are presenting here is suited for organizations operating highly interconnected networks at different levels, such as utility providers or critical infrastructure operators. Therefore, the HyRiM process is compliant with the general ISO 31000 process for risk management [5] and thus can also be integrated into existing risk management processes already running in the aforementioned organizations.

In detail, the generic risk management process of the ISO 31000 framework is adopted and each step of the process is supported with the tools developed in the HyRiM project. These

tools cover different analysis techniques and simulation methodologies that facilitate the risk process. The relevant HyRiM tools have been identified and mapped onto the risk management process as shown in Figure 2. Since the ISO 31000 is a generic process and is often used as a template in other ISO standards itself (like in the ISO 27005 [6], the ISO 28001 [10] or others), the HyRiM process described here can also be integrated into these standards. This makes it possible to apply the HyRiM process to multiple fields of application.

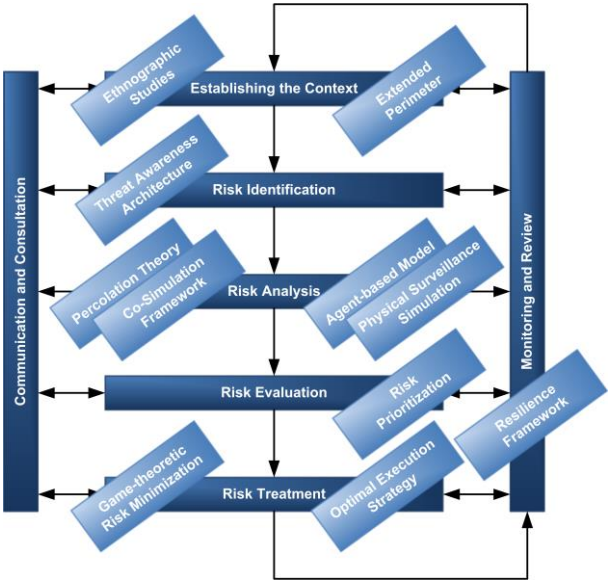

Figure 2: The HyRiM Risk Management Process

The general framework applied in HyRiM to model the interplay between different networks is game theory. Game theory not only provides a well-sound mathematical foundation but can also be applied without a precise model of the adversary's intentions and goals. Therefore, a zerosum game and a minimax approach [11] can be used, where the gain of one player is balanced with the loss of the other. This can be used to obtain a worst-case risk estimation.

As already pointed out above, a central part of the risk management framework is the identification and estimation of cascading effects due to the interrelations between the different networks. To achieve that, we apply percolation theory [12] [13] and co-simulation [14]. Both approaches use the given network infrastructure and the communication between the various systems to model how failures (e.g., malicious messages) propagate through the network. As a result, they provide the number of affected nodes and the potential damage over all different networks.

The game-theoretic framework we developed in HyRiM also allows modeling the intrinsic randomness and uncertainty encountered in real-life scenarios. This is realized using distribution-valued payoffs for the game [15]. These payoffs are coming from both the percolation and the co-simulation, since those are stochastic processes and the results are described as distributions.

The output of the game-theoretic framework is threefold and includes the maximum damage that can be caused by an adversary, an optimal attack strategy resulting in that damage and an optimal security strategy for the defender. The optimal defense strategy is, in general, a mixture of several defensive (i.e., mitigation) activities. These activities, if implemented correctly, provide a provable optimal defense against the adversary's worst case attack strategy. The implementation can be simplified and guaranteed, for example, by the use of a job scheduling tool.

Acknowledgements

This work was supported by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1).

References

[1] S. Fletcher, "Electric power interruptions curtail California oil and gas production," Oil Gas J., 2001.

[2] M. Schmidthaler and J. Reichl, "Economic Valuation of Electricity Supply Security: Ad-hoc Cost Assessment Tool for Power Outages," ELECTRA, no. 276, pp. 10–15.

[3] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Washington, USA, 2016.

[4] J. Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," 22-Dec-2016. [Online]. Available: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/. [Accessed: 03-Feb-2017].

[5] International Standardization Organization, ISO 31000: Risk Management – Principles and Guidelines. Geneva, Switzerland, 2009.

[6] International Standardization Organization, ISO/IEC 27005: Information technology - Security techniques - Information security risk management. Geneva, Switzerland, 2011.

[7] G. Stoneburner, A. Goguen, and A. Feringa, NIST SP800-30 Risk Management Guide for Information Technology Systems. Gaithersburg, USA, 2002.

[8] ISACA, COBIT 5 for Risk. Rolling Meadows, USA, 2013.

[9] "HyRiM | Hybrid Risk Management for Utility Providers." [Online]. Available: https://www.hyrim.net//. [Accessed: 28-Feb-2017].

[10] International Standardization Organization, ISO 28001: Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance. Geneva, Switzerland, 2007.

[11] M. Maschler, E. Solan, and S. Zamir, Game Theory. Cambridge University Press, 2013.

[12] G. R. Grimmett, Percolation Theory. Heidelberg, Germany: Springer, 1989.

[13] S. König, S. Rass, S. Schauer, and A. Beck, "Risk Propagation Analysis and Visualization using Percolation Theory," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 694–701, 2016.

[14] M. Faschang, F. Kupzog, R. Mosshammer, and A. Einfalt, "Rapid control prototyping platform for networked smart grid systems," in Proceedings IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society, Vienna, Austria, 2013, pp. 8172–8176.

[15] S. Rass, S. König, and S. Schauer, "Uncertainty in Games: Using Probability-Distributions as Payoffs," in Decision and Game Theory for Security, London, UK: Springer, 2015, pp. 346–357.

Big Data Analytics and Threat Prediction

Towards Protecting Maritime Supply Chain IT Infrastructures

Armend Duzha

Maggioli SPA
armend.duzha@maggioli.it

Abstract – Among the core innovation of the MITIGATE risk management system is its ability to deal with the identification, assessment and analysis of cyber-related threats in the scope of complex maritime supply chain environments, which are typically complex and comprise a variety of ICT elements, including several specialized systems and devices. Hazard and risk assessment in such environments needs to deal with large amounts of heterogeneous data of varying velocities, thereby giving rise to Big Data Analytics. As part of the MITIGATE framework, we apply Big Data Analytics techniques in hazard analysis for port's critical informative infrastructure (CII). To this end, we leverage datasets from all the participating ports (e.g., through their legacy security and incident management systems). MITIGATE incorporates also crowd-sourcing capabilities, through using diverse data sources (including data from social networks and RSS Feeds) towards enhancing its threat assessment and prediction functionalities.

1. Big Data Analytics in MITIGATE System

Within the context of the MITIGATE system, Big Data Analytics techniques are used to discover cyber-related threats in the normal operation of ports and other maritime supply chain participants' IT infrastructure. Threat detection will be mostly based on real-time information acquired from various heterogenous (trusted and untrusted) sources, including social networks and crowd-sourcing. Moreover, the correlations between specific parameters collected from the users and previous periods of attacks can be computed and used to train more customized risk detection algorithms, e.g. for specific types of attacks.

The high-level architecture is depicted in Figure 1.

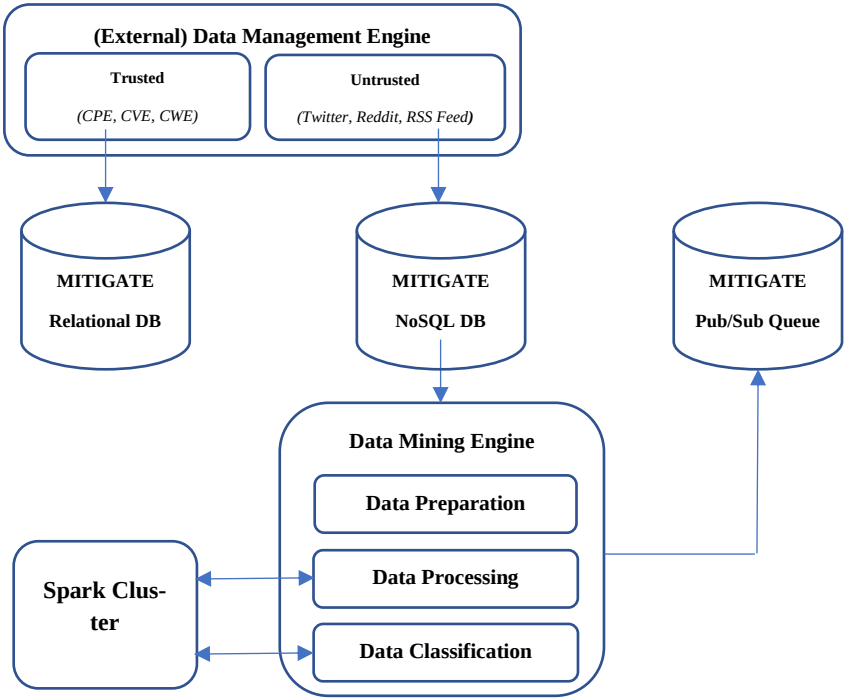

Figure 1: The Mitigate high-level architecture

(External) Data Management Engine: is responsible for storing the static and the real-time dynamic information acquired from various heterogeneous sources (trusted and untrusted).

Advanced Data Mining Engine: provides the business logic for the Big Data Analytics. Furthermore, this component is described by individual modules as well.

- ***Preparation:***

The pre-processing of data can be required due to the various structure of data. Therefor the Data Mining component has to offer a number of different possibilities to deal with the data. One possible pre-processing is described as follows:

The pre-processing of data can be performed through three steps. At the beginning a syntax analysis (parsing) is required. In this unstructured data are converted to a structured data. In step 2, the method for search and retrieval is defined. In this context, the data is subtracted

into key elements (i.e., keywords). These key elements can be described as words, phrases or objects. It is similar to the approaches of libraries or search engines. In step 3, the key items may be applied to the text.

- ***Processing***

In general, data analysis is performed by using techniques based on Natural Language Processing (NPL). For example, a record with the same contents vary only in the structure and therefrom have a different meaning for the interpretation by the receiver. Here, NPL tries to set and carry out on the basis of the recognition of statements. Based on content and mood, as well as a classification on this statement, an additional meaning can be extracted. On the basis of NPL some techniques have been developed for data analysis over time.

An example for text processing in MITIGATE could be to determine if a content contains zero-day vulnerability based on defined parameters. This module will interact with the Spark Cluster to perform the data processing.

- ***Classification***

The final component of the data mining component describes the classification of data depending on different parameters. The module classification summarizes data automated in categories. This data is then analysed step-by-step and categorized based on keywords and parameters attached to the analytics. Often more than one category or sub-categories are assigned to a document or text. A model for realizing the Text Classification is called the Latent Dirichlet Allocation (LDA). In this model, in contrast to more complex models, a predefined vocabulary is used. This module will interact with the Spark Cluster to perform the text classification.

2. Prediction and Forecasting Functionalities

The prediction and forecasting functionalities of MITIGATE system are tightly related to the Open Intelligence & Big Data Analytics component. The connection point is the automated usage of the indexed dataset in order to provide tailored information that can be interpreted to Zero-Day vulnerabilities.

Initially, the risk assessor has provided a valid asset mapping which consists of multiple assets along with their description and connectivity parameters. Next, the data reduction process is performed by the key extraction module in order to retrieve the meaningful keywords that will be used for analysis. This module relies on Natural Language Processing (NLP) algorithms and selects heuristically a basic set of keywords that are relevant with the overall infrastructural topology. These keywords may refer to brand names (e.g., Dell), protocol suites (e.g., SSL) or other things.

Taking under consideration the extracted keywords, MITIGATE auto-configures a scheduler which will identify cyber-related news relying on the indexed dataset. In order to make the searching as synchronous as possible, each scheduler is subscribed on a pub/sub queue in a topic related to data publication. In case of the data-aggregation of new elements from the external sources, a message is provided to the pub/sub which notifies all schedulers.

In this way, the risk officer will be able to consume all information relevant to his/her IT infrastructure as fast as possible. Beyond that, he will be able to estimate if s/he has to introduce a new vulnerability in the system which is not even reported in a vulnerability database. The risk officer will be in the position to re-evaluate the corporate defensive strategy based on risk calculations that will be performed on hypothetical yet meaningful attacks.

Acknowledgements

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653212, project MITIGATE. In addition, the author would like to thank all partners in this project for their contributions and efforts.

Automated Attack Paths Discovery

Michalis Pavlidis, Nikolaos Polatidis and Haralambos Mouratidis

University of Brighton
{m.pavlidis, n.polatidis, h.mouratidis}@brighton.ac.uk

Abstract – Critical Infrastructures rely on the use of information systems for collaboration, while a vital part of collaborating is to provide protection to these systems. Attack graph analysis and risk assessment provide information that can be used to protect the assets of a network from cyber-attacks. Furthermore, attack graphs provide functionality that can be used to identify vulnerabilities in a network and how these can be exploited by potential attackers. In this paper, we present a cyber-attack path discovery method that is used as a component of a maritime supply chain risk management system.

1. Introduction

The European Union Council defines Critical Infrastructure (CI) as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" [1]. It concerns sectors such as the communications, energy, healthcare, transportation, and financial services to name a few, which rely heavily on IT systems with a large number of software and hardware assets. Such systems are today severely exposed to cyber-attacks and their protection has become of utmost importance. Moreover, these systems are not isolated any more but highly interconnected and mutually interdependent [2], [3]. Although interdependency can improve their efficiency, it can also have negative effects. A security breach in one asset of an infrastructure can have cascading effects in other infrastructures. Cyber security of CIs therefore, encompasses the establishment of cyber situational awareness, which in turn contains the discovery of all attack paths which are the possible paths that an attacker can follow in order to compromise a specific asset of an infrastructure.

Attack graphs are one common way to display attack paths. They are a useful tool for analysing system vulnerabilities and enable security officers to assimilate all the required infor-

mation relatively easy and receive support in the decision-making process in terms of identifying appropriate security measures. Attack graphs also enable security offices to proceed to a more informed estimation of the impact of an attack and its likelihood and also to answer what-if questions by choosing among different network configurations and security controls.

Significant challenges for the generation of attack paths include scalability, as attack graphs grow in size when the network grows in size with a lot of hosts or the number of vulnerabilities of the assets grows. Another challenge also is the input data that the generation algorithm needs, which has to be complete and accurate and in the expected format.

The MITIGATE project is a European funded Innovation Action that aims to develop a risk management methodology for maritime supply chain services. Essential element of risk management, and of the MITIGATE methodology, is the mitigation of risks through the identification of attack paths and appropriate security controls [4], [5]. To this end, an attack paths discovery algorithm was developed as part of the project. In the next section the attack paths discovery algorithm is presented, while in section 2 we provide initial experimental results along with future work.

2. Attack Paths Discovery within MITIGATE System

The MITIGATE attack paths discovery algorithm examines how an attacker can exploit identified cyber asset vulnerabilities in order to perform undesired actions. The discovery algorithm is shown in Figure 1. For every attack, a set of related weaknesses (CWE) and vulnerability types are defined. Is it assumed that to perform this kind of attack the attacker must have access to an asset that has one or more vulnerabilities that are compatible with either the weaknesses or the type defined. Attack paths are then modelled by employing attack graphs. Each node in the graph represents a combination of asset and vulnerabilities that an attacker can exploit. Each edge represents the transition of an attacker from one asset to another.

The algorithm requires as input a physical network topology, an asset configuration, a set of entry points and target points, and an attacker's profile. In particular, the network topology includes a list of cyber assets and their relationships. For example, an asset may be installed on another asset or it just communicates with another asset. The asset configuration includes information about a particular asset. For example, the name of the asset, an id, the business partner to which this asset belongs, its vulnerabilities, and attributes from the CVE repository, such as access complexity and access vector. The entry point and the target points are specific cyber assets on which a business partner wants to focus on. The attacker's profile includes information about the assumed attacker, such as the attacker capability, which is the counterpart to a vulnerability's access complexity and the attacker location, which is the counterpart

to a vulnerability's access location. The attackers profile is used to induce whether a particular attack can exploit an asset vulnerability.

The output of the algorithm is a list of attacks paths. Each attack path contains an ordered list of cyber assets that an attacker with a particular attacker's profile can successfully compromise by exploiting their vulnerabilities. Each cyber asset in the attack path can be used as a stepping stone to an attack to the next cyber asset. A business partner must be able to locate all potential attack paths into the network and prevent attackers from using it. Business partners can hypothesize new 'zero-day" vulnerabilities of cyber assets, evaluate the impact of changing configuration settings, and determining the security effectiveness of adding new security controls.

Algorithm 1: Attack path discovery

Input: Asset graph (G), attacker location, attacker capability
Output: Graph, affected assets, attack paths

```
#We create two empty lists to hold attack paths and assets
   attackpaths = [] affectedassets = []
#We return all paths from source to target
   for e in parameters entry points
      If attacker location < required level of attacker location OR
      attacker capability < required attacker capability
      return empty graph
         else
         get single source shortest path length
         set propagation length for entry point e
                                        for target point t
#Create a list with all non-circular paths from entry e to target t
   get all paths in the graph G from entry e to target t that are up to
   the pre-specified path length
         for the size of paths found
                  add paths to attackpaths [] list, add affected
assets to affected assets [] list
#Return the graph, the affected assets and the attack paths found as
a direct input to #the attack visualization algorithm
return Graph, affected assets, attack paths
```

Figure 1: Discovery algorithm

3. Tool Illustration

We have implemented a prototype in Python that is capable of automatically computing the attack paths. To illustrate our approach, we employ the simple network depicted in Figure 2 which consists of four hosts. The network topology is modelled in a Neo4j graph database which is read by the tool.

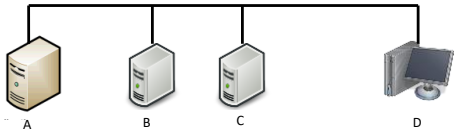

Figure 2: Example network

In each host, various software assets are installed. Information about the hosts, including their software assets and few of their respective vulnerabilities, is shown in *Table 1*. The attacker begins from host D, which is the entry point, and her goal is to reach and compromise the MS SQL Server that is installed in host A, which is the target asset. Moreover, we consider the attacker to be highly skilled.

Table 1 Information about hosts and vulnerabilities

Host	Software Assets	Vulnerabilities
A	MS Windows Server 2000	CVE-2016-0020
		CVE-2016-0016
		CVE-2016-0008
	MS SQL Server 2005	CVE-2008-5416
B	MS Windows XP	CVE-2007-2736
		CVE-2011-0026
C	MS Windows 7	CVE-2013-0074
		CVE-2010-3962
D	Linux Ubuntu 6.0	CVE-2008-4306

The resulted attack graph that depicts the possible attack paths that the attacker can follow is shown in Figure 3.

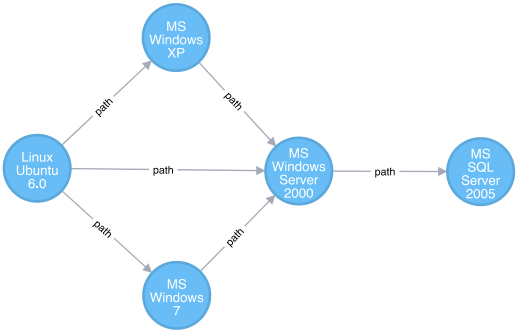

Figure 3: Discovered attack paths

As future work, we plan to compare our approach with other approaches available in the literature and also perform an evaluation of the scalability of the approach when there is a large number of assets, for example more than 50,000 assets.

Acknowledgements

This work has received funding from The European Union's Horizon 2020 research and innovation program under grant agreement No 653212.

References

[1] European Council, COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008.

[2] Rigole, T., et al. Agents controlling the electric power infrastructure. *International Journal of Critical Infrastructures 4.1-2*, 2008.

[3] Ouyang, M., Review on modelling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety*, 2013.

[4] J.L.J. Lee, H.L.H. Lee, H.P. In, Scalable attack graph for risk assessment, 2009 Int. Conf. Inf. Netw. 2009.

[5] N. Poolsappasit, R. Dewri, I. Ray, Dynamic Security Risk Management Using Bayesian Attack Graphs, IEEE Trans. Dependable Secur. Comput. 2012.

Detection of Cyber-Attacks Against SCADA

An evaluation of anomaly detection techniques

Antonios Gouglidis

Lancaster University
a.gouglidis@lancaster.ac.uk

Abstract – Attacks on critical infrastructures are on the rise and usually initiated by highly skilled attackers, who are capable of deploying advanced attacks to exfiltrate data or even to cause physical damage. In this presentation, we rehearse the rationale for protecting against cyber-attacks and evaluate a set of anomaly detection techniques in detecting attacks by analysing traffic captured in a SCADA network. For this purpose, we have implemented a tool chain with a reference implementation of various state-of-the-art anomaly detection techniques to detect attacks, which manifest themselves as anomalies. Specifically, in order to evaluate the anomaly detection techniques, we apply our tool chain on a dataset created from a gas pipeline SCADA system in Mississippi State University's lab, which include artefacts of both normal operations and cyber-attack scenarios.

1. Introduction

For characterising and identifying challenges, anomaly detection (AD) techniques have exhibited sufficient detection and accuracy. This is due to the fact that the statistical models embodied in these techniques allow the robust characterisation of normal behaviour taking into account various features (operational and network) to detect known and unknown patterns. However, these techniques are employed independently on certain parts of infrastructures and do not usually provide a holistic view of a system. Motivated by the importance of protecting modern and future critical infrastructures, in this presentation we outline our resilience reference framework, which aims towards the protection of utility networks, and elaborate on the performance analysis of various detection techniques that may provide protection against sophisticated attacks that manifest themselves in various anomalies.

2. Resilience Framework

The term *resilience* has been used in the past several decades in different ways to describe the ability of materials, engineered artefacts, ecosystems, communities, etc., to adapt to changes, and is also adopted by sciences (e.g., psychology) and organisations (e.g., business continuity life cycles). The resilience strategy that we use here, entitled D^2R^2+DR (Defend, Detect, Remediate, Recover, and Diagnose and Refine) defines resilience as '*the ability of a network or system to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation*' [1].

Our overall framework is depicted in Figure 1 [2], which consists of four functional planes implemented as software components. These include the *Monitoring*, *Detection*, *Analysis* and *Management* planes. These planes work in collaboration to provide overall resilience of infrastructures against challenges that manifest themselves in the guise of various anomalies (e.g., social engineering attacks, operator misconfigurations, unanticipated problems arising from organisational policies, etc.). Each plane has multiple sub-components to perform local tasks (e.g., pre-processing, internal storage, etc.) and provides input to a subsequent plane.

With reference to the D^2R^2+DR strategy, our resilience framework satisfies the role of the inner loop elements by realising them as software components, which when operated together form the basis of our framework. These components are capable of reconfiguring devices in response to challenges using suitable policies. Reconfiguration is not required to be applied on the same components in which the anomaly was detected. A policy engine is responsible for mapping detection events to reconfigurations. We further elaborate on the former two planes, which are related mostly with the detection of anomalous behaviours is critical infrastructures and can host software components that implement anomaly detection techniques.

The *Monitoring* plane is concerned with working on the resilience metrics that are reported to it by a set of collector agents. This involves pre-processing, feature extraction and selection, dimensionality reduction and transformation of metrics into feature vectors for subsequent AD instances, which are running in the *Detection* plane. The *Monitoring* plane acts as a controller for multiple instances of collector agents running on various points on the network. The classification of instances in various viewpoints helps to invoke most relevant and effective techniques for each viewpoint. This is due to the fact that different types of pre-processing techniques may be required for different types of metrics being collected for each viewpoint.

The *Detection* plane can be considered as a core component that performs detection of anomalies based on features gathered by the collector agents and processed by *Monitoring* instances. This component is designed to offer flexibility so that different types of AD techniques can be invoked at the same time. This is of special interest, since some techniques provide better detection capabilities compared to others and, consequently, have an impact on the overall

resilience of an infrastructure. Currently, our toolchain provides reference implementations for detectors based on K-means, PCA, GMM, Naïve Bayesian and a data-density technique. The main sub-task of this plane is to define statistical models to express normality. With better knowledge of the data, one can choose the appropriate detection techniques. For example, for small data metrics (i.e. data small enough for human comprehension), these can be analysed and labelled by experts. Such metrics might fall under the organisation or individual viewpoint, e.g. the monitoring of active remote connections to the internal network as part of an organisation's policy. In such a case, the application of a supervised technique might be considered more appropriate than an unsupervised technique. Conversely, it is difficult and time-consuming to label large data sets coming from the technology viewpoint.

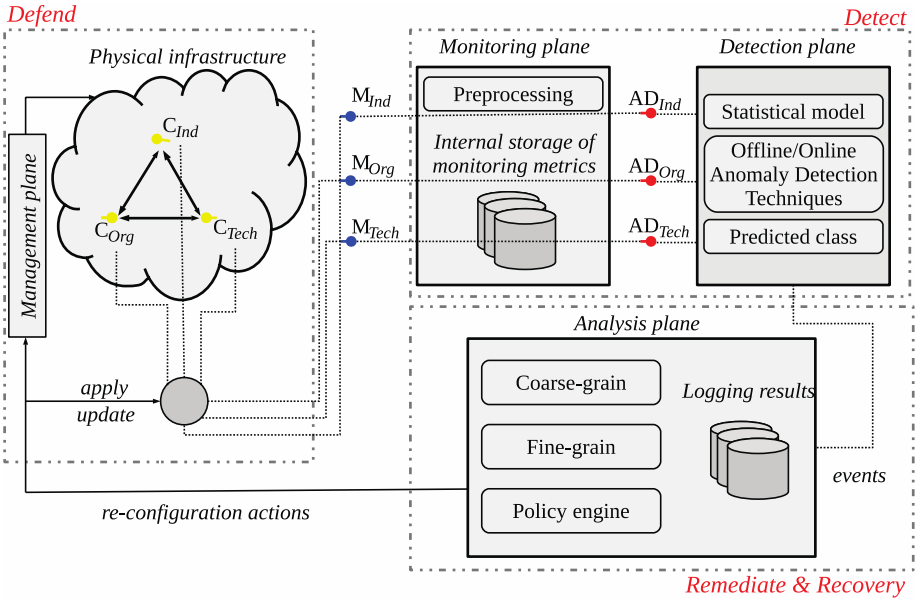

Figure 1: An overview of the resilience framework.

3. Evaluation of AD techniques

The evaluation of our resilience framework indicates that anomaly detection techniques perform differently depending on both the characteristics of the data during normal operation as well as the nature of the attack. Choosing an appropriate AD technique for use with SCADA systems requires an examination of their effectiveness in detecting anomalous SCADA opera-

tions, e.g. traffic between RTU and MTU. From an operational perspective, supervised techniques require training data to build the model and evaluate the fitness of the new test data with respect to this model. On the other hand, unsupervised techniques try to partition the feature spaces into normal and anomalous regions without training data, and AD techniques in this mode are much more flexible and easy to use since they do not require upfront human intervention and training [3].

In the following, we provide an evaluation, in the SCADA context, of state-of-the-art anomaly detection techniques as well as a data-density (DD) based memory-less AD method we developed for use with our resilience framework. Specifically, we present information about the dataset used for the evaluation, and the results of a detailed performance evaluation of supervised (K-Means, Naïve Bayesian) and unsupervised (PCA, GMM and Data-Density (DD)) anomaly detection techniques. The selection of this subset of state-of-the-art techniques is based on prior experience from SECCRIT's deliverable 4.1[1]

3.1 Dataset

The dataset we used was collected using a simulation of real anomalies and normal activity on a gas pipeline. Specifically, it constitutes Modbus traffic[2] stemming from a serial line and including '*read*' and '*write*' commands for a PLC. It contains three categorical features including payload information, network information and ground truth. The payload information indicates the gas pipeline's state, settings and parameters. The network information provides pattern of communications and ground truth details, i.e. if the transaction is normal or anomalous. In total 274627 instances and twenty raw features are provided. We refer the reader to [4, 5] for a detailed description of the individual features, dataset and test bed architecture that was used to capture the data.

3.2 Description of Anomalies

In total, the dataset contains seven different types of anomalies that are divided into four main categories. These anomalies include '*response injection*', '*reconnaissance*', '*denial-of-service*', and '*command injection*'. The response injection is further divided into naïve malicious response injection (NMRI) and complex malicious response injection (CMRI). The former leverages the ability to inject response packets in the network, but lacks information about the process being monitored. The latter on the other hand is more sophisticated and attempts to mask the real state of the physical process being controlled. Similarly, the com-

[1] https://www.seccrit.eu/upload/D4-1-Anomaly-Detection-Techniques-for-Cloud.pdf

[2] http://www.modbus.org/

mand injection is further divided into malicious state command injection (MSCI), malicious parameter command injection (MPCI) and malicious function code command injection (MFCI). MSCI changes the state of the process control system to drive the system from safe state to critical state by malicious command. MPCI changes PLC set points and MFCI injects command which misuse protocol network parameter. DoS attack targets communication link. Each sample is labelled with its ground truth from (0-7) where 0 represents normal class and 1-7 is for each class of anomalies.

3.3 Performance of AD Techniques

One of the main issues with the raw dataset was that it contained missing values, and thus, required from us to perform a set of pre-processing tasks in order to make the dataset suitable for use in our AD implementations. Otherwise, the results of the analysis would not be indicative of the actual performance of the examined AD techniques. Specifically, we pre-process the raw dataset by applying Z-score and principal component analysis techniques such that it remains representative of the original data, particularly in scope of the attack scenarios, while being better suited to use with AD techniques. Henceforth, we call this new derived feature-set as combined dataset since it contains artefacts of the normal data and all seven types of anomalies. Subsequently, we used the combined dataset as an input to our AD implementations. However, some of the operations regarding AD techniques required an excessive amount of time and memory to complete due to the size of the combined dataset (275,000 rows), e.g. normalisation of data. Therefore, in order to overcome the time and memory constraints, we shuffled the data in the combined dataset and selected a subset of it (30%) to perform the training of supervised AD techniques.

Table 1 depicts the results of the binary classification for the combined dataset. Basically, in this approach all anomalous classes are combined into a single anomaly class to be discriminated from the normal communications. Both the precision and accuracy results indicate that the supervised techniques (KM and NB) perform better in classifying anomalies when compared with state-of-the-art unsupervised techniques (PCA-SVD and GMM). However, we see that our Data Density based anomaly detection method out performs other unsupervised techniques. Specifically, the PCA-SVD becomes less accurate in detecting anomalies since it manages to accomplish only ~17% of accuracy. On the contrary, the DD technique shows both a high precision and accuracy level, i.e. ~95% and ~72%, respectively. In fact, DD has better precision of all the methods, and overall performs at par with the supervised techniques.

In order to further investigate the performance of the AD techniques in identifying the individual attacks, we created a separate set of a datasets. Each dataset included normal data and data from one of the anomalies. Each dataset is then used as an input to the detector. All datasets were run with the selected four AD techniques.

The output metrics for the DD method indicated, in general, that DD performs at par with supervised techniques. However, there is an outlier in the experimental results: DD performs poorly for the naïve malicious response injection (NMRI) anomaly. After removing the outlier, however, the average accuracy for DD is 0.6231. An examination of the output metrics for DD may explain the reason for the outlier. DD, being an unsupervised method, performs badly when the anomalous data packets are not so different from normal traffic on the network. Specifically, the NMRI anomaly injects only response packets in the network but lacks information about the process being monitored. Thus, it is a less potent attack. Conversely, for a more potent attack such as complex malicious response injection (CMRI), where the attack attempts to mask the real state of the physical process being controlled, and so the anomalous data packets are more different from normal traffic, the performance of DD improves dramatically. This is also the case for other un-supervised techniques as well. An examination of the precision and recall results reveals the exact anomaly types that are being classified incorrectly. The precision rate for denial-of-service, reconnaissance, MFCI and MSCI is over 80%, but that of NMRI and CMRI, is below the acceptable level. Furthermore, some attack types such as MFCI are detected with low recall rate and high precision. Also recall values appear to be lower in MPCI and MSCI attacks.

Table 1- Comparison of anomaly detection techniques (combined dataset)

Method	ADT	Recall	Precision	Accuracy	F-Score	G-Mean
Supervised	K-Means	0.5728	0.8319	0.5680	0.6751	0.6874
	NB	0.7692	0.8195	0.9036	0.8595	0.8605
Unsupervised	PCA-SVD	0.2796	0.6472	0.1714	0.2710	0.3331
	GMM	0.4416	0.7309	0.4516	0.5583	0.5745
	DD	0.7327	0.9508	0.7257	0.8231	0.8307

4. Conclusion

The performance of various AD techniques applied to SCADA communication is evaluated in terms of their ability to identify various attacks. We have analysed the communication between an RTU and MTU in a gas pipeline system. The data in our evaluation were developed by the Mississippi State University, and include artefacts of benign RTU transactions and various attack transactions generated specifically for conducting research in the area of critical infrastructures protection. We have analysed the performance of five AD techniques in correctly identifying anomalies using a set of statistical features. Results from our experiments

indicate that detection rate differs with respect to the type of the anomaly and the running mode of the applied AD technique. Specifically, AD techniques that run in supervised mode appeared to perform better. However, a dataset to train a technique is not always possible to have. Therefore, we argue that there is a need for using robust unsupervised techniques (e.g. data-density) in combination with supervised one to achieve better detection accuracy and increase our awareness. Last but not least, configuration modes, normalization techniques, etc. are yet more variables to consider when it comes to applying them operationally.

Acknowledgements

This research work has been conducted by Antonios Gouglidis (Lancaster University), Noor Shirazi (Lancaster University), Kanza Noor Syeda (Lancaster University), Steven Simpson (Lancaster University), Andreas Mauthe (Lancaster University), Paul Smith (AIT), Ioannis Stephanakis (OTE) and David Hutchison (Lancaster University). The research leading to these results has received funding from the European Union Seventh Framework Programme under grant agreement no. 608090, Project HyRiM (Hybrid Risk Management for Utility Networks).

References

[1] Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 54(8), 1245-1265.

[2] Shirazi, S. N., Gouglidis, A., Syeda, K. N., Simpson, S., Mauthe, A., Stephanakis, I. M., & Hutchison, D. (2016, August). Evaluation of Anomaly Detection techniques for SCADA communication resilience. In Resilience Week (RWS), 2016 (pp. 140-145). IEEE.

[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.

[4] Morris, T., & Gao, W. (2014, March). Industrial control system traffic data sets for intrusion detection research. In International Conference on Critical Infrastructure Protection (pp. 65-78). Springer, Berlin, Heidelberg.

[5] Morris, T. H., Thornton, Z., & Turnipseed, I. (2015). Industrial control system simulation and data logging for intrusion detection system research. 2015-05-15).

SAURON: From Physical to Hybrid Situational Awareness

Manuel Esteve and Israel Pérez

Universidad Politécnica de Valencia, Spain
{mesteve; ispello0}@upv.es

1. Introduction

Nowadays coordinated and increasingly complex terrorist attacks are shocking the world due to the progressive reliance of the industrial sector and many CI, in particular. EU ports on ICT systems, the impact of a coordinated physical attack, a deliberate disruption of critical automation (cyber) systems or even a combined scenario including both kind of attacks, could have disastrous consequences for the European Member States' regions and social wellbeing in general.

Taking into account this fact and this real threat on EU ports as one of the main CI in Europe, the SAURON project proposes an holistic situation awareness concept as an integrated, scalable and yet installation-specific solution for protecting EU ports and its surroundings (cf. Figure 1).

This solution combines the more advanced physical SA features with the newest techniques in prevention, detection and mitigation of cyber-threats, including the understanding of synthetic cyber space through the use of new visualization techniques (immersive interfaces, cyber 3D models and so on). In addition, a Hybrid Situation Awareness (HSA) application capable of determining the potential consequences of any threat will show the potential cascading effect of a detected threat in the two different domains (physical and cyber).

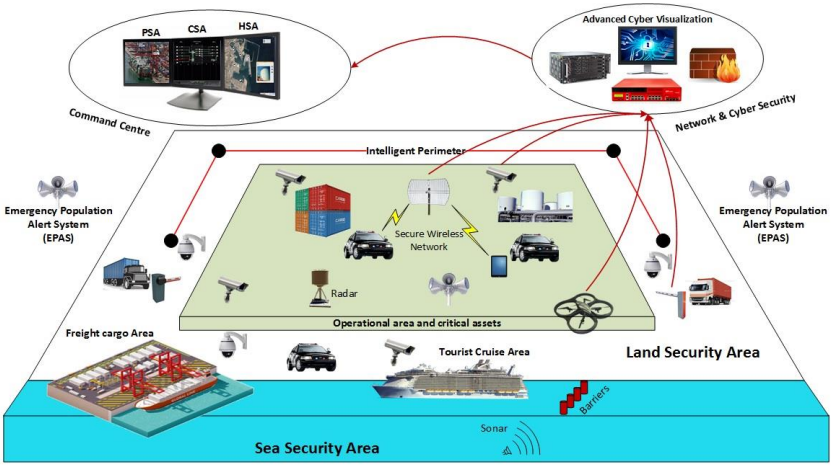

Figure 1: SAURON Concept

From the point of view of situational awareness, SAURON platform will provide three advanced features:

- **CSA:** An advanced and scalable cyber SA (CSA) framework capable of preventing and detecting threats and in case of a declared attack, capable of mitigating the effects of the infection/intrusion. This CSA system will include new visualization paradigms for the cyber space.
- **PSA:** A complete physical SA (PSA) system which includes novel features such as; dynamic location of resources and assets, location, management and monitoring of sensors, including cameras mounted on drones (under the conditions of and in compliance with all pertinent legal requirements at national and European level), security perimeter control, robust and secure tactical communication network and so on.
- **HSA:** A Hybrid SA (HSA) application receiving both physical and cyber alarms on potential threats from the real world and the cyber space respectively. The HSA application will show the potential consequences/effects of these threats in the other planes including cascading effects.

2. Physical Situational awareness application

PSA application proposed by SAURON can be adapted to different types of ports in order to cover their detected vulnerabilities and risks as well as effectively protect their main critical areas. This PSA will be based on the civil version of the Spanish Army Friendly Force Track-

ing (FFT) system developed by UPVLC and deployed in Afghanistan, Lebanon and Mali. This system is a complete SA solution capable of integrating a wide range of sensors and offering advanced SA and Command and Control (C2) capabilities. These capabilities will allow the PSA to be used for preventing and detecting any kind of physical threat and manage the resources in field for responding and mitigating any declared threat. Information on the current situation status will be transferred to the rescue/security teams that could intervene in the mitigation activities for their own protection.

The PSA high-level design schema is shown in Figure 2. Therein, the main blocks composing the PSA are depicted. These blocks will be described in the following paragraphs.

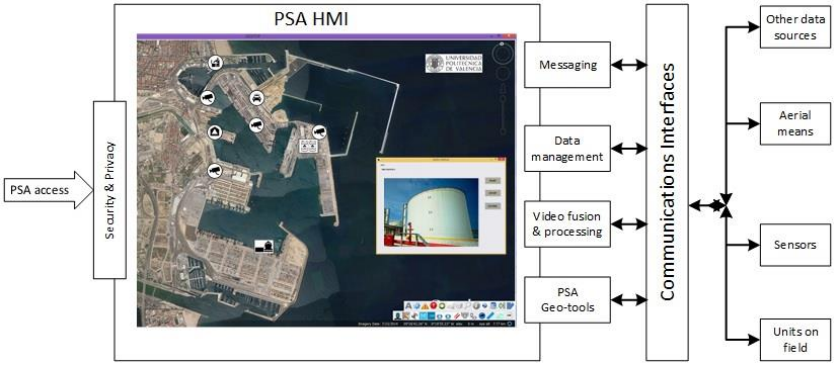

Figure 2: PSA Architecture

The PSA Human Machine Interface (HMI) presents different kind of information from different sources in real time in order to provide complete SA to the managers in charge of preventing, detecting and facing a declared threat. In addition, strict security and privacy policies will be taken into account in order to be consistent with the EU directives and the individual countries' legislations on these topics.

The information represented in the PSA HMI is as follows:

Geolocation of sensors, security units deployed in the theatre of operations and possible physical threats

Making use of advanced GIS and visualization techniques, included immersive virtual reality, will provide to users an adequate situational awareness and situational understanding of physical world.

The PSA includes a set of Geo-tools developed for performing some actions on the maps in an easy and quick manner. These actions would be the following:

- Quick distance measure between two points on the map.
- Dynamic data (units & assets) filtering and visualization
- Terrain 3D view
- Terrain profile between two points on the map.

Messaging

The PSA has a messaging module capable of sending and receiving text messages to/from the units on field. In addition, PSA has a voice over IP (VoIP) module capable of transmitting voice messages to the units.

Data management

Additionally, the PSA has a data management module in order to properly store all data received by the system from external sources or tools. This module also ensures the availability of all information stored in the database in order to be shown to the commanders where necessary.

Video processing and fusion unit

This relies on innovative video analytics suitable for robust person/group tracking and multi camera calibration for mobile (e.g., UAV or body worn) and fixed cameras. All legal requirements regarding data protection and privacy will be taken into consideration with respect to these developments.

The different video streams from the mobile/fixed cameras deployed in the field, will be made available to the PSA operators at the Control Center. In addition, these video flows will be fused and processed.

The video flows will be coming from fixed installations (both in visible light or infrared), or from mobile/worn cameras and UAVs (in visible light). Cross compatibility of the different acquisition devices will be checked. The video management module is compliant with a large number of codecs in order to be able to play video from different models of cameras.

PSA Communications interfaces and interoperability

The PSA is currently fully compliant with the following communication technologies; Internet protocol (Ethernet), WiFi, LTD,,WiMAX, Satellite means Inmarsat, Iridium and Thuraya, Tetra, Tetrapol, 3G and 4G. In addition, PSA application will provide interoperability implementations (e.g. Common Alerting Protocol CAP) for informing the security/rescue teams on the status of the situation before they start their response/mitigations activities once a threat/attack is confirmed.

PSA Security & Privacy

The PSA includes a security access module based on the user profile, which allows access to different system capabilities depending on the user's role in the organization. In addition, security transmission protocols such as HTTPS or Transport Layer Security (TLS) are used for transmitting all data from the PSA.

3. Hybrid Situational Awareness application

The Hybrid SA application goes one step beyond to the integration of the PSA and CSA applications. This innovative solution takes into account the real detected alarms of both applications and identifies and evaluates inter-correlations among different potential threats (cf. Figure 3).

This detection functionality will be supported using mathematical concepts of graph theory and percolation theory. In addition, models of both the local physical infrastructure and the local cyber infrastructure will be created with interdependencies between them. Those approaches will allow the Hybrid SA to characterize the physical and logical interconnections between the two worlds of PSA and CSA and to identify the systems reachable from a single starting point. Additionally, percolation theory can describe the potential propagation of a threat, i.e., indicate which systems are more likely to be reached based on predefined probabilities. In this context, it is not relevant whether an incident occurred in the physical or in the cyber world: the cascading effects in both the physical and cyber world can be described simultaneously.

This way once a real physical and/or cyber threat is detected the potential consequences including cascading effect in both planes (physical and cyber) will be automatically shown to the decisions makers in order to give them a holistic SA on what is happen and how the situation could evolve.

Once the potential consequences and cascading effect of a detected threat have been shown HSA will also show some decision support actions that could help the decision makers to prevent or even mitigate the future stated consequences.

For example, an incident in the physical plane, e.g., an explosion/fire, is detected in a building of the port. This event is detected by the PSA and is analysed by the HSA. The HSA shows in real time what potential consequences/effects this accident/attack could have in the near future in both planes. In this case study, several servers have been destroyed by the explosion. Consequently, a freight shipping application of a large company is at risk of being hacked and video flows and data have been lost from surveillance cameras and access control assets. This warns the decision makers that a physical attack and/or cyber intrusion in these items could

now happen, since that specific area now has no video surveillance and access control data are no longer being received.

In the other hand, the Cyber SA detects that a video server has been compromised by a cyber-attack. The HSA system shows in real time the potential consequences/effects of this attack on the real world. These consequences could be the loss of video flows from the surveillance cameras watching over the fuel tanks' area as well as from video surveillance cameras at a secondary entrance of the port. This warns the decision makers that a potential attack/intrusion in these areas could now happen, since there is no video surveillance there. Additionally, advice is provided, for example, to send a security patrol, tracked by the PSA, to the fuel tank area to ensure the protection of this critical area and to reinforce and alert the security staff in the secondary entrance that have lost the video surveillance flows.

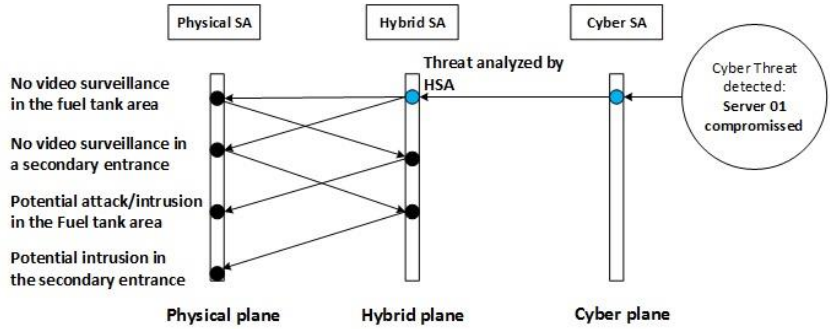

Figure 3 Hybrid SA cascading effect visualization

The complexity of the situation can be even larger and the cascading effect can be amplified in the presence of a combined threat, i.e., a combination of both of the above scenarios (See Figure 4).

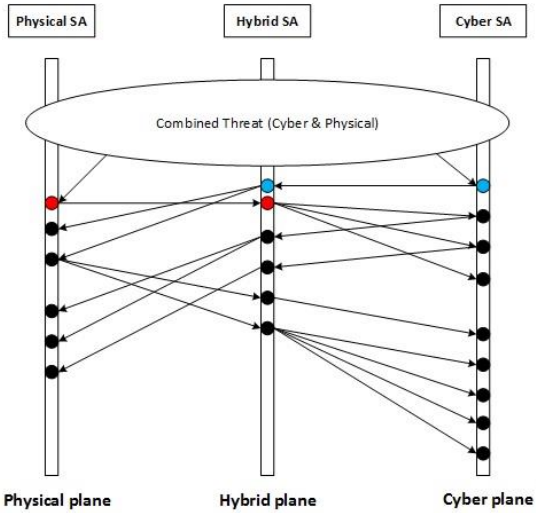

Figure 4: Hybrid SA cascading effect visualization

A Game-theoretical Decision-making Framework for Physical Surveillance Games

Ali Alshawish[1], Stefan Rass[2] and Hermann de Meer[1]

[1] Faculty of Computer Science and Mathematics
University of Passau
{ali.alshawish, hermann.demeer}@uni-passau.de

[2] System Security Group
Universität Klagenfurt
stefan.rass@aau.at

Abstract – Critical infrastructure protection becomes increasingly a major concern in governments and industries. Besides the increasing rates of cyber-crime, recent terrorist attacks have targeted critical infrastructures. Many critical infrastructures, in particular those operating large industrial complexes, incorporate some kind of physical surveillance technologies to secure their premises. Due to the fixed installation of traditional surveillance systems, such as Closed Circuit Television (CCTV), surveillance policies become more predictable and a potential adversary has a better opportunity to observe and bypass deployed surveillance devices. Therefore, it is important to maintain situational awareness within such environments so that potential intruders can still be detected. Regardless of whether personnel (e.g., security guards) or technical solutions (e.g., cameras) are applied, such surveillance systems have an imperfect detection rate, leaving an intruder with the potential to cause some damage to the infrastructure of interest. Hence, the core problem is to find an optimal configuration of the surveillance technology at hand to minimize the potential damage. Here, we present a decision-making framework which assesses possible choices and alternatives towards finding an optimal surveillance configuration and hence minimizing addressed risks. The decision is made by means of a game-theoretic model for optimizing physical surveillance systems and minimizing the potential damage caused by an intruder with respect to the imperfect detection rates of surveillance technology. This approach lets us conveniently capture the full uncertainty in the most general form by a categorical or continuous probability distribution over the potential damage that the adversary can cause. In this way, we avoid information losses by aggregating empirical data into crisp representatives (of damage and its uncertainty), and in using a proper stochastic order, we can optimize a surveillance system despite (and accounting for) its intrinsic imperfectness.

1. Introduction

Risk management plays an increasingly integral role in operations of critical infrastructures. This process mostly requires a deep understanding of the system's functions, processes, and assets as well as their mutual dependencies. Therefore, situational awareness turns out to be a core component of risk management approaches since it provides a means to develop a constantly updated understanding of the current state of the system of interest. Situational awareness enables involved security operators or risk managers to keep track of what is currently happening and to understand it or interpret it depending on what happened in the past time in order to foresee what could happen in the future and thus to be able to make decision and take action properly [1]. The substance that glues past, present, and future phases of the situational awareness process together is data, which varies across multiple scales in space and time (i.e. historical and real-time data). Further, data is an important element for a precise risk assessment process. Although there are several advanced biometric and access control techniques that can be used to secure critical facilities, visual monitoring and on-site observation are still indispensable practices to ensure persistent surveillance in such environments. However, covering a moderate-sized environment requires a substantial number of static cameras, which induces a heavy monitoring activity for security personnel behind monitoring screens, leading to poor efficiency due to potential fatigue [2]. Therefore, we target mainly scenarios in which mobile agents can be deployed in the environment for surveillance applications. In such scenarios, while potential adversaries are seeking for causing a maximum damage to the target infrastructure, the defenders or first responders are to the contrary seeking optimal resource allocation in an attempt to thwart any potential adversarial plans. Mostly, the security resources (mobile agents) are not adequate to track all targets at once. Thus, these resources have to be strategically assigned to maximize the benefits for the system's defenders. This problem already has a natural reflection in game theory known as “cops-and-robbers” game, but current models always assume that the game’s outcome (even if stochastic) can be quantified or described in exact numerical terms (say, by aggregating a set of possible random outcomes into their weighted average, which is a crisp number again). However, the decision making process in such application should consider uncertainty in form that preserves *all* information. Even if the defender and the adversary share the same site there is a probability that the defender misses the adversary inducing randomness in the player's outcomes, but speaking only about the average damage upon false-negative alarms tells us nothing about how likely a certain lot of damage really is. Modeling randomness based on domain knowledge usually culminates in an expected payoff (e.g., a success rate for the patroller, average damage for the attacker) for the players, but this is basically a reduction of information from the full-fledged probabilistic model (a distribution) back to a real value. In retaining the full featured distribution model and doing the decision making and prescriptive analyt-

ics over the more detailed object, we can obtain lot more from the model and data than what conventional (game-theoretic) models could give us.

The term *physical surveillance games*, will herein refer to distribution-valued games that model the interaction between at least two players (i.e. defenders/first responders/security personnel and potential adversaries/attackers/criminals) each equipped with a finite action set (i.e. strategies) as well as the chance is deemed as a hypothetical third player that induces randomness in the real player's outcome. Thus, a distribution-valued game takes the random outcome distribution as the payoff itself to avoid any information reduction [3]. That is, instead of computing the behavior that maximizes a numeric revenue, we can compute the behavior that shapes the payoff distribution at best for the defender (meaning that we seek an action prescription that shifts all likelihood to the lowest damage range). Further, the equilibrium strategy of a game will deliver the defenders with optimal surveillance policies and strategic allocation of the available resources within the environment of interest. Regarding the general setting of physical surveillance games, we consider a large environment, e.g. an industry complex of a utility provider, consisting of several areas of different importance and having a number of security guards, who are patrolling the area to detect potential violations. Broadly speaking, physical surveillance games have several important real-life manifestations such as physical border patrolling, scheduling random security checkpoints, mobile robots path planning, public transit security and fare enforcement planning, among others.

2. Game-Theoretic Model Using Uncertainty

In real-world surveillance systems there are several practicalities and imperfections that can significantly result in a fluctuating detection performance of the system. For example, every surveillance camera system has blind spots, and not every person in an inspected zone may be caught or available for a quick automated identity check. Emergency and unforeseen events, such as human errors or undisciplined inspection staff, as well as irregular (random) behavior of potential intruders are all factors that can significantly affect the ability of inspectors to adhere to planned schedules as well as the ability to deterministically assess the effectiveness and performance of specific surveillance (i.e. inspection) strategy, resulting in noticeable performance fluctuations and stochastic strategy effects. These are pieces of uncertainty that must be reflected in a good model. To describe the uncertainty stemming from the various limitations of surveillance systems, we assume the payoff of our game not to be quantified by a single number. Rather, it is described by a set of possible outcomes that either stem from simulations, surveys, or expert interviews.

Incorporating the probabilistic element into a (game-theoretic) model typically works by speaking about average outcomes to compile a set of possibilities with different likelihood into

a single number that the game can use for optimization. Obviously, this method burns almost all available information. In light that information about security incidents and their potential consequences is in most cases a scarce resource anyway, a method that preserves the (perhaps little) information that is available appears attractive. The idea of distribution-valued game theory is using a total stochastic order in replacement of the usual numeric order, so that the optimization of numbers becomes an optimization of probability distributions. Not all stochastic orders (among the many that exist) are equally suitable, and we designed a total such order based on the weight and length of the distribution's tails. The ordering thus prefers distributions with lighter tails, in alignment with the usual paradigm of risk management to focus on extreme events, which the tails of a distribution captures. The stochastic order designed for the purposes of the HyRiM method accounts for this explicitly. Based on the provably similarity in the properties of numeric and the HyRiM stochastic order, we can establish the core concepts and results of game theory within the new setting of distributions (replacing numbers in the optimization). In this way, we get a full featured game theory that suits our need to preserve all information about the uncertainty in the performance of the security systems.

3. Decision-making Framework for Physical Surveillance Games

Risk management based on surveillance involves a decision-making process, which identifies and assesses possible choices and alternatives towards finding an optimal usage pattern of surveillance and hence minimizing risks of a scenario of interest. Figure 1 depicts a six-step decision-making framework that applies the game-theoretic approach described in Section 1 to find an optimal solution for risk minimization through playing surveillance games with stochastic outcomes. The process is based on the ISO31000 risk management practice, for the sake of easy integration into established and proven processes of enterprise risk management.

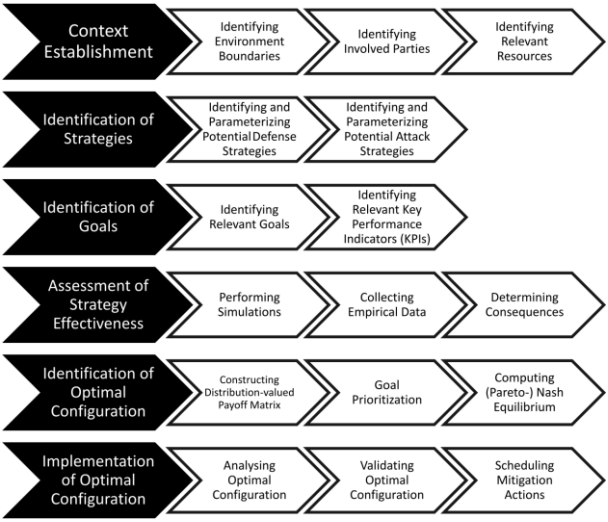

Figure 1: Schematic representation of the game-theoretic decision-making framework for physical surveillance games

4. Illustrative Scenario: Risk of Physical Intrusion in Critical Infrastructure Environment

We consider an industrial complex as a critical infrastructure involving several industrial processing units and auxiliary facilities (e.g., petroleum refining units, a water purification center, a gas production plant, or an electricity production plant). Being sensitive (i.e., the business and the industrial processes), this infrastructure can be a potential target of several attacks of different kinds. In the context of the risk management process, we aim to study the impact of potential attacks to identify the best defense strategy to enforce in order to protect these assets from potential external threats. For the sake of simplicity, we confine ourselves to the risk of physical intrusion and we describe briefly the application of our aforementioned framework for risk minimization. This scenario is derived from realistic environment settings and based on knowledge of experts operating in critical infrastructures.

1. **Context establishment:** The entire area is divided into zones; each of which having a specific security level. The criticality and implied security level of a specific zone depends on the assets located therein (e.g., areas where important machinery is operated or control room) or on the information stored in that zone (e.g., data centers, record storage

rooms, etc.). Although these zones are equipped with surveillance systems such as video cameras or access control systems, the presence of security guards is also required. In particular, these zones need to be checked on regular basis by a security guard to prevent an intruder from accessing these areas (which is partly covered by technical solutions), but also to identify personnel not permitted to be present in that zones. Every employee holds an individual security badge, or interchangeably an ID-card, proving her/his identity and right to be in a given subarea or zone. In addition, there are 15 security guards (i.e. available resources to serve as mobile badge inspectors). Every guard follows a schedule of checking missions where she/he is supposed to move around and check the identity of some randomly selected employees located in the different zones.

2. **Identification of strategies**: Here, we need to identify the set of strategies of both players (i.e. defender and intruder). We consider a set of 6 intruder strategies varying according to how areas are targeted: either randomly (*R*) or based on their criticality by targeting Higher Security Levels First (*HSLF*) as well as the number of involved intruders. On the other hand, we identify 8 defender strategies varying according to the number of missions per day (frequency of missions) as well as how do they target a given area: randomly (*R*) or Higher Security Level First (*HSLF*).
3. **Identification of goals**: The overall game has four goals of interest: *Caused Damage, Minimum Privacy Preservation, Maximum Comfort breach, and Detection Rate*. We stress that these goals are not optimized independently, but rather simultaneously by computing a defense that achieves the best possible performance in all these regards. Any attempt to improve the outcome in one of these goals is then tied to a reduction in at least one of the remaining three aspects. The defense strategy obtained from the game is therefore *Pareto-efficient*.
4. **Assessment of strategy effectiveness**: For each known configuration, the effectiveness with regards to all identified goals needs to be determined. Since the response dynamics of the game, e.g., people's reactions, etc., may be uncertain, we need to be careful on how to assess our different strategies. For instance, we may rely on some experts' opinion that will evaluate the different strategies in terms of our fixed goals. Another option would be to rely on simulation, which we do in this study.
5. **Identification of optimal configuration**: The assessment results of our strategies will be categorized into 5 fixed classes {Very low, Low, Medium, High, Very high}. This categorization is mandatory to be able to apply the game-theoretical framework that computes the optimal strategy of our multi-goal game [4]. As expected, there is no single optimal defense precaution, and the best we can do is a certain "mix" of defense measures as displayed in Figure 2. The concrete advice for an optimal defense is to randomly alternate between three defense strategies, (*D-NG15F8TR*, *D-NG15F5THSLF* and *D-NG15F8THSLF*), which should be launched with frequencies of 10%, 76.8% and 13.2% over time, respectively. Hence, a practitioner could abandon the remaining strat-

egies to be as options to defend, and randomly choose its actions from the three aforementioned ones, with different probabilities. This gives the best possible defense in the sense of minimizing the intruder's chances to cause large damages.

6. **Implementation of optimal configuration**: The optimal strategy has been implemented in the developed simulator to validate and verify its effectiveness over all the others. Afterwards, we replayed the game with 9 defender strategies including the equilibrium strategy computed in the previous step, referred to as *D-NG15ImplMixed*. The new computed equilibrium, depicted in Figure 3, clearly shows that *D-NG15ImplMixed* strategy is indeed the most effective with a probability of 99.5%. This result simply confirms that the defender's best choice to defend is by applying *D-NG15ImplMixed* almost all the time.

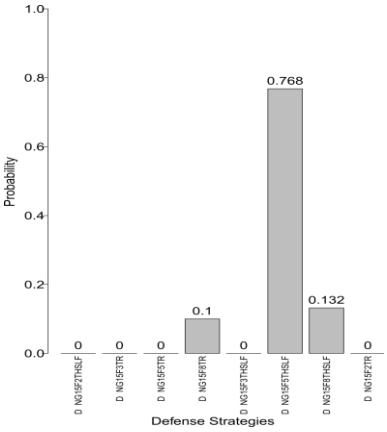

Figure 2: Optimal defense strategy: an equilibrium for multi-objective security games

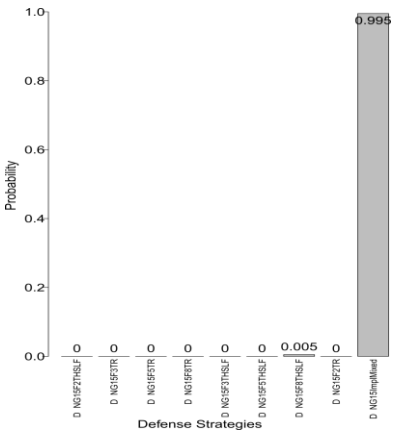

Figure 3 Validation of the optimal defense strategy

Acknowledgements

This work was supported by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1).

References

[1] Endsley, Mica R. *Toward a theory of situation awareness in dynamic systems.* Human factors 37.1 (1995): 32-64.

[2] Bhattacharya, Sourabh, Tamer Başar, and Maurizio Falcone. *Surveillance for Security as a Pursuit-Evasion Game.* International Conference on Decision and Game Theory for Security. Springer, Cham, 2014.

[3] Alshawish, Ali, Abid, M. Abid, Rass, Stefan, de Meer, Hermann: *Playing a Multi-objective Spot-checking Game in Public Transportation Systems.* p. 6. Neuchâtel, Switzerland, June 21-22, 2017. DOI 10.1145/3099012.3099019.

[4] Rass, Stefan. *On Game-Theoretic Risk Management (Part One)-Towards a Theory of Games with Payoffs that are Probability-Distributions.* arXiv preprint arXiv:1506.07368 (2015).

Managed Cyber Security for Protecting Critical Infrastructures

Tools and Procedures against Advanced Attacks

Stefan Beyer, Luis Búrdalo Rapa, David Monteagudo Sanz and Roberto Amado Giménez

S2 Grupo, Valencia, Spain
info@s2grupo.es

Abstract – Cyber security of critical infrastructure has become a major concern for society. These systems have become important targets for cyber-crime, cyber-terrorism and industrial espionage. Recent changes in the attack landscape mean that traditional cyber security monitoring, such as intrusion detection and malware detection has reached its limits, as security analysts are faced with an ever increasing number of advanced, persistent and targeted attacks. These attacks require proactive threat hunting techniques, which require expertise, time and tool support. In this paper, we present our current approach to providing security analyst with tool support for situational awareness and threat hunting and our ongoing research in this field.

1. Introduction

Cyber security has become one of the most pressing concerns for critical infrastructures. As recent attacks, such as the 2016 attack on the Ukrainian power supply [1] and the 2017 world wide WannaCry [2] attack have shown, cyber security incidents can have a large scale impact on IT systems, critical infrastructure and society as a whole. Reports on the actual costs of cyber-attacks vary widely, as pointed out in a 2016 study performed by the European Union Agency for Network and Information Security (ENISA) [3], but impact on critical infrastructure is estimated somewhere between 330 and 506 billion Euros at global level by McAffee.

At the same time as the number of incidents and the cost associated has increased, changes have taken place in the treat landscape, in that attacks are becoming more and more sophisticated and harder to detect by traditional means. So called Advance Persistent Threats (APT) are planned multimodal attacks, targeted at a specific organization or infrastructure, where several types of malware, under control of a command centre, are combined with techniques

like social engineering, use of insiders or access through third parties, with the objective of gaining access to critical physical or virtual assets (Intrusion phase) and exfiltrate information (for example, to obtain economic or politic advantage) or sabotage infrastructures.

Critical infrastructures are especially vulnerable to advanced attacks, as these systems are harder to protect for a variety of reasons:

- Industrial Control Systems (ICS) at the heart of critical infrastructures have a longer life cycle as most IT systems and are therefore often reliant on legacy hard- and software.
- There is a reluctance in ICS professionals to introduce security monitoring systems that might increase system complexity and degrade performance.
- Critical infrastructures have to be highly available and system downtime for software patching and vulnerability removal is often not acceptable.

As advanced attacks are targeted at a specific organization they are typically very stealthy attacks and hard to detect. This means that, in many cases, automated signature based malware detection does not detect these attacks. APTs have to be detected by means of threat hunting, an approach more akin to classic intelligence. Typically, an experienced security analyst aided by monitoring tools detects anomalies in network traffic, which may or may not indicate an attack and further investigates. To do this the analyst has to look at a large amount of risk related information obtained by a set of tools.

It is therefore essential to provide cyber security analysts charged with protecting critical infrastructures a set of tools to allow situational awareness of the cyber space related to an installation.

In what remains of this paper, we describe our approach to cyber situational awareness and tool support for threat hunting. We also discuss our current research aimed at increasing automation and effectiveness of these tools by introducing artificial intelligence based anomaly detection in network traffic in industrial protocols typically used in critical infrastructures.

2. Cyber Situational Awareness

2.1 Organisation and Procedures

Typically, Critical infrastructures are monitored by specialized Security Operations Centres (SOC) with additional procedures and workflows for industrial and critical infrastructure cybersecurity, a so called iSOC. The iSOC may be in house or managed by an external cyber security provider. We operate such a managed security service centre, in the form of a certified Computer Emergency Response Team (CERT). The center combines the capabilities of a

Network Operations Center (NOC), a SOC and an iSOC. The CERT provides 24x7 Managed Security Services in several manners and always trying to fit the customers' specific needs. In this way, we provide SOC services remotely from our CERT, and on the customer's premises.

It is essential for any SOC to be secure itself, both in terms of cyber security and physical security. To this end, the CERT is technologically equipped with powerful management and monitoring systems, both physical and logical, to guarantee the security of the center and its contents, beyond the standards: biometric access control, video surveillance, uninterrupted power supplies, burglar alarm, HVAC system, data processing center, Service Desk, CND, CNA, IT management, product development, consulting and lab. Furthermore, the CERT has an operational backup facility in a geographically different location.

2.2 Toolchain

As has been explained above, in order gain situational awareness, the security analysts need to be provided with an effective toolchain. In what follows of this section we describe our own toolchain, using at as example for describing the type of support required at each level of cyber security monitoring.

Our managed security services rely on ***emas*® *SOM (Security Operations Manager*)** [5], a comprehensive software suite developed in house, which is structured around a CMDB (ISO 20000 or ITIL compliant) and provides security events monitoring and collection capabilities, along with a flexible orientation towards network surveillance, including IT (Information Technology) for computer network and information systems environments, OT (Operational Technology) for industrial environments (Industrial Control Systems – ICS) and also the Internet of Things (IoT), advanced intelligence using complex event correlation techniques or the analysis of patterns for the identification of anomalies, as well as service processes management (including Incident Handling process, Quality of Service, configuration or knowledge management).

The volume of data to be monitored in any critical infrastructure of a certain size would be unmanageable without such an automated system that helps in the collection, normalization, storage, analysis and correlation of events, thus achieving a significant reduction of the amount of information to be finally managed the security analyst.

Our toolchain is based on a funnel model for the automatic analysis and extraction of relevant information from huge amounts of security data (cf. Figure 1).

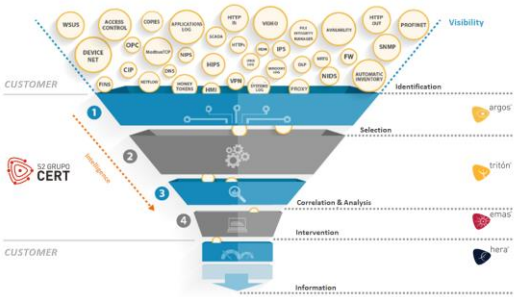

Figure 1: S2 CERT funnel event processing model

The funnel event processing model is based on these five stages, directly related to the security incident management cycle:

- **Identification** of security information sources is the input to the funnel.
- **Selection and detection**. The **argos®** monitoring platform collects all data from the different distributed sources. This information consists of security events that will become the input to the next stage.
- **Correlation and analysis**. Automatic correlation and analysis of all selected events are performed by **tritón®**, the **emas® SOM** correlation engine, based on pre-defined and customized correlation rules. **tritón®** intelligence allows for detecting true security events, minimizing false positives, and thus optimizing SOC resources for next stages.
- **Intervention.** As a result of the previous analysis and correlation, security events are issued at the security operations management console, **emas®**, where they will be managed by the security analysts and incident responders in order to perform and coordinate contention, eradication and recovery activities.
- **Reporting and post incident activities.** All activities are documented in the Known Errors Database and the Solutions Database, as well as the documentation repository. Furthermore, **hera®** automatically collects specific security indicators to build a real-time security dashboard for the customer with the most relevant information.

3. Detecting Advanced Attacks

3.1 Threat Hunting Techniques

Whilst the operation described above goes beyond the capabilities of traditional Security Information and event Management (SIEM), in that it provides intelligent correlation and is able to deal with large amounts of data, it follows a typical model for managed security ser-

vice. However, as has been explained above, in order to affront advanced and targeted attacks, experienced cyber security analysts need to employ threat hunting techniques. This usually consist in browsing logs of network services for anomalies which may indicate lateral movement of a malware, i.e. the spreading of the malware within the network, or external communication with the command-and-control server of the malware.

3.2 Tool Support

In order to support the security analyst in the difficult task of threat hunting, we have developed **Carmen** [6], Europe's first threat hunting solution, aimed at detecting APTs, in collaboration with the Spanish National Centre for Cryptology.

Carmen provides capabilities for threat detection in the persistence stage, so one of its fundamental objectives is to identify external movements, such as exfiltrations or communications with command systems and lateral movements to maintain persistence or information theft in the corporate network. The acquisition and analysis capabilities of the tool allow covering the main channels of communication of these threats with the outside (web browsing, DNS queries and electronic mail) as well as different mechanisms of internal communication in the compromised network.

For each of the collected data sources, **Carmen** allows the automatic, semi-automatic and manual analysis of the network traffic of the organization for the detection of improper usage and, especially, for the detection of significant anomalies: statistics, time series, in text strings or knowledge-based, for example. In addition to the persistence stage, **Carmen** provides capabilities for threat detection in the intrusion stage, mainly anomaly conditions for the detection of habitual infection mechanisms, such as watering hole or exploit kits, as well as deployment and integration of Sandboxing capabilities for the detection of mail scams specially directed to the organization such as spear phishing.

These identified situations provide the security team with the possibility of prioritizing the elements to be analyzed from the entire volume of data acquired, thus facilitating decision-making and the identification of threats in the organization. Figure 2 shows an example of an open investigation in Carmen in which the security analyst traces the origin of suspicious activity.

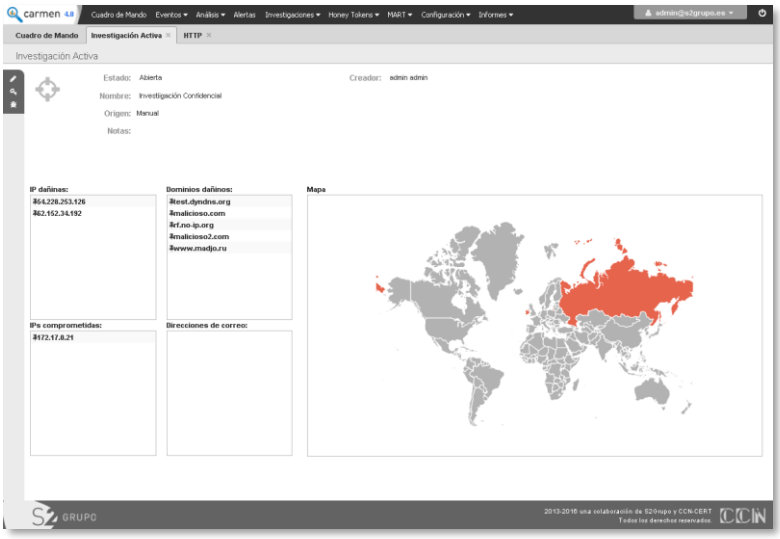

Figure 2: Carmen - Investigation Screen

4. Artificial Intelligence based Anomaly Detection

Our current research focuses on using machine learning to automate some of the anomaly detection carried out by security analysts during threat hunting. Individual machine learning modules can be used to detect anomalies in certain protocols. For instance, an algorithm focusing on industrial protocols, such as Modbus might be trained to detect changes in the timing and sequence of SCADA commands, or a more general purpose algorithm may use features such as packet size, sequencing of incoming and outgoing connections on certain ports or changes in order of header fields to detect anomalies in HTTP traffic.

Industrial control systems used in critical infrastructures lend themselves to his approach, as traffic in these system is more deterministic than general purpose IT traffic and normality is thus easier to model. In addition to the above example, we perform deep packet inspection; that is, we not only analyse protocol headers, but also use machine learning to analyse protocol payload for anomalies.

Inspecting the payload of network packets in order to detect potential attacks is a very complex task that can be addressed in different ways. One these ways is analysing byte sequences in packets' payload in order to detect any anomaly which could be indicative of the presence

of a potential intrusion in the system. Our current approach for detecting anomalies in payload using LSTM neural networks [7] analyses packet flow as a sequence of bytes corresponding to the different payloads. An n-byte sliding window is used to analyse the byte sequence. The LSTM neural network is trained with pairs <n-byte sequence, following byte>, so that it can later determine the probability of each byte in a payload, attending to previously observed ones. The probability of the entire payload is later calculated as a result of the individual probabilities of each byte.

The above algorithm is currently work in progress, but we expect to incorporate modules based on this and similar techniques in our toolchain.

Acknowledgements

This work was partially supported by the Spanish Ministry for Economics, Industry and Competiveness under grant number RTC-2016-4847-R and the European Horizon 2020 Programme under grant agreement number 740477

References

[1] Ukranian Power Supply Attack, *BBC News:* http://www.bbc.com/news/technology-38573074, 2016.

[2] WannaCry Cyber Attack, *Symantec Security Center:* https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99, 2017.

[3] The cost of incidents affecting CIIs, *European Union Agency for Network and Information Security (ENISA):* https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis, 2016.

[4] Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, *McAfee Center for Strategic and International Studies:* https://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf, 2014.

[5] emas Security Operations Manager, *S2 Grupo:* https://s2grupo.es/en/emas-security-operations-manager-en, 2017.

[6] CARMEN Threat Hunting Tool, *S2 Grupo:* https://s2grupo.es/en/carmen-en, 2017.

[7] S. Hochreiter y Schmidhuber, J., Long short-term memory, *Neural computation,* vol. 9, nº 8, pp. 1735-1780, 1997.

Is my Grid Bouncing Back? A Cyber-Physical Resilience Metric for Smart Grids

Ivo Friedberg[1,2], Kieran McLaughlin[1] and Paul Smith[2]

[1] Centre of Secure Information Technologies
Queen's University Belfast
{ivo.friedberg; kieran.mclaughlin}@qub.ac.uk

[2] Center for Digital Safety & Security
AIT Austrian Institute of Technology
{ivo.friedberg; paul.smith}@ait.ac.at

Abstract – The need for novel smart grid technologies is often motivated by the need for more resilient power grids. While the number of technologies that claim to increase grid resilience is growing, there is a lack of widely accepted metrics to measure the resilience of smart grid installations. The design of effective resilience metrics is made difficult by the diversity of challenges and performance measures that a smart grid is subject to. Our work identifies attributes that are required for a complete and effective resilience metric and shows that previous work falls short. As a consequence we propose a novel approach to measure resilience that focuses on the complex interdependencies between challenges and performances in smart grids. This enables transparent and informed decision making in resilient grid design.

1. Introduction

The motivation for smart grid technologies that is often put forward is the increase in system resilience that can be achieved. However, the term resilience is used inconsistently throughout recent work. Terms like robustness, reliability, availability and even security are often used interchangeably with resilience [1]. Recent efforts to explore the definition of resilience for cyber-physical systems in general [2] and power grids in particular [1], [3] were made with the goal to achieve an understanding about resilience that encompasses all aspects of smart grids. However, research on descriptive metrics to quantify resilience cannot keep up with the requirements. This is problematic for grid design and maintenance. Current resilience metrics are limited to evaluate limited aspects of grid functionality (e.g. power flow during extreme weather events). The lack of a more descriptive metric does not only prevent a better integration of novel smart grid technologies. It further limits the understanding of the impact these technologies have on different aspects of smart grid resilience.

In this work, we first highlight the requirements of a general and descriptive resilience metric and show that previous work is insufficient. We then propose a more complete approach to measure resilience in smart grids and explain how it can help with operators with grid design and maintenance

2. Metric Requirements

A descriptive and generally applicable metric has to fulfill seven requirements to be useful in all important aspects of grid design and operation:

- **Comparability:** I should provide the ability to quantify systems with respect to a specific performance measure in order to make two systems comparable.
- **Measurement Evaluation:** At runtime, the metric has to be applicable to real measurement data rather than models. This is important as complex systems easily deviate from the designed system behavior over time.
- **Performance Prediction:** In contrast to the evaluation of real measurements, the metric needs to be able to model system behavior and predict resilience to evaluate intended system changes or new technologies before actual deployment.
- **Resilience Potentials:** According to work by Arghandeh et al. [1], the resilience of a system depends on three potentials: The absorbing potential (the ability to withstand negative effects), the recovery potential (the ability to recover during or after a challenge) and survivability (the ability to prevent system collapse). These are often ensured by different means, so the metric should allow the operator to identify the weak potential in a system.
- **Flexibility:** The metric needs to allow resilience to be evaluated based on various performance measures and system challenges.
- **Performance Interdependencies:** Through interaction subsys-tems become dependent; a decreased performance in one is a potential challenge to performance measures in others which has to be captured by the metric.
- **Scalability:** Although a metric should be applicable to all poten-tial performance measures, not all performance measures are relevant for each evaluation. To make the complexity manageable, a metric needs to be scalable; it should be possible to abstract aspects of the system that are irrelevant for a specific evaluation.

3. Proposed Resilience Metric

The performance of a system can be described by a vector of all performance measures

$$\vec{p}(t) = \begin{pmatrix} p_1(t) \\ p_2(t) \\ \dots \\ p_n(t) \end{pmatrix}$$

where each performance measure $p_i(t)$ has a nominal performance p_i^N – the performance in a challenge free environment –, a collapse threshold $p_i(t)$ – a performance level from which the system cannot recover on its own – and is bound by $0 \leq p_i(t) \leq p_i^N$. Based on a single performance measure $p_i(t)$ the resilience of the system with respect to this performance measure is defined as R_{p_i} as given by:

$$R_{p_i}: \mathbb{R} \to [0;1]: t \to 1 \frac{\int_{t_0}^{t} p_i(\tau) d\tau - p_i^T \cdot (t - t_0)}{(t - t_0)\,(p_i^N - p_i^T)}$$

It describes the ratio between the actual system performance (the area between $p_i(t)$ and $p_i(t)$) and the worst case system performance. This metric is supported by a framework that models each performance measure p_i in dependence to other performance measures, as well as external challenges. The quantitative results from the metric can then be rooted in the complete system. The framework can further be used to predict the resilience of the system through estimation without applying real challenges at runtime. Each performance measure is modelled as a differential equation which is solvable as an initial value problem (IVP) where $p(t_0) = p_0$.

$$\dot{p}_i(t) = \left[f\left(t, r, p_i(t), p_i^N\right) - g\left(t, \vec{c}(t), \vec{p}(t)\right)\right] \cdot \Theta_{p_i}(p_i(t))$$

Here, f represents the recovery potential of a degraded system. It depends on the time t, a recovery rate r which needs to be identified for each system and can be a constant or a complex function, the current performance $p_i(t)$ and the nominal performance p_i^N. On the other hand, g represents the absorbing potential and depends on the time, a set of external challenges $\vec{c}(t)$ and all other performance measures. The dependence on other measures is important as they can pose a challenge to the measure in focus. Finally, $\Theta_{p_i}\left(p_i(t)\right)$ is a Heaviside function that describes the performance threshold p_i^T under which the system is considered collapsed.

In first tests the metric framework was applied to a synchronous islanding testbed (see [8] for details). Here a microgrid's frequency is controlled locally based on remote measurements from a reference grid. In this evaluation the performance measure of interest is the phase error between microgrid and reference grid. The system is subject to two independent challenges.

First, the microgrid is subject to a step load change. Secondly, the communication between the controller and the reference signal is subject to network delay.

Figure 1 shows the predicted system resilience for different step changes and network delays. From the graphs it can be seen that both, network delay and load step size have an impact on the system resilience. However, for load steps greater than 30MW, a further increase in step size impacts the resilience only in a limited way. In contrast, no such limit can be found with respect to communication delay. An increase in delay always further impacts the resilience.

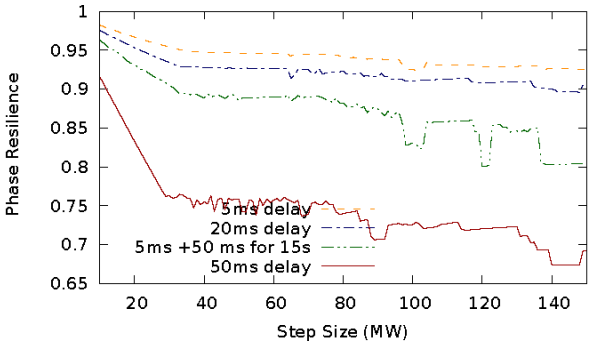

Figure 1: Resilience of frequency controller in synchronous-islanded microgrid with respect to phase error. The system is challenged concurrently by a network delay between PMU and controller and by a load step (size varies).

The resilience framework design is described in Figure 2. It shows how the metric framework models the interdependencies between external challenge (i.e. load step change), an internal performance measure that becomes a challenge (i.e. frequency deviation) and the final performance measure on which resilience is computed.

This approach to measure resilience can now be leveraged by a system operator. The metric shows where system improvements are most effective. In the presented case, an improvement of the frequency controller would be effective. As the phase error is highly dependent on the controlled frequency, a better absorption or recovery rate for the frequency error will effectively increase resilience. However, this will not limit the effects of network delay efficiently. There is only so much the controller can do with insufficient feedback. So to increase overall resilience, a sufficient transmission time needs to be ensured by the network as well.

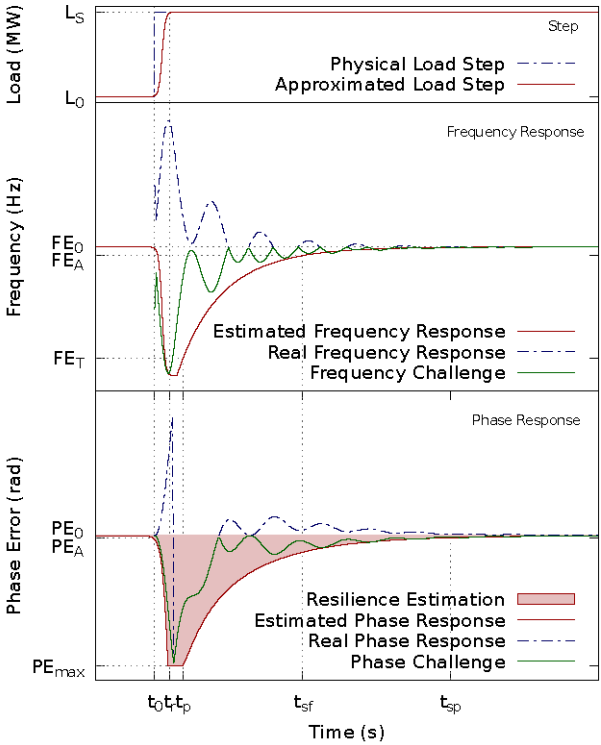

Figure 2: Performance measure interdependencies as modelled in the resilience framework.

We showed, that our novel metric introduces the ability to analyse resilience with respect to various performance measures (flexibility) while the relationships between the system domains are considered. These aspects are most often left out by existing work although they are most vital for operators to understand system resilience.

References

[1] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," Renewable and Sustainable Energy Reviews, vol. 58, pp. 1060–1069, May 2016.

[2] D. Wei and K. Ji, “Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights,” in Resilient Control Systems (ISRCS), 2010 3rd International Symposium on, Aug 2010, pp. 15–22.

[3] S. Chanda and A. K. Srivastava, “Defining and Enabling Resiliency of Electric Distribution Systems With Multiple Microgrids,” IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2859–2868, Nov 2016.

[4] I. Friedberg, K. McLaughlin, P. Smith, and M. Wurzenberger, “Towards a resilience metric framework for cyber-physical systems,” in 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR 2016), 8 2016, pp. 19–22.

Data Protection and Critical Infrastructures in the EU

The impact of the General Data Protection Regulation and the Networks and Information Systems Directive on Critical Infrastructure Protection

Laurens Naudts, Plixavra Vogiatzoglou and Anton Vedder

imec-CiTiP (Centre for IT & IP Law)
KU Leuven
{laurens.naudts; plixavra.vogiatzoglou}@kuleuven.be

Abstract – The EU General Data Protection Regulation, which will come into effect in 2018, is set to bring along substantial changes to the regulatory landscape governing critical infrastructures. This presentation seeks to provide a high-level analysis of the interaction between the European data protection regime and the protection of Critical Infrastructures. For a better understanding of the nature and extent of obligations weighing on operators of CI, the principal concepts as well as several potential challenges, are pointed out with attention to the distinction between the wider right to data protection and the Directive on Security of Network and Information Systems.

1. Introduction

The European Data Protection Framework provides for certain obligations to operators of Critical Infrastructures (CIs). When carrying out functional and regular activities within the context of each CI and more specifically when safeguarding the CI's cybersecurity, processing of personal data may take place and to that specific rules must apply. The General Data Protection Regulation (GDPR) becomes applicable on 25 May 2018 across all EU Member States [1] and, even though some room for national manoeuvre will remain, the GDPR will further harmonize and strengthen the regulatory framework on personal data processing by private and public entities. In the narrower context of cybersecurity, the new Network and Information Systems (NIS) Directive introduces a minimum set of requirements for the security of critical networks and information systems, including the protection of personal data therein

[2]. The NIS directive entered into force in August 2016. Since then, EU Member States have 21 months to transpose the Directive into their national laws. In this context, please note that regulations, such as the GDPR, are directly binding, while directives, such as the NIS directive have to be transposed in national laws, and as such they may present differences from one Member State to another.

Against the background of the upcoming changes to the regulatory environment, it is of paramount importance that CI operators are aware and understand the new rules they will have to comply with. Therefore we will, not only give an introduction to the main definitions and obligations deriving from the GDPR and NIS regarding personal data; we will also identify and clarify specific issues that we deem to be particularly challenging within the context of CIs.

2. Main definitions and obligations

While the GDPR regulates the processing of personal data in a very wide domain - in public and private, as well as commercial and non-commercial contexts in general - the NIS directive introduces rules very specifically on the security of networks and information systems within sectors of essential services. As defined in the directive, essential services refer to the sectors of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure. Both the GDPR and the NIS directive are applicable to CIs. The overlap between the two legal instruments pertains to the occasions where operators of essential services process security related personal data, including the exchange of data between operators of essential services. The NIS directive expressly states that the provisions of the GDPR are to be respected. The directive nevertheless also includes additional obligations, as will be further explained in the Section 2.

Since data are so important in the cyber-risk mitigation strategies of CIs, and for the sake of coherence, it is important to delineate the main concepts and definitions of the GDPR. The GDPR defines personal data as any information relating to an identified or identifiable living natural person, i.e. the data subject. Personal data may consist of any sort of information, not only information concerning what is traditionally considered to be the private sphere. It may refer to a person's family life or intimate relationships, but also to any type of activity or relationships such as working relations, or even identification numbers of people, their computers or their cars. The data may also be personal regardless of the form they take, e.g. written communication, image, footage, recorded sound or even human tissue [3]. An identifiable person is one who can be identified by reference to an identifier such as a name, an identification number, location data, an online identifier, etc. Moreover, the data subject can be either directly or indirectly identified or identifiable, as long as she or he may be distinguished from

other individuals on the basis of the data involved. For instance, smart grid data may not only provide information on individuals' energy consumption, but also on their daily habits that can be deduced from their energy consumption patterns. On the basis of both types of data, individuals can be distinguished and – in principle – be identified.

Data processing refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Since it is important to ensure that the responsibilities involved in the data processing are well defined the person, or organization assuming the role of the data controller must be clearly determined [4]. The controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The GDPR evaluates such decisional competence in a functional manner. The role of controller is thus determined not only on the basis of contractual designation but also on a factual assessment. That is why the first element constituting a data controller is the control over the decisions regarding the personal data processing that stems from explicit legal or implicit competence or from factual influence. Furthermore, the controller determines the purposes and means of the processing, i.e. the "why" and the "how" of the specific processing activities.

Specification of the purpose for the processing of personal data is one of the basic elements required for the legitimization of the processing activity. The means, however, are also important because they relate to technical and organisational issues, such as the categories of data to be processed, the levels of access to these data, the outsourcing of the processing activities to third companies and so on. In the context of CIs, the controller will most likely be the legal entity owning and operating the CI. Lastly, it may be good to note that the GDPR's definition of the data controller anticipates the possibility that a number of parties may jointly be involved in and determine the purpose and means for a single processing operation. In that case, it is important to assess the different degrees in which these parties may interact or be linked, as well as the level of control that they hold with regard to the processing operation. Such assessments may help clarify the responsibilities and ultimately the liability of each party.

The controller is not necessarily the party that actually processes the personal data. Since the GDPR imposes responsibilities also on the party actually processing the data, identifying the processor(s) and their relationship with the controller is necessary. A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The existence of a data processor, therefore, depends on the decision on

behalf of the controller to assign specific processing tasks to a separate legal entity. As such, the processor must only act within the limits of the documented instructions that he has received with regard to the processing activities. Nevertheless, the controller is responsible and accountable for the compliance of all processing operations with the GDPR. The controller must therefore ensure the lawful processing of personal data by basing all processing on a legal ground, restricting processing to its specific purpose and implementing appropriate technical and organisational measures. An exhaustive list of legal grounds is provided by the GDPR. The GDPR provides six legal grounds, but the processing of personal data by CI operators will most likely be based on (one or some or all of) three of them. Processing will be lawful if it is necessary a) for the performance of a contract, for instance with regard to the employees, or, with regard to physical and cyber security, or b) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or c) for the purposes of the legitimate interests pursued by the controller or by a third party. Since the controller must predefine the specified, explicit and legitimate purpose for each and every processing activity, if personal data are processed for the purpose of the regular operation of the CI, they may not be processed for another purpose. Commercial exploitation of these data, for instance, is not allowed if that exploitation is not covered by one of the six legitimizing conditions applies.

Finally, the controller must facilitate the exercise of the data subjects' rights, by, for example, providing the necessary information on the processing activities and their purposes to the data subject. In the course of all processing, the controller must implement and must ensure that the processor applies appropriate technical and organisational measures to protect the personal data.

3. Particular Challenges for CIP

The obligation to secure the processing of personal data is further translated in the privacy and data protection by design principle. According to the GDPR, the controller must implement appropriate technical and organisational measures, such as pseudonymisation, designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and protect the rights of data subjects. This principle calls for an assessment of the risks that the processing raises for the rights of individuals as well as an assessment of the means to mitigate these risks available to the controller. In essence, data protection by design refers to a technical integration of the principles set out by the privacy and data protection framework into a customised automated treatment of personal data depending on their specificities. With regard to data protection by design principles in a security context, the European Union Agency for Network and Information Security (ENISA) has made a distinction between data and process

oriented design strategies. Data oriented strategies primarily address the GDPR principles of necessity and data minimisation. Data oriented strategies refer to mechanisms that enable personal data to be minimised, hidden, separated or aggregated. For instance, they prescribe that the amount of personal data should be restricted to the minimal amount possible (minimize) or that personal data and their interrelations should be hidden from plain view (hide). Process oriented strategies are aimed towards the transparency, control, in the sense that data subjects should have agency over the processing of their data, and enforcement of data processing policies. In addition, data controllers must be able to demonstrate their compliance with data protection policies.

In this regard, it is important to note that the GDPR and the NIS Directive serve different purposes. Whereas data protection legislation focusses on safeguarding the fundamental right to data protection through ensuring fair and lawful data processing, the NIS Directive aims to increase the (cyber) security of information networks. Data protection enhancing technologies, which are integral to design strategies, are not security enhancing technologies. When the data protection and security frameworks require the implementation of technical and organisational measures, those measures will differ depending on whether the basic functions or purposes of the GDPR or those of the NIS directive are to be considered. Data protection enhancing technologies can limit or diminish the possibilities in strengthening a CI' security, while security enhancing technologies can delimit data protection. For instance, when CIs monitor their network traffic for the purposes of detecting anomalies indicating cyber-attacks, a balance must be maintained between security on the one hand, and confidentiality and data protection on the other hand. The detection of anomalies might require deep packet inspection. This however may necessitate that the integrity of the data processed can be verified and maintained. In order to ensure confidentiality and data protection, CI might favour the adoption of encryption techniques. Yet, encryption would then disallow the integrity of data to be verified, which, in turn, limits the adequate detection of cyber-incidents.

Of course, it may often be the case that operators of CIs in their role of controllers, assign a part of the processing activities to external companies, i.e. the processors. In those cases, such outsourcing must meet the conditions set by the GDPR. An assignment of processing activities must be based on a contract or another type of valid legal act setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. A potential processor must provide for sufficient guarantees of compliance with the requirements of the GDPR. The controller may be held liable for the damage caused by a processing activity infringing the GDPR, while the processor may be held liable for the damage caused only where the processing has not complied with the obligations specifically directed to processors or where the processor has acted outside or contrary to lawful instructions of the controller.

With regard to potential cyber-attacks, both the GDPR and the NIS directive provide for notification requirements. These are not, however, in total alignment. On the one hand, the GDPR regulates personal data breaches that must be brought to the attention of the competent national supervisory authority within 72 hours, or, if unfeasible, without undue delay after the controller has become aware of the breach. In addition, data breaches must be communicated to the data subject without undue delay either. According to the GDPR the notion of personal data breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The NIS directive imposes the notification of incidents having a significant impact on the continuity of the essential services to the competent authorities without undue delay. If security breaches also pertain to personal data, the CI will have to comply with the notification requirements in the GDPR and the NIS Directive. As these regimes are different, both procedurally and content-wise, they may induce additional administrative burden to operators of CIs.

Moreover, due to the GDPR's focus on demonstrating accountability, the administrative burden for CI operators is likely to increase in general. The importance of transparency concerning data processing affects the detail of information that is to be given to data subjects. In turn, CIs face the challenge of making their internal data processing activities, e.g. type of data used or the purposes for data collection, understandable to the outside world, while at the same time not compromising security purposes. The GDPR also imposes stricter rules with regard to the internal documentation of data policies and procedures in order to demonstrate compliance. In addition, CIs will have to carry out data protection impact assessments, in particular when using new technologies and where data processing is likely to result in a high risk to the natural persons involved. Also in this respect they may be confronted not only with additional administrative burdens, but with conflicts between the quest for personal data protection and the protection of the infrastructures as well.

Before concluding this brief analysis on the impact of the GDPR and the NIS directive on the protection of CI, mention should be made of another important issue for operators of CI, which, to a degree, remains unaffected by these legal instruments. In particular, while, as already mentioned, in case of a data breach or incident, operators of CIs are obliged to notify the competent authorities, the exchange and sharing of security related information amongst CIs and with public authorities beyond the said notification requirements is not being regulated specifically at an EU level in a consistent and comprehensive manner. Information sharing may be challenging due to inclusion of personal data. In addition, data might include intellectual property or confidential or business related information. Currently, CI operators may voluntarily participate in platforms such as the Critical Infrastructure Warning Information Network (CIWIN) and the European Public Private Partnership for Resilience (EP3R) to share information related to prevention and distribution of best practice documentation or the EU

Civil Protection Mechanism for the coordination of responses following a physical or cyber incident. The GDPR seeks to facilitate information sharing on a general note, while it is the NIS directive that aims at promoting cooperation via a more specialised framework on cyber-security risks and incidents information sharing.

4. Conclusion

The central concepts and principles of the GDPR and some principles of the NIS Directive relating to personal data have a strong bearing on the operators of CIs. Some of these concepts and principles may be specifically challenging for CI operators. CI operators face the difficult task of fulfilling the obligations resulting from the regulation and the directive regarding personal data, while they have to combine two sometimes highly diverging perspectives, i.e. the fundamental right to data protection of the individual on the one hand and the public interest of the protection of CIs on the other.

Acknowledgements

This work was supported by the Horizon 2020 SAURON project on enhancing security and protection of EU ports.

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

[3] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

[4] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

Legislative Framework for CIP in Austria

Critical Infrastructure Protection in Austria Implementation of the NIS-Directive in Austria

Sylvia Mayer

Federal Ministry of the Interior
sylvia.mayer@bvt.gv.at

Abstract – Critical Infrastructure Protection became one really important field in Austria's Security Strategy. On the basis of this strategy, the adopted second release of the Austrian Program for Critical Infrastructure Protection was published in 2014. One main principle of this Strategy is the so called development of a Public Private Partnership. An important measure to implement here was the adoption of several legislative frameworks, regarding responsibilities and security measures taken by the Austrian authorities. In contrast to this Public Private Partnership, the new EU NIS-Directive determines several obligations for the so called essential services. This directive will be implemented in a separate act in Austria and will come into force not later than Mai 2018 with consideration of existing national organizations, structures and processes.

1. Introduction

In the aftermath of the terrorist attacks in London and Madrid 2004 and 2005, the EU-Directive for Protection of Critical Infrastructure was announced in December 2008 and had to be transposed by the member states not later than January 2011. Critical Infrastructure Protection is about ensuring that services vital to the society continue to function. An EU Critical Infrastructure is an "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." [1] One main goal here is to increase the resilience against all threats and hazards.

2. Legislative Framework for CIP in Austria

On the basis of the European Program on Critical Infrastructure Protection (EPCIP), the Austrian Program for Critical Infrastructure Protection (APCIP) was first published in 2008. Because of several national developments, the second release of the Program was announced in November 2014, which is currently worked with.

The main principles of Austria's Program with the strategic goal of enhancing resilience of Critical Infrastructure are the following:

- Operator based approach
- Subsidiarity and voluntary commitment of private industry
- Complementarity
- Confidentiality
- Cooperation
- Proportionality
- All-harzards-approach

Authorities' responsibilities are regulated in the Security Police Act more in detail, more precisely in Article 22 "Preventive Protection of Legal Interests". According to that, security authorities shall be responsible for offering particular protection to assets of critical infrastructure, like systems for the provision of energy, water, information- and communication technology and health care.

According to Article 55b, employees of these services can be required to undergo a security vetting, if their work responsibility is within a sensitive area in the company. In 2016, an amendment of the Austrian Criminal Code was implemented, where CIP also played an important role.

Article 74 spells the definition of Critical Infrastructure in Austria, which is identical with those of the Security Police Act (Article 22).

In addition, the theft, damage and destruction as well as a cyber-attack against Critical Infrastructure is subject to severe punishment.

The latest legal development took place in October 2016, when the Provincial Program on Critical Infrastructure Protection was published. The main goal of this Program is to identify essential services on a regional level.

3. Implementation of the NIS-Directive in Austria

The EU Directive on security of network and information systems (NIS Directive) [2] was adopted by the European Parliament on 6 July 2016 and came into force in August 2016. Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

A national working group was set up in February 2016 to develop a draft for implementing the directive with a federal law on cyber security. The main goal here was to take the existing national structures, organizations and processes in Austria into account and to implement a law which would be effective and efficient to put into practice.

One point is that the essential services should be closely linked to the existing list on critical infrastructure in Austria. Further, existing organizations dealing with cyber security, like the cyber security center in the Federal Ministry of the Interior, should in future as well be designated as one of the NIS authorities and Single Point of Contact for other member states.

References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The Role of ENISA in the Implementation of the NIS Directive

An overview at EU level

Anna Sarri

Officer in NIS, ENISA
anna.sarri@enisa.europa.eu

Abstract – The objective of this presentation is to provide an overview of the developments in the EU Member States regarding the recently adopted Directive on Security of Network and Infor-mation Systems (the 'NIS Directive') and how ENISA and EC supports Member States to achieve convergence while transposing the NIS Directive into their national laws.

1. Introduction

The NIS Directive aims to bring cybersecurity capabilities on the same level of development in all the EU Member States. Its purpose is to ensure that exchange of information and cooperation related to security amongst Member States are efficient at national and cross-border level. With NIS becoming a requirement, the introduction of specific laws in this area across the European Union will have a significant impact to all industry sectors.

It is essential for all Member States to make sure that they have adopted minimum capabilities to ensure a high level of NIS in their territory and to improve the functioning of the internal market. Commonly defined security measures can support harmonized security practices across EU Member States and potentially enhance the overall level of NIS in the EU.

2. NIS Directive Overview

By imposing a certain number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity *'with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market'.*

The main points of the NIS Directive can be summarized as follows (cf. Figure 1):

- **Improved cybersecurity capabilities at national level:** Each Member State should take actions in the following areas:
    - Adopt a **national strategy on the security of network and information systems** defining the strategic objectives and appropriate policy and regulatory measures.
    - Designate one or more **national competent authorities** for the NIS Directive and a national single point of contact, to monitor the implementation of the Directive at national level.
    - Designate one or more **Computer Security Incident Response Teams** (CSIRTs) for comprehensive incident management nationwide.
- **Increased EU-level cooperation:**
    - Establishes an EU level Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence.
    - Establishes an EU level network of the national CSIRTs and CERT-EU, in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation. ENISA will provide the secretariat of the group.
- **Security measures and incident reporting obligations** for operators of essential services and digital service providers:
    - Identified operators of essential services (OES) and digital service providers (DSP) will have to take appropriate security measures and to notify serious incidents to the relevant national authority

Cooperation Group

ENISA is a member of the strategic Cooperation Group (CG). The European Commission will act as secretariat to this group, which will consist of representatives of the Member States, the Commission and ENISA. The objective of the group is to support and facilitate strategic cooperation among Member States in order to achieve an equal level playing field for all Member States.

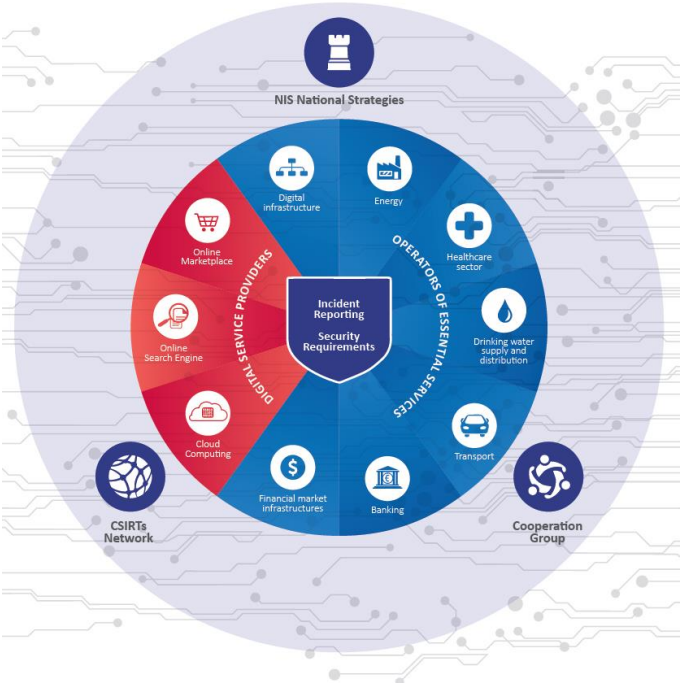

Figure 1: Graphical overview of the NIS Directive

ENISA will assist the cooperation group in its tasks when requested to do so by the members. The Agency will also proactively guide the group by sharing the knowledge and experience gained through the execution of its work programs, but the right of initiative is with the group itself.

Areas in which ENISA is particularly qualified to offer assistance are the following:

- Providing strategic input and support to the Commission and Member States for the definition of minimum security measures and incident notification requirements for OES and DSPs.
- Assisting Member States in the identification of OES.
- Assisting Member States in capacity building.
- Promote sharing of good practices among Member States on specific topics.
- Execute targeted studies on specific topics on behalf of the cooperation group.

National Cyber Security Strategies

The NIS Directive requires Member States to establish and execute a national NIS Strategy. The description of what constitutes such a strategy is largely compatible with the term National Cyber Security Strategy (NCSS) as used by ENISA.

ENISA has worked together with the Member States to develop good practices on how to achieve this and coordinates an active network of Member States that share expertise and knowledge on good practices in this area. Currently 27 Member States have a national cyber security strategy. For this reason, the Agency expects to continue supporting Member States in their efforts to define, implement and maintain the national NIS Strategies referred to by the NIS Directive. Till today ENISA has published guidelines on how to design and implement a strategy, how to evaluate a strategy, how to create effective PPPs and governance models for CIIP.

Security measures

ENISA supports the Cooperation Group in order to provide guidance to operators of essential services covering the 7 sectors (Energy, Transport, Banking, Financial Market Infrastructures, Health, Drinking Water Supply & Distribution, Digital Infrastructures) referred to in ANNEX II of the NIS Directive. The guidance will portray the security measures that the OES need to implement in order to achieve a minimum adequate and converged level of security in networks and information systems.

ENISA's contribution will contain a list of security measures, categorized in broader security domains and objectives and ranked in sophistication levels depending on their complexity and effectiveness. Additionally, Risk Assessment and Management methodologies will be presented, along with the respective Audit Standards and Frameworks that could be of use to any of the OES.

Identification Criteria

According to the NIS Directive, 'Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services. In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States'.

ENISA assists the Member States by providing guidelines and good practices of methodologies that allow the identification of operators of essential services. In addition, ENISA contributes to the work of the EC and cooperation group for the development of a consistent and coherent approach that all MS will be able to implement based on the requirements and criteria defined in the NIS Directive regarding the OES identification.

Incident reporting

The NIS Directive incident notification requirements refer to the obligation of essential operators to report significant incidents related to the continuity of their services.

ENISA provides the support for the Cooperation Group in defining guidelines to be used by the member states in the transposition process.

In this respect ENISA has undergone a major project this year trying to better understand the specificities of each sector so that the proposed items will be in line with the sectorial developments.

Impact of a Malware Attack on a Utility Network

How a Cyber Incident Affects a Utility Network

Sandra König

Austrian Institute of Technology
sandra.koenig@ait.ac.at

Abstract – Utility networks are becoming more and more interconnected. Especially, there is an increasing number of connections between the physical utility network and the Industrial Control System (ICS) monitoring it. While such systems enhance the level of control over utility networks, they also enable new forms of attacks, including cyber-attacks. Recently, cyber-attacks have occurred more frequently with sometimes significant impact on society. One part of preventing such incidents is to understand how an attacked component influences other parts of the network. Here we illustrate how a stochastic model helps to estimate the damage in the utility network due to a cyber-attack. Further we determine optimal ways to protect a system against such attacks based on a game theoretic model.

1. Introduction

During the last years the number of cyber-attacks with significant impact on society increases. Besides the well-known Stuxnet worm [1], especially the recent ransomware attacks such as WannaCry [2], [3] and Petya (as well as its variant NotPetya) [4] have drawn public attention to malware attacks.

In order to defend against such an attack it is crucial to understand how the malware spreads inside the ICT network but also how such an incident affects the underlying utility network. Most existing models for spreading assume a homogeneous network, an assumption that is violated when working with hybrid networks. Approaches taking into account some heterogeneity such as [5] tend to become very complex. We here apply a spreading model that respects the diversity in a hybrid network but remains relatively simple by grouping connections depending on their properties [6].

Once the malware propagation is described, a game theoretic model allows finding optimal ways to protect a utility network [7]. To this end we look at the situation where a malware attack starts by infection of an employee's personal device, i.e. we consider a BYOD (bring your own device) scenario [8].

2. Analysis of Malware Spreading

In order to analyze the spreading of a malware in a network two ingredients are necessary. First, the topology of the network needs to be known, including a characterization of the connections. This characterization is an essential part since it affects the chances that an infected node transmits this infection to its neighbor. Second, the propagation mechanism of the malware needs to be estimated. Such an estimate is usually based on historical data from reports and experiences.

In this use case we consider an electricity provider that operates a network as shown in Figure 1. We distinguish between social connections (between employees), technical connections (in the actual network) and logical connections (e.g., links between a person and her/his device). Depending on the design of the malware the characteristic of a link may change the likelihood that the malware reaches the neighbor of an infected component.

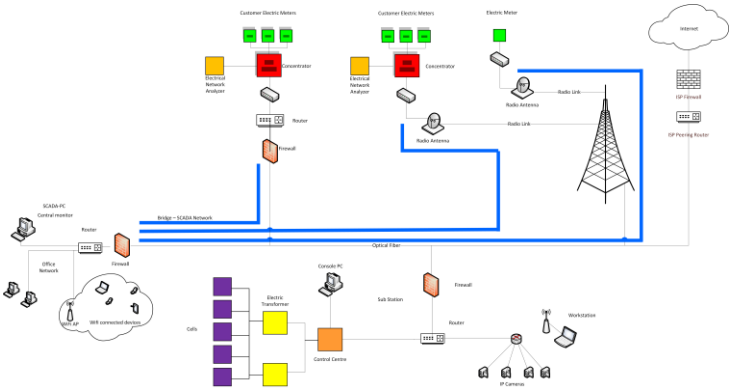

Figure 1: Network diagram of a utility provider

As for the malware itself we focus on a ransomware (such as WannaCry or Petya) that targets the computer system and aims to prevent users from accessing their files. Depending on which components of the network are affected the company may lose customer data as well which in turn may yield to a loss of both money and reputation. Considering a BYOD scenario we assume that the ransomware starts spreading from one specific component (potential starting

points can be identified based on existing threats, see Section 2) and propagates further by either email exchange or by copying itself on the shared network server.

The actual spreading inside the (hybrid) network is assumed to be random due to the many factors that influence the actual transmission. For example, in a spear phishing attack the malware may spread via email and is only activated through user interaction. Whether the user clicks on a link contained in an email also depend on where the message comes from: if he trusts the sender he is more likely to click on the link. On the other hand he may be more cautious if he attended a training event on cyber security recently. So the actual likelihood of transmission depends on the specific malware but also on the connection between two components. Based on this assumption of random spreading we are able to simulate the spreading process and thus estimate the damage in terms of affected components.

3. Analysis of Threats

There exist several ways to start a ransomware attack. Probably the most promising method uses social engineering by sending phishing emails to employees or placing infected USB sticks near a company building. Further, an attack can be launched by attacking the shared file server, which is used to exchange files, the SCADA server, which collects information from the underlying utility network (e.g., the concentrators) or the camera server, which records information from field sites.

In a game theoretic model these possible attack vectors constitute the following attack strategies:

- Send spear phishing email
  We here consider three different cases depending on the level of education (high/average/low) of the employee as we assume that more educated people are less likely to respond to such an attack
- Infect shared server
- Infect SCADA server
- Infect camera server
- Infect USB stick and place it near a company building
  This attack may target an engineer using a maintenance laptop in order to interrupt maintenance services

On the other hand the utility provider identifies countermeasures that may help minimizing the damage in case of an attack. These include existing defense mechanisms and new options (as well as the current state of the network to measure the benefit of each countermeasure).

Technically speaking we end up with the following defense strategies:

- Current state of network (no changes)
- Train employees (annually, every two years or only new personal)
- Backup data (weekly, monthly or yearly)
    - On a local system (e.g. file server)
    - On a remote system (e.g. cloud service)
    - On external media (e.g. CD, DVD, USB flash)
- Patch devices (automatically, yearly or apply only major updates)

Having identified both attack and defense strategy it remains to estimate the damage for each scenario. This is done by applying the simulation described in section 1 and by collecting expert opinions where simulation is not applicable (e.g. for the costs caused by a specific defense strategy). Once this is done, a generalized game theoretic model [7] yields an optimal way to protect the system against these identified attacks. We illustrate how such a solution looks and how it can be put into practice in the next section.

This framework additionally allows optimization of several goals simultaneously. In case of a utility provider such goals typically include minimization of data loss, minimization of monetary loss and minimization of reputation damage.

4. Results

The analysis of a malware attack can conveniently be computed in a software such as R. Simulating the propagation through a network is straightforward [9] and the game theoretic analysis described can be done by using the 'HyRiM' R package [10].

For the use case described above, the algorithms yield a Nash equilibrium as shown in Table 1 where the strategies not listed are assigned a frequency of zero.

Strategy	Train yearly	Train every 2 years	Weekly remote backup
Relative Frequency	0.05	0.61	0.34

Table 1 Nash equilibrium for security game

The result of the theoretical analysis to protect the system optimally against the considered attacks should be understood as follows. The utility provider should apply only the three strategies listed in Table 1, each with the corresponding relative frequency. That is, in 61% of the time all employees shall attend one training course every two years, with only 5% of the

time used in annual training. In the remaining 34% of the time a weekly remote backup shall be applied.

As long as the overall frequencies correspond to the optimal solution, the defender can randomly choose the order in which these strategies are enforced. In this sense, the solution has a certain degree of freedom as if one strategy cannot be applied at some point in time (e.g., due to the absence of an employee) it can be postponed and another defence mechanism can be used instead.

Further, the analysis yields a likelihood for each attack (i.e., an optimal strategy for the attacker). However, the actual behavior of the attacker does not influence the defense strategy of the utility provider since any deviation from the optimal attack strategy causes less damage as long as the defender sticks with his optimal strategy.

Acknowledgements

This work was supported by the European Union Seventh Framework Programme under grant agreement no. 608090, Project HyRiM (Hybrid Risk Management for Utility Networks).

References

[1] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” 2011, pp. 4490–4494.

[2] CERT, “Indicators Associated With WannaCry Ransomware,” 2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-132A. [Accessed: 08-Aug-2017].

[3] C. Cimpanu, “WannaCry Ransomware Infects Actual Medical Devices, Not Just Computers,” *Bleeping Computer*, 19-May-2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/wannacry-ransomware-infects-actual-medical-devices-not-just-computers/.

[4] CERT, “Petya Ransomware,” 2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-181A. [Accessed: 08-Aug-2017].

[5] J. C. Miller, “Bounding the size and probability of epidemics on networks,” *J. Appl. Probab.*, vol. 45, no. 2, pp. 498–512, Jun. 2008.

[6] S. König, S. Schauer, and S. Rass, “A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks,” in *Secure IT Systems: 21st Nordic Conference,*

NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings, B. B. Brumley and J. Röning, Eds. Cham: Springer International Publishing, 2016, pp. 67–81.

[7] S. Rass, S. König, and S. Schauer, "Uncertainty in Games: Using Probability-Distributions as Payoffs," in *Decision and Game Theory for Security: 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015, Proceedings*, M. Khouzani, E. Panaousis, and G. Theodorakopoulos, Eds. Cham: Springer International Publishing, 2015, pp. 346–357.

[8] B. Morrow, "BYOD security challenges: control and protect your most sensitive data," *Netw. Secur.*, vol. 2012, no. 12, pp. 5–8, Dec. 2012.

[9] S. König, S. Schauer, and S. Rass, "A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks," in *Secure IT Systems: 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings*, B. B. Brumley and J. Röning, Eds. Cham: Springer International Publishing, 2016, pp. 67–81.

[10] S. Rass and S. König, "Package 'HyRiM': Multicriteria Risk Management using Zero-Sum Games with vector-valued payoffs that are probability distributions." 2017.

Risk Management for Advanced Persistent Threats

A Water Utility Case Study

Antonios Gouglidis

Lancaster University
a.gouglidis@lancaster.ac.uk

Abstract – The level of sophistication and frequency of cyber-attacks in utility networks are on the rise. A rationale behind these observations is the high-level of complexity introduced in the design and implementation of utility networks as a need for fulfilling operational requirements, such as support of legacy devices, etc. The increased complexity results eventually in introducing vulnerabilities, and thus more threats. One of the most concerning type of threat is advanced persistent threats (APT). An APT usually refer to a sophisticated, targeted, and costly attack that employ multiple attack vectors to gain access to the target system, operate in stealth mode when penetration is achieved and capture and exfiltrate data or cause failures. In this presentation, we demonstrate how a set of processes developed in the context of HyRiM's risk management framework can assist in minimising the damage caused to a utility organisation in the threat of an APT.

1. Introduction

Advanced Persistent Threats (APTs) naturally respond to the increasing diversity of security precautions by mounting attacks in a stealthy and equally diverse fashion to remain *under the radar* for as long as it is required, and until the target system has been compromised. They combine a variety of different attack vectors ranging from social engineering to technical exploits that are being tailored to and optimised for specific organisations, their information technology (IT) network infrastructure and the existing security measures therein. In particular, the application of social engineering in the opening stages of an APT lets the attacker bypass many technical measures like intrusion detection and prevention systems, to efficiently (and economically) get through the outer protection (perimeter) of the IT network. Thus, countermeasures may then come too late to be effective any more, since the damage has already been caused by the time the attack is detected. The diversity and usual stealth of APTs

turn them into a central problem of contemporary practical system security since the information on the attacks, the current system status or the attacker's incentives are often vague, uncertain and in many cases even unavailable. With regards to their frequency – their number has increased rapidly and numerous related security incidents were reported all over the world [1]. With regards to their propagation techniques – APTs are focusing not only on a single vulnerability in a system (which could be detected and eliminated easily), but are using a chain of vulnerabilities in different systems to reach high-security areas within a company network. In this presentation, we apply processes developed within the HyRiM risk management framework to ensure certain goals are met under the threat of an APT. The HyRiM risk management approach is preventive in the sense of estimating and minimising the risk of a successful APT from the beginning.

2. Case Study Description

In this case study, we examine a water utility organisation that provides its services to more than hundred municipalities in its region. In the following, we provide further information with regards to its water department, which will be considered throughout our case study. The water department is focused on the water quality. And is responsible for the planning, building and maintenance of the whole water network. To ensure a sustainable water quality, the company has its own institute for water-processing, sewage-cleaning and research. The management of generation, storage and delivering is supported by an Industrial Control System (ICS). After analysing the network of the utility organisation, we compiled the collected data and prepared a high-level network architecture of the organisation's network and elaborate on its main characteristics and security posture.

3. Risk Management Processes

The first process in the risk management framework is to establish the context. This includes the definition of objectives that should be achieved and attempts to understand the external and internal factors that may influence the goals. Thus, this summarises a description of the external and internal environment of the organisation. In the examined case study, we are mostly concerned with the following goals:

- Minimise the damage that can be caused by an attack to the provided service. The service is related with the provision of water;
- Minimise monetary damage caused by an attack, which may be of technical (e.g. substitute devices), of legal nature (e.g. fines), or of any other cost-related damage;

- Minimise reputation damage caused to the organisation as a result of an attack. E.g. an organisation may lose reputation when consumers start to disbelieve in it [2].

Assuming the above goals, several steps are considered in the subsequent risk management processes to ensure that are achieved adequately. This included a Purdue-model-based analysis, where the details of the teams responsible for operating and maintaining systems used to support core OT functions are covered. We examined existing systems, devices, and employees across all six levels. Covering a broad range of devices, from sensors to servers, prevented any in-depth analysis, yet allowed for a high-level view of security in a more holistic sense.

A subsequent process is that of risk identification. This involves the application of systematic techniques to understand a range of scenarios describing what could happen, how and why. Therefore, the infrastructure within the scope of the risk management process needs to be defined, including technical assets, organisational roles and individual personnel as well as their interdependencies. Based on that, potential vulnerabilities and threats were identified.

Furthermore, we required to conduct a vulnerability assessment of the devices and systems. However, to avoid any service interruptions on the actual utility network we argue instead to conduct a vulnerability assessment of devices and systems installed in our ICS test-bed [3]. This eventually helped us to identify the likelihood of vulnerabilities of devices/systems in an emulated environment, and thus avoid any privacy and security concerns with regards to the actual infrastructure of the participant organisation. The estimation of likelihood values for the vulnerabilities was discovered through the CVSS exploitability metric. The result of this analysis will be combined with additional semantic information, using the Purdue model. This process resulted in mapping likelihood values of vulnerabilities with elements of a network/system diagram, as depicted in Figure 1. Vulnerabilities were looked for on the SCADA server, management servers, network switches, controllers, Human Machine Interfaces (HMIs) and media convertors.

During the next process of risk analysis, we developed an understanding of each risk, its consequences and the likelihood of these consequences. In general, the level of risk is determined by taking into account the present state of the system, existing controls and their level of effectiveness. Since an APT attack is considered to be highly sophisticated, we can assume that the attacker can obtain information about the structure and the various devices of the network of the utility provider. Thus, such an attack can be tailored to the specific company and aims to exploit existing vulnerabilities. However, it can be argued that in such an attack the likelihood for it is more difficult to estimate. Generally, the applied model can work with different types of data, e.g., with vulnerability assessments such as CVSS. Still, in case of an APT these likelihoods are fraught with uncertainty since we only have limited knowledge about the attacker. Thus, the most feasible approach is to ask as many experts as possible, compile an empirical distribution and then aggregate the received information to a single

number [4]. Figure 1 depicts consolidated information, including the various components of the OT network, main systems in the IT network that may provide access to the process network, as well as the likelihood of an APT to propagate from one system/device to another. Thus, it provides an understanding of the major risks and gives an indication for potential attack vectors and attack paths.

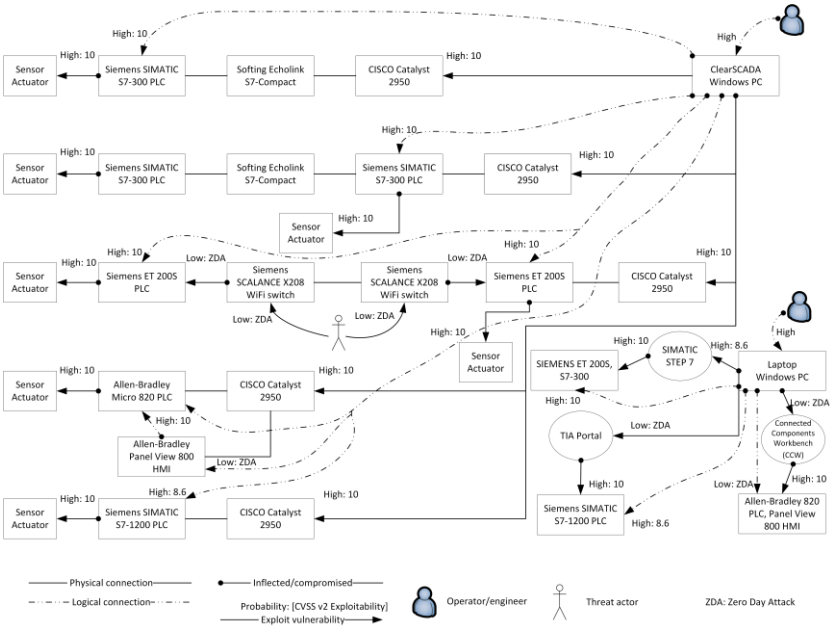

Figure 1: High-level view of OT data-flows.

A first attack vector may include a social engineering attack on the operator of the SCADA server. This may include sending to the operator a spear-phishing e-mail that is read on the server, or the operator to insert an infected USB removable device on the server. In both cases, a malware will be automatically executed on the host machine and try to scan the network for weak points, gain access to them and escalate. Another attack vector would be to conduct a social engineering attack on an engineer of the organisation or on an external partner who can visit the various field sites. In these cases, the laptop should be physically connected to a device to perform any required maintenance operations. The attack vector assumes the user of the laptop to be deceived to install a malware on it. Subsequently, when the laptop is connected on a device of the OT network, the APT may propagate and escalate to cause damage. A threat actor can attack the WiFi switches located in OT network of the organisation. This

would require either to exploit a zero-day vulnerability or try to decrypt the password through brute-forcing or rainbow tables.

Assuming the above attack scenarios, we examined the following defence strategies implemented in various frequencies: Status Quo (do not change anything); train employees; password change policy; update systems; apply patches/replace devices; manual checking of water. The damage is assessed by experts on a 5-tier scale, i.e., *'very low'*, *'low'*, *'medium'*, *'high'* and *'very high'*. Each expert is asked to estimate the damage in a set of scenarios. This may result in either collecting or not an estimation from an expert, with the latter being the case for the expert to refuse to provide information. In our case study, four experts were asked to estimate the damage for three goals, i.e., minimise the down-time of a service, minimise monetary damage and minimise reputation damage. Depending on the goal, an APT may have different optimal attack strategies. These are illustrated in the three lower rows of Figure 2 (each labelled with the corresponding goal) together with the likelihood for the damage to the defender in case this optimal strategy is applied (and the defender also follows his optimal strategy).

When thinking in terms of service disruption, it may cause maximal damage by mainly choosing attack vector `Operator -> ClearSCADA/Windows PC -> Siemens SIMATIC S7-300 PLC -> Sensor/Actuator` (approximately 48% of time) and attack vector `Threat actor -> Siemens SCALANCE X208 WiFi Switch -> Siemens SIMATIC ET 200S PLC -> Sensor/Actuator` (approximately 46% of time), occasionally applying attack vector `Operator -> ClearSCADA/Windows PC -> CISCO Catalyst 2950` (approx. 6% of the time) and rarely playing attack vector `Operator -> ClearSCADA/Windows PC -> Siemens SIMATIC ET 200S PLC -> Sensor/Actuator` (less than one percent). With regards to the cost caused to the defender, the APT may cause highest damage when deploying attack vector `Engineer/contractor -> Laptop/Windows PC -> SIMATIC STEP 7 -> SIEMENS S7-300 PLC -> Sensor/actuator` (which got a weight of 99.5% in the mixed equilibrium), while for the reputation, the APT, is aiming to mix between attack vector `Operator -> ClearSCADA/Windows PC -> Siemens SIMATIC ET 200S PLC -> Sensor/Actuator` (58% of the time), attack vector `Engineer/contractor -> Laptop/Windows PC -> SIMATIC STEP 7 -> SIEMENS ET 200S PLC -> Sensor/actuator` (26% of the time) and attack vector `Threat actor -> Siemens SCALANCE X208 WiFi Switch -> Siemens SIMATIC ET 200S PLC -> Sensor/Actuator` (14% of the time) and rarely choosing attack vector `Operator -> ClearSCADA/Windows PC -> Siemens SIMATIC S7-300 PLC -> Sensor/Actuator` (2% of the time). Since the APT may deploy several attack vectors in parallel, it might be able to choose its strategies according to all three equilibria so that it will not

deviate from the optimal behaviour, which in turn causes higher damage to the defender. On the defender's side, the organisation should apply the optimal defence strategies to protect against an attack strategy by an APT. Specifically; the defender shall apply only the five strategies listed in the corresponding relative frequency identified per se. To this extend, in 2.8% of the time all employees shall attend an annual training course, with only 1% of the time used in training new personnel. In 88.3% of the time major updates of computer systems shall be applied. With regards to patching devices such as PLCs or HMIs, this is done upon failure in 0.2% of the time, while in 8.6% of the time patches shall be applied on devices with known major vulnerabilities.

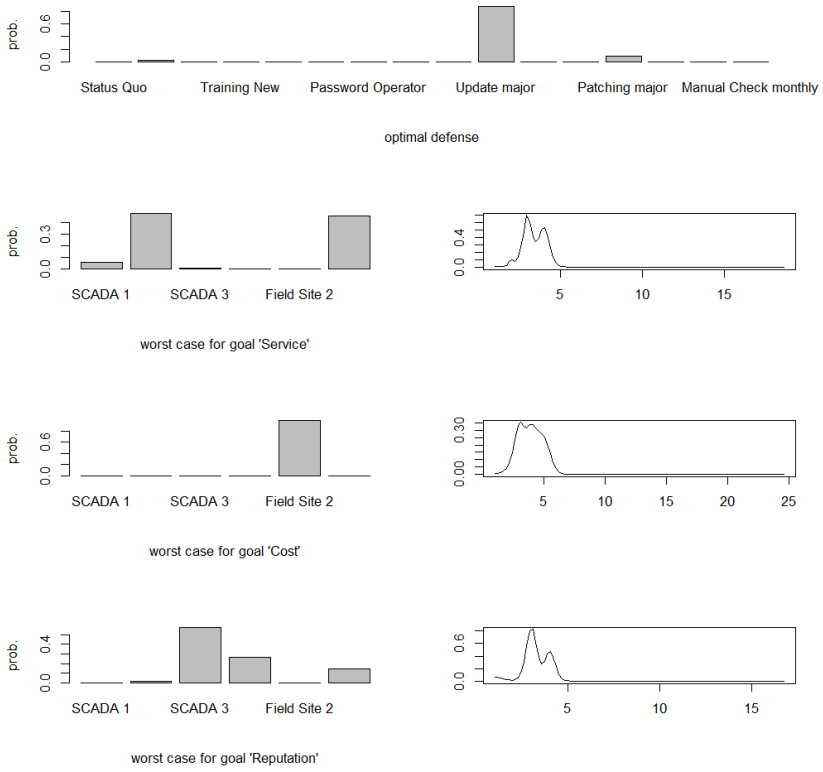

Figure 2 High-level view of OT data-flows.

4. Conclusion

In this presentation, we elaborated on a water utility case study and demonstrated how the risk management framework defined in HyRiM can be of benefit when applied in utility organisations. The application of the framework on the water utility organisation resulted in defining optimal protection strategies against an APT, and eventually improving its security posture. Specifically, the analysis showed that – based on the data provided by the experts – many of the identified defence strategies do not contribute in reducing the damage to the organisation given the identified set of attacks. The relative frequencies of application of the selected five defence strategies have been determined by a generalised game-theoretic framework and the worst-case damage has been estimated for each security goal.

Acknowledgements

This research work has been conducted by Antonios Gouglidis (Lancaster University), Sandra König (AIT), Benjamin Green (Lancaster University), Stefan Rass (Universität Klagenfurt), Stefan Schauer (AIT), Karl Rossegger (Linz AG Telekom) and David Hutchison (Lancaster University). The research leading to these results has received funding from the European Union Seventh Framework Programme under grant agreement no. 608090, Project HyRiM (Hybrid Risk Management for Utility Networks).

References

[1] Zetter, K. (2016). Everything we know about Ukraine's power plant hack. Wired.

[2] Busby, J. S., Gouglidis, A., Rass, S., & König, S. (2016, October). Modelling security risk in critical utilities: The system at risk as a three player game and agent society. In Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on (pp. 001758-001763). IEEE

[3] Green, B., Paske, B., Hutchison, D., & Prince, D. (2014). Design and construction of an industrial control system testbed. In PG Net-The 15th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting.

[4] König, S., Rass, S., Schauer, S., & Beck, A. (2016). Risk propagation analysis and visualization using percolation theory. Int. J. Adv. Comput. Sci. Appl.(IJACSA), 7(1).

Demonstrations

Simulation of a Malware Attack

Propagation and Optimal Defense

Sandra König and Manuel Warum

Austrian Institute of Technology
{sandra.koenig; manuel.warum}@ait.ac.at

Abstract – Analysis of security incidents such as a malware attack is often supported by simulations of the attack on a given infrastructure. Here, we present a tool which allows modeling an organization's infrastructure network and simulating the propagation of an incident through that network based on a mathematical model (i.e., Percolation theory). Furthermore, several potential attack vectors together with corresponding security measures can be analyzed and the tool will present a set of actions to optimally protect the system against such an attack.

1. Introduction

Protection against a malware attack requires a deeper understanding of these attacks and their consequences. This can be achieved by simulating the spreading process, providing an estimation of the damage as well as an estimation of the time until a specific component is infected. Based on the estimated damage, optimal protection measures can be selected by applying game theoretic algorithms. As a byproduct, an upper bound for the expected damage can be computed. In this way, the tool presented here supports risk managers of different organizations analyzing and treating specific risks. We illustrate the application of the tool by modelling a malware attack on a utility network.

2. Simulation of Incident Spreading

The tool allows visualizing the effect of compromised elements within an inhomogeneous infrastructure. To that end, the user has the capability to draw his network as a directed graph, representing ICT, SCADA or utility components but also employees as nodes. The connections between these nodes are modelled as edges pf type "social", "logical" or "network". These networks can be saved and loaded as JSON (JavaScript Object Notation) files. This

approach also makes it easier to use external tools to automatically generate network diagrams, which is the recommended approach for very large networks that cannot be reasonably generated or maintained by hand.

For a utility provider, the network may look as shown in Figure 1. The nodes represent devices and employees using these devices with different connections between them.

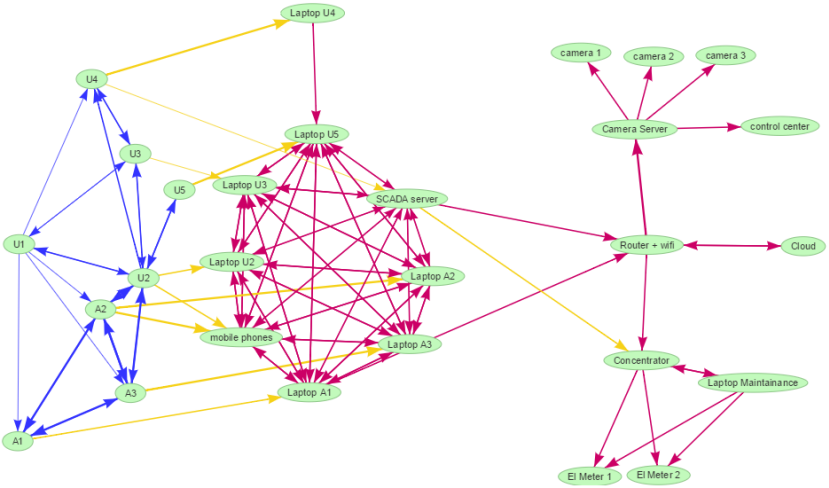

Figure 1: Example for a network modelled with the HyRiM tool. Blue edges are used for social connections, yellow edges for logical connections, and magenta edges for network connections.

In order to simulate the effect on an infection of components as described in [1], the user needs to define propagation probabilities for all type of connections. To make this assessment easier (and more realistic), these probabilities are determined for different levels of trust (namely, "low", "medium" or "high"). Additionally, nodes have a criticality property ranging from "low" to "high" that represents its importance. These values may vary for different goals to reflect that some nodes are more vital to the operation in some contexts than in others. Further, the user should define a mapping from the number of infected nodes of various criticalities to an ordinal damage scale ranging from 1 (not critical) to 5 (very critical).

Once the network is described, the propagation of an incident (e.g., an infection with malware) can be simulated. For this purpose, the user can select any node in the graph and mark it as infected. The user can now either run a single simulation where the process of the infection spread can be inspected on a logical timeline, where each step of the infection can be followed.

To get a more thorough impression of which nodes have a higher tendency for infection, any number simulations can be run in parallel (cf. Figure 2).

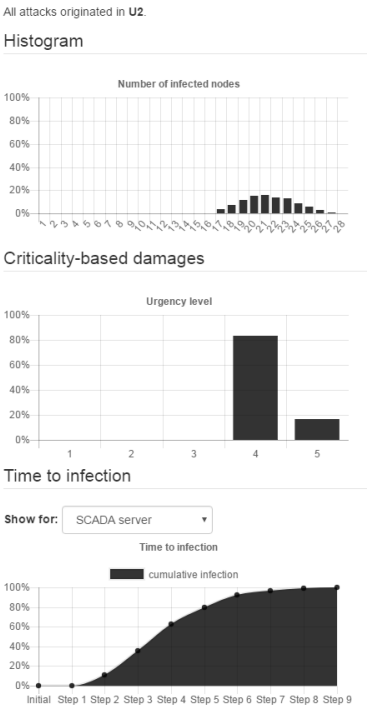

Figure 2: Evaluation of parallel running simulations with regards to spread, urgency, and infection time for individual components of the modelled network.

3. Choosing Optimal Protection Measures

Even though the simulation of the spreading provides some information about the consequences of an incident, this does not directly show how to protect best against such an attack. Therefore, the following information is needed:

- All attack strategies, characterized by their starting point in the network
- All defense strategies, characterized by how they change the transmission likelihoods

By default, the first defense strategy represents the status quo to measure the difference due each of the other defense strategies (cf. Figure 3).

In case of a malware attack, potential attack strategies involve employees using their private devices at work (i.e., a BYOD scenario [2]) or an attack on a shared server. In this context, potential defense strategies involve providing awareness training for employees in order to reduce the probabilities of responding to a spear phishing attack and thus reduce the transmission likelihood. For further details see section "Invited Talks", article "Impact of a Malware Attack on a Utility Network".

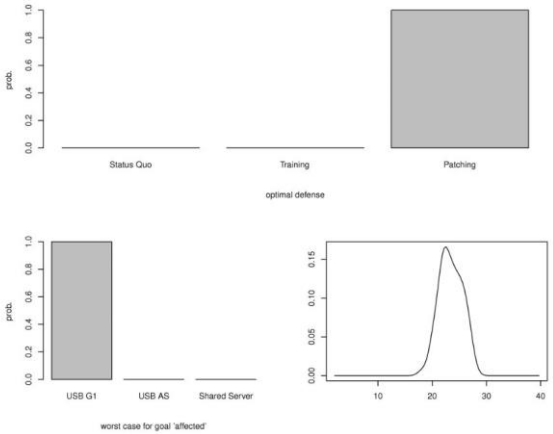

Figure 3 Optimal defense strategy (on top) and worst case attack with estimated damage in this situation (below).

For each combination of an attack and a defense strategy, the damage (loss) in this scenario needs to be estimated. Due to the uncertainty contained in such estimation, this is conveniently done using histograms. These histograms follow the same mapping to an ordinal scale as described above. The resulting payoff matrix characterizes a (generalized) game; the corresponding Nash equilibria are computed as laid out in [3]. For this purpose, the histograms calculated during the previous step are submitted to an OpenCPU-powered server for further calculations. For security reasons, the data transmit during this process only contains raw histogram numbers and as such does not send any confidential or critical information that would allow potential eavesdroppers to obtain information about the network's structure.

The result from this analysis is twofold. First, it provides an optimal defense strategy to the risk manager. Second, it returns the worst case damage if the risk manager applies the identified optimal strategy, that is, whatever strategy the attacker is using (out of the set of potential

attack strategies identified earlier) the damage to the organization is upper-bounded by the given loss distribution.

Acknowledgements

This work was supported by the European Union Seventh Framework Programme under grant agreement no. 608090, Project HyRiM (Hybrid Risk Management for Utility Networks).

References

[1] S. König, S. Schauer, and S. Rass, "A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks," in *Secure IT Systems: 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings*, B. B. Brumley and J. Röning, Eds. Cham: Springer International Publishing, 2016, pp. 67–81.

[2] A. Scarfo, "New Security Perspectives around BYOD," in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*, 2012, pp. 446–451.

[3] S. Rass, S. König, and S. Schauer, "Uncertainty in Games: Using Probability-Distributions as Payoffs," in *Decision and Game Theory for Security: 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015, Proceedings*, M. Khouzani, E. Panaousis, and G. Theodorakopoulos, Eds. Cham: Springer International Publishing, 2015, pp. 346–357.

The MITIGATE Risk Assessment System

Armend Duzha

Maggioli Group
armend.duzha@maggioli.it

Abstract – The ICT systems that control ports' supply chains (SCs) and their operations are at risk. Damages caused by cyber-attacks have been increasing in the recent years. Multidimensional, dynamic and collaborative risk management (RM) methodologies and tools targeting ports' IT infrastructures are needed. Motivated by these limitations, we have developed and are validating a novel RM system (i.e., MITIGATE), which empowers stakeholders' (e.g., port security operators, port facility operators, shipping agent, customs, policy makers, and other supply chain participants) collaboration for the identification, assessment and mitigation of risks and related cyber-threats associated with ports' assets and MSC processes/sub-processes. The MITIGATE system is compliant with prominent security standards and regulations for the maritime sector, i.e. ISPS, ISO 27001, ISO 27005, ISO 28000 etc.

1. System Overview

The objective of MITIGATE is to realize a radical shift in risk management methodologies for the maritime sector towards a collaborative evidence-based Maritime Supply Chain Risk Assessment (MSCRA) approach that alleviates the limitations of the state-of-the-art risk management frameworks. To this end, we have developed and are validating a dynamic, collaborative, standards-based RM system for port's IT Infrastructure, which considers all cyber-threats arising from the international Maritime Supply Chain (MSC), including threats associated with ports' IT infrastructures interdependencies and associated cascading effects.

The RM system enables port operators to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from the international MSC. In this way, port operators are able to predict potential security incidents, but also mitigate and minimize consequences of divergent security threats and their cascading effects based on evidence associated with simulation scenarios and security assurance models.

MITIGATE emphasizes the collaboration of various stakeholders in the identification, assessment and mitigation of risks associated with the cyber assets and MSC processes/sub-processes. This collaborative approach will boost transparency in risk handling by the various stakeholders, while at the same time generate unique evidence about risk assessment and mitigation. The collaborative approach is empowered by an Open Risk Assessment Simulation Environment (ORASE) which enables the participants in the international MSC to model, design, execute and analyze attack-oriented simulation experiments using novel simulation processes. Particular emphasis is paid on the estimation of the cascading effects, as well as on prediction of future risks (on the basis of common metrics across sectors). Based on evidence-based simulations, port operators, decision makers and other stakeholders are able to select cost effective countermeasures and compile holistic port security policies going beyond the port's IT infrastructure isolated domain, but also to ensure the MSC security. Furthermore, the system is equipped with real-time decision support systems, which aims at automating the process of estimating risk and enacting risk mitigation measures. MITIGATE integrates also open source intelligence data, including data from social media (e.g. Twitter, Reddit, and RSS feeds) and trusted sources (e.g., NIST National Vulnerability Database), towards enhancing its threat assessment and prediction functionalities.

2. High Level Architecture

MITIGATE aims to provide a holistic solution regarding risk management in the frame of Maritime Supply Chain Services (MSCSs). To do so, several services have to be provided such as collaborative risk management, advanced simulation and visualization of potential cyber-attacks, open intelligence services etc. In order to archive this, we have formulated a high-level architecture that comprises eight (8) coarse grained components that complement each other. These components include:

- the Asset Modelling and Visualization component that allows users to declare their assets along with the cyber relationship and serialize this declaration in a strict format. Each organization that participates in the MSC will use this component in order to create its own mapping, which will be automatically linked to available vulnerabilities/threats and attack-types that are relevant to the individual assets declared.
- the Maritime Supply Chain Service Modelling component that allows users to model the MSCSs that are performed by their organizations, while also allowing to provide the mapping of existing cyber assets with the various processes and sub-processes that are defined in the context of MSCSs.
- the Simulation and Game Theory component that is responsible for the discovery of attack paths given a specific asset mapping and a specific MSCS and the calculation

of the best defensive strategy regarding the protection of a specific asset based on the game theoretical principles.

- the Collaborative Risk Assessment component that is responsible to guide the user to perform the appropriate steps that are required for the conduction of the risk assessment for a specific MSCS as defined in the MITIGATE Methodology. This component offers all supportive features required for an error-free execution of the methodology.
- the Open Intelligence and Big Data Analytics component that is responsible to provide near real-time notifications regarding potential vulnerabilities related to the assets of one organization that participates in the MSC. These notifications will be generated through the text-processing of open sources (e.g. Twitter, Reddit, and RSS Feeds). However, such mining techniques are extremely computational intensive; thus, the component will rely on a big-data framework (SPARK [3]) in order to achieve linear scalability.
- the Notification and Reporting component that is responsible to provide push notifications to the user regarding any type of messages are published in the pub/sub queue (such as the conduction of a vulnerability assessment, the calculation of risks, the processing of an open source information etc).
- the Administration component is responsible for the management and the consistency of the various 'enumerations' that are required by all the other components. Such enumerations include mainly vulnerabilities, attack-types and business partners. This component also implements the semi-automated update of these enumerations from open sources.
- the Access Control and Privacy component provides security guarantees in a horizontal manner to all the other components. More specifically, since the information that is provided and processed (e.g., asset cartography, attack paths, risk calculations etc) is extremely sensitive, the specific component undertakes the responsibility of implementing the appropriate authentication, authorization and encryption schemes that are required in order to protect MITIGATE services and data end-to-end.

The architecture is complemented by a persistency layer and a pub/sub system. The persistency layer consists of two types of databases; one relational (MySQL) that is used to store fully structured data and one NoSQL (MongoDB) that is used to store semi-structured data that change frequently (e.g., vulnerability reports). The pub/sub system (ActiveMQ) is used to decouple the communication of the components and more specifically to eliminate any blocking communication that may be required. Elimination of blocking communication is a prerequisite for the creation of scalable system.

Simulating Physical Intrusion Attacks in Critical Infrastructures

OMNeT++ simulation framework to assess surveillance strategies against physical intrusion attacks in critical infrastructures

Mohamed Amine Abid and Hermann de Meer

Faculty of Computer Science and Mathematics
University of Passau
{amine.abid, hermann.demeer}@uni-passau.de

Abstract – Surveillance technologies represents a standard practice for protection of critical infrastructure systems such as utility networks. Although surveillance systems may be in place and operating within a utility provider's premises, they are prone to technical as well as organizational failures resulting in a fluctuating performance. Furthermore, several emergency and unforeseen events such as human errors can significantly impact the effectiveness of specific surveillance activities. To assess the effectiveness of the different surveillance (defense) strategies, we may need an easy, costless, and efficient methodology, to be used to evaluate present and future strategies to be deployed. In our case, we propose to relay on simulation as a best alternative for critical infrastructure managers to master costs and time. For that, we developed a tool that simulates realistic physical intrusion scenarios, and assess the effectiveness of the deployed defense strategies.

As a demonstrative scenario, we will use the actual setup given within a critical infrastructure. For reasons of simplicity, we will focus solely on the use of security guards, who are controlling the area. Taking the details of the physical infrastructure (buildings, roads, etc.) as well as personnel requirements (working hours, available number of guards, etc.) into account, we will run various scenarios of real-life attacks and defense strategies. The tool will provide us with measurements of various key performance indicators to compare the different deployed strategies.

1. Introduction

Critical infrastructures are physical or virtual assets that are essential for the functioning of a society and economy. The destruction of such systems and assets can adversely affect security, national economy, public health and safety. Most countries identify the following critical infrastructures: telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services and emergency services [1]. Critical infrastructures interact at multiple levels to enhance their overall performance. These interactions often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries. Therefore, these organizations constantly tend to extend beyond their physical perimeters to include other entities such as vendors, business partners, service providers or even costumers into their premises. Thus, access to the facilities is not only allowed to regular employees but further to external entities inside the workplace, such as temporary workers, interns, independent contractors and subcontractors, or even visitors. Broadly speaking, all these entities need an easy access to their workplaces. Therefore, surveillance and access control technologies are mostly deployed at the outer layer of the infrastructure system to ensure the efficient movement inside the facility.

Although surveillance systems may be in place and operating within a critical system's premises, they are prone to technical as well as organizational failures. For example, security badges might be stolen without notification to the security personnel or without revoking them in a timely manner. Moreover, badges issued to employees, who no longer work for the company, or to temporary visitors and workers might not always be recovered before leaving the site. This might give adversaries the possibility to exploit these circumstances to gain easy access to facility. As a consequence, the perimeter-centric physical security measures such as traditional surveillance technologies (e.g., Closed Circuit Television (CCTV) systems or entry access control solutions) that use static surveillance devices mounted at specific locations are not adequate to detect and prevent such potential intruders [2].

Such a dynamic nature makes it very hard to predict the effectiveness of any surveillance strategy. Besides, running real-life attack scenarios in a large scale turns to be very costly and different from a real due to the absence of surprise factor. Moreover, and to better assess the variability of every attack/defense case, each scenario should be reproduced several times, which makes a real case attack a bad option that needs to be avoided at all costs. In the other hand, simulation seems to be the perfect much for our need: costless, reproducible, insensitive to the lack of the surprise factor, etc.

In this demo, we will present our developed tool based on the INET framework of the OMNET++ simulator, and meant for simulating physical intrusion of critical infrastructures. It allows its user to reproduce the physical layout of the infrastructure, the deployed personnel

and their behavior, and the potential attacks that may occur. The tool allows each scenario to run several times (results can be then presented as distributions). It provides measurements of various key performance indicators such detection rate, privacy, damage and incurred costs, to compare the different deployed strategies. Using these results, one can better assess and compare strategies or even find the optimal inspection strategy.

2. Simulation tool

In this section, we describe our simulation model. We choose to use the INET 3.4 framework, on top of OMNeT++ 5.0 discrete event simulator to integrate our model. Through this model, we need to be able to reproduce a faithful image of the physical environment of our monitored facility. We also have to reflect all the applied policies (zone restrictions, employees' profiles, id check policies, etc.) as well as actors' behaviors (security guard, simple employee, malicious employee or intruder).

The Physical Environment:

Our environment consists in a geographic surface, divided into several zones or areas as described in Figure 1. In this figure, we can observe several zones (like the one framed in red), reachable through a web of ways/paths to follow when moving from/towards any of these areas. These areas represent the smallest level of granularity of our site. Each of which has an attribute, called "security level", indicating the criticality of the respective area.

In our simulation model, we need to be able to describe our site as a set of areas interconnected through paths. With no lack of genericity, we model each area as a convex polygon, $\wp$, whose center of gravity is located at position $p = t_{(x \quad y \quad z)}$, and with orientation (*Euler angles*) $\Theta = (\alpha \quad \beta \quad \delta)$ relatively to a fixed reference frame. All this information describing our set of areas are presented in an XML file, parsed on the run time, to build and render the physical structure of our site.

In the same way, paths are modeled as a non-oriented graph $G = (V, E)$, where V is the set of vertices, and E is the set of edges; just as depicted in Figure 1. Vertices in V represent waypoints, characterized by their geographic coordinates, and corresponding to particular locations in our site, such intersections, area gates, etc. For every couple of vertices $\langle e_i, e_j \rangle \in V \times V$, an edge (e_i, e_j) is added to E if the two waypoints corresponding to our vertices are directly related by a path in the actual map. It is worth mentioning we are assuming that we can only move straight from waypoint e_i, to waypoint e_j if they form an edge (e_i, e_j) in E.

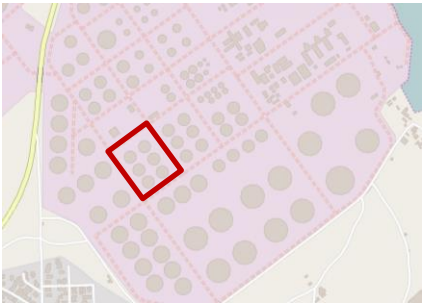

Figure 1: Site map sample

Thus, the more waypoints we create, the more precise we'll be. The advantage of such representation, is that we can define one or more weight functions to help select the best (i.e. optimal or near optimal) way to go from one source point (e.g. the head quarter of a security guard) to another destination point (e.g. the gate of a selected area). Note here that we associated to each area a gate, represented as waypoint (i.e. the blue vertex in Figure 2) in V. Once again, our graph (i.e. V and E sets) is described in an XML file, parsed on the run time, to build and render the physical structure of those paths in our site.

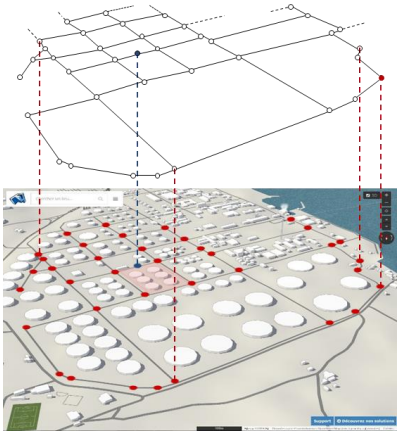

Figure 2: Modeling of paths

Actors:

In our case study, we can identify two main actor categories: Employees and Intruders. An employee could be either a worker or a security guard. They all hold an ID card meaning that they are known to the system. Unlike an employee, an intruder is someone from outside the facility. So, he either don't hold an ID card, has a fake one, or has a stolen card that do not correspond to his biometrics (i.e. finger print or facial photo, etc.). In all these cases, he will not be recognized by the system as a regular employee. Thus, he should be caught at the first ID check, whenever it is done, and wherever he is located inside the facility.

Employees, depending on the job they are supposed to do, are allowed to access some areas of the facility but denied access to some others. This restriction is not always the same for all employees. In our simulation model, we define a set of profiles, each of which indicates a subset of allowed areas. Using an XML file, we assign to each worker one of these profiles, indicating areas he can access. This information is stored in his ID card. Security guards are allowed to access all the areas in the facility. A special profile is then created just for them.

A regular worker is a person who does respect areas' restrictions. He will never access an area not figuring in his profile. Thus, upon a security check, his situation would always be fine. In the other hand, a "Malicious" worker is an employee with a valid ID card, but who intends to physically harm the facility. In our work, we are supposing that such a suspicious behavior consist in targeting areas, probably with high security level, that he is denied to access. During a security check, a malicious worker can only be caught if his is behaving suspicious at that time (i.e. his is in a restricted area when the check takes place).

A security guard owns two main devices: A navigator, and an ID Checker. The navigator serves as a mission scheduler. Checking missions are assigned to a security guard using this device. It first indicates which area a security guard needs to check, shows the way to follow to reach this area, and decides the strategy to be adopted during the ID check. The ID checker is used to verify the identity of an employee. It starts with verifying the ID and the biometrics of the employee. If they match, it verifies whether this employee is allowed to be in the area where the check is performed.

Figure 3 summarizes the hierarchy of actors involved in our simulation. It shows that all of them are able to move in the facility (i.e. they all have a mobility module). Unlike intruders, all employees hold an ID card. Security guards are also equipped with an ID checker and a Navigator devices (they are virtually two separate devices, but could also be integrate into one single physical device). Finally, workers could be of two kinds: regular or malicious.

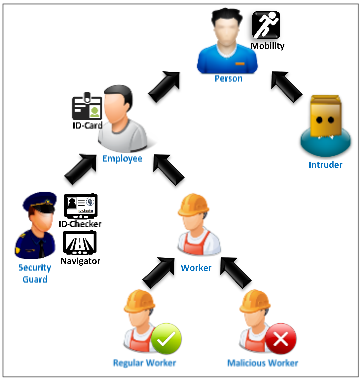

Figure 3: Actors

Acknowledgements

This work was supported by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1).

References

[1] Moteff, J., Parfomak, P.: *Critical infrastructure and key assets: definition and identification*. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2004.

[2] Pang, H., Jiang, L., Yang, L., Yue, K.: *Research of android smart phone surveillance system.*

Research Projects

The Hybrid Risk Management for Utility Networks (HyRiM) Project

Funding Body: European Union (EU), Seventh Framework Programme

Start Date: 1st April 2014
Duration: 3.5 years
Website: www.hyrim.net

Contact Person:
Dr. Stefan SchauerAIT Austrian Institute of Technology GmbH
Center for Digital Safety and Security
Lakeside B10a
9020 Klagenfurt
Austria

Consortium:

1. AIT Austrian Institute of Technology GmbH
2. Universität Passau
3. Lancaster University
4. ETRA Investigacion Y Desarrollo SA
5. Akhela SRL
6. Suministros Especiales Alginetenses Coop V.

7. Linz AG für Energie, Telekommunikation, Verkehr und Kommunale Dienste
8. Alginet Distribucion Energia Electrica Sociedad Limitada

Overview

Risk management is a core duty in critical infrastructures like utility networks. Despite the existence of numerous risk assessment tools to support the utility providers in estimating the nature and impact of possible incidents, risk management up till now is mostly a matter of best practice approaches. Looking at the network-oriented structure, risk management tools are mostly focused on one out of several networks operated by utility providers, e.g., the utility's physical network infrastructure (consisting of gas pipes, water pipes, power lines, etc.), the Supervisory Control and Data Acquisition (SCADA) network and the Information and Communication Technology (ICT) network. Nevertheless, these network types exhibit a significant interaction and therefore risk management methods that focus on just one of these network types might be insufficient.

The main objective of the HyRiM project is to develop a novel risk management approach for identifying, assessing and categorising security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms. In the course of the project, we are focusing on sensitive service parameters representing interconnection points between control networks and individual utility networks, via which a security incident in the ICT or SCADA network may result in cascading effects in the utility network. Due to this particular "hybrid" view of our approach, i.e., the strong emphasis on the interrelation between networks and the corresponding cross-network risks, we refer to our approach as "Hybrid Risk Management" and "Hybrid Risk Metrics".

The risk measures we developed in HyRiM support a quantitative risk analysis as well as simulation tools for decision makers and security specialists in their evaluation of threats. This has a particular significance, since the risk measurement can be in qualitative terms in order to avoid the illusion of "hard facts" based on subjective numerical risk estimates provided by humans. To unify the advantages of quantitative assessment with the ease and efficiency of a qualitative analysis, our framework supports a qualitative assessment with a sound quantitative mathematical underpinning.

Furthermore, we consider "the human factor" in our investigations. As a result of this, the full sociological and economic effects over the different networks are well understood. Special attention will also be paid to scenarios in which personally owned digital/communication devices used in business day to day life compromise the security of a utility control network. Another core topic of interest in this investigation is the combination of monitoring and surveillance of the extended perimeter by triggering "on demand" surveillance by monitoring

events to provide the foundation for novel surveillance mechanisms. We evaluate the identified security measures and Hybrid Risk Metrics in use cases in which various attack scenarios on the control network are considered.

The project provides utility network operators with a risk assessment tool supporting qualitative risk assessment based on numerical (quantitative) techniques. For that matter, our methodology explicitly accounts for a utility provider's manifold nature in terms of diverse network infrastructures. The expected impact is thus a movement away from best practice approaches, towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation. The HyRiM project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

Multidimensional, InTegrated, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTurEs

Funding body: European Union (EU), Horizon 2020 research and innovation programme

Start Date: 1st September, 2014
Duration: 30 month
Website: https://www.mitigateproject.eu/

Contact Person:
Ralf Fiedler
Fraunhofer Center for Maritime Logistics and Services CML
Am Schwarzenberg-Campus 4, Building D
21073 Hamburg
Germany
Email: Ralf.Fiedler@cml.fraunhofer.de

Consortium:

1. Fraunhofer-Center für Maritime Logistik und Dienstleistungen (DE)
2. University of Piraeus Research Center (GR)
3. Austrian Institute of Technology (AT)
4. Gruppo Maggioli (IT)
5. SingularLogic (RO)

6. FEPORTS (ES)
7. University of Brighton (GB)
8. Piraeus Port Authority (GR)
9. I.M.S.S.E.A (IT)
10. Valenciaport Foundation (ES)
11. dbh Logistics IT AG (DE)
12. Port Of Ravenna Authority (IT)
13. North Tyrrhenian Sea Port Authority (IT)
14. Hansestadt Bremisches Hafenamt (DE)

Overview:

The IT infrastructure of the maritime supply chain, and especially ports, is particularly vulnerable, because it is located at the intersection of information flows from many different users and countries, which on account of the continuously increasing digitization of business processes have to offer access and exchange capabilities for digital information. In order to ensure that these processes do not allow malware to shut down operations or allow manipulation of data for illegal purposes, a solution for identifying threats along the maritime supply chain is urgently needed.

The MITIGATE project, which is funded by the European Commission in the H2020 framework, develops a dynamic cloud-based software solution which allows ports, logistics companies or administrations to check the software and hardware assets they use for vulnerabilities regarding the risks for cyber-attacks. The software is based on a thorough analysis of user requirements, actual real-time threats and potential countermeasures. In this context, MITIGATE

- detects vulnerabilities of the IT infrastructure;
- enables to develop optimal security measures;
- uses Social Media to disclose new cyber threats;
- supports collaboration amongst supply chain partners.

Further, MITIGATE examines the cyber security of maritime supply chains, e.g., of liquefied natural gas, container and bulk goods as well as vehicle transport chains.

The main goal of MITIGATE is to realize a shift in risk management methodologies for the maritime sector towards a collaborative evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA) approach that alleviates the limitations of state-of-the-art risk management frameworks. To this end, the project will integrate, validate and commercially exploit an effective, collaborative, standards-based risk management system for port's Critical Infor-

mation Infrastructures (CIIs), which shall consider all threats arising from the supply chain, including threats associated with interdependencies among port CIIs and their associated cascading effects.

Thus, MITIGATE provides a holistic view of the ICT infrastructure required for the provision of the supported SCS spanning across business partners and organization boundaries, in order to identify and evaluate all SC cyber threats and risks within the SC. MITIGATE promotes collaboration between business partners and takes into account the involvement of the business partners in the provision of the SCS under consideration. The methodology by design is compliant with international standards (e.g., from the ISO27k and ISO28k families and ISPS) and capitalizes on them and other well-known and proved guidelines and good practices (e.g., NIST SP800-30), following standardized notations. Beyond the already mentioned standards and guidelines, the g-MSRA approach also builds upon existing risk assessment and security management methodologies and frameworks including the Secure Tropos, CYSM and MEDUSA methodology.

In doing so, MITIGATE ensures the IT-safety and security of international maritime transport chains, and thus the international trade itself, founding on a legislation the countries involved have given themselves.

Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports

Funding body: European Union (EU), Horizon 2020 research and innovation programme

Start Date: 1st May, 2017
Duration: 3 years
Website: https://www.sauronproject.eu/

Contact Person:
Rafael Company
Valenciaport Foundation,
Spain
Email: rcompany@fundacion.valenciport.com

Consortium:

1. The Valenciaport Foundation (ES)
2. The Universitat Politècnica de Valencia (UPVLC) (ES)
3. S2 Grupo (ES)
4. The University of Piraeus Research Center (GR)
5. The AIT Austrian Institute of Technology (AT)
6. Piraeus Port (GR)
7. Thales (FR)

8. Morpho (Safran) (FR)
9. InnovaSec (UK)
10. Livorno Port Authority (IT)
11. KU Leuven (KU LEUVEN) (BE)
12. ETRA (ES)
13. NOATUM (ES)
14. Luka Koper (SI)

Overview:

The numbers 9/11 strike a chord with us all, marking a 'before' and 'after' watershed in our views on security. From that time on, we have all become increasingly aware of the threat of terrorism and many of our nations have witnessed a sea-change in the human and technological resources dedicated to detecting, preventing and countering acts of terrorism.

In the modern era, ports have become lately targets for attacks attracting the attention of terrorism (e.g., ISIS), cyber-hacktivism organizations, militias (e.g. Anonymous, LulzSec) and agencies. In particular, adversaries are able to realize complex threat scenarios for the purpose of disrupting ports' operations or facilitating illegal activities aimed at obtaining financial, political/military or even ideological gain and benefits. Usually, a threat scenario is realized by conducting a combination/series of physical and/or cyber attacks. For example, they are able to steal vehicles from the vehicles terminal of the port or to smuggle illegal material of any kinds (such as drugs, weapons etc) or illegal immigrants, or event to destroy a critical port facility, by locally or remotely disrupting, modifying, interfering or gaining access a variety of information/documentation as well as physical systems.

It should be noted that attacks on the ports' infrastructures cause not only disruption of their services but tremendous damage to the maritime operations, national and EU safety, economies, societies and environment. For example, the environmental effects of the explosion in the ports' LNG storage facilities could significant in terms of thermal radiation, overpressure blast wave and flying shrapnel; an attack on a container terminal management system could disrupt intermodal container services involving maritime, rail and truck transportation; attacks (e.g. bombing) in a dry bulk storage area of coal products may create and carry dust by wind to tourist terminals or nearby residences. According to 2016 estimates by the RAND Corporation and the USA Congressional Research Service, an attack on a ports' CI could cause tens of thousands of deaths and cripple global trade, with losses ranging from $45 billion to more than $1 trillion.

Responding to this new situation, the SAURON project proposes a holistic situation awareness concept as an integrated, scalable and yet installation-specific solution for protecting EU ports and their surroundings.

This solution combines the more advanced physical security features with the newest techniques in prevention, detection and mitigation of cyber-threats, including synthetic cyberspace aspects through the use of new visualization techniques such as immersive interfaces and cyber 3D models. In addition, a Hybrid Situation Awareness (HSA) application capable of determining the potential consequences of any threat will show the potential cascading effect of a detected threat both in the physical and cyber domains.

SAURON can be used to engage with the public in surrounding areas and rescue/security teams will be able to communicate any potential event or situation that could put their safety at risk.

Thus, SAURON proposes as a main objective to ensure an adequate level of both physical and cyber protection for EU ports and to limit, as far as possible, the detrimental effects for society and citizens of a potential combined physical and cyber-attack.

The Smart Grid Protection Against Cyber Attacks (SPARKS) Project

Funding body: European Union (EU), Seventh Framework Programme

Start Date: 1st April, 2014
Duration: 3 years
Website: https://project-sparks.eu/

Contact Person:
Dr Paul Smith
AIT Austrian Institute of Technology GmbH
Centre for Digital Safety & Security
Donau-City-Straße 1
1220 Vienna
Austria
Email: paul.smith@ait.ac.at

Consortium:

1. AIT Austrian Institute of Technology GmbH (coordinator) (AT)
2. Fraunhofer AISEC (DE)
3. The Queen's University Belfast (UK)
4. The Energy Institute at the J. Kepler University Linz (AT)
5. EMC Corporation (IE)
6. KTH Royal Institute of Technology (SE)

7. Landis + Gyr (CH)
8. United Technologies Research Center (IE)
9. SWW Wunsiedel GmbH (DE)

Overview:

The future smart grid represents a significant evolution in the way electric grids function. At the core of this change is an increased use of Information and Communications Technology (ICT) to implement enhanced monitoring and control. This increased use of ICT makes future smart grids vulnerable to cyber-attacks. Ensuring the cyber security and resilience of smart grids was the target of the EU-funded SPARKS – Smart Grid Protection Against Cyber Attacks – project.

The project spent significant effort on analysing and providing guidance on how best practice guidelines and standards for smart grid security, from organizations such as NIST, IEC, and CEN-CENELEC-ETSI, can be applied. The result of this activity is a series of documents that enable smart grid stakeholders to contextualize and apply these resources within their organization. A gap analysis has been performed that can be used by organizations to inform and formulate a position on the future direction of standards for smart grid security.

Cyber security risk management for the smart grid has some specific challenges that stem from the fact that it is a cyber-physical system. Consequently, cyber-attacks can have operational – power systems – consequences, as was seen in the attack that took place in the Ukraine in December 2015. The SPARKS project has developed guidelines and tools to support cyber security risk assessment for the smart grid. For example, approaches to threat analysis, using attack graphs, have been developed, along with a classification of the consequences of cyber-attacks. To support the implementation of these guidelines, a toolchain has been developed and validated using the SPARKS demonstration sites.

Ensuring the resilience of the smart grid, while under attack, is important. This involves detecting and remediating the effects of cyber-attacks. The SPARKS project has developed two cyber-attack detection capabilities that identify malicious activity in Supervisory Control and Data Acquisition (SCADA) communication traffic and in big data that is collected from operational systems. They close an important gap for detecting cyber-attacks to physical systems. These detection capabilities have been coupled with resilient control strategies that rationalize malicious controller input, and mitigate its potential effect on the physical power system. This novel cyber-physical resilience capability was demonstrated in the AIT SmartEST laboratory.

Important field devices, such as smart meters, could be subject to physical tampering. To mitigate this threat, and to have a strong anchor for device authentication, the project has investigated the use of Physical Unclonable Functions (PUFs). This involved developing a

unique PUF array, in terms of its size, that can be used to test designs under adverse environmental conditions. The outcomes of this research have fed into standardization activities and supported the realization of a spinout company.

These scientific and technology advances need to be considered in the context of important social, legal, and economic aspects. An outcome of the project is an exploration of issues regarding the implementation of the Network and Information Security (NIS) Directive for the smart grid. Furthermore, a study of consumer attitudes towards smart grid cyber security was implemented, which provides useful insights when making strategic investments in security technology. Moreover, the project has developed economic case studies that clearly show the socio-economic impact of not implementing cyber security for the smart grid – the aim is to stimulate investment.

All the public deliverables, which summarize these findings, are available on the SPARKS project website (https://project-sparks.eu), including references to the stakeholder engagement events that were organized by the project. This includes the final project symposium, which was held in March 2017 in Vienna, and involved contributions from seven closely-related European projects.

Agenda

Tuesday, September 19th, 2017

Time	Session
09:00 - 10:00	Registration
10:00 - 10:10	**Workshop Opening**
	Welcome Message and Workshop Overview *Stefan Schauer, AIT*
10:10 - 10:45	**Introduction of Research Projects**
	The SPARKS Project *Paul Smith, AIT*
	The MITIGATE Project *Ralf Fiedler, Fraunhofer CML*
	The SAURON Project *Rafa Company, Valencia Port Foundation*
	The HyRiM Project *Stefan Schauer, AIT*
10:45 – 11:45	**Session 1: Risk Management for Critical Infrastructures**
	Risk Assessment for Cyber-Physical Smart Grid Systems *Paul Smith, AIT*
	The MITIGATE Methodology – An Overview *Christos Douligeris, UPRC*
	A Hybrid Risk Management Process for Interconnected Infrastructures *Stefan Schauer, AIT*
11:45 - 12:15	Coffee Break

Time	Session
12:15 - 13:15	**Session 2: Threat Identification and Processing**
	Big Data Analytics and Threat Prediction *Armend Duzha, Maggioli Group*
	Automated Attack Paths Discovery *Michalis Pavlidis, University of Brighton*
	Detection of Cyber-Attacks Against SCADA *Antonios Gouglidis, Lancaster University*
13:15 - 14:15	Lunch Break and Networking
14:15 - 15:45	**Session 3: Physical & Cyber Situational Awareness**
	SAURON: From Physical to Hybrid Situational Awareness *Israel Perez, Technical University of Valencia*
	A Game-theoretic Decision-making Framework for Physical Surveillance *Ali Alshawish, University Passau & Stefan Rass, University Klagenfurt*
	Managed Cyber Security for Protecting Critical Infrastructures *Stefan Beyer, S2 Grupo*
	Is my Grid Bouncing Back? A Cyber-Physical Resilience Metric for Smart Grids *Ivo Friedberg, AIT*
15:45 - 16:15	Coffee Break
16:15 - 17:30	**Session 4: Legislative Frameworks and their Implementation**
	Data Protection and Critical Infrastructures in the EU *Laurens Naudts, KU Leuven*
	Legislative Framework for CIP in Austria *Sylvia Mayer, Federal Ministry of the Interior*
	The Role of ENISA in the Implementation of the NIS Directive *Anna Sarri, ENISA*
17:30	**End of Day 1**
19:30	Social Dinner Restaurant „Zum Leupold“ (Schottengasse 7, 1010 Vienna)

Wednesday, September 20th, 2017

Time	Session
08:00 - 09:00	Registration
09:00 - 10:00	**Session 5: Use Cases and Solutions**
	Impact of a Malware Attack on a Utility Network *Sandra König, AIT*
	Risk Management for Advanced Persistent Threats *Antonios Gouglidis, Lancaster University*
10:00 - 11:30	**Demo Session: Tools and Prototypes from the Projects**
	Simulation of a Malware Attack *Sandra König & Manuel Warum, AIT*
	Simulating Physical Intrusion Attacks in Critical Infrastructures *Amine Abid, University Passau*
	The MITIGATE Risk Management System *Armend Duzha, Maggioli Group*
	Smart SecPlan *Santiago Caceres, ETRA I+D*
	Mobile ID Checks for Physical Infrastructure Protection *Bernhard Strobl & Christoph Weiß, AIT*
11:30 - 12:45	**Panel: Experience Reports on Critical Infrastructure Protection**
12:45 - 13:00	**Closure of the Workshop**
	Concluding Remarks & Farewell *Stefan Schauer, AIT*
13:00 – 14:00	Lunch Break and Networking