European CIIP Newsletter

March 16 - June 16, Volume 10, Number 1

CRITIS 2016
Call for Papers

CYCA Young researcher Competition

ECN

Contents

CIPR Net

> About ECN
ECN is coordinated with
The European Commission, was initiated by Dr. Andrea Servida,
today funded by the European Commission
FP 7 CIP Research Net CIPRNet Project
under contract, Ares(2013) 237254

>For ECN registration ECN registration & de-registration:
www.ciip-newsletter.org

>Articles to be published can be submitted to:
editor@ciip-newsletter.org

>Questions to the editors about articles can be sent to:
editor@ciip-newsletter.org"

>General comments are directed to:
info@ciip-newsletter.org

>Download site for specific issues:
www.ciprnet.eu

>Founders and Editors
Eyal Adar, Founder and CEO, WCK www.wck-grc.com
Christina Alcaraz, University of Malaga, alcaraz@lcc.uma.es
Bernhard M. Hämmerli, HTA, Initiator and Main Editor bmhaemmerli@acris.ch
Eric Luiijf, TNO, eric.luiijf@tno.nl
Erich Rome, Fraunhofer, erich.rome@iais.fraunhofer.de

>Country specific Editors
For France: Michel Riguidel, ENST, riguidel@enst.fr
For Spain: Javier Lopez, UMA, jlm@lcc.uma.es
For Finland: Hannu Kari, HUT, kari@tcs.hut.fi
to be added, please report your interest

> Spelling:
British English is used except for US contributions

Editorial: About the importance of soft factors in C(I)IP

Increasing the resilience of European Critical Infrastructures through science requires closer collaboration of projects with similar scope, close communication with end users and links to EU policy.

Research on Critical Infrastructure (Information) Protection (C(I)IP) has tremendously developed over the last 25 years. The rapid expansion of engineering and computer sciences has led to an impressive progress on modelling, simulation and analysis in order to better respond to a variety of threats, either natural or man-made.

However, there is less knowledge nowadays about the human emotion, cognition and behaviour in crisis situations. Behavioural and social sciences as well as research on human factors have still much to offer in this applied area. This could be achieved in the future by fostering collaborative research in at least three directions: better preparing first responders, raising awareness among citizens and learning from survivors.

The professional responding bodies such as the staff working in fire brigade, police, medical emergency, civil protection, command and control centres etc. may face poor communication, lack of relevant information or inappropriate decisions that may impair their professional performance and interfere with rescue procedures. Human factor research can bring more in-depth knowledge on the needs and requirements of these professional categories, in order to optimise decision-making, resource allocation and ultimately improve their response actions. Research results can be used for developing better recommendations and training programs for the concerned professional categories.

Moreover, crisis research has shown that lay citizens react more effectively than we would intuitively expect, and often respond at least as effective as well-trained emergency personnel. While fear is the dominant emotion across different types of disasters, it appears that in most cases panic does not take over the rational behaviour. Yet, the ongoing challenge is to find solutions to raise citizen awareness and improve their preparedness. Current research shows that citizens will prepare for a specific event only if they believe that preparation is useful and the event is indeed likely to occur. Social science can shed more light on how people perceive and accept risk, and can reveal their needs in terms of well-being during a disaster management. Social studies can also show the citizen's role is mass crisis dissemination and information flows for example through social media.

Last but not the least, disaster survivors and witnesses may provide useful feedback and lessons learned from their experience with various threats. The little existing research based on interviews and focus-groups suggests that during a crisis situation people's responses may depend on one's ability to recognise and to make sense of cues to life-threatening stimuli. There have also been insights that people tend to underestimate such cues and there are still conflicting results about the post-traumatic stress and the amount of accurate information that survivors and witnesses are able to recall.

Further research is needed to clarify these unanswered questions and help complement the CI resilience with a better psychological preparedness and resilience.

Some of these challenging topics will be addressed during the **11th edition of the CRITIS conference** which is scheduled from 10–12 October 2016 in Paris: www.critis2016.org

Enjoy reading this issue of ECN!

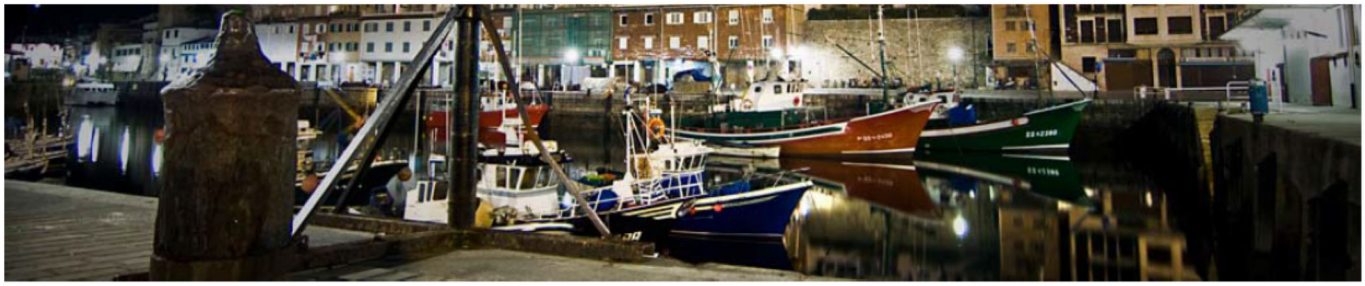
Grigore M. Havârneanu
is Traffic and Transport Psychologist with a PhD in Social Psychology. He is Research Advisor within the International Union of Railways' Security Division

e-mail: **havarneanu@uic.org**

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

e-mail: **bmhaemmerli@acris.ch**
He is ECN Editor in Chief

13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment



July 7-8, 2016 - Donostia-San Sebastián, Spain

DIMVA 2016

The annual DIMVA conference serves as a premier forum for advancing the state of the art in intrusion detection, malware detection, and vulnerability assessment. Each year, DIMVA brings together international experts from academia, industry, and government to present and discuss novel research in these areas.

DIMVA is organized by the special interest group Security – Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI). The conference proceedings will appear in Springer Lecture Notes in Computer Science (LNCS) 8850 series.

Central topics of the conference

INTRUSION DETECTION
Novel approaches and domains
Insider detection
Prevention and response
Data leakage and exfiltration
Result correlation and cooperation
Evasion and other attacks
Potentials and limitations
Operational experiences

Privacy, legal and social aspects
Targeted attacks
MALWARE DETECTION
Automated analyses
Behavioural models
Prevention and containment
Classification
Lineage, Forensics and recovery
Underground economy

VULNERABILITY ASSESSMENT
Vulnerability detection
Vulnerability prevention
Vulnerability analysis
Exploitation prevention
Situational awareness
Active probing

Organising Committee

- General Chair: Urko Zurutuza, Mondragon University, Spain
- Program Chair: Juan Caballero, IMDEA Software Institute, Spain
- Publication Chair: Ricardo J. Rodríguez, Universidad de Zaragoza

Join DIMVA 2016

http://dimva2016.mondragon.edu/en

Towards a competitive European Digital Single Market

EOS represents the interest of European security suppliers including large companies, SMEs, research centres, universities, clusters and associations. Our work and purpose is to provide a platform of collaborative work, insightful exchange of ideas and best practices between the European Institutions, the Member States and our Members.

Europe has taken important commitments and concrete actions towards building a sustainable Digital Single Market. The European strategy developed in this regard comes at the right time as Europe is in danger of falling behind in the international digital economy.

EOS welcomes this strategy that aims at creating the right conditions and a level playing field for advanced digital networks and innovative services along with maximising the growth potential of the digital economy.

This important objective should, however, be supported by an effort to protect and develop the European Digital Single Market (DSM).

Against this background, EOS has produced, in collaboration with its Members, an extensive in-house study of the European cybersecurity market. In this unique study, EOS gives an overview of the current cybersecurity market and describes the challenges ahead providing recommendations and concrete actions to be taken in order to raise Europe to its full potential in the global cyber chessboard.

The European cybersecurity market

Following the revelations made by Mr. Snowden, the questions of privacy and data protection figure highly among societal concerns. Todays, and thanks to fruitful societal and high level political debates and actions, Europe is seen as a trusted stakeholder in the world when it comes to data security and privacy.

This status should be sustained and developed with the support of a strong and competitive European cybersecurity market in line with EU privacy and data protection requirements. Unfortunately, the European cybersecurity market has inherited some of the problems faced by the general European security market.

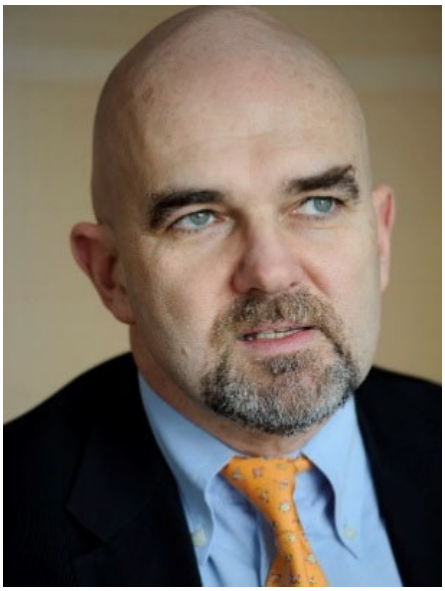
In a nutshell, the cybersecurity market, currently, suffers from a large fragmentation which is partly due to the fact that security in general and cybersecurity in particular (especially as a component of critical infrastructures and national assets protection) remains a national prerogative. The 28 EU Member States have different regulations and approaches towards cybersecurity as well as data privacy concerns which inevitably lead to the development of different specific solutions not necessarily competitive on a global scale.

At the same time, even though innovation is strong in Europe (coming from ICT labs, SMEs, research centres, and large companies) it often lacks the necessary funding based on a consistent transnational approach. Research and Development (R&D) and Research and Innovation (R&I) in cybersecurity, like in security in general, hardly reaches market deployment and is exacerbated by weak public procurement policies.

All in all, Europe is far from being at the right level of preparedness. The full implementation of an EU single digital market calls for more coordination at the EU level with a clearly identified industrial strategy and investment plan.

The main questions for Europe are:

- What is the level of strategic autonomy that Europe needs to achieve in the cybersecurity domain?
- In which cybersecurity areas can European industry make a breakthrough and become a global and competitive player?



Luigi Rebuffi

Luigi Rebuffi is the CEO of EOS. After having worked on the development of high power microwave systems for the next thermonuclear fusion reactor (ITER) he continued his career at Thomson CSF / Thales where he took on increasing responsibilities for European Affairs (R&D) in different sectors: telecom, industrial, medical, scientific. He became in 2003 Director for European Affairs for the civilian activities of the Group.
He is a Member of the European Commission's Protection and Security Advisory Group on EU Security Research and President of the Steering Board of the French ANR for security research.

e-mail: luigi.rebuffi@eos-eu.com

European Organisation for Security (EOS), 10, rue Montoyer 1000 Brussels / Belgium

The need for technological autonomy

Networks do not know boundaries and the continuous interconnection between information systems make cybersecurity a transnational issue by nature. In addition, the globalisation of trade makes network interconnection and interoperability a necessary requirement between the various economic agents increasing cooperation at regional and international level. Cyber attackers / hackers use this feature to their advantage to bounce from one country to another to cover their tracks.

In this scenario, the weakest link in the supply chain endangers the activity of many stakeholders' especially critical infrastructure managers and operators.

Because of current highly fragmented cybersecurity market, European users depend largely on non-European solutions for their cyber-protection. The increasing demand for cybersecurity products and services are often met by non-EU originating companies due to a lack of European policies designed to strengthen the European offer.

These technologies might potentially include built-in backdoors and with time, increase our vulnerability to the risks posed by cyber threats especially towards vital and critical infrastructures.

The question we need to ask ourselves today is how Europe can overcome these challenges and control its data when it is not even controlling its own ICT infrastructure and services?

Some EU Member States like Germany, France, Finland and the UK have started a discussion on how to achieve a greater autonomy and authority over ICT services and equipment. Several solutions have been proposed at national level but no convergence has been reached for a common approach based on certified, trusted EU solutions.

It is however essential to define a common, standardisation procedure for EU products and services among the Member States to avoid further fragmentation and higher costs. It is also of paramount importance that all the players in the ICT value chain, operating or not from a European Member States, adhere to similar requirements concerning data protection and cybersecurity. All market operators of the Digital Economy should share the responsibility for a secure cyber space and all players involved must be committed to secure digital products, software and services.

Developing trusted EU solutions and securing the supply chain

To achieve this goal, and due to rapidly emerging threats, we must plan the coming years in a smart and strategic way.

Massive investment campaigns to build the entire supply chain for IT components and services in Europe would demand a too large effort.

Instead, Europe should find a good balance between the use of certified trusted non-EU technologies and the development of European solutions in vital areas (e.g. ICT infrastructure and public services), and in applications where Europe is a market leader (e.g. aeronautics, car manufacturing, finance services and all sectors falling under the Industry 4.0).

In parallel, areas of higher competence in Europe like Identification and Access Management (e.g. smart cards) as well as Data Security (e.g. encryption) should be continuously improved to maintain leadership, while competitiveness should be increased in strategic components for Network Security Systems and Management of Security Services.

In this respect, EOS has been actively supporting the creation of a European Public-Private Partnership (PPP) on cybersecurity which will be set up in 2016. This collaborative platform will be a major opportunity to build a stronger technology base, and outline a common European industrial strategy to effectively meet the interests of Europe.

EOS and its members are confident that the work stemming from this partnership will lay down the basis for a "European Cybersecurity Flagship" harmonising capacity building in Member States and allowing, by 2025, our industry to become a world leader in key strategic sectors, implementing trusted European cybersecurity solutions and ensuring a greater digital autonomy.

EOS' cybersecurity Flagship initiative

The Flagship initiative developed and advocated by EOS and its members is built upon two main objectives:

1. The creation of a Flagship initiative for an EU Cybersecurity Investment Programme supported by adequate funding (initial estimate of €13 billion over 10 years), which would be composed of:

- Research & Innovation Programme based upon a competitive growth strategy.
- Capacity deployment across Europe according to an agreed Roadmap, including short term focus on concrete strategic projects on capability and capacity building.

The Public-Private Partnership (PPP) foreseen in the DSM Strategy could well be the initial step of this Flagship.

2. The development of a European Cybersecurity Industrial Policy touching upon several dimensions including: standards, certification and EU labels, innovative funding initiatives, education / training / awareness, support to SMEs and clusters, etc. This Industrial Policy will support the implementation of the DSM Strategy and the EU Cybersecurity Strategy (as well as the Cybersecurity Flagship objectives) at EU and Member State level.

More information can be found on the EOS website: www.eos-eu.com

EOS is registered at the EU Transparency register: 32134385519-64

CI2C Critical Infrastructures and Cloud Computing: understanding cross-sectorial criticalities and security practices

The goal of the CI2C project is to investigate and is focused on enhancing the security and resiliency of Cloud Computing and Critical Information Infrastructures (CIIs).

The CI2C project is a new project co-funded by the European Commission under the under "The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS) programme. The project started on September 1st 2014 and runs until May 2016.

The coordinator of CI2C project is Maria Cristina Brugnoli, Coordinator of the ICT4People Research Unit (ict4people.cnit.it).

"CI2C Observatory "

In order to widespread the research activities realised the project will develop a web portal, the "CI2C Observatory", to support to provide all involved CI2C stakeholders with a practical way for identifying vulnerabilities and weaknesses of the CI2Cs and for consolidating best practices. The "Observatory" will also support the cooperation and results exploitation over the long term and to collect and disseminate recommendations, experiences, expectations, needs from CIIs stakeholders, Cloud providers, CII and Cloud specialists through an intense stock-taking study.

Background

In the last years EC has highlighted the relevance of introducing Cloud Computing (CC) in EU Member States (MS) and has unveiled its ambitious cloud strategy – which aims to boost the use of CC in the European Union area. In the next future, the diffusion of cloud services will then spread over many critical sectors, like for examples public sectors as well as strategic private sectors. An uncontrolled take-up of CC in CIIs would have unpredictable effects.

Focus

The CI2C project is focused on enhancing the security and resiliency of Cloud Computing and Critical Information Infrastructures (CIIs) by assessing and evaluating cross sectors criticalities that could amplify effects and impacts in case of failures.

The CI2C project will create the foundation for securing and protecting CIIs with intense use of CC (CI2C systems). It will execute in-depth analysis and map of the best practices and policies for CIIPs and research on CC and security's state of the art, to form a complete picture of the EU CI2C systems and of their protection and security practices. CI2C will perform cross sector criticalities analysis, and will identify patterns and provide metrics for the quantification and modelisation of interdependencies in CI2C systems.

Maria Cristina Brugnoli

Maria Cristina is the Coordinator of the "ICT4People" of CNIT (Consorzio Nazionale Interuniversitario per le Telecomunicazioni), a Research Unit that aims to promote a unique and challenging way of studying ICT innovation, bridging the gap between Technology and Human Society. Maria Cristina is a researcher specialised in the evaluation and validation of ICT service and applications with more than 10 years of experience in the EU RTD funded projects. In CNIT since 2010, her current research interest are focused on the investigation and evaluation of end users aspect of security of distributed systems, critical infrastructures, and cloud computing.

e-mail: mariacristina.brugnoli@cnit.it

ICT4people Research Unit Coordinator
www.cnit.it
ict4people.cnit.it
Department of Electronic Engineering
University of Roma, Tor Vergata

Objectives

The project main objectives are to enhance security and resiliency of CC and CIIs by assessing and evaluating cross sector criticalities, to increase security awareness on Clouds within CII operators and the larger community, and to provide relevant information in order to foster coordination on the topics at EU level.

1) Proposing recommendations and technical guidelines for the protection of CI2C systems and the enhancement of security of the critical cloud services

2) Enhancing the capabilities of the cloud community and the CIIs as users of the cloud services to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in CC and security of CIIs

3) Strengthening the protection of the CI2Cs with practical contributions for circumventing the main security concerns

4) Contributing to the EC's efforts and strategy for the enhancement of the awareness of the shared culture of security and protection of CIIs within EU MSs

5) Demonstrating models and metrics for quantifying cross sector criticalities in support of C2ICs risk assessment activities with realistic case studies

6) Developing a project observatory for C2ICs, extended at all the EU MSs, and will provide the stakeholders with practical way for identifying risks and vulnerabilities of the CI2Cs and for consolidating best practices. The cooperation portal will ensure transferability of project results (to MSs and critical sectors not covered in the project).

CI2C Online survey

CI2C has launched a survey on how cloud computing (CC) services are used by critical infrastructures and organizations providing critical services. As a first step of our work we have launched an online survey: the final results of the CI2C will be published in the course of 2016 on our website (www.ci2c.eu). We would be very interested in having your opinion on these topics, so if you wish to have your say please go to: https://it.surveymonkey.com/s/ci2c_survey

CI2C methodologies

During the first phase of the project, the work will be conducted realising a stock taking of current CC and CIIs security practices (orientations, expectations, criticalities, concerns). This work will be based on a number of methodologies used to collect and analyse data gathered from multiple relevant stakeholders across Europe. In particular will be leveraged a wide range of investigation techniques (survey, interviews and questionnaires, panel assessment, workshops) as well as quali-quantitative methods of analysis to identify existing and innovative security practices for CI2Cs systems.

The second and final phase step will focus on the mapping cross-sector criticalities emerging in CI2C systems and to propose models and metrics for quantifying them. The analysis and quantification of cross-sector criticalities, widely known as inter-dependencies, is an activity core in critical infrastructures risk assessment. The methodology will be based on complex networks modelling and analysis methods and will be used for the quantification of interdepen-dencies in CI2C systems and the evaluation of the cross sectors criticalities (and the criticality level) in real use cases identified during the project.

CI2C Consortium

The CI2C Consortium consists of 5 partners:

- CNIT Project Coordinator– ICT4People Research Unit (Coordinator), www.ict4people.cnit.it, ITALY
- Deloitte ERS – Enterprise Risk Services, – www.deloitte.it, ITALY
- LIMS London Centre for Mathematical Science, www.london-institute.org, --- UNITED KINGDOM
- Eurocloud Europe,
- www.eurocloud.com, LUXEMBOURG
- Associazione Italiana Infrastrutture Critiche ITALY, www.infrastrutturecritiche.it/aiic/

If you would like to know more about CI2C please visit the project website: www.ci2c.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No. 603960 .

WISER helps organisations implement effective cyber risk management

WISER is a European collaborative Innovation Action that puts cyber-risk management at the very heart of good business practice, benefitting multiple stakeholders in particular critical infrastructure operators and process owners, and ICT-intensive SMEs.

Cyber-attacks are becoming a clear obstacle for European economies to strive. It is decreasing trust of the users and slowing down the growth of the Digital Single Market. Damage is not only economical, but also has high societal impact, since attacking sensitive information and critical infrastructures that provide essential services for society that, in the most dramatic case, may lead to loss of human lives.

Cyber threats are evolving and becoming more sophisticated, what should compel organisations to be in a position of permanent surveillance, monitoring continuously each system. But in spite of the big risk, available solutions still keep weak.

The lack of cyber risk awareness is becoming a very serious problem. Enterprises and SMEs are not able to cope with the dynamicity and complexity of cyber risk which is putting them in a vulnerable position.

Started in June 2015, WISER project will deliver, by 2017, a cyber-risk management framework able to dynamically assess cyber risk based on a continuous risk monitoring. It is also incorporating socio-economic impact assessment and is building on current state of the art methodologies and tools, leveraging best practices from multiple industries.

Risk management frameworks lack integrated agile methodology to analyse cyber risks. There is also demand for the continuous monitoring of related events and dynamic assessment of risk,

To give the best answer when cyberattack threatens valuable assets, a reliable support for decision-making is needed. WISER helps to adopt the correct measures while maximizing the ROI.

Besides, they often lack tools or qualified teams to support the decision-making process regarding the mitigating measures.

Cyber risk detection and assessment is usually a manual process, mainly performed periodically at static points of time. In addition, current focus is on the ICT side, not considering business or societal impact. This perspective contrasts with the cyber risk dynamic nature that sometimes demands rapid ad-hoc mitigation measures.

Objectives

WISER faces this changing risk landscape by focusing on areas that complement each other to make progresses beyond the state of the art:

1. Provide tools that enable continuous cyber risk monitoring solution, e.g. access to relevant freshly updated information, in order to feed module for continuous assessment of risks.

2. Multi-level risk assessment, focusing not only at ICT system (or combination of interdependent systems), but also considering the business processes or services that depend on it, and including also the implications of cyber disruptions at a wider level, considering all the societal impact (in public services, industrial capacity, resource availability for the functioning of societies and the economy, and in general well-being of the population).

3. Provide decision support tools to facilitate selection of optimal mitigation options based on integrated overall risk impact (IT, societal, business…).

Elena González

Elena González is Exploitation and Dissemination Manager at Atos.

She is involved in the WISER Project, in exploitation/ dissemination tasks.

email: elena.gonzalez@atos.net

Antonio Álvarez

Antonio Álvarez is Research and Innovation Consultant at Atos. He is involved in the WISER Project participating in technical, dissemination and management tasks.

Methodology and tools

To reach this new level in cyber security WISER will develop a methodology, based on best practices, with a set of taxonomies for cyber risk concepts, as well as a set of cyber risk checks and metrics.

The cyber risk framework will have to reflect the changes in cyber threat climate, not only at the level of information systems but also at the level of business processes and services that run on top of these processes, as well as societal services and support functions depending on the given ICT system.

It will provide decision support tools to facilitate selection of mitigation options based on dynamic and integrated risk impact assessment at different levels (qualitative and quantitative techniques for assessing the level of cyber risk exposure). Focus is on integrating technological advancements related to implementation of the continuous monitoring, assessment and mitigation mechanisms for cyber risk management in real time.

Focus on SMEs

WISER also has focus on SMEs needs that often do not have means to handle cyber risk with advances methodologies & tools. WISER will deliver a pre-packaged risk management solution for SMEs that combines sophistication of the solution with simplicity of use and adoption by the end-user. Among all the different goals defined in WISER, the most important one, having the highest priority, is to make cyber security affordable for SMEs.

WISER Pilots

From the very beginning of the project, WISER project will develop its activities in a market driven and market oriented manner. The goal is to make possible the early roll-out and application of WISER in different verticals. The project has started with the engagement of 10 different companies from a range of sectors. These companies will provide an overview of their business goals, their business processes and their current practice regarding cybersecurity in order to identify their emerging and future needs, and shape the product according to operational requirements.

Besides, the definition of the project has also considered three different full-scale pilots carried out with the consortium partners, playing the role of early adopters. By doing this, valuable feedback will be obtained early in the project and the likelihood of successful marketability of WISER will be notably increased.

WISER Consortium

WISER is executed by a consortium of technology providers, risk management experts, market experts and service providers for piloting:

- ATOS (Spain)
- Trust-IT (UK),
- SINTEF (Norway)
- XLAB (Slovenia)
- AON (Italy)
- REXEL (France)

If you would like to know more about WISER please visit our website:

www.cyberwiser.eu

WISER has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 653321

SECRET EU project: Security of Railways against Electromagnetic Attacks

This FP7 EU project ended in November 2015 and delivered a series of recommendations to better prevent and protect rail infrastructure from intentional electromagnetic interferences

Cyber threats are an increasing concern for every business. Barely a week goes by without new reports of sophisticated IT systems – even of the largest organisations or intelligence services – falling victim to cyber-attacks. It was therefore important to check what further precautions could be taken within the railway sector should the need arise.

In this context, the project SECRET was selected by the European Commission as part of its fourth call for 'transport' proposals, under the 7th Framework Programme for Research and Development.

The SECRET EU project addressed the issue of electro-magnetic (EM) attacks targeting rail infrastructure and contributed to reinforce the signalling systems. The EM attacks considered in SECRET were low power intentional interferences that could break the communication links and affect voice communication and the good transmission of signalling information.

The SECRET consortium came together to assess the risks and consequences of EM attacks, to identify preventive and recovery measures and to develop protection solutions to ensure the security of the rail network, subject to intentional EM interferences, which can disturb a large number of command-control, communication or signalling systems.

SECRET objectives

- identify the vulnerability points at different levels (from the electronic to the systemic vision)
- identify EM attack scenarios and risk assessment (service degradation, potential accidents, economic impacts…)
- identify public equipment which can be used to generate EM attacks
- develop protection rules to strengthen the infrastructure (at electronic, architecture and systemic levels)
- develop EM attack detection devices and processes
- develop resilient architecture able to adequately react in case of EM attack detection
- extract recommendations to ensure resiliency and contribute to standards

SECRET Approach

The project illustrated the risk by implementing some electromagnetic attacks and analysing their effects, thereby inciting the different railway actors to work together to strengthen the resilience of a system that must remain effective and safe for the serenity of our society.

Then, the project opened ways to resilience solutions regarding this type of attack. Preferring to avoid unconstructive and alarming rhetoric, which is unjustified as the European railway system is above all a very safe means of transport, the project identified and proposed strategies in which each actor would be able to inspire itself in order to act towards resilience.

The strategies developed mainly concern:

- The tests that can be performed to assess the susceptibility of individual network components dealing with intentional interferences and allowing each designer, integrator or operator to build, evaluate and compare the susceptibility of these products.

Virginie DENIAU
SECRET technical coordinator

Virginie Deniau holds a PhD in Electronic University of Science and Technology of Lille. She is researcher at IFSTTAR (French Institute of Science and Technology for Transport, Development and Networks) since July 2003. She conducts works in the field of electromagnetic compatibility (EMC), the characterization and modeling of EM transportation environments, and the immunity test methodologies for embedded systems. Since 3 years, she is involved in hardening the transport systems vis-à-vis the cyber attacks, such "electromagnetic attacks.". She is also chair of the URSI Committee E (Electromagnetic Interference) French section.

e-mail: virginie.deniau@ifsttar.fr

Marie-Hélène BONNEAU
Security Advisor at the UIC Security Division, leader for dissemination in the SECRET Project

e-mail: bonneau@uic.org

- The methods of detection of electromagnetic attacks that are essential for several reasons: Detecting means to be able to demonstrate that we have been a victim of an electromagnetic attack, detecting avoids confusing an electromagnetic attack with a technical failure which could unduly jeopardize the operator, who could initiate unnecessary diagnostic inquiries. And, finally a reliable detection can instigate a fast and appropriate reaction to the threat.

- The resilient architecture which is a compulsory issue when we consider a critical infrastructure which is a network. The resilient architecture has to ensure the maintenance of communication for the transmission of critical information, thus maintaining the control of the network. We worked on an adapted architecture permitting us to assess the impact of certain technological solutions on reliability and responsiveness.

SECRET results

About 40 recommendations at organisation, standardization and technical levels have been identified, classified and described. These recommendations are organised in three categories described below.

The first category called "**prevention from EM jamming effects**" groups the recommendations which can be adopted permanently and can permit to inhibit or reduce the impact of jamming signals (precautionary principle). In order to prevent from jamming attacks on the railway environment the first recommend-dation that can be done is the provision of risk assessments. The Bow-tie and TVRA were used in Secret to assess railway incidents and railway communication system incidents. Operational recommendations have also been identified like minimising train emergency brake impact. Finally a series of engineering recommendations focusing on the system architecture, the radio network features, rolling stock, train antenna and the BTS (Base Transceiver Station) antenna were defined.

The second recommendation category is dedicated to the **EM attack detection solutions**. It presents the different detection techniques which were studied in SECRET and gives their potential applications. The different detection techniques are based on the monitoring of different parameters like the Error Vector Magnitude (EVM), frequency spectrum occupation, excess of energy in the operated band and the Quality of Services (QoS). These techniques were studied for on board train, on the track side and in train station conditions.

The third category is "**Mitigation of EM jamming effect**". In this category, the recommendations are focused on solutions which can be activated temporally when EM jamming is detected. All recommendations in this category are classified as operational considering their activation will depend on the operational context. Some of the recommendations focus on temporarily improving the system radio coverage. These recommend-dations shall meet the EIRENE specifications to ensure a minimum received radio level for voice or ETCS applications. The recommendations are not necessarily linked and, most of the time, can be implemented separately. Such temporary recommendations require important guidelines to decide the conditions in which they can be used by taking into account the environmental criteria: jamming location, train location, level of communication degradation, railway lines category, and presence of alternative radio bearer. Their activation can be made automatically using the jammer detection system or manually from the train or control centres.

Conclusion

In the European railway sector, the homogenisation of network technologies and the increasing use of wireless communications have made the scenario of an EM attack very likely. The communications could potentially be jammed, with trains being delayed, blocked or even diverted.

The secret project has contributed to this problematic by assessing the real risks concerning EM attacks, identifying areas for strengthening the railway network and developing detection solution and to designing a resilient architecture. As a result the SECRET white paper gives an overview of the recommendations on preventive and recovery measures as well as the suitable methodology to evaluate and mitigate EM attacks in the railway context. Finally, the recommend-dations consider the possible evolutions of the system architecture following the introduction of next generation technologies.

The next step is to take into account these recommendations (especially regarding the system architecture permitting resilient reconfiguration) in the various existing standardisation bodies (especially ETSI) and to incorporate the results into International Railway Standards.

The project was coordinated by the French research centre IFSTTAR and the consortium was composed of 9 other members: Research centres (Fraunhofer Institute IAIS from Germany, Politecnico di Torino from Italy, University of Liege-Institut Montefiore from Belgium, University of the Basque Country-UPV/EHU, ZANASI & Partners from Italy, industries (ALSTOM TRANSPORT S.A. from Belgium, TRIALOG from France) and railways representatives (SNCF – French railways and UIC – International Union of Railways based in France).

If you would like to find out more about the project please visit our website at www.secret-project.eu

Foreign policy's role in improving critical infrastructure protection in cyberspace

Foreign policy and diplomacy are enablers of international cooperation, which is essential for countering global cyber risks to critical infrastructures. Switzerland is committed to promoting the three core components of international cooperation: a framework of rules, trust and capacity.

Three components of international cooperation

When it comes to improving Critical Infrastructure Protection (CIP) in cyberspace, foreign policy and diplomacy play an important role. Because of its global and almost ubiquitous nature, cyberspace creates significant interdependences between critical infrastructures located in different states.

No country alone can guarantee the security of its critical infrastructure in isolation. We therefore need close and efficient international cooperation to tackle the ever-growing risks emanating from the malicious use of Information and Communication Technologies (ICT). It is the role of foreign policy and diplomacy to enable this cooperation.

In Switzerland, the Federal Council recognised in its National Cyber Strategy (NCS) the importance of international cooperation to improve protection against cyber risks. Within the Swiss federal system, close-knit cooperation among different actors to ensure security takes place quite naturally. This also needs to be promoted at the international level.

A cooperative approach with three pillars is required for greater security in the cyber domain: a clear framework of rules, trust among the involved actors, and a minimum level of capacity to fight threats and cooperate effectively. These three elements are at the core of the Swiss cyber foreign policy and this article outlines how they are promoted.

Framework of rules

For a secure cyberspace, we need first and foremost a clear framework of rules that defines what is acceptable behaviour in cyberspace.

In Switzerland's view, the existing international legal order provides a strong foundation for the rules in cyberspace. International law is equally applicable online as it is offline. This view has also been confirmed by the UN Group of Governmental Experts (UNGGE).

A clear framework of rules is particularly important for the security of critical infrastructures, which are increasingly becoming the targets of cyber-attacks. In the case of critical infrastructure, these attacks can have particularly devastating effects.

International law is directly relevant for purposes of CIP. General principles of international law, such as the principle of non-intervention or the prohibition of the use of force, outlaw cyber-attacks on critical infrastructure that would reach a certain threshold of severity or intensity. Other bodies of international law also provide for specific legal protection. As an example, international humanitarian law forbids the parties of an armed conflict to attack certain critical infrastructures, namely dams, dykes and nuclear electrical generating stations. Such provisions also apply to cyber-attacks.

In addition to the legal framework, voluntary, legally non-binding norms of responsible state behaviour can further clarify the framework of rules in cyberspace. Because these are political and not legal in nature, they can often be negotiated in a more flexible and timely manner, which is a significant advantage in the quickly evolving cyber domain.

Ambassador Benno Laggner

Ambassador Benno Laggner is currently the Head of the Division for Security Policy and Ambassador for Nuclear Disarmament and Non-Proliferation in the Swiss Federal Department of Foreign Affairs.

Prior to this appointment, Benno Laggner was the Deputy Chef de Cabinet of the President of the 65th session of the United Nations General Assembly. Earlier postings included serving as Head of the UN Coordination Unit in the Federal Department of Foreign Affairs (2007-2010), as Head of the Political Section at the Swiss Embassy in Berlin (2004-2007) and as Head of the Political Section at the Permanent Mission of Switzerland to the United Nations in New York (2000-2004). Benno Laggner holds a Master's Degree in International Relations (University of St. Gallen, Switzerland) and also completed postgraduate studies in European Affairs at the College of Europe in Bruges, Belgium.

In its report of July 2015, the UNGGE recommended for consideration a first set of norms of responsible state behaviour for cyberspace. One of these norms provides specific protection for critical infrastructures (see box below). This constitutes an important recognition of the special protection that critical infrastructures should enjoy in the view of the international community.

Building upon this norm, we should now work towards clarifying its scope of application and explore mechanisms that would ensure compliance with it.

> *"A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."*
>
> UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (July 2015, A/70/174)

Trust

A second prerequisite for a more secure cyberspace is an adequate level of trust among the involved actors. Since the anonymous nature of cyberspace leaves much room for ambiguity, building confidence through transparency and cooperation is vital to reduce the danger of miscalculation, misperception and misunderstanding. Trust in a way is the glue holding the decentralised network that cyberspace constitutes together.

Switzerland is therefore engaged in efforts to apply the tool of Confidence-Building Measures (CBMs) to cyberspace. CBMs were invented by the Organisation for Security and Cooperation in Europe (OSCE) in the context of the East-West conflict four decades ago. It is therefore no coincidence that the OSCE in 2013 was the first regional security organisation to formally adopt CBMs in the realm of cybersecurity, too.

The initial set of OSCE CBMs aims at increasing transparency and confidence. To this end, the 57 participating States committed to exchange information on their cybersecurity policies, organisation and strategy. They also committed to defining national contact points in order to facilitate cooperation.

Because cybersecurity depends upon trust and cooperation between all relevant actors it is important to also include non-governmental actors in CBM activities. During the Swiss Chairmanship of the OSCE in 2014, Switzerland organised an event on cyber CBMs. For the first time, the private sector and critical infrastructure operators were also included in the confidence-building activities between states. It is important to further develop this multi-stakeholder cooperation.

Switzerland will continue to promote cyber CBMs, both within the OSCE context and beyond. At the OSCE, we push towards implementation of the initial set of CBMs, while also contributing to the adoption of additional measures, which would take the cooperation in this forum to the next level.

Given the global nature of cyberspace, it is also important to engage in confidence-building measures across regional boundaries and organisations. This is why we reach out to actors in different regions of the world, for example by supporting a regular dialogue between European countries and China, with participants from government but also the private sector and academia.

Capacity

The third element that is necessary for securing cyberspace is the capacity to do so. We understand capacity as a broad concept: It clearly includes technical skills and resources, but also a strategic and policy framework that guide states' efforts to tackle cyberrisks. Capacity further includes the ability to engage in international processes and cooperation, without which it is impossible to cooperate.

It is important to highlight that capacity-building in the cyber domain is in the interest of all states. In cyberspace, we are only as secure as the weakest link in the network – and that is particularly true for critical infrastructure.

Switzerland therefore contributes to the global effort to raise the level of capacity in cybersecurity. Last year, Switzerland became a founding member of the Global Forum on Cyber Expertise (GFCE) alongside more than 40 other states and actors from the private sector committed to boosting global capacity-building efforts.

One project that Switzerland supports in the GFCE is the "Meridian" initiative, which aims at making best practices and policy recommendations in the field of Critical Information Infrastructure Protection (CIIP) available to a wider range of actors, thereby promoting CIIP throughout the world.

Switzerland also launched the Geneva Internet Platform (GIP) which pursues the objective of empowering actors from all stakeholder-groups to actively participate in the relevant international processes. To this end, the GIP teaches online courses in the field of digital policy and provides an online policy observatory that allows all interested actors to follow the current policy debates and international processes (see http://digitalwatch.giplatform.org/). Finally, the GIP is also a neutral platform for debates and discussions.

Conclusion

Technical and defensive measures are not sufficient to improve the security of CIP in cyberspace. Geared towards the decentralised network that cyberspace constitutes, a truly collaborative approach to security is necessary. This means that we must closely cooperate across country borders and regional boundaries.

Switzerland is committed to advancing this approach by promoting a solid and globally shared framework of rules, fostering trust among the different actors and contributing to building capacity worldwide.

Understanding Systemic Interdependencies

The increasing complexification of our society is creating and tightening interdependencies among all its component systems; it is thus crucial to understand the consequences of such evolution. We will discuss how such interdependences can lead to systemic risk, i.e. to the emergence of unforeseen behavior that could have not been predicted from the understanding of the single systems. In this chapter we will pose some examples of systemic interdependencies and introduce some tools and models that allow to understand their possible consequences in socio-technical systems; we will then revise some reference literature with particular attention to complex networks approaches.

The structural organisation of the society in the countries of elevated development is experiencing a terrific enhancement of its complexity. Tools and devices employed in our ordinary life are becoming increasingly more technological and smart. Both the materials and the technology involved are constantly improved, whilst a cyber layer is becoming an essential component of smart devices. In general, we are immersed in a world consisting of interdependent systems, which functioning critically depend on each other (like the Internet depending on the electric power network and vice versa). Those different systems form actually a "System of Systems" (SyoSy). Single domain systems are strongly engineered infrastructures and, to some extent, we do understand their functioning and related risks; however the interaction among such systems lays ground for new emerging phenomena. In fact, the ability to reduce everything to simple fundamental laws does not imply the ability to start from those laws and reconstruct everything: such constructionist hypothesis breaks down when confronted with the twin difficulties of scale and complexity. At each level of complexity, entirely new properties appear and we are nowadays convinced that the whole becomes very different from the sum of its parts [1]. The former considerations do apply to all different sectors of modern society; however they become more stringent when applied to Critical Infrastructures (CI) [2]. The huge concentration of people in the metropoles and the general increase of the world population requires giant provisions of basic goods, such as both edible and sanitary water, food, electric energy, gas, fuels etc. To securely deliver and distribute such a variety of services represents one of the main issues in modern society. It is worth noting that the term infrastructure here is employed in the broad sense referring to the synergistic functioning of the allocated humans and devices. Human intervention can be "a priori" while defining and assessing "contingent plans" or "ex post" by real time management of the operational setting of the infrastructure. There are several reasons for which static rules are not sustainable to manage infrastructures in the long run; among them the following are worth mentioning: the advent of "Smart Society" including the Internet of Things (IoT); the improvements in the materials and devices; the rise of new types of attacks (new threats) both on physical and cyber side; the discovery of new vulnerabilities of the system; the reduction/increase in the allocated funds or humans; the increase in the demand; and even possible climate changes.

During last decades, the owners and handlers of infrastructures have reached a very high level of performance concerning the management, the protection and the defence. They are able to face most of the predictable and even unpredictable adversities, behaving according to predefined rules coded in the "contingency plans" and practiced during continuous exercises. However, most of the countermeasures foreseen to deal with contingencies do rely on the availability of other commodities or services. For instance, small fires can be doomed by autonomous systems, yet larger ones require the intervention of firemen rescue teams. Similarly, infrastructures providing communications can stand short electric power outages by resorting to their UPS (Uninterruptible Power Supplies) and their fuel reservoirs, yet long enough ones require either re-fuelling or recovery of the Electric Systems (ES).

Gregorio D'Agostino is Senior Scientist scientist at ENEA. He is visitor Scientist at London Institute of Mathemathical Studies. He is al so president of the Netonets Association.
e-amail:
gregorio.dagostino@enea.it

Antonio Scala is Staff Scientist at CNR, Professor at Institute of Advanced Studies IMT (Lucca) and Visitor Scientist at London Institute of Mathemathical Studies

He will also chair Critis 2017 conference in Lucca.

Similarly, telecommunications can be reactivated after a main event (such as a earthquake or a flood) providing the transports (mainly highways and roads) are available to allow mobile bridges appropriate allocation and deployment "in situ".

Generally speaking an infrastructure is said to depend on one other when the second is required for normal functioning of the first or to enforce contingency plans upon undesired events. When two infrastructures do depend on one other they are said to be "mutually or reciprocally dependent". Sequential dependence is an asymmetrical chain of one way interactions. When different infrastructures do exhibit a series of dependencies in closed chains they are said to be interdependent. Interdependence represents a resource for efficient provision of services, since it allows savings and allocation "on demand", yet it may hid "systemic risks". "Systemic interdependence" is the term we employ to refer to indirect or hidden dependencies in a System O Systems. The Systemic Interdependence implies a "systemic risk", that is one not strictly related to a part of the system, but just arising globally, while the different parts function together.

The term "systemic risk" arose to the chronicles after 2008 crises in finance. No company was exhibiting any apparent problem, nevertheless a liquidity lack triggered the largest financial crisis after 1930. Generally speaking, "systemic risk" may be defined as a global risk not related to a vulnerability of a specific part of the system, but to its "global" behavior. The system may collapse as a whole entity while none of its components appears vulnerable. The reason is basically related to interdependency: banks as well as stocks depend on each other and a fall in the prices of one results in that for another, thus possibly leading to a domino effect. In general, the complexity of a system lays the grounds for the possibility of systemic risk, i.e. for system-wide failures that cannot be predicted from the analysis of the single components, but emerge from the interdependencies of the constituting system(s). Thus, systemic interdependencies are a central issue in our world.

Systemic interdependencies have been shown to be relevant even in the human body where Network Physiology reveals relations between network topology and physiological function [21]. In this case one does not observe specific symptoms but a complex global syndrome. Again, details on functioning of specific organs (and relative treatments) are not enough to deal with the general pathology.

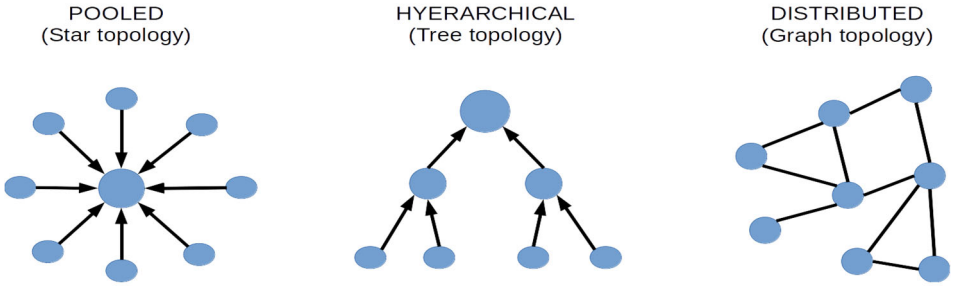


Figure 1 " The different basic topologies for systemic interdependences. Notice that the natural way to represent such topologies is in the form of graphs or networks, where nodes represents the systems, arcs represent mutual relations and oriented arcs (arrows) represent dependencies "

During last six years the authors have devoted a significant part of their efforts to understand systemic interdependence and to build up a community merging experts and scientists to deal with the problem from both the academic and the applied perspectives. This resulted in the Netonets organisation (www.netonets.org). In the following, we will explicit some models for systemic interdependencies that highlight the emerging properties of a SyoSy.

Models for interdependence

There are several organisational models to integrate different units into a coordinated system of systems. Pooled interdependence is the lowest form of interdependence resulting in the least amount of conflict. Departments (or single infrastructure in our case) do not directly depend or interact with one another; however they do draw resources from a shared source. This model is rarely representative of real systems where pairwise provision-demand agreements dominate. More complex organisations normally imply pair (and in some rare case multiple) interactions. In principle, there could be a thinking entity responsible to plan these interactions (and in the future there will possibly be); however, generally speaking the different owners of the infrastructure will establish agreements to receive and/or provide services or commodities. In other words the systems are self-assembled according to individual goals. It is worth noting that even if the pooled interdependence is a very simple one it may explain several phenomena, such as for instance a volatility crisis in a network of loans. Normally several bank and financial institutions have both credits and debits. The provide credits when the beneficial owns goods (real estates etc) or other valuable assets. When looking at the system locally (that is from any single unit perspective), no problem is seen. However it may happen that one (even a small one) o the entity needs some liquidity and hence claims its credits; this may induce a cascading effect on the whole system [3]. The effect is also predicted assuming that all entities take their money from a common source that experiences a deficiency. This represents a kind of "mean field approximation" to the real situation where credits are claimed on a specific network. The same applies to the electric system. When an extra power is injected it may produce a chain of faults; however, even homogeneous distribution of the extra power, that corresponds to both the mean field approach and to simplified pooling dependence, may induce cascading effects [4]. These are typical systemic risk problems: the system appears in perfect shape locally and yet it experiences collapse.

Generally speaking when modelling a system of systems one has to perform basically the following steps:

1. Turn all the information of the systems into a treatable representation.
2. Select the appropriate level of abstraction (including granularity) of possible representations, depending on the goal of the analysis
3. Analyse the system to outline the interdependencies of the different component systems.
4. Simulate the system or run the developed analytical tools.
5. Provide a means to outline the emergent behaviours of the system. This step is just to understand the systemic behaviour.

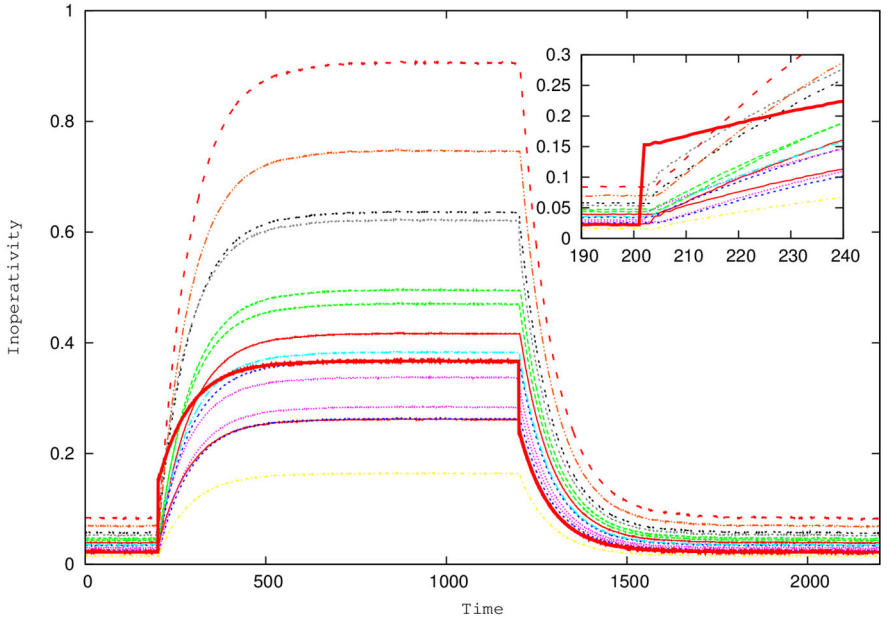


Figure 2 The typical evolution of inoperabilities upon a disturbance of one component only (red bold line). Inset: initial evolution of the system after the shock. Due to systemic interdependencies, the fault propagates and shortly after the failure the component suffering the maximum inoperability is not the one subject to the initial fault.

Models can be classified according to general types. Among several of them we will discuss the most diffused models with a focus on those employed to study systems of infrastructures.

A very neat application of such representation is represented by the "Design Structure Matrix" [5], a very useful tool for managing and coordinating projects. A DSM lists all the information exchange, interactions, and dependency patterns among the constituent element of a project (subsystems/activities). DSMs can be broadly distinguished in two main categories: static and time-based [6]. Static DSMs represent systems of systems where all of the elements exist simultaneously and are equivalent an adjacency matrix or a graph. The main analysis tool for static DSMs are usually clustering algorithms [7] that help separate the systems of the SyoSy in groups that are mostly related. On the other hand, time-based DSMs are directed graphs and can be thus analysed using sequencing algorithms [8].

Another approach originates from works of economists of the fifties of the last century: the Nobel laureate Leontief introduced a simple linear model for interaction of the different sectors in economy [9]. Moving from similar reasoning a simple approach, based on inoperability, has been developed to describe interdependent systems. In the Inoperability I/O Model (IIM) [10] each infrastructure is modelled by a node i in a network with a given "inoperability" Qi ∈ [0, 1] measuring to what extent the node i is performing the function it is devised for. These ideas were further developed leading to stochastic differential equations describing the phenomenon:

$$dQ_i = \sum_{j=1,N} h_{ij}\, Q_j \quad + \gamma_i\, dD_A$$

For some further information one can see [25,26]. In the simple case of constant disturbance, the system, with initial inoperabilities Qi(0) tends to an equilibrium Qeq = H−1γ(0) □d(0) which depends (linearly in this case) on the impact of the external disturbance d (disturbance per unit time) on the inoperabilities of the different components. Figure (2) shows how starting from a disturbance localised on one infrastructure it may spread to the others. Again this surprising effect is due to systemic interdependence.

There are several other examples of model where the systemic interdependence plays a crucial rule in the emergent behaviour. Possibly one of the most promising is the group of "Fault propagation models" inspired by epidemics. In this case each component is given a Boolean value representing its operability. Null operability is transmitted to those components that are directly connected. The typical example is given by local "fault propagation"; again each component can be in a operable or non operable state; there exists a probability rate of restoring normal behaviour and a probability rate that a fault induces an other one on a component that depends on it. We can name this model VIV (Vulnerable, Inoperable, and Vulnerable). From the mathematical point of view it would just correspond to the classical SIS (Susceptible, Infected, and Susceptible) model of epidemiology. If one further assumes that after the first fault the lesson is learned and a component cannot undergo the same type of fault, there exists a third state to be accounted corresponding to invulnerable nodes. Hereby, this simple model will be referred to as VIP (Vulnerable, Inoperable, and Patched): it corresponds to the classical SIR (Susceptible, Infected, Recovered) model in epidemics. Since several different independent faults may take place, one should deal with competitive multiple epidemics spreads.

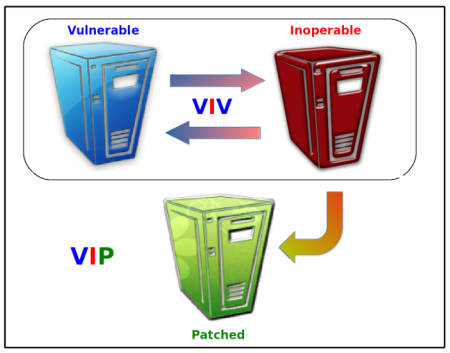


Figure 3 *V IP* Model: Each platform in a network can be in one of three states: Vulnerable (Susceptible), Inoperable (Infected) and Patched (Recovered).

The evolution is again stochastic and it is dominated by the healing rate roughly corresponding to the Mean Time to Repair, which is a common index of resilience capability of the infrastructure, and by the infection rate that corresponds to the mean time to fault that is also a common metric for infrastructural vulnerability.

According to the ratio between infection and healing rate, the initial fault may spread all over the network or extinguish. The critical value at which this phenomenon takes place is the epidemic threshold of the system and it depends on the **topology** of the network only. It has been demonstrated that the inverse of the maximum eigenvalue of the adjacency matrix is lower bound for the epidemics threshold, [12, 13]. The threshold can also be estimated by neglecting correlations [14].

Diffusion is the most fundamental dynamical mechanism allowing the propagation on a system [15]. It describes the propagation of any scalar quantity on the system through random exploration. Generally speaking the diffusion-like equations can be applied to different fields including synchronisation among different infrastructures. These models were also applied to interdependent infrastructure and it can be proven that for small couplings among the infrastructures, the SysoSys behaves as components were separate; while for large couplings the SysoSys behaves as a whole [16]. In general, synchronisation is the capability of the systems to function in unison and is often modelled with the non-linear Kuramoto model [17] (especially for electric systems); it is an example of a non-linear dynamics where special tools like the master stability function [18] must be applied. Ref. [19] provides a wide review of synchronisation on networks.

Conclusions

The interest in systemic interdependencies is witnessed by the blossoming of the related field of networks of networks: over the course of 2014, one book [22] and several reviews [23, 24] have been published and a major EU project (MULTIPLEX - Foundational Research on MULTIlevel comPLEX networks and systems www.multiplexproject.eu/) involving 23 research groups and producing more and resulting in almost two hundred publications has ended in 2015.

Beside the efforts in understanding the systemic behaviour, the research in the field is spreading along several directions. Dealing with real infrastructures requires models to assess operational parameters and the systemic approach cannot provide such information. To such an aim, agent based models can be introduced to simulate the behavior of the different infrastructures (or their components) and interdependence analysis provides information on how they interact. Since the systems are brought around some desired stable condition, the simulation are carried in the discrete event paradigm which consists in finding novel equilibria after undesired events. In some rare case one may employ accurate domain specific codes to simulate the different infrastructure in details while using the interdependencies as reciprocal boundary conditions. This type of approach is named "federated modelling and simulation". The fundamentals of all the previous approaches can be found in the references above [22, 23, 24]. However, at the present stage, models catching the emergent behaviors are not able to provide applicable recipes to manage real infrastructures and systems of systems; on the other hand, detailed models can mimic the accurate evolution of the systems often hiding the global picture.

Our society in experiencing a remarkable change due to the advent of the smart society, that is the introduction of computer aided networks to control any activity of our life from domotics and internet of things (IoT) to smart grids, buildings, cities and nations. The theory of complexity may enhance the awareness in the scientific community and hopefully in the whole society of the systemic risk that is not limited to finance or other known systems, but is a general mechanism related to the increasing amount of interactions among people, systems and devices needed to implement a smart society.

Acknowledgements

GD acknowledges interesting discussion with participants to the CIPRNET network of excellence. The authors acknowledge interactions within the MULTIPLEX project.

References

[1] P. W. Anderson. More is different. *Science*, 177(4047):393–396, 1972.

[2] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25, 2001.

[3] Xuqing Huang, Irena Vodenska, Shlomo Havlin, and H. Eugene Stanley. Cascading failures in bi-partite graphs: Model for systemic risk propagation. *Sci. Rep.*, 3:–, February 2013.

[4] Sakshi Pahwa, Caterina Scoglio, and Antonio Scala. Abruptness of cascade failures in power grids. *Sci. Rep.*, 4:–, January 2014.

[5] SD Eppinger. Innovation at the speed of information. *Harvard Business Review*, 79:149–158, 2001.

[6] T.R. Browning. Applying the design structure matrix to system decomposition and integration problems: a review and new directions. *Engineering Management, IEEE Transactions on*, 48(3):292–306, Aug 2001.

[7] Vladimir Estivill-Castro. Why so many clustering algorithms: A position paper. *SIGKDD Explor. Newsl.*, 4(1):65–75, June 2002.

[8] S.D. Eppinger and T.R. Browning. *Design Structure Matrix Methods and Applications*. MIT Press, Cambridge, 2012.

[9] Wassily W. Leontief. *Input-Output Economics*. Oxford University Press, 2nd edition, 1987.

[10] Kenneth G. Crowther and Yacov Y. Haimes. Application of the inoperability inputoutput model (iim) for systemic risk assessment and management of interdependent infrastructures. *Systems Engineering*, 8(4):323–341, 2005.

[11] Stefano Battiston, Michelangelo Puliga, Rahul Kaushik, Paolo Tasca, and Guido Caldarelli. Debtrank: Too central to fail? Financial networks, the fed and systemic risk. *Sci. Rep.*, 2:–, August 2012.

[12] Yang Wang, Deepayan Chakrabarti, Chenxi Wang, and Christos Faloutsos. Epidemic spreading in real networks: An eigenvalue viewpoint. In *22nd Symposium on Reliable Distributed Systems (SRDS 2003), 6-8 October 2003, Florence, Italy*, pages 25–34, 2003.

[13] Cong Li, Huijuan Wang, and Piet Van Mieghem. Epidemic threshold in directed networks. *Phys. Rev. E*, 88:062802, Dec 2013.

[14] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic spreading in scale-free networks. *Phys. Rev. Lett.*, 86:3200–3203, Apr 2001.

[15] G. D'Agostino, A. Scala, V. Zlatic, and G. Caldarelli. Robustness and assortativity for diffusion-like processes in scale-free networks. *EPL (Europhysics Letters)*, 97(6):68006, 2012.

[16] J. Martin-Hernandez, H. Wang, P. Van Mieghem, and G. D'Agostino. Algebraic connectivity of interdependent networks. *Physica A: Statistical Mechanics and its Applications*, 404(0):92 – 105, 2014.

[17] Yoshiki Kuramoto. Self-entrainment of a population of coupled non-linear oscillators. In Huzihiro Araki, editor, *International Symposium on Mathematical Problems in Theoretical Physics*, volume 39 of *Lecture Notes in Physics*, pages 420–422. Springer Berlin Heidelberg, 1975.

[18] Louis M. Pecora and Thomas L. Carroll. Master stability functions for synchronized coupled systems. *Phys. Rev. Lett.*, 80:2109–2112, Mar 1998.

[19] Alex Arenas, Albert Diaz-Guilera, Jurgen Kurths, Yamir Moreno, and Changsong Zhou. Synchronization in complex networks. *Physics Reports*, 469(3):93 – 153, 2008.

[20] Ludwig von Bertalanffy. *General System theory: Foundations, Development, Applications*. New York: George Braziller, revised edition 1976: isbn 0-8076-0453-4 edition, 1968.

[21] Amir Bashan, Ronny P. Bartsch, Jan. W. Kantelhardt, Shlomo Havlin, and Plamen Ch. Ivanov. Network physiology reveals relations between network topology and physiological function. *Nat Commun*, 3:702–, February 2012.

[22] Gregorio D'Agostino and Antonio Scala, editors. *Networks of Networks: The Last Frontier of Complexity*. Understanding Complex Systems. Springer International Publishing, 2014.

[23] S. Boccaletti, G. Bianconi, R. Criado, C.I. del Genio, J. Gómez-Gardeñes, M. Romance, I. Sendiña-Nadal, Z. Wang, and M. Zanin. The structure and dynamics of multilayer networks. *Physics Reports*, 544(1):1–122, 2014. The structure and dynamics of multilayer networks.

[24] Mikko Kivelä, Alex Arenas, Marc Barthelemy, James P. Gleeson, Yamir Moreno, and Mason A. Porter. Multilayer networks. *Journal of Complex Networks*, 2014.

[25] G. D'Agostino and A. Scala "Sistemic Interdependence" in "Handbook of Science and Technology Convergence" by W- S. Bainbridge, and M. C. Roco - Springer International Publishing 2015

[26] G. D'Agostino, R.Cannata, V. Rosato, "On modelling of inter-dependent network infrastructures by extended Leontief models" LNCS - Critical Information Infrastructures Security 1-13, 2009, Springer Berlin Heidelberg

Layer 2 Encryption: Securing Carrier Ethernet and MPLS Networks against Espionage and Attacks

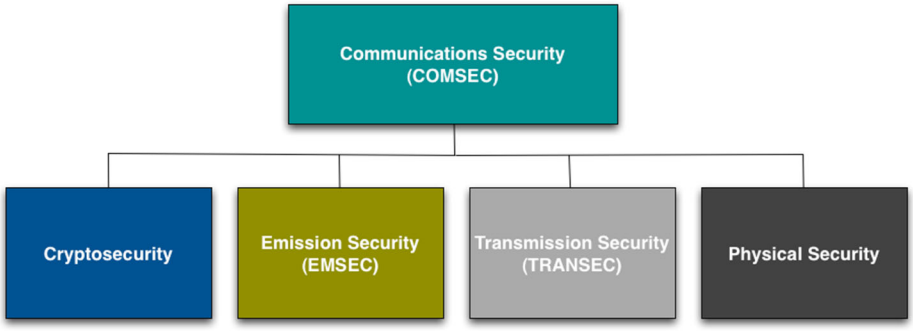
Advanced encryption solutions provide protection for mission-critical data networks at layer 2, 2.5 and 3 of the OSI network protocol stack.

Network Security

In today's world data networks are mission-critical. Metro (MAN) and Wide Area Networks (WAN) handle the data traffic between different sites. Due to their function and the data they carry, MANs and WANs are a prime target for espionage and attacks. Foreign governments, state-sponsored actors, criminals, terrorists and lone actors are increasingly targeting data networks. On their agenda: Espionage, infiltration and disruption. The tapping of network data is unpreventable. It is common practice and the difference in behaviour between state and criminal organizations in that respect is minimal. The goals are used to justify the means. Next to the simple "passive" tapping of networks there is a multitude of possibilities to actively attack networks. It is thus not a question if security measures are needed; it is only a question which security measures are the most efficient and the most secure. Fortunately there are adequate means to minimize the impact or even completely prevent the success of such attacks. It is the combination of crypto security, emission security, transmission security and physical security. The sum of it is known as Communications Security (COMSEC).

Today's network security architecture is based on the principle of network segmentation, also known as zoning. A zone demarcates a logical area within a networking environment with a defined level of network security. Zones are used to define the network boundaries and their associated perimeter defence requirements. Segmentation comes with security and cost benefits. It allows using the most efficient security approach for each zone as security challenges differ dependent on usage scenario and network layer. Metropolitan and Wide Area Networks can either be in separate groups or in a combined segment, as both are static mission-critical networks crossing public ground and often using a third-party network transport infrastructure.

For network security simple data encryption is insufficient. The requirements are substantially higher as the integrity of the transmitted data has to be ensured as well as the authenticity of the sender. On top of that any intrusion has to be detected and prevented. What makes network encryption particularly challenging is the fact that it must not limit network functionality and must cope with network-specific behaviour. This requires additional functionality such as variable encryption offsets and replay windows.



Christoph Jaggi

Christoph Jaggi works as technology, strategy and marketing consultant.

e-mail: cjaggi@uebermeister.com

http://www.uebermeisster.com

More detailed information is available on the author's website.

If attacks on an encrypted network fail to provide the desired results, the attacker will concentrate its efforts on the encryption devices. Therefore the security of the cryptographic module must be assured as well as the security of the encryption devices.

Secure Encryption Device

Network security starts with a secure encryption device. It is less complex to secure a dedicated device than a portion of a larger device. Although there are many less access possibilities to a dedicated device than to and within an integrated appliance or a virtual appliance, there is still the requirement to secure every single one of them. The encryption device must be fully secured against attacks from the inside and the outside. This is quite difficult by itself. The more access possibilities, the higher the complexity and the risk of vulnerabilities. Most dedicated appliances are optimised for security and meet the highest assurance requirements. The systems form a closed and tested environment that has been proved to be secure. They only provide the interfaces that are absolutely necessary. For integrated and virtual appliances it is between difficult and impossible to provide such a security level. There are simply too many gateways to be secured.

Secure Keys

Weak or accessible keys compromise any encryption. Key security starts with key generation and continues with key storage and key exchange. Hardware plays again an important role. For generating a secure key you need true random numbers. A properly engineered hardware-based true random-number generator will provide the needed randomness. Software-based random-number generators lack the needed entropy source and can only generate pseudo random numbers. It is often the lack of real and sufficient randomness that compromises key security from the beginning.
Most dedicated appliances provide hardware-based true random number generation, a fully secured key storage and a secured casing. The protection can include measures against emissions. Any attempt to tamper with the unit will result in the immediate emptying of the key storage and the notification that an attempt at tampering took place. The casings are tamper resistant.
One fact that often doesn't get the attention it deserves: Encryption uses the key in plaintext. The security of the environment in which key is used is thus a decisive factor.

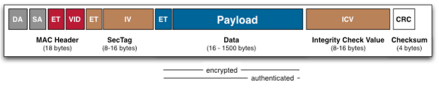
Processing Layer	Processing Mechanism
Layer 3: IP (Internet Protocol)	routed based on IP address
Layer 2.5: MPLS (Multiprotocol Label Switching)	switched based on MPLS tag
Layer 2: Ethernet	switched based on MAC adress

Encryption Layer	Usage Scenario and Protection
Layer 7: Application Layer	Remote Access
Layer 4: Transport Layer (TLS/SSH)*	Remote Access
Layer 3: Network Layer (IP)	Remote Access Site-to-Site Network Multi-Site Network
Layer 2: Data Link Layer	Hop-to-Hop Network (direct link) Site-to-Site Network Multi-Site Network
Layer 1: Physical Layer	Hop-to-Hop (direct link)

*Layer 4 establishes the foundation, but the actual encryption takes place on layer 7

Protecting Data in Transit

State-of-the-art encryption algorithms such as AES-GCM provide protection of the frames in transit by combining a set of different basic security measures.



1. Payload encryption provides confidentiality of the data.

2. The foundation for the detection of data manipulation is provided by an integrity check value (ICV).

3. The signing of the integrity check value by the sender ensures the authenticity of the frame.

4. A counter ensures that no frames can be inserted into the network without being detected.

For networks that are part of a critical infrastructure additional transport-specific security measures come into play:

1. Tunneling hides the internal network addresses and exposes only the network address of the encryptor.

2. Traffic Flow Security (TFS) fills unused network bandwidth with dummy traffic to prevent traffic analysis.

Securing Carrier Ethernet and MPLS Networks

Metro and Carrier Ethernet networks are layer 2 networks. It is thus obvious that the best approach to secure them is at layer 2. The lower the layer in the OSI network protocol stack, the more comprehensive are the protocols that can be encrypted and the more efficient the protection and the processing. Over 99% of attacks

happen at layer 3 or above. Encryption at layer 2 or below locks down all network data and prevents successful attacks on layer 3 or above.

MPLS networks operate at layer 2.5 and can either run over layer 2 or layer 3 networks. By securing at layer 2 and tunnelling over IP, layer 2 encryptors can support different MPLS scenarios. Some of them also provide a secure alternative to GET VPN for securing high-bandwidth WAN connections.

Key System

Ethernet frames come in three different variants, depending on the number of recipients of a frame:

- Unicast for the communication of one MAC address with a single other MAC address
- Multicast for the communication of one single MAC address with multiple MAC addresses
- Broadcast for the communication of one single MAC address with all other MAC addresses

Ethernet frames can also carry a VLAN tag (IEEE 802.1q). A VLAN is a virtual network that is logically separated from the other frames on the network. The VLAN tag also provides facilities for class of service (CoS) through a 3-bit Priority Code Point (PCP).

There are two different approaches to ensure that next to unicast frames also multicast and broadcast frames are properly encrypted: Pairwise keys and group keys.

For pairwise key systems a network consists of a multitude of point-to-point connections. Each encryptor is connected with each other encryptor by a point-to-point connection. Traditional pairwise key systems use unidirectional keys for the connection between the encryptorn endpoints.

Group keys are based on the principle that for the communication within a defined group the same key is used to encrypt the communication. The membership in one group does not exclude a member from concurrent membership in other groups. For the communication within different groups different keys are used. Keys are unique to a group and separate the groups cryptographically. A group consists of two or more members. Group membership can be e.g. based on VLAN-ID, multiple VLAN-IDs, MAC addresses and multicast group membership. Group key systems normally use a redundant key server setup or are set up in a distributed way. The key server takes care of providing the right group keys to each encryptor, so that the group members can communicate across sites. Another task of the key server is to ensure that a new key is generated and put in use if there is any change in the membership of the group. With the new key the old data traffic cannot be decrypted and with the old key the new data traffic cannot be decrypted.

Key Exchange

There are two different approaches to key exchange: One is symmetrical and the other one is asymmetrical. The asymmetrical approach needs more computing power but is considered to be more secure. Some physicists, technologists and mathematicians are assuming that a quantum computer with the proper algorithms could solve the mathematical problems used as foundation for asymmetrical key exchange within minutes and that powerful quantum computers might become a reality within the next decade. A big jump in security that also prevents successful attacks by quantum computers is therefore provided by a combination of asymmetrical and symmetrical key exchange, such as the combination of Diffie-Hellman with symmetrical encryption of the partial keys. A 256 bit AES key is used as signature and makes the key exchange immune against attacks from quantum computers.

In a symmetrical approach, all keys are directly derived from each other. First, a shared secret is entered into the encryptor. Then the encryptor generates internally a master key and encrypts the master key with the shared secret. The session key is also generated by the encryptor and is encrypted with the master key. Master key and session key are transmitted to the other encryptor in encrypted form. The big issue with this approach is the shared secret. If that shared secret ever becomes known, then all previously recorded data communication can be decrypted.

In an asymmetric approach the partial keys are generated completely inside the encryptor, without any user having access to it. After exchanging the partial keys both sides calculate the same shared secret. Contrary to a symmetric approach, nobody knows the shared secret. Subsequently the encryptor generates internally the master key and encrypts it with the shared secret. The encryptor also generates the session key and uses the master key to encrypt it. The transmission of the master and session keys from one encryptor is always encrypted.

Common asymmetrical approaches are Diffie-Hellman and RSA. Diffie-Hellmann uses in its basic variant the discrete logarithm problem, which comes with the disadvantage of needing very long partial keys to be really secure. The same is true for RSA. A more state-of-the-art variant is the use of Diffie-Hellman with elliptic curve cryptography (ECC), which provides better security with shorter partial keys. The security of ECC is heavily dependent on the curves used. Among experts the security of the NIST curves is severely in doubt. Appropriate security requires the choice between NIST curves, Brainpool curves and custom curves.

Asymmetrical approaches sign the partial keys that are exchanged to ensure that the correct remote station sends them. There are different ways to accomplish this: Either by using a certificate (X.509) in combination with appropriate procedures (RSA, DSA or ECC) or by encrypting the partial keys with a pre-shared secret. Most systems use a hybrid approach. Session keys are always symmetric.

The more frequent the sessions keys in use are replaced, the lower the probability that the key will be compromised. The security of the key does not only depend on the secrecy of the key, but also depends on the process used and the parameters chosen. The length of the counter and the ICV play an important role. E.g. in counter mode the key has to be changed before the counter starts back at 0. With group key systems it is therefore required that the system automatically changes the session key after a given number of minutes.

The same is true for the key encryption key (master key), which is used to encrypt the session keys. The exchange frequency is lower as it is only used to encrypt the session key and thus is used less often and encrypts less data. The regular exchange of master keys should take place automatically after a certain period of time. Key exchanges using Elliptic Curve Diffie-Hellmann are compute-intensive. Sufficient processing power of the encryptor is a requirement for keeping the lifecycle of a master key low, especially in large, complex networks.

The initial secrets should be exchanged every 12-24 months. They are the only manual key exchanges.

Management

Device management is an often-overlooked issue. Not everybody needs to have access to all the different management functions, especially network and security management need to be separated. Such a separation is also a pre-condition for Managed Security Services and Managed Encryption Services. The authentication of the user is based on the user identity, while the access is granted according to the role of the user. Typical roles include crypto officer, network management, maintenance and user). Roles with hierarchy levels allow mirroring actual hierarchies and responsibilities. Such a setup is also commonly used in managed security settings in which the customer needs the final control over changes to the security settings.

While preferable, a strict internal separation of users is difficult to achieve, as it also requires a separate memory space for each user.

Performance and Scalability

Dedicated appliances are optimised for performance. There is no competition for the available resources between different functionalities.

Integrated appliances are optimised for specific performance features that hardly ever can be fully exploited in parallel. Often cost considerations favour the use of ASICs (Application Specific Integrated Circuits) over FPGAs. Those ASICs support only a limited set of functions. If functions are used that are not implemented in hardware, they are executed in software, which leads to a performance loss. If the entire processing is executed on a standard CPU, the performance is limited to low and medium bandwidths and latency and jitter are increased. If the CPU is dedicated to a dedicated encryption appliance, the performance characteristics can be properly predicted and remain constant. A CPU that has to serve a range of different applications – as is typically the case with integrated appliances and virtualised environments – has a performance characteristic that is dependent on the particular load generated by other applications at a given time and thus is variable and unpredictable.

While scalability is less of an issue with point-to-point networks, it becomes an issue with point-to-multipoint and multipoint-to-multipoint networks. Dedicated appliances can often handle everything from small to large networks. Some deployments serve networks with more than 500 peers and group sizes exceeding 150 members.

Upgradeability

Dedicated layer 2 encryptors tend to be specified and dimensioned in a way that al-lows the expansion of the functionality at a later point in time. This is an essential requirement to keep the device state-of-the-art for the years to come. Amply dimensioned FPGAs (Field Programmable Gate Array) fit the bill, but they increase the cost. Underpowered FPGAs are quickly saturated and draw a high amount of power, which leads to extensive heat development.

Upgradeability and expandability are cost drivers and thus not high on the priority list for developers of integrated appliances. They prefer to focus on initial cost containment rather than on mid- to long-term cost efficiency and high assurance security. The cheapest way in mass-production is the use of ASICs, The only way to upgrade an ASIC is to replace it.

Software-based real and virtual appliances running on standard CPUs can easily be upgraded, but are substantially less powerful. Extensions of the software functionality can accentuate this lack of performance.

Links to in-depth background:

www.uebermeister.com/files/inside-it/2014_Introduction_Encryption_Metro_and_Carrier_Ethernet.pdf
www.uebermeister.com/files/inside-it/2014_Evaluation_Guide_Encryptors_Carrier_and_Metro_Ethernet.pdf
www.uebermeister.com/files/inside-it/2015_market_overview_Ethernet_encryptors_for_Metro_and_Carrier_Ethernet.pdf

Evolving threats and vulnerability landscape: new challenges for the emergency management

The International Emergency Management Society Conference, Roma September 30- October 2, 2015

Nowadays, communities rely on services provided by technological infrastructures. These are modern "lifeline systems" physically tying together urban areas, communities, and neighbourhoods, and facilitating the growth of local, regional, and national economies. These (inter)dependent systems work together to provide essential services to modern societies which are thus strictly dependent on the capability of exploiting the capacities provided by such technological resources and assets. The use of infrastructures contributes furthermore to reshape and improve relationships between communities, government, private sectors, non-profit communities and citizens. For that reason, citizens are more and more directly involved in supporting public services and infrastructure systems (e.g. transportation, energy, education, health and care, etc.) for example through so-called open data, living labs and tech hubs. These future developments will further improve the sustainability of our societies.

On the other side, crises due to natural (or anthropic) related events might seriously endanger these infrastructures and weaken the fruitful feedbacks they supply. Disasters are thus dramatic events which, other than producing casualties, break the connections between citizens and between citizen and the community, thus producing relevant social damages.

The TIEMS Conference, organised by the TIEMS Chapter Italy and hosted by the Istituto Superiore Antincendio (i.e. Italian Firefight Academia) has been aimed at investigating what are the new challenges in the field of risk and disaster management (also in relation to infrastructure integrity and service continuity) to face old and new type of threats by bring together leading researchers, practitioners and industries from all areas of emergency management to take advantage of the presented methodologies and practical applications. In particular the Conference aimed at evaluating gaps and the constraints that need to be overcame to improve the response capacities of first responders and the resilience of communities exposed to several type of hazards and threats.

The Conference covered all aspects related to Emergency Management, Risk Analysis and Preparedness activities, either for predicting Critical and/or for managing hot phases.

Presentation included aspects like:

- risk reduction and mitigation techniques,
- cyber-physical threats and vulnerability analysis,
- model-based and experimental assessment of safety, reliability and security,
- human and social aspects in emergency managements, and
- management of complex emergency scenarios and epidemic spreading.

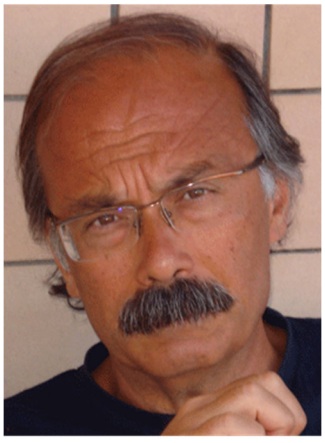
With more than 250 registered participants and 67 oral presentations, the organiser's expectations were overcome. The broad variety of topics is also reflected in the topics covered by keynote speeches and the related thematic sessions:

- Dr. Meen P. Chhetri (NCDM, Nepal) - "Nepal earthquake aftermaths";
- Ing. M Dolce (General Director of Italian Department of Civil Protection, Italy), "The Italian Dept. of Civil Protection (DPC) and its role in the Emergency Management";
- Dr. Kim, Jae-Kwon (Korean Society of Disaster & Security), "Sewol Ferry Disaster and Emergency Response Management in Korea";

Carmelo Di Mauro

Carmelo is an environmental Engineer with more than twenty years experience in the applied science, in particular in the field of risk-based decision-making processes.

e-mail: carmelo.di-mauro@jrc.it



Vittorio Rosato

Head of the Laboratory for the Analysis and Protection of Critical Infrastructures at ENEA Casaccia Research Centre in Roma.

e-mail: vittorio.rosato@enea.it

- Scenario prof. John Hamilton (Kestrel Group, New Zealand), "Emergency Management after the Christchurch earthquake" (video interview by dr. Sonia Giovinazzi, University of Canterbury in Christchurch, NZ);
- Prof. Dirk Helbing (ETH Zurich, Switzerland), "How to Increase Systemic Resilience in an Information Rich World";
- Dr. Nicola Perra (University of London-Greenwich Business School), "Modelling and Forecast of epidemic events"
- Dr. Daniel Stevens, (Director of Emergency Management at City of Vancouver - Canada) "Emergency Management and Resilience in the metropolitan area of Vancouver";
- Dr. David Bamaung, (Scottish Government, Scotland, UK), "Critical Infrastructure Resilience and Public Private Collaboration";
- Dr. Ji Zhang, (Harmony Technologies Ltd, CHINA), "Ten years development in China Emergency Management 2006-2015".

Besides many invited and contributed talks, the conference participants especially enjoyed a vivid roundtable discussion titled "Lesson Learnt from the Nepal Earthquake event: what still are the main challenges to improve the disaster management and the role of emerging technologies" with the main contribution of

- Prof. Dr. Meen B. Poudyal Chhetri – President, Nepal Centre for Disaster Management
- Dr. Guosheng Qu, Dep. General Team Leader of CISAR, China
- Dr. Kailash Gupta - Honorary Managing Trustee, TIEMS India Chapter
- Jaroslav Pejcoch, T-SOFT (Crisis management, Interoperability, Security), Czech Republic
- Prof. Carl W. Taylor, Fraser Institute for Health and Risks Analytics, Princeton
- Ing. Mauro Dolce, Italian Civil Protection, Italy

Due to the proximity of the Conference to the tremendous disaster hitting Nepal on April 25, 2015, the Conference has focused the first day around that event, by hosting a number of relations documenting the event (which produced over 8.000 casualties and more than 21.000 injured) and its aftermaths. An extensive report has been provided by prof. Meen Chhetri, President of the Nepal Center for Disaster Management through a clear exposition of the facts and the management actions of several international groups called to collaborate. A similar focus has been also provided on another recent disaster occurred in New Zealand in 2009 (Christchurch earthquake) provided by the keynote of prof. John Hamilton, former Director of New Zealand Civil Protection that, through a video interview recorded by dr. Sonia Giovinazzi of the University of Canterbury (NZ) has recalled the major problems arising in the Christchurch earthquake and the following lesson learnt incorporated into the NZ Disaster Management protocols.

The Conference also hosted a special workshop co-organized by Dennis Andersson (FOI), Josine van de Ven (TNO), Maciej Szulejewski (ITTI) on "Pan EU lesson sharing crisis management: DRIVER Project" which aimed to identify what types of methods and tools can support the lesson sharing process European Member states and how such lessons can be transferred to other organisations.

Large emphasis and interest has been triggered by prof. Helbing's keynote on the revolutionary project of providing the planet of a "nervous system" made by open and shared data collected by mobile devices which could contribute to build a digital democracy, also providing invaluable support to Emergency Management.

The main outcome of the Conference was that many approaches in the disaster risk management area are still mainly sector-specific. The concept of resilience is becoming a key reference in disaster risk management, acknowledging that arising awareness of experts and as well as laypeople that all social assets can be protected. The conference discussions also identified the strengthening of infrastructures as an important field for disaster risk reduction. Although the respective research is valuable in order to learn more about the system characteristics and potential disaster risk reduction measures, it remains often vague how society is or could be affected by their failure. In order to reduce societal effects, a broader perspective needs to be carefully evaluated since the CIs impact on the functioning of many societies are not yet fully understood. This aspect will increase its importance in the future when communities will become more "Smart" i.e. they will heavily rely on ICT technologies and other advance infrastructure services. If from one side the future development will link networks supporting and positively feeding off each other, from the other one such inter-dependency may be prone to failures that can be propagate through a number of systems and that may results in a more severe impact for the communities. In other terms, future communities will count on more efficient services but at the same time may become more vulnerable due to complexity of interconnection of sophisticated infrastructure and services. This implies the need to develop new approaches and strategies to cope with hazards and disasters.

The all TIEMS Chapter Italy would like to thank again all participants and speakers that contributed to make this event a success.

ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids

The goal of this project is to mitigate electricity theft due to attackers who hack smart meters and under-report electricity consumption. Such attacks have begun taking place in Europe and, if gone unchecked, pose a threat to the availability of power supply, a critical infrastructure resource.

In addition to the well-known benefits of smart meters, such as automated data collection and estimation of the state of the electric distribution grid, utilities such as BC Hydro believe that these meters would aid them in detecting electricity theft. This belief was challenged in 2010, when the Cyber Intelligence Section of the FBI reported that smart meters were hijacked in Puerto Rico, causing electricity theft amounting to annual losses for the utility estimated at $400 million. More recently, in October 2014, BBC News reported that smart meters in Spain were hacked to cut power bills. These reports indicate that there could be a growing number of thieves, referred to as attackers, in the power network, which could lead to electricity theft on a large scale.

Smart meters are increasingly being deployed to measure electricity consumption of residential as well as non-residential consumers. It has been recently reported that consumers were hacking their meters to under-report consumption. Compromising meter readings can cause operators, who rely on these readings, to misjudge true demand, and not schedule the required generation potentially leading to outages. The contribution of this work is to ensure that theft is drastically mitigated, so that theft cannot adversely impact power grid operation.

Objectives

The anomaly detection methods presented in this paper assume that an attacker has compromised the integrity of smart meter consumption readings, and aim to mitigate the impact of such an intrusion in the context of electricity theft. How the attacker can get into a position where he is capable of modifying communication signals is not a focus of this work and is discussed in related work. Our approach is to validate the data reported to the utility by modelling the normal consumption patterns of consumers and looking for deviations from this model. We use data-driven insights on consumption characteristics, similar to our award-winning work "PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure", which employs Principal Component Analysis and clustering. Also, our algorithms for intrusion detection are specific, as opposed to high-level security guidelines for network administrators.

Summary of contribution

The Auto-Regressive Moving Average (ARMA) and Auto-Regressive Integrated Moving Average (ARIMA) models are used to predict future data points in a time series. We show that the ARIMA model is a better model for capturing consumption behaviour and forecasting future behaviours. We evaluate the effectiveness of ARIMA forecasting in the context electricity theft. Finally, we propose additional checks that can mitigate the total amount of electricity that can be stolen by an attacker by 77.46%. Our evaluation is based on an open dataset of meter readings from a real deployment with 450 consumers.

Varun Badrinath Krishna

Varun is a graduate student in the Electrical and Computer Engineering department and a research assistant in the Information Trust Institute, University of Illinois at Urbana-Champaign, USA. With Prof. William H. Sanders, Varun is researching data-driven methods to secure communications in power grids, a critical infrastructure. He is Co-PI on that project, partially supported by the Siebel Energy Institute, and leveraging the Blue Waters supercomputer at National Center for Supercomputing Applications, USA. His papers won the best paper award at QEST 2015 and CYCA at CRITIS 2015. This work received contributions from Prof. Sanders and Prof. Ravishankar Iyer.

e-mail: varunbk@illinois.edu
University of Illinois at Urbana-Champaign,
1308 W. Main Street, Urbana, Illinois, 61801

Dataset Used in the Study

The data we used was collected by Ireland's Commission for Energy Regulation (CER) as part of a trial that aimed at studying smart meter communication technologies. This is the largest, publicly available dataset that we know of. The fact that the dataset is public makes it possible for researchers to replicate and extend this paper's results. The data is accessed via the Irish Social Science Data Archive at www.ucd.ie/issda. The providers of the data, the CER, bear no responsibility for the further analysis or interpretation of it.

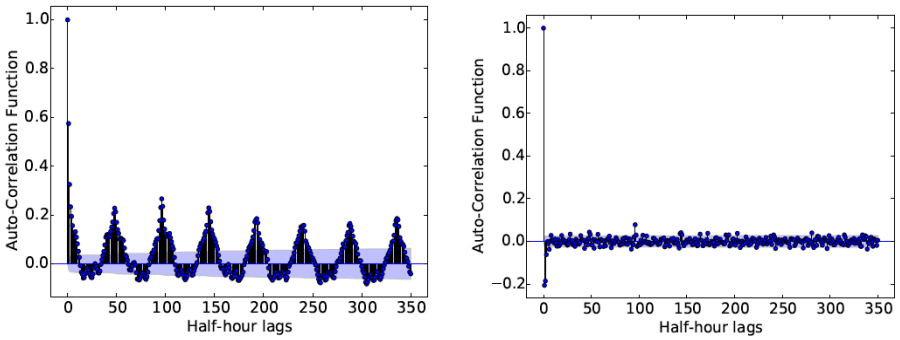
We evaluate our models and algorithms on 450 consumers from this dataset. For each of these consumers, the smart meter readings are collected at a half-hour time resolution, for a period of up to 74 weeks. The consumers include 377 residential consumers, 18 small and medium enterprises (SMEs), and 55 unclassified by CER.

We assume that this dataset is free from maliciously compromised measurements, and use the data to understand and model normal consumption behaviour.

Modelling Approach

The underlying assumption of the ARMA model is that the time series data is weakly stationary. Stationary data has three characteristics: (1) the mean is constant, (2) the variance is constant and (3) the covariance of the signal with itself at different time lags is constant. We define a weakly stationary signal as one that fails condition (1), but satisfies conditions (2) and (3). The moving average component of ARMA automatically adjusts for changing means, so condition (1) is not important for the suitability of ARMA for a given time series.

The ARMA model does not handle largely changing covariance in non-stationary signals. Fig.1 (a) illustrates the Auto-Correlation Function (ACF) for a single consumer. The ACF is the correlation of the time series with itself at a specified lag. We extract the time series for a single consumer and depict the ACFs for 350 half-hour lags. There are 336 half-hours in a week, so the figure captures a little over a week. As expected, high auto-correlation was observed for this consumer at multiples of 48 half-hour



(a) ACFs without differencing (b) ACFs with first-order differencing

Figure 4: Auto-Correlation Function (ACF) of the electricity consumption of a single consumer

(or 1 day) time periods. These high correlations persist for all lags throughout the consumption history captured in the dataset.

Further, the plot demonstrates failure of the third requirement for stationarity since the ACFs change significantly over time. This lack of stationarity implies that the ARMA model would fail to provide a reliable prediction of the next point in the time series. The ACFs need to rapidly decrease to constant or insignificant values in order for the ARMA model to reliably work. The rate of ACF decrease will determine the model order.

We propose an alternative model, the ARIMA model, which has an additional differencing term. We find that first-order differencing causes rapidly decreasing ACFs for consumers who have non-stationary consumptions. Instead of predicting the next value in the time series, we predict the difference between the current and next value in the time series as a linear function of past differences. After applying first-order differencing, we observe Fig.1 (b). Clearly, the ACFs are close to zero beyond 3 time lags. Therefore, the order of the ARIMA model is finite. In addition, the order is small, which is important to ensure minimal computational costs.

We have applied first-order differencing and observed its benefits for one consumer, but visual inspection is impractical for our dataset of 450 consumers. Therefore, we employ the Hyndman-Khandakar algorithm to estimate the model order. This method combines cross-validation techniques, unit root tests, and maximum likelihood estimation. The results revealed that for 92% of consumers, first-order differencing is required, justifying our ARIMA model proposal.

Once the ARIMA model is estimated, the next consumption point in the time series is forecast. From this point forecast, a 95% confidence interval is constructed with the assumption of independent and identically distributed Gaussian errors in the Moving Average model.

Electricity Theft Attack

The ARIMA confidence interval provides a bound on the amount of electricity an attacker can steal. Without the ARIMA detection mechanism in place, the attacker can steal an arbitrary amount of electricity. He is only constrained by the physical limits of the electric distribution system. Specifically, electric distribution lines are rated based on the maximum current that they can carry. If the demand from the attacker increases (while the distribution voltage is kept approximately constant by reactive power compensation), the current in the distribution lines will increase. If the current increases beyond the rated threshold, the lines will exceed their thermal limits. The ensuing damage may lead to blackouts or other equipment failures. Although this is not an electricity theft attack, it highlights what can happen if operators rely on meter measurements that may be compromised.

We consider a specific attack model in which the attacker steals electricity from a neighbor for monetary gain. The attacker compromises his own smart meter and under-reports his consumption. In addition, to avoid detection by industry techniques, he also compromises his neighbour's smart meter and over-reports the neighbour's consumption. To further mitigate the amount of electricity that can be stolen by the attacker, we augmented the ARIMA confidence interval with checks on

mean and variance of the attacker's consumption pattern. The mean and variance were compared against historic data in the dataset.

Evaluation

The evaluation of our anomaly detection method was performed using the CER dataset from Ireland. We injected well-crafted attacks, as described in the publication, that maximise the attacker's gain in electricity theft. For each of the 450 consumers, we evaluated the maximum amount of electricity that could be stolen.

Results

Although the ARIMA confidence intervals bounded the attack, an attacker could steal up to 285,914kWh from 450 neighbours in one week. However, with additional checks on mean and variance of the data reported by the attacker, the worst-case attack would lead to 64,447kWh being stolen.

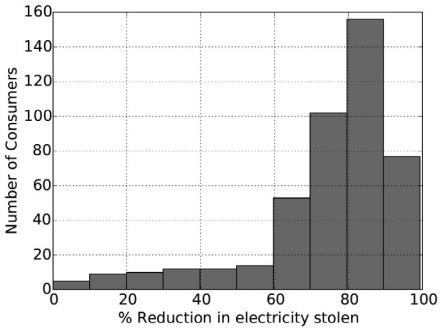


Figure 5: Savings obtained by additional checks on mean and variance of data reported by attacker per consumer.

The maximum amount of electricity that could be stolen from each neighbour was naturally reduced by additional checks on mean and variance, leading to the aforementioned reduction for the entire week. Fig. 2 captures this reduction. For most neighbours, a savings of over 70% was observed. In the best case, 99% of theft was reduced, which emphasises the benefit of the additional checks.

CYCA 2015

This work was presented as a research paper at the 10th International Conference on Critical Information Infrastructure Security (CRITIS 2015), and Varun was awarded the CIPRNet Young CRITIS Award (CYCA). As the authors of this work, we are truly honoured to have received this recognition from CIPRNet.

Collaborators

This work performed with guidance of Varun's PhD advisor, Prof. William H. Sanders, and Prof Ravishankar K. Iyer.

Prof. William H. Sanders is the Donald Biggar Willett Professor of Engineering and Head of the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign. He is a Fellow of the IEEE, the ACM and the AAAS, a past Chair of the IEEE Technical Committee on Fault-Tolerant Computing, and past Vice-Chair of the IFIP Working Group 10.4 on Dependable Computing. He was the founding Director of the Information Trust Institute at Illinois (2004-2011), and served as Director of the Coordinated Science Laboratory at Illinois from 2010 to 2014. His research interests include security and dependability metrics and evaluation, with a focus on critical infrastructures. He has published more than 250 technical papers in those areas. He was the Director and PI of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center, which is at the forefront of national efforts to make the U.S. power grid smart and resilient.

Prof. Ravishankar Iyer is the George and Ann Fisher Distinguished Professor of Engineering at the University of Illinois at Urbana-Champaign. He holds joint appointments in the Department of Electrical and Computer Engineering, the Coordinated Science Laboratory (CSL), and the Department of Computer Science, and serves as Chief Scientist of the Information Trust Institute. Iyer has led several large successful projects funded by NASA, DARPA, NSF, and private industry. He currently co-leads the CompGen Center at Illinois. Funded by NSF and partnering with industry leaders, hospitals, and research labs, CompGen aims to build a new computational platform to address both accuracy and performance issues for a range of genomics applications. Professor Iyer is a Fellow of the AAAS, the IEEE, and the ACM. He has received several awards, including the American Institute for Aeronautics and Astronautics (AIAA) Information Systems Award, the IEEE Emanuel R. Piore Award, and the 2011 Outstanding Contributions award from the Association of Computing Machinery - Special Interest Group on Security for his fundamental contributions in secure and dependable computing. Professor Iyer is also the recipient of a degree of Doctor Honoris Causa from Toulouse Sabatier University in France.

If you would like to access this publication, and other related publications by Varun and Prof. Sanders, please visit Varun's University of Illinois profile:
http://www.ece.illinois.edu/directory/profile/varunbk

This project was supported by the U.S. Department of Energy under Award Number DE-OE0000097 and the Siebel Energy Institute.

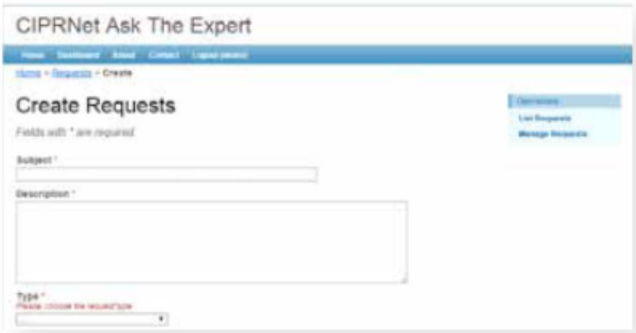
Ask the Expert service

Brought to you by CIPRNet –
the Critical Infrastructure Preparedness and Resilience Research Network

A chance to reach a critical mass of experts in CIP

The Ask the Expert service is a platform of experts in various domains of crisis management and critical infrastructures protection created to answer questions and help solving problems in the areas such as:

> Technical challenges for CIP;
> CI management, crisis management for CI;
> CI-related documentation, e.g. national and EU regulations, policies, public reports and statistical data;
> Practical aspects of CI operation.



Who are the experts?

CIPRNet consortium partners and key representatives from CIP research communities and in area of:

> Modelling, simulation and analysis,
> Monitoring and control,
> Risk analysis, assessment and management,
> Telecommunication and cyber security,
> Transportation, and many others.

How can we help you?

By answering the questions, Ask the Expert service of the CIPRNet project and portal helps solving current and future problems and challenges of critical infrastructures. We can explain past cases, discuss emerging problems and direct you to relevant documents, regulations and strategies.

For Whom?

> Public administration,
> CI operators,
> CIP experts,
> Practitioners in the CIP area,
> Citizens and society.

Exemplary questions

> Where can I find reports about CI cascading effect after the L'Aquila earthquake in 2009?
> What are the cyber security challenges to be taken into account while designing smart grids?

Where and how?

1. Register to access the service: http://ciprnet.casaccia.enea.it/ate/
2. Check your e-mail to activate your account
3. Log in to the service
4. Once you are logged in, you can use your service dashboard to ask the question

CIPRNet

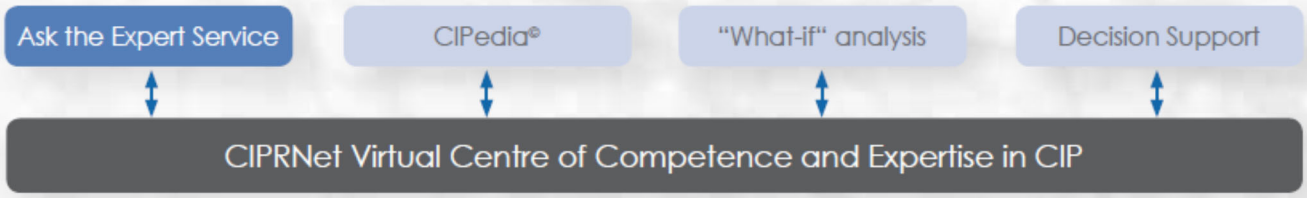
Critical Infrastructure Preparedness and Resilience Research Network – background information

CIPRNet establishes a Network of Excellence in Critical Infrastructure Protection (CIP). CIPRNet performs research and development that addresses a wide range of stakeholders including (multi)national emergency management, critical infrastructure operators, policy makers, and the society. By integrating resources of the CIPRNet partners acquired in more than 60 EU co-funded research projects, CIPRNet will create new advanced capabilities for its stakeholders. A key technology for the new capabilities will be modelling, simulation and analysis for CIP. CIPRNet builds a long-lasting virtual centre of shared and integrated knowledge and expertise in CIP.

Co-funded	EU FP7
Instrument	Network of Excellence (NoE)
Start date	March 1, 2013
Duration	48 months
Partners	12
Proposal number	312450

CIPRNet partners:

1. Fraunhofer IAIS	Fraunhofer IAIS	7. Deltares	Deltares
2. ENEA	ENEA	8. University of Cyprus	
3. TNO	TNO innovation for life	9. UTP	
4. UIC	uic	10. UCBM	
5. CEA	cea	11. University of British Columbia	UBC
6. Joint Research Centre		12. ACRIS GmbH	acris



CIPRNet Virtual Centre of Competence and Expertise in CIP

CIPRNet will create the tangible VCCC already during the project term. The VCCC serves as the foundation of a long-lasting network of facilities providing enduring support from research to CI stakeholders in EU Member States. This network of facilities has the working title EISAC (European Infrastructures Simulation and Analysis Centre). A European headquarters shall foster standardisation of technology, organise cross-border collaboration, and provide support at EU level.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The European Commission's support is gratefully acknowledged.
The contents of this document and the view expressed in the publication are the sole responsibility of the author and under no circumstances can be regarded as reflecting the position of the European Union.

European CIIP Newsletter
Call for Papers

October 16 – February 17, Volume 10, Number 3

Special Issue on Cybersecurity:

Challenges Landscape and Solutions

Call for Papers ECN Special Issue:

Cyber security landscape, challenges, initiatives & solutions

Guest editors are calling for European and International contributions to reach best possible coverage for depicting state-of-the-art.

Nowadays, cyber security should be considered as a crucial aspect of critical infrastructure protection. Currently, the networked mission critical systems and national critical infrastructure might be vulnerable to cyber threats, cyber-crime and cyber terrorism. The same hazards apply to citizens and small scale ICT systems (e.g. used by SMEs).
Therefore, we cordially invite prospective authors to submit ECN-like papers (https://www.ciprnet.eu/ecn.html) on the following topics (list is not exhaustive, and my be prolonged by your contribution):

- Information and presentation about past and ongoing cyber security research projects
- Research lines, directions, results and ideas
- Information on current initiatives (groups, strategies, formal and informal bodies) in the area of cyber security
- Presentation of cyber security strategies
- Emerging research areas and techniques in cyber security
- Presentation of cyber security labs
- Cyber security case studies
- End-users views, needs and opinions

Guest Editors:

Prof. Michal Choras and Dr Rafal Kozik

University of Science and Technology, Bydgoszcz, Poland

Contact:
chorasm@utp.edu.pl

Paper submission deadline: 15.06.2016

Please send your submission to:

chorasm@utp.edu.pl

Smart grid networks: models & communities

Overview on standards, communities and advancement

Introduction

In this paper we address the Next Generation Infrastructures and smart grids in particular. Those new networked approaches and technologies bring new opportunities, but also new challenges and threats.
Next Generation Infrastructures operation and secure design are also a part of the analysis performed in the FP7 project CIPRNet.
Hereby, we focus on smart grids, and present the smart grids models, architectures as well as the communities involved in smart grid technology.

Smart grid models

There is not a one definition of a smart grid and no one-fit-all model. There are different models of implementing smart grids and they have to be based on and adjusted to the potential of existing grids and specific local requirements.

A smart grid is a highly complex system where ICT play a crucial role, ensuring communication between different smart grid system components. These different components have to be interoperable and thus there is a need for standardisation as regards the technical solutions used in the smart grid, interfaces, communication protocols and also processes. There exist a number of standards related to introducing smart grids developed by the International Electrotechnical Commission (IEC) and the National Institute of Standards and Technology (NIST). There are initiatives that aim at giving guidance on how to introduce the standards and to provide the models describing smart grid functions and technology. A group of institutions in Europe, the European Commission's Mandate 490 (M/490) for Smart Grid, the European Telecommunications Standards Institute (ETSI), European Committee for Standardization (Comité Européen Normalisation – CEN), and the European Committee for Electrotechnical Standardization (CENELEC), created the CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture. NIST developed a Framework and Roadmap for Smart Grid Interoperability Standards. The experts behind those initiatives in Europe and in the United States have started a cooperation with the aim to align their work results.

The European Reference Architecture was proposed in November 2012 but the work continues and the update is to be expected soon. The NIST Framework was proposed in September 2014 (3rd release).

Smart Grid Reference Architecture
The European Commission's Smart Grid Reference Architecture is a widely accepted model in Europe. The mandate presents a consistent architecture composed of a set of standards, digital computing and communication technologies and electrical architectures, the processes and services. Its aim is to foster an easier adoption of smart grids in Europe. The mandate does not cover business models. The Smart Grid Architecture Model (SGAM) has been proposed in the mandate, which is based on different approaches and methodologies of building a smart grid infrastructure. The SGAM is composed of five core viewpoint layers: Business, Function, Information, Communication, and Component, taken from the Gridwise Alliance Architecture Council (GWAC). The Business layer focuses on business strategic goals, processes and services and it also concerns regulations. The Functional layer contains the description of use cases including logical functions or services independent from physical implementation. The third, Information layer, provides the information objects and data models that are being used and exchanged between functions, services and components and that ensures interoperability in information exchange by providing the common semantics for

Prof. Michał Choraś

Prof. Michał Choraś holds the professor position at University of Science and Technology (UTP) where he is the Head of ZST Division. He also works as the consultant in security and coordinates projects (e.g. FP7 CAMINO on cyber crime and cyber terrorism). He is the author of over 150 publications.
e-mail: **chorasm@utp.edu.pl**

Patrycja Młynarek
Consultant at ITTI Sp. z o. o., Poznan, Poland. Manages and contributes to EU and commercial projects. Work areas: IT@telecom market and services, ICT, security, technology transfer, evaluations and market research, regulations, funds acquisition (e.g. FP6, FP7, H2020, structural funds).
patrycja.mlynarek@itti.com.pl

functions and services. The Communication layer contains protocols and mechanisms for the exchange of information between components. The last, Component layer, describes physical components which host functions, information and communication means.

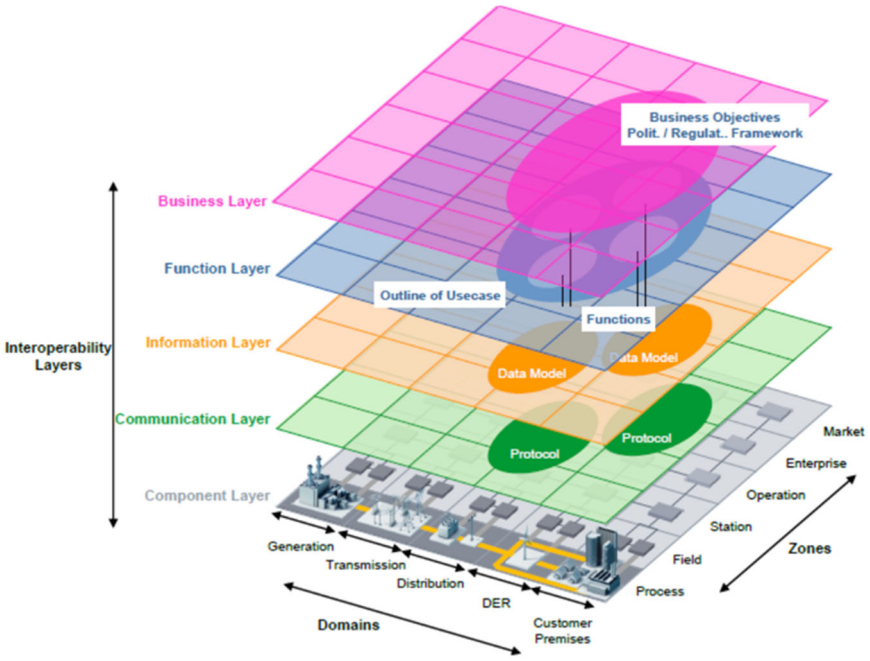


Figure 6: SGAM Framework (source: CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture 2012)

The SGAM layers are divided each into five domains and subdivided in six zones. The domains are Generation, Transmission, Distribution, DER, and Customer Premises. The zones are Market, Enterprise, Station, Operation, Field, and Process. The SGAM framework (called SGAM cube) is presented in Figure 1.

The presented model may be used to make a description of the current infrastructure, the possible data flows, the comparison of the current situation to the future, planned one. It will help identify standards that should be applied in the individual layer, domains and zones and to verify whether there is no overlap between standards. A crucial advantage of SGAM is that it provides a good visualisation of an overall smart grid infrastructure, which is a highly complex system of systems, and of the interactions of the stakeholders concerned. The SGAM is flexible and will be updated in order to address new technical deployments.

Framework and Roadmap for Smart Grid Interoperability Standards

The NIST Framework and Roadmap for Smart Grid Interoperability Standards is a reference architecture model for Smart Grids developed in the USA. In its latest release, 3.0, the model has been harmonised with the European Smart Grid Reference Architecture. NIST was made responsible to undertake such work under the U.S.' Energy Independence and Security Act (EISA) of 2007.

The NIST framework provides a holistic vision for the smart grids for the United States, based on relevant policies regarding the energy market in the U.S. NIST has been working on the subsequent versions of the framework with Smart Grid Interoperability Panel (SGIP), the smart grid community that it established in order to accelerate the development of standards and protocols for the interoperability of the smart grid. The status of SGIP has changed over the years and is now an industry-led non-profit organisation. An important feature of the NIST framework is that it provides a list of protocols and standards that support interoperability of smart grid devices and systems and that are the building blocks for the smart grid. The framework now contains over 65 standards or families of standards that ensure the smart grid system elements are interoperable and work seamlessly, be it wind turbines, solar panels, conventional generators, batteries, smart meters, transmission and distribution sensors etc.

The NIST architectural framework provides a general view of smart grid architecture, the processes and methodology of introducing the smart grid, with diagrams and descriptions that help identify the characteristics of the grid. Based on this high-level model different standard organisations may propose more detailed propositions.

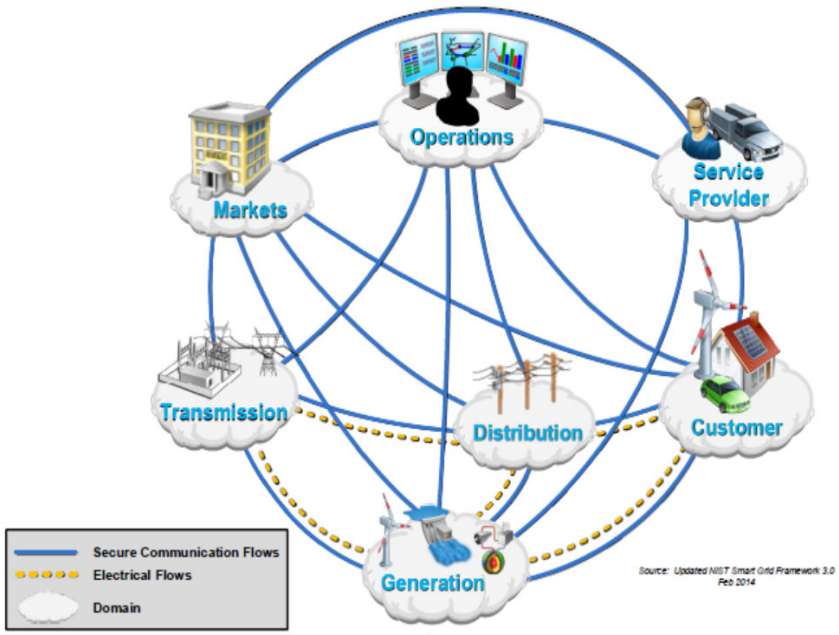


Figure 7: Original NIST Conceptual Domain Model (source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, 2014)

The cybersecurity framework describes standards, guidelines and strategies for the electric sector to ensure the security of the IT systems in smart grids, their confidentiality, integrity and availability. The issue of cybersecurity has been deepened in NIST Guidelines for Smart Grid Cybersecurity (NISTIR 7628), the most recent version of which dates from November 2014.

Domain Model and proposed an architecture matrix, presented in Figure 3.

NIST proposed the conceptual architecture in order to provide smart grid stakeholders building blocks they could use to easily and rapidly build the architectures of their own systems. This architecture contains abstract roles and

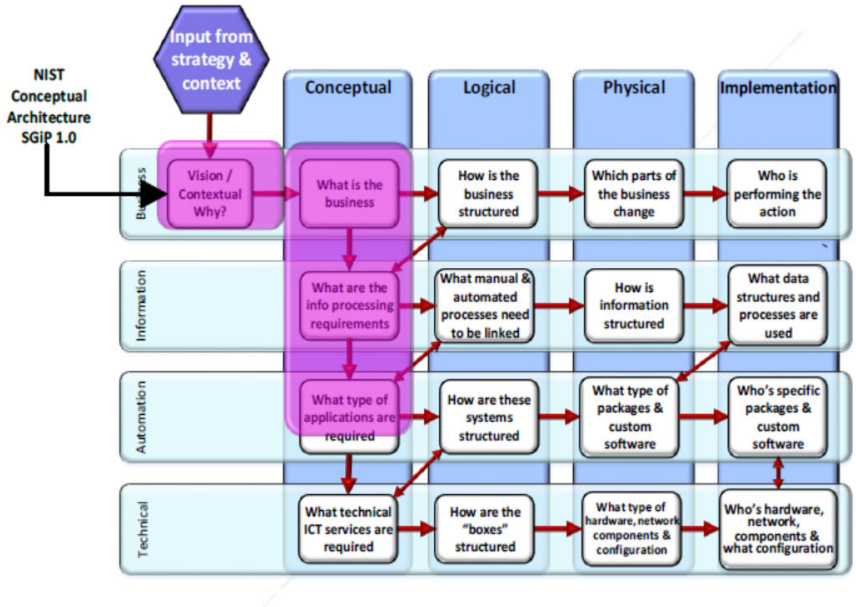


Figure 8: NIST Conceptual Architecture mapped onto the Architecture Matrix Service Orientation and Ontology (source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, 2014)

The framework is technology neutral and it enables all electric resources to contribute to the smart grid.
NIST originally created a conceptual domain model useful in activities such as planning, requirements development, documentation, and organisation of the diverse, expanding collection of interconnected networks and equipment composing the smart grid. The smart grid was divided into seven domains: Customer, Markets, Service Provider, Operations, Generation, Transmission, Distribution. The model is shown in Figure 2.

Each domain is assigned conceptual "roles" and "services" describing types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing identified goals, such as: customer management, distributed generation aggregation, and outage management.

NIST in its further work and in cooperation with different stakeholders modified the Conceptual

services necessary to support smart grid requirements and does not present details concerning application or interface specifications.

Smart Grid Maturity Model

There are several models that are very helpful for an electric power utility to assess itself and see where it is now in its way towards a smart grid and to get inspiration for the actions that are still needed. The first such model was the Smart Grid Maturity Model (SGMM) maintained by the Carnegie Mellon Software Engineering Institute (SEI) and it is addressed to electric power utilities that want to introduce the smart grid innovations. SGMM is a tool that will help utilities manage all aspects related to passing to smart grids. Using SGMM utilities will be able to tell in which areas they already made progress and to measure the progress, to prioritise the actions planned and to ensure all areas are covered.

SGMM covers eight domains and has overall 175 characteristics of a mature utility using smart grids. The eight domains are as follows:

- Strategy, Management, and Regulatory,
- Organisation and Structure,
- Grid Operations,
- Work and Asset Management,
- Technology,
- Customer,
- Value Chain Integration,
- Societal and Environmental.

A utility may make a self-assessment by analysing its own characteristics against the ones in the model.

The Electricity Subsector Cybersecurity Capability Maturity Model

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) covers the area of the electrical grid security. It has been created by the initiative of the USA government. This model has been created based on the Cybersecurity Capability Maturity Model (C2M2) that was designed to be used by any organisation to enhance its own cybersecurity capabilities (regardless of size, type, or industry) but it contains in addition some part that specifically concern the electricity subsector. Basing on this model it is also possible for an entity to make an assessment of its own maturity in the area of cybersecurity. Ten domains have been specified.

Smart grid communities

Smart Grids are an important concept that yet has a long way ahead before it is fully implemented and becomes an everyday reality. Research in Smart Grids is on-going and there are different initiatives that are pushing it forward.

There are thousands of grid operators worldwide that operate in different environments and many solutions emerge to meet their local needs and this fragmentation of research and of existing solutions is a big challenge. There does not exist a one organisation or initiative at a global or a European level that would coordinate the progress in Smart Grids, in research and in technology implementation but there are some initiatives that are important in this context and should be mentioned.

At the global level there exists the IEEE & Smart Grid organisation that aims at facilitating and guiding the evolution toward the Smart Grid. It gathers key stakeholders at different events, it fosters publications and standards and host a Smart Grid-related website. It has 395,000 members being research institutions, governments and companies and thus has the critical mass to take the leading role. IEEE runs the Xplore digital library with scientific articles on latest research in the Smart Grids area. Nearly 2,500 papers relevant to smart grid have been published in over 40 IEEE journals. The events organised by IEEE are e.g. "IEEE Innovative Smart Grid Technologies 2010" and the new "IEEE Smart Grid World Forum". IEEE has approximately 100 standards and standards in development focused on smart grid.

At the European level, there are a number of initiatives in the fields of Smart Grids. There are approximately 200 research, development and demonstration projects focused on Smart Grids. But the coordination between different activities is lacking, which constitutes a very big challenge, as without it the resources are not used as efficiently as they could be. Separate activities, even very good ones, do not have a chance to have a real impact on the whole or even on the majority of the Smart Grids community.

The European Strategic Energy Technology Plan (the SET-Plan) is an initiative aiming at accelerating the development and deployment of low-carbon technologies. It coordinates research and innovation and co-finances projects focusing on technologies enhancement and on ensuring their cost-effectiveness. The SET-Plan was adopted by the European Union in 2008 and it is the main tool supporting decision makers in the area of the European energy policy. The first major timeline for the SET-Plan is 2020, for a 20% reduction of CO2 emissions, a 20% share of energy from low-carbon energy sources and 20% reduction in the use of primary energy by improving energy efficiency. The second major timeline is 2050, for the worldwide transition to a low carbon economy (limiting climate change to a global temperature rise of no more than 2°C, in particular by considerably reducing greenhouse gas emissions). The SET-Plan's budget is approximately of €71.5 billion.

The SET-Plan encompasses several implementation mechanisms, such as the SET-Plan Steering Group, European Industrial Initiatives (EII), the European Energy Research Alliance (EERA), and the SET-Plan Information System (SETIS). One of the European Industrial Initiatives is focused on the Smart Grids sector: the European Electricity Grid Initiative (EE-GI). EEGI is a 9-year programme (until 2018) for research, development and demonstration to foster innovation of the electricity networks. EEGI brings together all stakeholders in the Smart Grids sector, such as researchers, industry, EU Member States and the European Commission and its focus is on system innovation and on integration of new technologies in real life conditions.

An important initiative that considerably contributes to the SET-Plan is ERA-Net Smart Grids Plus. Its ambition is to expand the EEGI initiative. ERA-Net Smart Grids Plus gathers 21 European countries and regions with the aim to achieve the Smart Grids vision and goals of Europe. The initiative fosters new technologies and market designs, as well as prepares customers to the adoption of new solutions. The members of ERA-Net Smart Grids Plus are entities responsible for national and regional programmes funding research in the fields of Smart Grids and the initiative is building a structure for cooperation between those entities and with external initiatives at the European level. The initiative promotes the electric power system that integrates renewable energies and is more flexible, efficient and secure, with low greenhouse gas emissions and with an affordable price. It promotes open markets for energy products and services. The initiative also seeks Europe's leading role at the world arena in low-carbon energy technologies. All this requires the research to be both cross-sectoral and interdisciplinary. ERA-Net Smart Grids Plus has the ambition to be the most important platform in the fields of all smart grid-related research in Europe. A number of leading European distribution system operators (DSOs) have created EDSO for SmartGrids, with the aim to coordinate research on smart grids and influence regulations at the national and European level. It considers itself the main interface between DSOs and the European institutions. EDSO for SmartGrids focuses e.g. on development of new models for smart grids and on testing the models on a large scale.

One other initiative is KIC InnoEnergy, i.e. a Knowledge and Innovation Community (KIC) focused on sustainable energy, fostered by the European Institute of Innovation and Technology (EIT). It is a European network, a commercial company with the shareholders being top ranking industries, research centres and universities, key players in the energy field. Its goal is to reduce costs in the energy value chain, increase security and reduce CO2 and other greenhouse gas emissions. Smart Electric Grid is one of the technology areas (out of eight) KIC InnoEnergy focuses on.

One of the FP7 projects that contribute to creating Smart Grid communities is e.g. ETP SmartGrids (Thee European Technology Platform for Electricity Networks of the Future), which is the basic forum in Europe for the crystallisation of policy and technology research and development pathways for the smart grids sector, as well as the link between EU-level related initiatives. One other is GRID+, a Coordination and Support Action with the aim to support the development of EEGI.

Some other initiatives worth mentioning are the International Energy Agency (IEA), an autonomous organisation promoting reliable, clean and affordable energy for its 28 member countries and beyond, International Smart Grids Action Network (ISGAN), promoting an international cooperation on smart grids adoption in the world and Global Smart Grid Federation (GSGF) aiming at development of smarter, cleaner electricity systems around the world.

CRITIS 2016: 11th International Conference on Critical Information Infrastructures Security – Call for Papers

The 11th edition of CRITIS takes place in Paris, France, October 10–12, 2016

In 2016, the International Conference on Critical Information Infrastructures Security faces its 11th anniversary. CRITIS 2016 aims at bringing together researchers and professionals from academia, industry and govern-mental organisations working in the field of the security of critical (information) infrastructure systems.

As in previous years, invited keynote speakers and special events will complement a programme of original research and stakeholder contributions. The conference invites the different research communities and disciplines involved in the C(I)IP space, and encourages discussions and multi-disciplinary approaches to relevant C(I)IP problems.

CRITIS 2016 continues the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP) and fostering the dialogue with stakeholders.

Call for Papers

CRITIS 2016 covers five thematic foci. Topic category 1 focuses on technologies and innovative responses for the protection of cyber-physical systems; topic category 2 covers the procedures and organisational aspects in C(I)IP including policies, best practices and lessons learned; topic category 3 includes advances in Human Factors, decision support, and cross-sector CI(I)P approaches; additionally topic category 4 is dedicated to railway stakeholders. Last but not least, CRITIS 2016 aims to encourage and inspire early stage researchers demonstrating outstanding research performance through topic category 5: Young CRITIS and CIPRNet Young CRITIS Award (CYCA).

Topic 1: Technologies: Innovative responses for the protection of cyber-physical systems

- C(I)IP – Critical Information Infrastructure Protection
- Cyber security in critical infrastructure systems
- Fault tolerant control for cyber-physical systems
- Security and protection of smart buildings
- Self-healing, self-protection, and self-management architectures
- Modelling and analysis of cyber-physical systems for monitoring and control
- Modelling, Simulation, Analysis and Validation Approaches
- C(I)IP applications in transportation, energy, communication, finance, health and water infrastructures
- CI in modern Warfare and cyber-warfare

General Chair:
Jean-Pierre LOUBINOUX, General Director of UIC, represented by UIC Security Division
e-mail: loubinoux@uic.org

INTERNATIONAL UNION OF RAILWAYS

Programme Co-Chairs:
Roberto SETOLA, Campus Bio-Medico University of Rome
e-mail: **r.setola@unicampus.it**

Hypatia NASSOPOULOS, Ecole des Ingénieurs de la Ville de Paris (EIVP)
e-mail: hypatia.nassopoulos@eivp-paris.fr

Local Chair:
Jacques COLLIARD, Head of UIC Security Division
e-mail: colliard@uic.org

Programme Organizing Chair:
Grigore HAVARNEANU, Research Advisor, UIC Security Division
e-mail: havarneanu@uic.org

Publicity Chair:
Cristina ALCARAZ, University of Malaga
e-mail: alcaraz@lcc.uma.es

Publicity Co-Chair:
UIC Communications Department

Topic 2: Procedures and organisational aspects in C(I)IP: Policies, best practices and lessons learned

- Preparedness, prevention, mitigation and planning
- Risk management in C(I)IP
- Security, protection, resilience and survivability of complex cyber-physical systems
- CI Preparedness and Emergency Management
- C(I)I exercises and contingency plans
- Crisis Management and CI
- CI Resilience Assessment
- Impact and consequence analysis of C(I)I loss or reduction of quality of service
- Public-private partnership for critical infrastructure resilience
- C(I)IP policies at national and cross-border levels
- The role of C(I)I in the implementation of the EU directive on European Critical Infrastructures in EU Member States
- C(I)IP R&D agenda at national and international levels
- Economics, investments and incentives of critical infrastructure protection
- Defence of civilian C(I)I in conflicts with cyber elements
- Forensics and attribution in C(I)I

Topic 3: Advances in Human Factors, decision support, and cross-sector CI(I)P approaches – focus on end-users

- Analysis of Human Factor and Security Awareness in C(I)IP
- Advanced decision support for mitigating C(I)I related emergencies
- Social aspects and public communication in C(I)IP
- Psycho-social dimensions of crisis management and intervention
- Training for C(I)IP and effective intervention
- Coping with Social Media in C(I)I-related Crisis Management
- Recent trends in cyber economy (clouds, quasi-monopolies, new payment methods etc.) and implications for C(I)I and C(I)IP

Topic 4: Special private stakeholder session

- C(I)IP specificities in the railway sector
- Constraints, challenges and opportunities for railway infrastructure
- Tunnel protection and tunnel control systems
- Protection of depots and marshalling yards
- Power stations
- Railway bridges
- Railway construction

Topic 5: Young CRITIS and CIPRNet Young CRITIS Award (CYCA)

- Topics of interest include all topics mentioned under topic categories 1 and 4.

Paper submission

We encourage submissions containing original ideas that are relevant to the scope of CRITIS 2016. Researchers are solicited to contribute to the conference by submitting research papers, work-in-progress reports, R&D project results, surveying works and industrial experiences describing significant advances in C(I)IP. Stakeholders from governments, Critical Infrastructure operators, and industry are encouraged to submit papers which describe their current and future challenges to be engaged by researchers and multidisciplinary research teams.

It is required that papers are not submitted simultaneously to any other conferences or publications; and that accepted papers not be subsequently published elsewhere. Papers describing work that was previously published in a peer-reviewed workshop are allowed, if the authors clearly describe what significant new content has been included.

All papers need to be written in English. There will be full papers and short papers. Full papers should be no longer than 12 pages, including bibliography and well-marked appendices. Short papers should be 4 to 6 pages long. Any submission needs to be explicitly marked as "full paper" or "short paper".

All paper submissions must contain a title, a short abstract, and a list of keywords. All submissions will be subjected to a thorough double blind review by at least three reviewers. The paper submissions should be anonymised and all author names, affiliations, acknowledgements, and obvious traceable references should be eliminated.

Paper submission will be done via the EasyChair conference system. The submitted paper (in PDF or PostScript format) must be formatted using the template offered by Springer LNCS and be compliant with Springer's guidelines for authors.

CRITIS 2016 continues the "Young CRITIS" community-building activities for fostering open-minded talents.

Acceptance policy

For publication in the CRITIS 2016 proceedings, all accepted papers (full and short) must be presented at the conference; at least one author of each accepted paper must register to the conference by the early date indicated by the organisers.

The conference **pre-proceedings** will appear at the time of the conference. All accepted papers will be included in full length in the pre-proceedings.

As in previous years, it is planned that **post-proceedings** are published by Springer-Verlag in their Lecture Notes in Computer Science (LNCS) series. Accepted full papers will be included in full length in the post-proceedings. However, we recommend that the authors produce a revised version of the paper, based on feedback received at the CRITIS event.

For accepted short papers, a four page extended abstract will be included in the post-proceedings.
Any accepted paper (full paper and extended abstract) that shall be included in the post-proceedings requires that its authors sign Springer's copyright agreement.

Call for Sponsors and Exhibitions

A limited number of opportunities are available for organisations and companies that wish to exhibit at this conference.

As a Sponsor or Exhibitor you will be able to present your products and services in the Exhibition Area, which will be located in the heart of CRITIS 2016 event. Conference attendees will have full and frequent access to the Exhibition Area, which will be open continuously during all three days of the conference, so that the Sponsors and Exhibitors will get most of the attention value.

There are three Sponsoring Packages and two Exhibition Packages to choose from (please check conditions and details on the website):

Platinum Sponsor (only one)
- one stand 6 m^2 (with table, 2 chairs, electricity, internet connection)
- one presentation included in the Conference programme (not included into the post-conference proceedings)
- one flyer/brochure in conference bag
- logo on conference bag
- logo on CRITIS 2016 website
- free access for 2 persons (3 days conference and full social programme)

Gold Sponsor
- one stand 6 m^2 (with table, 2 chairs, electricity, internet connection)
- one flyer/brochure in conference bag
- logo on conference bag
- logo on CRITIS 2016 website
- free access for 1 person (3 days conference and full social programme)

Silver Sponsor
- space for one poster/roll-up
- one flyer/brochure in conference bag
- logo on conference bag
- logo on CRITIS 2016 website
- free access for 1 person (3 days conference and full social programme)

Exhibition & Demo Desk (3 days)
- one stand 6 m^2 (with table, 2 chairs, electricity, internet connection, including space for one roll-up)
- logo on CRITIS 2016 website

Poster area (3 days)
- space for one poster / roll-up

Venue

CRITIS 2016 will take place at the International Union of Railways (UIC) Headquarters, in the very heart of Paris, between the banks of the Seine and Champs de Mars, only a foot away from the Eiffel Tower.

Street address:
16 rue Jean Rey, F-75015 Paris, France

More information

If you would like to find out more about CRITIS 2016, travel directions, preliminary programme, etc, then please visit the website at

www.critis2016.org

Photo credit: UIC / P. Frayssеix

Key dates

Submission of full papers:
10 May 2016

Registration open:
1 July 2016

Notification of acceptance:
15 July 2016

Camera-ready papers:
1 September 2016

CRITIS event:
10-12 October 2016

CRITIS 2016

11th International Conference on
Critical Information Infrastructures Security
October 10–12, 2016, Paris, France

Call for Papers open until May 10, 2016, see

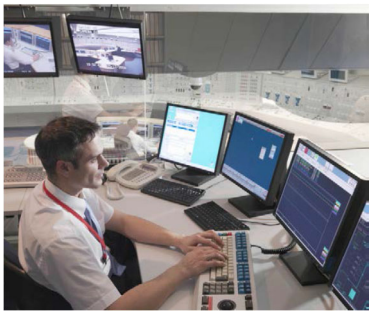
www.critis2016.org

With

3rd CIPRNet Young CRITIS Award

www.critis2016.org/ciprnet-young-critis-award

If you are less than 32 years and you contribute,
You may win extra money: Please apply!



Links

ECN home page	www.ciprnet.eu	
ECN registration page	www.ciip-newsletter.org	Please register free of charge
CIPedia©	www.cipedia.eu	the new CIP reference point

Forthcoming conferences and workshops

ACM CPSS'16	http://icsd.i2r.a-star.edu.sg/cpss16	Call for Paper, Xi'an, China – May 30, 2016
DIMVA 2016	www.dimva2016.org	July 7&8 San Sebastian ES. Call for participation
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016, Davos Switzerland
TIEMS 2016 Annual Conference	http://tiems.info/About-TIEMS/tiems-2016-annual-conference.html	13 – 15 September 2016, San Diego, USA
11th CRITIS Conference	www.critis2016.org	Call for Paper, open to May 10, 2016 Conference Oct,10-12, 2016 in Paris
Cyber Storm	www.swisscyberstorm.com	Oct. 19, 2016 in Lucerne Switserland

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu
European Organisation for Security	
Netonets organisation	www.netonets.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu
Effective cyber risk management for organisations	www.cyberwiser.eu
Critical Infrastructures and cloud computing	www.ci2c.eu
Security of Railways against Electromagnetic Attacks	www.secret-project.eu
MULTIPLEX - Foundational Research on MULTIlevel comPLEX networks and systems	www.multiplexproject.eu/

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection" I this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security	https://resilience.enisa.europa.eu/nis-platform
Platform Current policy debates	http://digitalwatch.giplatform.org

Cloud Computing and Critical Infrastructure
www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

Websites of Contributors

Acris	www.acris.ch
Campus Bio-Medico di Roma	www.unicampus.it
CINIT National Inter-University Consortium for Telecommunications	www.cnit.it/node/103
EC Joint Research Centre	https://ec.europa.eu/jrc
EOS European Organisation for Security	www.eos-eu.com
H2020	http://ec.europa.eu/programmes/horizon2020
Italian National Agency for new Technology	www.enea.it/en
French Institute of Science and Technology for …	www.ifsttar.fr/en
ITTI Sp. z o.o. e-technology and business	www.itti.com.pl
Übermeister	http://uebermeister.com/homepage.html
Union International Chemin de Fer	www.uic.org
University of Illinois	http://illinois.edu/
University of Malaga	www.uma.es
University of Science and Technology	www.utp.edu.pl/en/start
School for advanced Studies Lucca Italy	www.imtlucca.it

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

CIPedia© has more than 250.000 qualified clicks and is still growing. Join and look!

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardisation, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

The CIPedia© service aims at establishing itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

Your contribution is essential for putting even more value in the CIPedia© effort.

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.