




Move securely within the cyberworld**itrust consulting s.à r.l.**

55, rue Gabriel Lippmann

L-6947 Niederanven

 Carlo Harpes – Managing Director +352 621 451 945 info@itrust.lu

Niederanven, 28 June 2018

Steve Muller of itrust consulting to be awarded Doctoral degree with grade Excellent for his work on Risk Monitoring and Intrusion Detection for Industrial Control Systems

On 26 June Steve Muller of itrust consulting defended his PhD thesis in Computer Science on Risk Monitoring and Intrusion Detection for Industrial Control System (ICS) at the University of Luxembourg.

Steve presented a comprehensive description of new risk management techniques and algorithms for monitoring an organisation's risk in real time, including an intrusion detection system applied to ICS. He found an efficient (polynomial-time) algorithm to calculate attack probabilities in arbitrarily complex dependency graphs. This makes it possible to compute the likelihood of interdependent risk scenarios by taking into account the probability that one scenario is the consequence of another.

He also considerably optimised the computation time of existing branch and bound algorithms that find the optimal set of countermeasures in attack-defence trees with respect to the Return on Security Investment (ROSI). Such trees allow risk assessors to estimate the current risk in a context where countermeasures are operated with changing performance, and are thus a complementary approach to dependency graphs.

To translate alerts coming from intrusion detection systems and similar agents into notions of risk, Steve described them as a time series based on exponential functions. That way, only the estimated amplitude and half-life have to be transmitted to the monitoring platform. He designed and developed an interface (API) that aggregates the risk of multiples alerts. After replacing the static parameters of the dependency graph by the dynamic risk factors obtained from the various alerts, he can predict the current and future risk level, both in the current setup and in a simulated situation with new countermeasures in place. His algorithms may then guide the operator of an industrial control system through the activation of appropriate countermeasures when alerts occur.

In a prototype implementation, he replaced the static values of the risk assessment tool 'TRICK Service' by formulae that involve the risk parameters reported to the API in real time, thus transforming the static assessment into a real-time monitoring tool called 'TRICK Cockpit'.

In the final part of his thesis, Steve studied how such risk parameters can be extracted from security appliances, such as intrusion detection systems (where he used anomaly-based detection, which is complementary to signature-based techniques), firewall log parsers, and patch management tools.

Yves Le Traon, dissertation supervisor: « The committee confer to Steve the degree of 'Doctor' with the highest possible grade 'Excellent' for his ability to come up with novel and effective solutions when faced with challenges. »

Carlo Harpes, Managing Director ofitrust consulting: "Steve Muller developed risk management techniques that, although they can be used independently on any risk management methodology, have been integrated in the tool TRICK Service byitrust consulting, preparing the path towards TRICK Cockpit, a real-time risk monitoring tool. They have already been applied for the benefit of our current customers, such as Luxmetering, and will improve the quality of estimation of future risk assessment and monitoring activities, not only for ICS, but for all complex ICT (Information and Communication Technology) systems."

This work was funded via an AFR grant by Luxembourg National Research Fund FNR. The hosting and management were ensured byitrust consulting in the framework of a Private-Public Partnership with Uni.lu and *IMT Atlantique Bretagne-Pays de la Loire* in France. This management and support were co-funded by the nationally-funded research project SGL Cockpit, the EU-funded FP7-projet TRESPASS on risk management and attack-defence trees and the EU-funded project ATENA on Cybersecurity for Critical Infrastructures. The academic part was supervised by Prof. Yves Le Traon and Prof. Jean-Marie Bonnin of the University of Luxembourg and *IMT Atlantique Bretagne-Pays de la Loire* respectively, who jointly issued the Doctoral degree.

Aboutitrust consulting

itrust consulting, an SME from Luxembourg specialising in Information Security helps its customers from both the public and private sectors to protect their information against any divulgation, manipulation, or unavailability. Its services are related to building, implementing, and auditing Information Security Management Systems, assessing and treating risk with its own TRICK Service tool, deploying security experts whenever needed (SECaaS, or Security as a Service), on request hacking of our customers and handling cybersecurity incidents (malware.lu CERT), or designing and operating security solutions for ICT. These services benefit intensively from co-funded national and European research projects.

About SnT

The Interdisciplinary Centre for Security, Reliability and Trust (SnT) is a research centre at the University of Luxembourg. Through its Partnership Programme, SnT researchers, together with industry and public partners, address present-day challenges in ICT. The Programme fosters the development of innovative ideas, establishing Luxembourg as a European Centre of Excellence and Innovation in the field of secure, reliable, and trustworthy ICT systems and services.

About IMT Atlantique

IMT Atlantique Bretagne-Pays de la Loire is an Elite Graduate School specialized in digital technology, energy and environment. The Department of Network Systems, Cyber Security and Digital Law (SCRD) is situated on IMT Atlantique's Rennes Campus. Its areas of activity cover all aspects of teaching and research in:

- network systems, including technologies for fixed and mobile networks and the Internet of Things. In addition, the complex systems that make it possible to construct and secure the systems that support energy, industry, and cities and intelligent transport;
- cyber security, through reinforcing the security of complex systems, industries of the future and critical infrastructures;

- law and the economics of digital technology, particularly at the European and international level.

About SGL-Cockpit

SGL-Cockpit (Smart Grid Luxembourg) aims at designing, developing, and testing tools and methodologies that are needed to monitor the cybersecurity aspects of the SGL 2.0. It receives funding from the Luxembourg Ministry of Economy. The project is managed by itrust consulting, and the other partners are CREOS and the University of Luxembourg.

About TREsPASS

TREsPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security) is a European FP7 project with 17 partners from nine European countries. Its aim is to develop methods and tools for predicting, evaluating and prioritising attack scenarios on the IT infrastructure of a business. The project will develop meta-models of integrated physical, digital and social engineering risks, collect empirical knowledge about socio-technical attacks, and develop quantitative methods for assessing the risk of these attacks. These models and techniques will be integrated into risk assessment methods, and be implemented in an "attack navigator" to support security decision-making. <http://www.trespas-project.eu/>

About ATENA

ATENA (Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures) is a European project funded by the Horizon 2020 programme on 'Digital Security: Cybersecurity, Privacy and Trust, H2020-DS-2015'. The ATENA project aims at achieving the desired level of Security and Resilience of the considered CIs, while preserving their efficient and flexible management. ATENA, leveraging the outcomes of previous European Research activities, particularly the CockpitCI and MICIE EU projects, will remarkably upgrade them by exploiting advanced features of ICT algorithms and components, and will bring them at operational industrial maturity level; in this last respect, ATENA outcomes will be tailored and validated in selected use cases. <https://www.atena-h2020.eu/>