definition, we develop ICS that execute the (executable) specification in parallel with the application code, we monitor the application code execution and identify deviations between specification execution, which produces predictions, and the application code execution, which produces observations. Importantly, this approach to behaviour definition enables systems to detect all types of behavioural deviations from the specification, independently of motive, i.e., both malicious and accidental, integrating security with fault tolerance in the same approach.

Exploiting this approach, we have been developing ARMET, a middleware system for ICS shown in Figure 1, working in three main security research directions:

- Safe code derivation from specifications, based on the FIAT approach [1], in order to develop safe application code (App Implementation in Figure 1) with specified security properties from the application specification (App Specification)
- Monitor development (Behavioural Differencer) that accurately detects (without false positives or negatives) deviations between application specification and execution [2], and
- Methods to identify vulnerabilities for false data injection attacks and encode them in the Abstract Data Machine, so that the monitor can protect against them. Our work has already provided promising results for power (smartgrid) systems [3].

This approach is practical today, capitalising on the significant recent advances in software verification and formal methods that enable analyses of large programs, and especially in cyber-physical and ICS, which implement specific processes or applications ('plants' in control system terminology). Advantages include automated development of safe code and design and implementation of robust monitors that can identify when security properties are violated.

References:

[1] B. Delaware, et al.: "Fiat: Deductive Synthesis of Abstract Data Types in a Proof Assistant", in Proc. of POPL'15. Jan. 2015.

[2] M.T. Khan, D. Serpanos, H. Shrobe: "Sound and Complete Runtime Security Monitor for Application Software", arXiv:1601.04263 [cs.CR].

[3] S. Gao et al.: "Automated Vulnerability Analysis of AC State Estimation under Constrained False Data Injection in Electric Power Systems", in Proc. of IEEE CDC'15. Dec. 2015.

Please contact:

Dimitrios Serpanos,
University of Patras and ISI, Greece,
Tel: +30 261 091 0299
serpanos@isi.gr

The TISRIM-Telco Toolset – An IT Regulatory Framework to Support Security Compliance in the Telecommunications Sector

by Nicolas Mayer, Jocelyn Aubert, Hervé Cholez, Eric Grandry and Eric Dubois

The objective of our project is to adapt and facilitate Information System (IS) security risk management in the telecommunications sector. To this end, we have developed: first, a model-based approach and a tool to support the adoption of IS security risk management by Luxembourg's telecommunications service providers (TSPs); and second, a framework to analyse the data collected by Luxembourg's National Regulation Authority (NRA).

There is currently a strong emphasis on the security of information systems (IS) and the management of information security risks. Numerous regulations are emerging that impose a risk-based approach for IS security on entire economic sectors. In the telecommunications sector, the EU Directive 2009/140/EC introduces Article 13a about security and integrity of networks and services. This article states that member states shall ensure that providers of public communications networks 'take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services'. To harmonise the implementation of this at a national level, the European Network and Information Security Agency (ENISA), as the centre of network and information security expertise for the European Union, published in December 2011 a document entitled "Technical Guideline for Minimum Security Measures" [L1].

As part of the adoption of this directive at the national level in Luxembourg, we have developed a project that aims to adapt and facilitate IS security risk management in the telecommunications sector. To this end, the project is composed of two parts. In the first part we have developed a model-based approach and a tool to support the adoption of this regulation by telecommunications service providers (TSPs) at the national level [1]. The second part involves developing a framework to analyse the data collected by the NRA through this standard approach [2].

For the first part of this project, the starting point of our analysis is that the different TSPs in Luxembourg have very different levels of expertise in security risk management. Thus, letting them report to the NRA without strong guidance would have resulted in very different types of reports, with various quality levels. In order to build a harmonised reporting approach and to meet the needs of the users' (i.e., TSPs in Luxembourg), we decided to define both the methodology and its associated tool in collaboration with the TSPs. Furthermore, we established shared business and architecture models supporting the methodology. Regarding the definition

of these sector-specific models, the first task consisted of defining the different processes composing each regulated telecommunications service. Process reference models such as Business Process Framework ("eTOM") of the TMForum [L2] or the Telecommunications Process Classification Framework of the American Productivity and Quality Center [L3] were used as input. Then the second task was to describe the IS supporting each telecommunications service. The works of The Open Group and TMForum have been specifically analysed and confronted with the state of practice of the national TSPs. Finally, we defined for each telecommunications service the most relevant threats and vulnerabilities, based on the reference IS architecture previously defined, and the most relevant impacts, based on the business processes previously defined. Finally, we have represented the resulting knowledge in ArchiMate [L4]: an Enterprise Architecture modelling language. We have extended ArchiMate with the appropriate concepts from the risk management domain [3]. We then integrated all of the different models into a software tool. This task was performed by adapting TISRIM, a risk management tool developed in-house, that was initially released in 2009. TISRIM is currently the tool recommended to the TSPs by our national NRA to comply with the regulation.

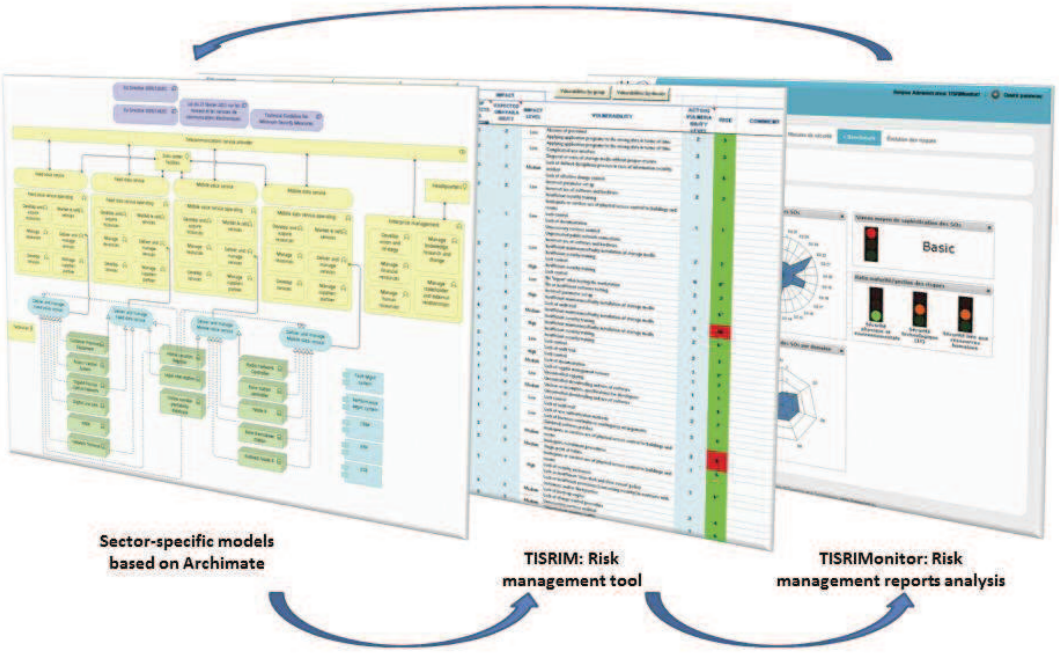

Figure 1: Overview of the TISRIM-Telco toolset.

After having defined and implemented a method to support the adoption of the regulation by TSPs, there was also a strong need to develop a platform in order to manage the reports received annually by the NRA, and to be able to efficiently analyse their contents. The purpose was therefore to define a set of measurements depicting the trust the NRA can have in the security of TSPs, as well as in the whole telecommunications sector. The outcome for the NRA is to be able to provide recommendations to the TSPs and to facilitate policy-making. The first task when defining the measurement framework was to establish a template for the measurement constructs, inspired by the state of the art, and in particular the template proposed in ISO/IEC 27004. Then, once the measurement template was established, two types of measurements were defined: compliance measurements, measuring the compliance to requirements imposed by legislation and performance measurements, measuring the effectiveness of IS security. The final set obtained is composed of 10 measurements defined for TSPs and 11 measurements defined for the whole telecommunications sector. Finally, the measurements were implemented in a tool named TISRIMonitor, which is currently under evaluation by the NRA.

Our objective is now to extend this approach to other critical and regulated sectors, such as the health and finance sectors, or the privacy regulator. All of these approaches will be managed and linked in a regulatory framework called 'RegTech platform' – a technological platform to conduct regulation activities. Another follow-up of this project is to adopt a more holistic approach. The objective is to extend the scope of risk management to networked enterprises, and to lead to systemic risk management, i.e., risk management on the entire system formed by networked enterprises, to avoid perturbations of the ecosystem due to local, individual decision-making.

Links:

[L1] https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/guidelines/technical-guideline-on-minimum-security-measures

[L2] https://www.tmforum.org/business-process-framework/

[L3] https://www.apqc.org/knowledge-base/documents/apqc-process-classification-framework-pcf-telecommunications-pdf-version-50

[L4] http://www.opengroup.org/subjectareas/enterprise/archimate

References:

[1] N. Mayer, J. Aubert, H. Cholez, E. Grandry: "Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation", EuroSPI 2013.

[2] Y. Le Bray, N. Mayer, J. Aubert: "Defining Measurements for Analyzing Information Security Risk Reports in the Telecommunications Sector", SAC 2016.

[3] E. Grandry, C. Feltus, and E. Dubois: "Conceptual Integration of Enterprise Architecture Management and Security Risk Management", EDOCW 2013.

Please contact:

Nicolas Mayer
Luxembourg Institute of Science and Technology (LIST)
Tel: +352 275 888 1, Nicolas.Mayer@list.lu