Number 92, January 2013

ERCIM NEWS

www.ercim.eu

Special theme:

Smart Energy Systems

Also in this issue:

Secure Smart Grids or Say 'Goodnight Vienna!'

by Florian Skopik, Paul Smith and Thomas Bleier

With the increasing use of novel smart grid technologies, a comprehensive Information and Communication Technology (ICT) network will be established in parallel to an electricity grid that, owing to its large size and number of participants and access points, will be exposed to similar threats to those experienced on the current Internet. Whilst there have been a number of guidelines and best practices for securing future smart grids, further work is required in this area to make them readily applicable. In this article, we introduce the (SG)^2 project, which aims to address these issues and provide practical advice to smart grid stakeholders in Austria.

The smart grid will revolutionize electricity networks, allowing increased use of decentralized clean energy sources. It will make use of Information and Communication Technology (ICT) in a number of ways, for example, to manage decentralized energy sources, such as from photovoltaic and the associated markets. In general, the smart grid will be more open than current electricity grids, and will incorporate a greater degree of measurement-based control deeper within the network, eg, in distribution systems, based on data acquired from smart meters. This openness together with new automatic control loops make smart grids more vulnerable than current power grids to potentially serious attacks [1]. Personal privacy concerns abound, for example, issues relating to unauthorized access to metering data: it will be possible to determine detailed usage patterns of electrical appliances, including the television channel house occupants are watching, based on metering data [2]. Therefore, it is vital that security and privacy issues are a primary concern for the future smart grid.

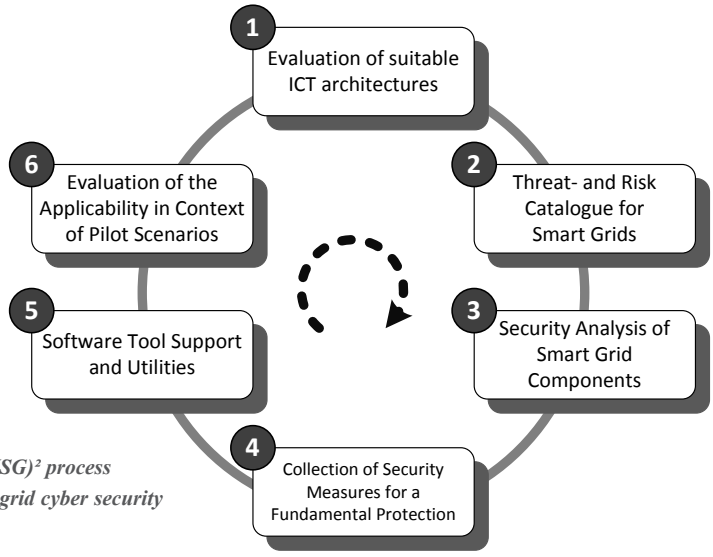

Figure 1: The (SG)² process model to smart grid cyber security

Various international organizations, such as NIST in the USA and ETSI in Europe [3], have developed guidelines and frameworks that can be used to improve the security of Smart Grids. However, because they do not consider factors such as local market conditions, requirements and deployments, and legal constraints, these guidelines cannot be directly applied. Furthermore, they have seen limited real-world application, making it unclear how suitable they are for their intended purpose. Our research aims to build on these existing guidelines and frameworks, in order to make them functional.

An Austrian perspective: the (SG)² project

The goal of the Smart Grid Security Guidance (SG)² project is to study effective countermeasures to smart grid security threats. The project investigates and develops methods, concepts and process models, and accompanying software tools to minimize the risk posed by cyber threats and to ensure the security of smart grids in Austria (see Figure 1). Novel approaches to the modelling of complex ICT-supported smart grid architectures will be defined in the project, which will form the basis for an analysis and evaluation of primary forms of attack and attack surfaces. This information can be used to estimate the potential impact of attacks.

Architectural models are examined with respect to threats and vulnerabilities, in order to determine the most effective protective measures against possible attacks. Electricity providers have traditionally focused on ensuring the safety and reliability of their infrastructure. However, in the future, malicious attacks that hinder the increasingly networked ICT components within their systems need to be accounted for. An important outcome of the (SG)² project will thus be a taxonomy and catalogue of countermeasures that can be applied to ensure the security of smart grids for a given threat. For a realistic risk assessment, the project also deals with penetration tests and security analysis of smart grid components. Because of the complexity of securing a smart grid, software tools are being developed to support the use of the guidelines and methodologies produced in the project.

A strong collaboration between industry, research and government

In order to attain the ambitious goals of the (SG)² project and to ensure the wide applicability of developed tools, major stakeholders in important sectors related to smart grids in Austria need to be involved. These stakeholders create a well-balanced consortium including security research institutions, companies from the security industry sector, energy utilities, and governmental organizations. The project is led by the AIT Austrian Institute of Technology. Other large research partners are the University of Technology Vienna, and the Siemens AG – Corporate Technology Austria. Practical security expertise in penetration testing is contributed by SECConsult Unternehmensberatung GmbH. The Energieinstitut an der JKU

Linz GmbH investigates societal impact of (SG)² research results; additionally the participation of the Ministry of the Interior (BM.I) and the Ministry of Defence and Sports (BMLVS) ensures the development of applicable solutions from a governmental perspective. Finally, the developed guidelines will be evaluated within the context of three energy utilities in Austria, which, owing to their different sizes, require different solutions: LINZ STROM GmbH, Energie AG Oberösterreich Data GmbH, and Innsbrucker Kommunalbetriebe AG.

This two year project runs from 2012 to 2014 and is financially supported by the Austrian security-research program KIRAS and by the Austrian Ministry for Transport, Innovation and Technology (BMVIT).

Links:
http://kwz.me/4l
http://kwz.me/4p

References:
[1] F. Skopik, et al: "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures", International Journal of Smart Grid and Clean Energy, vol 1, issue 1, September 2012, pp 22-28
[2] U. Greveler, B. Justus and D. Loehr: "Multimedia Content Identification through Smart Meter Power Usage Profiles", 2012 International Conference on Information and Knowledge Engineering, Las Vegas
[3] European Telecommunications Standards Institute (ETSI): Smart Grid Technologies; http://www.etsi.org/website/Technologies/SmartGrids.aspx (2012)

Please contact:
Florian Skopik, Paul Smith, Thomas Bleier
AIT Austrian Institute of Technology / AARIT, Austria
E-mail: florian.skopik@ait.ac.at
paul.smith@ait.ac.at,
thomas.bleier@ait.ac.at

Preparing for the Smart Grids: Improving Information Security Management in the Power Industry

by Maria Bartnes Line

The power industry faces the implementation of smart grids, which will introduce new information security threats to the power automation systems. The ability to appropriately prepare for, and respond to, information security incidents is of utmost importance, as it is unrealistic to assume that one can prevent all possible incidents from occurring. Current trends show that the power industry is an attractive target for hackers. A major challenge for the power industry to overcome are the differences regarding culture and traditions, knowledge and communication, between ICT staff and power automation staff.

Two major technological changes make smart grids interesting from an information security point of view. One is that new technologies are introduced into the power automation systems; commercial off-the-shelf products replace proprietary hardware and software. The other is integration; ICT systems and power automation systems will be much more tightly connected than before. Smart grids consist of complex power grids that interact with equally complex ICT systems. This implies that well-known information security threats like computer break-ins, industrial espionage, malware attacks and denial-of-service attacks will be highly relevant for the power industry in the near future, if not already. ICT security incidents targeting power automation systems, or other types of SCADA systems, are not science fiction - they are already happening. We have had Stuxnet, Duqu and Flame, and we should expect to see more of the kind in the near future.

Figure 1: The complete incident management process (ISO 27035)

Power automation systems and general communication oriented ICT systems have traditionally been operated separately. There have been limited, if not zero, logical connections between them, and they have served quite different purposes. The staff operating the two systems tend to have different backgrounds; electric power engineering and computer science. The technology bases are different, and so are management routines. Facilitating and achieving understanding and well-functioning collaboration in this intersection between ICT staff and power automation staff will be the most important task on the way to successful information security incident management for smart grids.

Incident management is the process of detecting and responding to incidents, including supplementary work such as learning from the incidents, using lessons learnt as input in the overall risk assessments, and identifying improvements to the implemented incident management scheme. ISO/IEC 27035:2011 Information Security Incident Management [1] describes the complete incident management process as consisting of five phases; 1) Plan and prepare, 2) Detection and reporting, 3) Assessment and decision, 4) Responses, and 5) Lessons learnt.