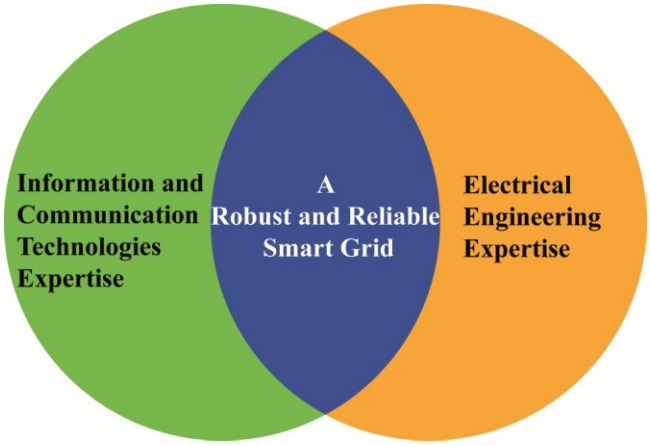
Cybersecurity in the Smart Grid

by Magnus Almgren, Davide Balzarotti, Marina Papatriantafilou and Valentin Tudor[1]

In the past, the easiest way to attack the electrical grid would have been to physically access and destroy components. However, with the introduction of the smart grid and its increased dependence on information and communication technologies (ICT), the future grid may be vulnerable to pernicious cyber attacks performed remotely. In CRISALIS and SysSec, we are studying the properties of the envisioned smart grid to be able to anticipate and mitigate future attacks against this critical infrastructure.

In Europe and elsewhere, the electrical grid is being transitioned into the "smart grid" in order to increase flexibility and accommodate large scale energy production from renewable sources. This transition involves, among other steps, the installation of new, advanced equipment – for example, the replacement of traditional domestic electrical meters with smart meters - and remote communication with devices – for example, allowing remote access to an unsupervised energy production site. Together with the new functionalities, this transition introduces concerns about how the technology can be misused by adversaries [1].



The security issues associated with the smart grid include the following. Many of the new security issues in the smart grid are well-known problems in the information and communication technology (ICT) domain, such as buffer overflows in devices and sloppy implementations of cryptographic protocols. However, the solutions from the more mature ICT domain may not be directly applicable to the smart grid due to resource-constrained devices (smart meters), the life cycle of components (there will always be legacy systems) or the impossibility of immediately shutting down and patching a machine that needs to run 24/7. Other issues originate from the electrical and power engineering domain (device tampering). There are also challenging new problems originating from the intersection between the electrical engineering and ICT domains, for example where a cyber attack (buffer overflow) in turn affects properties of the electrical grid (power quality), which in turn may propagate back to the ICT domain (vulnerability of control loop) [2]. An interdisciplinary approach is required to identify possible solutions to these problems.

In SysSec, a network of excellence in Europe, and CRISALIS, a European research project, we are working on improving the security in critical systems, in particular the smart grid, through two orthogonal approaches. One major problem is the lack of cross-domain expertise in both ICT security

[1] Published in ERCIM News #92, http://ercim-news.ercim.eu/images/stories/EN92/EN92-web.pdf

and power engineering. Being a network of excellence, SysSec organizes several activities to bring together researchers and practitioners from different domains. For example, we organized a summer school for students across Europe for a hands-on approach to learn more about reverse engineering of malware targeting critical infrastructure. To our surprise, we hit the ceiling on the number of students we could accept within less than a week of the announcement, forcing us to create a waiting list. This points to the need of better education in this area and we will also include modules for hardware security and critical infrastructure protection as part of the effort in SysSec to provide a common curriculum on cyber security.

Another major problem hampering the analysis of security properties of the smart grid is the proprietary nature of the technologies and protocols involved: there are few open source tools available to perform an in-depth analysis of a system. For this reason, we are developing a toolset in CRISALIS that can be used by researchers to validate security claims made by vendors and increase the overall security of the deployed components. One of the first deliverables will be an open-source fuzzer to test the protocols used in this domain. By working closely with industrial partners, the goal is to provide new tools to detect intrusions and effective techniques to analyse infected systems.

Even though the smart grid is a necessity, it is important to understand the security risks before complete systems are deployed and interconnected across Europe. Learning from and avoiding simple problems that have already been encountered in the ICT domain, we may focus on the new types of threats that arise as a consequence of the interdisciplinary nature of this complex environment. For this reason, projects such as SysSec and CRISALIS, which bring together experts from different domains, are crucial at this stage.

CRISALIS (http://www.crisalis-project.eu/) may be contacted at contact@crisalis-project.eu. SysSec (http://www.syssec-project.eu/) may be contacted at the corresponding contact@syssec-project.eu, followed in twitter (twitter:syssecproject) and Facebook (http://www.facebook.com/SysSec).

References:

[1] National Institute of Standards and Technology Interagency, “Guidelines for Smart Grid Cyber Security (NISTIR 7628),” vol. 1-3, http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628, 2010.

[2] Costache, Tudor, Almgren, Papatriantafilou, Saunders, “Remote control of smart meters: friend or foe?,” EC2ND-2011, Gothenburg, Sweden.

Please contact:

Magnus Almgren
Chalmers University of Technology, Sweden
+46 31 772 1702
magnus.almgren@chalmers.se