Security Classification

Advanced Metering Infrastructures (AMI) open up several new attack surfaces that do not exist in traditional metering. We have experience in analyzing AMI topologies and how to identify security threats, attack surfaces, and impacts of attacks on the Electrical Grid. New threats and vulnerabilities get discovered all the time and their mitigation is a never-ending story. Therefore, one usually needs to apply a well structured methodology to analyse the security aspects of a system; often providing also recommendations for redesigning of the system based on standard security requirements in order to be able to enhance the security of systems to a required level. **We call this methodology, Security Classification.**

Security cannot be easily quantified, and what we cannot measure is harder to manage. Security is also dynamic and context dependent, thus needing a framework able to evaluate the security of the system at any given time and deployment configuration. We are using a framework specially developed for Smart Grid systems, that extends existing standards from ANSSI and ENISA, and uses recent advancements in measurable security.

A Security Class results from evaluating the of exposure of the system to attacks and the impact of successful attacks on the system. Exposure is the result of connectivity of the system and protection mechanism that have been implemented. Exposure comes in two forms: IT and Physical. To compute a security class, we decompose the system into smaller components and compute the exposure and impact of each individual component. The security class for the whole system is computed by aggregating the measured components to the system level using our multi-metrics approach.

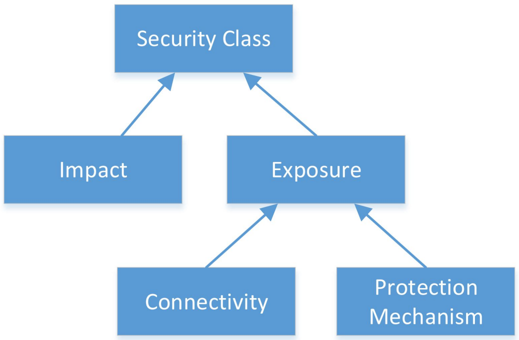

Figure: Components studied when identifying a Security Class for a complex Smart Grid system.

Our Security Classification Framework can be utilized by the relevant organizations like utility companies, regulatory/standardization bodies, and expert security analysts. Security Classes can be used to set demarcation criteria for system or component security to comply with. For implementations of smart grid systems companies need to be more aware of the new security challenges introduced by the communication aspects. Security classes help by giving an overview of where each component lies in the class hierarchy and why. The companies can comply with the minimum required security class specified by regulatory bodies like NVE. However, in order to achieve the specified class, they are guided into making the proper decisions when purchasing equipment and technologies from their vendors and decide on appropriate configurations and protection mechanisms.

Catastrophic	Class E	Class E	Class E	Class E
Major	Class D	Class D	Class D	Class E
Moderate	Class C	Class D	Class D	Class D
Minor	Class A	Class C	Class C	Class C
Insignificant	Class A	Class A	Class B	Class B
Impact/Exposure	1	2	3	4+

*(Class **A** security refers to the most secure systems and **F** having the weakest security)*

A Security Class can be elevated either by reducing the impact or by reducing the exposure of the system. Depending on the context and requirements, exposures can be controlled by either controlling the connectivity or setting the correct protection level. In this way security classification can help system designers to reach the targeted security level by providing suggestions of improvements.

Security classification can be done either for whole systems like AMI deployments, using more resources in the evaluation process, or otherwise we can classify critical components of a system like smart meters or SCADA, which would thus require less efforts and time. Our framework makes use of automated techniques to some extent, which help alleviate some of the manual tasks that otherwise require security experts knowledge.

CONTACT: *University of Oslo* through: **Josef Noll**, **Manish Shrestha**, **Christian Johansen**.
WEB: www.IoTSec.no