On Demand for Situational Awareness for Preventing Attacks on the Smart Grid

Thoughts on how situational awareness
might help to secure critical energy infrastructures

A small piece of the EU – FP7 project: ECOSSIAN

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

ECOSSIAN

European Control System Security Incident Analysis Network

- Yegor Shovgenya, Florian Skopik
  - AIT Austrian Institute of Technology GmbH Vienna, Austria
  - yegor.shovgenya.fl@ait.ac.at
  - florian.skopik@ait.ac.at
- Klaus Theuerkauf
  - ifak - Institut für Automation und Kommunikation e.V. Magdeburg, Germany
  - klaus.theuerkauf@ifak.eu

Outline

- Motivation and purpose
- Changes in energy infrastructure
- Challenges and problems of those changes
- Threats and need for state awareness
- Mitigation approaches
  - Traditional security by design
  - ECOSSIAN approach over situational awareness

Motivation

- Purpose of this paper:
  - Raising awareness regarding new threats to electrical energy infrastructure
  - New capabilities of the smart grid approach must be accompanied by security and not only safety aspects
- Not provided:
  - Detailed description of energy infrastructure
  - Detailed description of imminent threats

Changes in infrastructure

- Traditional generation
  - Discrete number of Coal and nuclear power plants distributed across europe
- Traditional distribution
  - From plants over high and medium voltage distribution lines to customers
  - Last sensing units are deployed on medium to low voltage transformation

Smart Grid approach

- Comprehensive communication infrastructure
- Local generation as well as traditional generation
- Storages (in chemical, potential, physical energy form)
- Virtual power plants as connection from generation, storage, consumption in a region
- Dynamic load management and dynamic pricing of electrical energy
- Stochastic effects in generation planning and operation because of renewable sources

Challenges

- Safety infrastructure components must be interconnected due to distributed generation
- Renewable(stochastic) generation poses the need of further simulation onto the grid operators
- Simulation inputs consists of broad knowledge of grid state i.e. sensor values on every level(even low voltage)

Smart Grid

- Smart meters for consumption measurement
- Inverters or small transformer stations for power generation sensing and control
- Interconnected protection devices
- Load management devices in private consumer space
- Gateways to existing grid control infrastructures.
- Central control centres as data concentrators of the sensing units

Possible attack on SG infrastructure

- Multiphase attack with highlighted parts where situational awareness might help to prevent a blackout
- Phase 1 *Attacking the grid control center*
- Phase 2 *Attacking smart power generators*

Attacking the grid control center

- 1. Obtain technical documentation on targeted smart meters, communication channels and protocols used.
- 2. **Obtain physical access to smart meters.** Conduct reverse engineering of available smart meters or test them for vulnerabilities known to the attacker.
- 3. **Connect to the communication medium** between a functioning smart meter and its data concentrator.
- 4. Decrypt signals sent by smart meters by sniffing their communication with a data concentrator.

Attacking the grid control center

- 5. Simulate a smart meter to a data concentrator. **Send malicious signals to the concentrator.**
- 6. Establish a foothold in the concentrator: execute malicious code on it, **obtain limited or full control over the concentrator.**
- 7. Begin communicating with the grid control center on behalf of the concentrator, or inject malicious input into their communication.
- 8. Run or plant malicious software on the control center server, possibly obtain limited or full control over it using known vulnerabilities.

Attacking smart power generators

- Obtain documentation on smart grid structure and power lines architecture in the targeted regions.
- **Engineer a tariff update message that sets a very low price for received power.**
- Distribute the fake tariff among consumer tariff management devices. Consumers start perceiving the current energy prices as very low and the power demand raises.
- Using the provider control center's resources, the attacker commands **all available small-scale energy generators to stop feeding power to the grid.**
- Due to the high demand the grid becomes instable.

Traditional Security by Design

- Even if this should be obvious the components in critical infrastructures should follow good Security by Design guidelines
- For smart grid components:
  - Separation on actuation from sensing units
  - Actuation only on commands from multiple sources
  - Encrytion and verification of commands
  - Avoidance of real-time-clocks where possible
  - Strategies to change credentials

ECOSSIAN project approach

- ECOSSIAN -**E**uropean **CO**ntrol **S**ystem **S**ecurity **I**ncident **A**nalysis **N**etwork(FP7)
- Detection, analysis and mitigation of threats to critical infrastructure on company/national/european level
- Interconnected situational awareness enables more complex analysis, forecasting and prevention of attacks
- See http://www.ecossian.eu

Conclusion

- Traditional security by design approaches in device development might not be sufficient if connected infrastructure is compromised
- Situational awareness at all levels enables complex analyses to detect missbehaviour of infrastructure, even if single decisions, states or commands seem plausible

ECOSSIAN Grant Agreement No. 607577

"The **ECOSSIAN** project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number SEC-607577."

If you need further information, please contact the coordinator:
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@ecossian-project.eu