Smart grid security analysis

Paul Smith et al.
paul.smith@ait.ac.at

SPARKS Stakeholder Workshop
20th May, 2014, Graz
SPARKS Objectives

The SPARKS project has three main objectives regarding security analysis:

1. Develop a **methodology for risk assessment** that addresses the specific challenges of the smart grid
2. Create appropriate **tools to support** this methodology
3. Build a **simulation environment** that can be used to measure the impact of a cyber-attack

These items will be applied to the project’s demonstration facilities
Cybersecurity Risk Assessment

- Risk assessment is concerned with understanding the probability of a cyber-attack and its impact

\[
\text{risk} = \text{probability} \times \text{impact}
\]

- The basis for prioritising how to mitigate threats and apply resources for cybersecurity

Based on an understanding of threats and vulnerabilities

For example, financial loss, damage to equipment, loss of power, …
A Smart Grid Risk Assessment: Motivation

- The smart grid will consist of **legacy** systems and **new ICT components** that implement advanced measurement and control functions.

- The precise nature of a smart grid deployment is (**at least**) country specific:
  - For example, regulatory norms differ between countries.
  - Different approaches to Advanced Metering Infrastructures.

- A risk assessment method should account for these characteristics of the smart grid.
Risk Assessment Method for Smart Grids

- Two-tier risk assessment method
  1. **Conceptual level** is used to assess risks to novel ICT systems
  2. **Implementation level** is used to assess risks of existing (or prototype) systems

- The starting point of the assessment is a national reference architecture derived from SGAM

- The two processes interact, e.g., the conceptual assessment is used to determine the System Under Test (SUT) for the security audit
Risk Assessment: An Austrian Case

- Create a national reference architecture Based on SGAM
- Populate with implementation details and identify vulnerabilities
- Identify architecture clusters for assessment
- Apply threat catalogue to the architectural clusters and perform a risk assessment using Delphi
- Determine audits and System Under Test based on high risk categories
- Make security architecture recommendations
- Make security implementation recommendations
- Perform a security audit on the System Under Test
Analysing Multi-stage Attacks

- Attacks are becoming increasingly sophisticated and using numerous steps to achieve their goal
  - See Bob’s presentation on Security Analytics

- Threat analysis techniques often require the assessor to think like an attacker
  - This is difficult to do, and is not a widely available skills set

- Vulnerability analysis tools can generate a deluge of information
  - How can an analyst prioritise this data?
Vulnerability-centric Threat Analysis for APTs

- **Aim:** identify the paths of technical vulnerabilities through an infrastructure that can be used by an attacker
  - This information can be used to prioritise vulnerability data
  - Does not require attacker knowledge to gain actionable information

- **Four stage process:**
  1. Identify hosts in the infrastructure and their connectivity
  2. Enumerate the vulnerabilities associated with hosts, using public information, e.g., NIST National Vulnerability Database
  3. Chain vulnerabilities together based on connectivity and vulnerability information
  4. Identify attack paths to targets in the infrastructure by searching the connectivity-vulnerability graph

![Diagram](image)
An Example Attack Path
Simulating Cyber-attacks

- It is not possible to perform all attacks in reality
  - Large-scale attacks and the potential of **physical damage** cannot be readily implemented
  - This motivates the need for suitable **simulation tools**

- Simulators can be used to study two aspects
  - Attacks to the ICT infrastructure, e.g., DoS attacks
  - The **impact** to the power grid

- Simulation can give an indication of the effectiveness of security measures
Simulation Environment: Approach

- To develop a hybrid simulation environment based on the interconnection of existing tools

1. **Power Distribution Simulators** (GridLAB-D, etc.)
   - Adapt power grid models from US network standards to European network standards
   - Achieve a realistic model of the real environment and generate comparable results which are directly applicable to real European infrastructure

2. **ICT network simulation tools**
   - Examples include ns-2, OMNeT++, ...

3. **Real smart grid hardware**
   - Automation equipment (AIT SmartEST Lab)
     - E.g., Secondary substation
   - Smart meters
Safety and Security Co-Analysis

- Safety analysis methods are widely used in the energy domain
  - Examples include HAZOP, fault-tree analysis, event-tree analysis, FMVEA, STAMP/STPA, …

- There are parallels in the security domain, e.g., attack trees

- Benefits can be had by performing security and safety co-analysis
  - Reuse of results across analyses
  - Ability to consistently prioritise different types of threats, i.e., attacks versus faults
SPARKS Objectives: Restated

- The SPARKS project has three main objectives regarding security analysis:
  
  1. Develop a **methodology for risk assessment** that addresses the specific challenges of the smart grid
  2. Create appropriate **tools to support** this methodology
  3. Build a **simulation environment** that can be used to measure the impact of a cyber-attack

- These items will be applied to the project’s demonstration facilities
Discussion Points

- What (if any) security (risk) assessment techniques or methods do you currently use in your organisation?
  - Why did you choose to apply these?
  - Do you make use of tool support to implement these? If so, which ones?

- Are there any particular regulatory requirements or standards that you must (or choose to) adhere?
  - For example, is ISO 27K relevant to your organisation?
  - Are there any EU directives, etc., current or upcoming that will be relevant to your organisation in this area?

- Security and safety analysis, e.g., analysing faults and their consequences, are closely related; do you perform any safety-related analysis currently?
  - If so, which ones, e.g., HAZOP, FMVEA, fault-tree analysis?
Discussion Points (contd.)

- What information sources do you use to inform your security analyses, regarding current threats, etc.?
  - Examples might include security advisories, news media, national CERTS, stakeholder groups, ...

- In your opinion, what is the main challenge a project like SPARKS should look to address in the area of security / risk analysis?
  - Examples include safety and security co-analysis, cyber-physical impact analysis, determining reliable threat probability figures, etc.