Threat analysis and adversarial model for Smart Grids

DECISION: Accept

AUTHORS: Javier Sande Ríos, Jesús Canal Sánchez, Carmen Manzano Hernández and Sergio Pastrana

Summary of Reviews

- Review 1: 2 (4)
- Review 2: 0 (3)
- Review 2: 0 (2)

Reviews

Review 1

Total score: 2

Overall evaluation: 2

Reviewer’s confidence: 4

The paper presents an analysis of the smart grid components and attack surface, as well as an analysis from the adversarial perspective on motivation, goals, and capabilities. The paper then introduces an adversarial model for smart grids, which is validated through the analysis of actual incidents against the smart grid during the last ten years.

Improvements:

- Authors should do a better job highlighting the contributions of the paper to distinguish from what is already done in the area.

- Section 3.1 Attack Surface could benefit from more technical depth; the breakdown per domain is good, but at the end, for the reader, it is not clear how these domains are attacked. E.g., 3.1.1 states that outdated equipment represents a significant cybersecurity risk but does not clarify if this risk is at the application level or operating system level, or about network access controls, etc.

- Section 4 could benefit from a clear overview of attacks on the power grid. The analysis presents some, and researchers mention they are 'growing', but the reader cannot know the scale of the attacks. I suggest adding some total number of known attacks, e.g.: Between 2015 and 2024 x smart grid incidents were confirmed, we will look at 3.

- Section 5 lacks depth, and authors should present a better conclusion of their work without repeating the abstract and introduction concepts.

Overall, this paper presents an interesting survey and analysis of the smart grid threats and can be a stepping stone for more research in the area.

Review 2

Total score: 0

Overall evaluation: 0

Reviewer's confidence: 3

In this work, the authors conduct a threat analysis of smart grids from an adversarial model perspective. They highlight the knowledge, goals, motivation and capabilities of the attackers and present real-world examples from known vulnerabilities.

Strengths:

The paper uses clear language which makes it an easy read

I like the real-world examples presented in Section 4 and how they are broken down

Weaknesses:

Some claims need more clarification and expansion

1) In Section 3, for Data Theft, the authors say:

"This information can be used to commit other actions, such as blackmailing or fraud, and also it might allow to conduct further steps of a cyberattack."

While it is certainly possible that data theft can lead to blackmailing and/or fraud etc, but in the context of smart grid attacks, is there such a case where this has happened?

2) In Section 3.5. I am a little confused how the authors identify these categories of attackers (i.e., state-sponsored, cyber-terrorist etc). Section 4 shows examples from state-sponsored attackers and cyber-criminals. Are there examples for a cyber-terrorist as well? I would also like a little more information about how these adversaries are identified and grouped?

3) Building upon from the last point, the authors provide a list of adversarial models in Table 2 and have some discussion around that in Section 3.5, such as,

"cyber-terrorist is an actor that resembles a statesponsored, but its goal is to harm the society or individual users of a targeted victim, i.e., with a main goal of disrupting the generation of energy. Due to potentially having less resources, it might posses fewer capabilities for lateral movement and persistence or evasion."

Since it is a little tricky to prove intent or understand exact motivation or goals behind certain actions. Are there cases of cyberterrorists performing targeted attacks with the goal of harms?

Minor sentence and/or spelling errors:

-> First, §2 presents a theoretical background about the Smart Grid, and present the related work.

-> Based on the attacker motivations, the attackers might have conduct activities to achieve one or more of the following goals

-> e.g., controling over devices via command injection, inducing false positives on security devices through the injection of false data

-> “All doamins” in Table 2

Review 3

Total score: 0

Overall evaluation: 0

Reviewer’s confidence: 2

This paper performs a threat analysis on the smart grid ecosystem. The paper is mostly an overview of many security concepts applied to the smart grid ecosystem. The first 4 pages provide an overview of the different elements that compose a smart grid system and connections between them, including ways of attacking them. Next pages deal with more security related concepts such as motivation of attackers, goals, adversarial capabilities, etc.

I don’t agree with how the human factor is considered as a transversal attack surface. The different people in each of the analysed domains have different ways of interacting with the systems and these should be taken into account. This is, isolating the humans from the systems they use will probably lead to issues when considering the possible threats correctly.

Overall, the paper provides a good overview of how security concepts can be applied to the smart grid ecosystem but I am not sure how this really contributes to a field that has already explored many of these aspects during the past few years. If the goal of the authors is to provide a systematic review I believe this should be done with a more systematic approach. Having said this I really appreciate the appendix that are provided as they explain how the authors have performed this review and the methodology they used to collect the data used for the study.