SIMULATIONS ON RESILIENCE AND MALWARE CONTAINMENT IN SMART GRID COMMUNICATION ARCHITECTURES

Peter Eder-Neuhauser, Tanja Zseby, Joachim Fabini

[a]E389 - Institute of Telecommunications at TU Wien

INTRODUCTION

Smart grids utilize Information & Communication Technology (ICT) to increase efficiency and reliability, by managing dynamics in power grids. However, ICT opens additional vulnerabilities affecting critical infrastructures, by increasing their attack surface. According to Igure et al. [1] legacy control systems experience an increasing number of attacks, as they were developed for good performance and with emphasis on features that meet network constraints, without security concerns. They argue that almost 70% of the current incidents are attacks originating from outside the network. Smart grids must be designed with security features in mind. Systemic resilience in critical infrastructures is of key importance. It therefore must include attacks, aside from technical failure.

PROBLEM STATEMENT

Malware poses a serious threat to communication networks, as it propagates with the goal of infecting vulnerable hosts. It can exploit several attack vectors to destabilize the power grid e.g. manipulating control events in power-switching equipment or denial of service attacks similar to the events described by Christiner [2]. Therefore, it is important to develop methods that employ security by architecture among other features. Considering that software vulnerabilities are discovered over time, a number of hosts in a network may be vulnerable before security patches are available.

METHODOLOGY

Several scenarios were developed for simulating malware propagation in the simulation environment ns-3. Figure 1 illustrates three types of malware attacking four types of ICT-topologies with the goal of infecting all nodes. Resilience criteria are derived from the containment properties of each topology. The architecture of communication networks can provide security features and disrupt the propagation of malicious code.

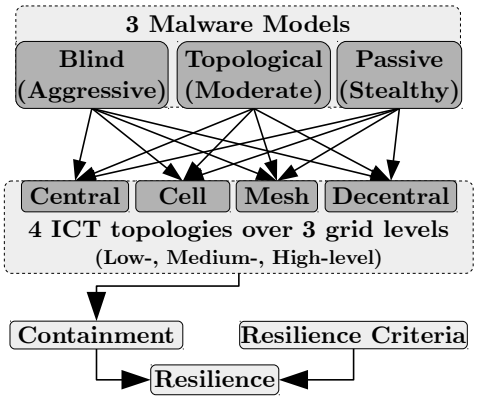

Figure 1: Scenarios: 3 malware models over 4 ICT typologies

RESULTS AND DISCUSSION

Four different topologies are instigated with the goal of improving resilience, security, and malware containment. Figure 2 illustrates a fully centralized approach, dedicated cells, mesh networks, and a fully decentralized approach. [3]

The fully centralized topology (Figure 2.a) provides situational awareness and resource control, due to a single control node. It lacks resilience because failure of the central node can result in catastrophic failure. Furthermore, malware can infect the control center and lead to a similar result.

Cell structures (Figure 2.b) allow decentralized control features, resource control, and resilience on low-level nodes. The high-level ICT is connected via uplinks, yet the cells act autonomously. This

approach provides security because propagation is inhibited by warning adjacent cells of anomalies.

Mesh networks (Figure 2.c) on the low- and medium-level provide good resilience features against failures because alternative communication paths exist. However, malware may use these paths to propagate quickly through such a network, infecting nodes in other hierarchy levels.

The fully decentralized topology (Figure 2.d) provides a mesh network throughout all levels of the hierarchy. This approach promises increased resilience against failure, at the drawback of ideal conditions for malware propagation and decreased situational awareness.

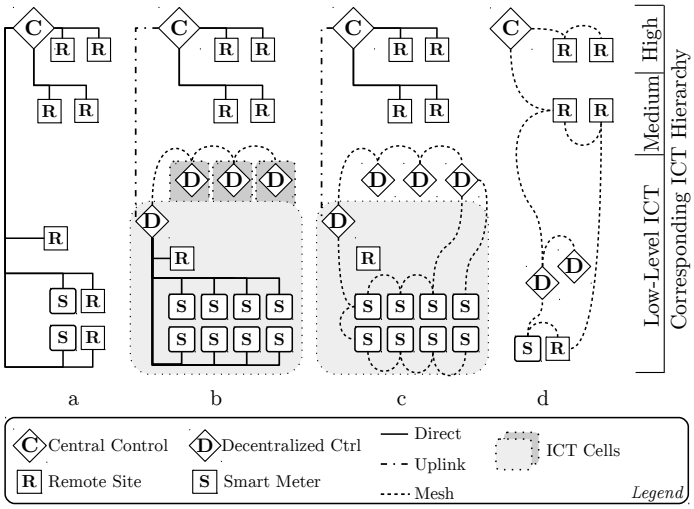

Figure 2: Control scheme with ICT cells connected via a mesh network for added resilience on the medium ICT-level

CONCLUSION & OUTLOOK

Smart grids can be secured with proactive measures such as the logical separation of networks, physical security of critical nodes, penetration testing, white-listing, regular updates or access management. Alternatively, reactive security measures allow anomaly- and intrusion-detection of unknown adversaries. Disaster recovery plans and fall-back systems can support seamless operation and recovery.

In future work the impact of three malware models on the architectures above will be simulated and appropriate defense strategies derived from the simulations. The malware features are as follows:

An aggressive ”blind scan” malware aims to infect as many hosts in the shortest time possible. It employs horizontal scanning of the IPv4 address space and therefore, produces conspicuous traffic. On successful connection with a host, the payload is transferred via TCP.

Another type uses a moderate strategy which employs a ”topological scan” of the home subnet. This approach does not produce failed connection attempts outside its subnet. Furthermore, it informs other instances of failed attempts and immune nodes. Such a partitioning of the address space allows more stealthy behavior, which makes it harder to detect.

The ”passive scan” malware spreads only to such nodes initiating a connection. It therefore generates no failed attempts. This even more stealthy behavior comes at the cost of propagation-speed.

REFERENCES

[1] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” *Computers & Security*, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[2] G. Christiner, “Die Rolle der APG für die Stromversorgungssicherheit - nationale und internationale Herausforderungen,” E-Control, Tech. Rep., May 2013, p. 13.

[3] P. Eder-Neuhauser, T. Zseby, and J. Fabini, “Resilience & Security: A Qualitative Survey of Urban Smart Grid Architectures,” *IEEE Access Journal - Special Section on Smart Grids: A Hub of Interdisciplinary Research*, Feb. 2016.