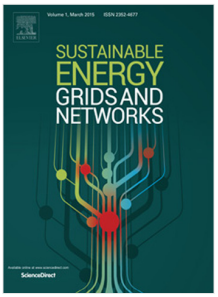
Accepted Manuscript



Cyber attack models for smart grid environments

Peter Eder-Neuhauser, Tanja Zseby, Joachim Fabini, Gernot Vormayr

PII: S2352-4677(16)30104-7
DOI: http://dx.doi.org/10.1016/j.segan.2017.08.002
Reference: SEGAN 114

To appear in: *Sustainable Energy, Grids and Networks*

Received date : 5 October 2016
Revised date : 11 July 2017
Accepted date : 9 August 2017

Please cite this article as: P. Eder-Neuhauser, T. Zseby, J. Fabini, G. Vormayr, Cyber attack models for smart grid environments, *Sustainable Energy, Grids and Networks* (2017), http://dx.doi.org/10.1016/j.segan.2017.08.002

Cyber Attack Models for Smart Grid Environments

Peter Eder-Neuhauser*, Tanja Zseby, Joachim Fabini, Gernot Vormayr

Institute of Telecommunications, TU Wien, Gusshausstraße 25 / E389, 1040 Vienna, Austria

Abstract

Smart grids utilize communication technologies that make them vulnerable to cyber attacks. Because the power grid is a critical infrastructure, it is a tempting target for sophisticated and well-equipped attackers. Cyber attacks are usually based on Malicious Software (malware) that must communicate with a controlling entity over the network to coordinate and propagate.

In this paper we investigate communication and spreading of malware in smart grids, proposing a comprehensive, generic model for cyber attack life-cycles, and addressing the specific characteristics of smart grid environments. The generic model includes the building blocks for all major known malware types as well as different propagation methods, access vectors, scanning techniques, control structures, attack methods, triggers, and cleanup mechanisms. Supported by an extensive review of earlier work, we examine the techniques of many different existing malware types with respect to their potential impacts on smart grids, and then discuss countermeasures. Toward this end, we analyze and evaluate a variety of types of malware – well-known but persistent malware, malware featuring outstanding or innovative concepts, as well as very recent malware – with respect to metrics that are fundamental to the generic model. We then introduce three novel superclasses of malware that are particularly suited for smart grid attacks, and evaluate their methods and impacts. Our model provides a basis for the detection of malware communication and extrapolates from existing technologies in order to predict future malware types. The smart grid specific malware types thus extrapolated provide insight into new threats and help utility companies to prepare defenses for future attacks.

Keywords: Communication Networks, Malware, Smart Grids, Cyber-Physical Systems, Cyber Attacks

1. Introduction

Smart grids, i.e., networked power grid control equipment, depend on Information & Communication Technology (ICT) for managing power flux and energy balance. A smart grid hosts several types of devices, including but not limited to measurement equipment (e.g., Phasor Measurement Units (PMU) and smart meters), actuators (e.g., breaker-switches and disconnectors), and networking equipment (e.g., gateways and control nodes). These critical devices are just as susceptible to Malicious Software (malware) as are classical Internet technologies and consumer electronics. However, unlike consumer electronics, traditional power grid environments have a focus on long-term stability and plan for hardware life-spans of 10 years or more. As devices age, unknown vulnerabilities of hardware, operating system, software, and protocols emerge. Such vulnerabilities pose a serious threat to the infrastructure. While consumer electronics need not fulfill the same life-cycle requirements of industrial devices, their base technology is similar.

Today, few malware implementations that have actually caused severe physical damage to cyber-physical systems are known. However, during the last decade the number of such highly evolved malware, capable of orchestrated cyber-physical attacks has increased. The complexity and sophistication of these malware implementations lead to the assumption that massive resources were invested in their development and that they may be financed by large stakeholders such as nation states [1–3]. The detection and analysis of existing malware is of paramount importance for the implementation of countermeasures, which are critical to the safe operation of smart grids. However, the danger of extensively documenting malware algorithms is that it decreases the effort required to craft novel malware. Malware families could be created that combine existing mechanisms with unpublished, highly effective zero-day-exploits (zero-days) and then be exploitable by less equipped adversaries to attack critical infrastructures.

The remainder of this paper is structured as follows. Section 2 reviews the state of the art of modern malware. Section 3 identifies the most important characteristics of smart grid environments with respect to networking and security, placing particular emphasis on the differences from the classical Internet. Section 4 proposes a generic model for the life-cycle of malware-based cyber attacks, describing all involved stages. Several subsections then explain the specific parts in more detail. A classification in Section 5 identifies similarities, benefits, shortcomings, and differentiating features of existing malware. We concentrate on sophisticated modern as well as older but prevailing malware. Section 6 investigates the most distinct features that are effective in smart grid environments and their pos-

*Corresponding author

Email addresses: peter.eder-neuhauser@tuwien.ac.at (Peter Eder-Neuhauser), tanja.zseby@tuwien.ac.at (Tanja Zseby), joachim.fabini@tuwien.ac.at (Joachim Fabini), gernot.vormayr@nt.tuwien.ac.at (Gernot Vormayr)