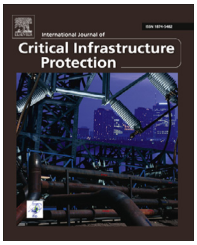
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP



Security analysis of an advanced metering infrastructure

Aaron Hansen, Jason Staggs, Sujeet Shenoi[*]

Tandy School of Computer Science, University of Tulsa, 800 S. Tucker Drive, Tulsa, Oklahoma 74104, USA

ARTICLE INFO

Article history:
Received 28 December 2016
Revised 23 February 2017
Accepted 25 February 2017
Available online 3 April 2017

Keywords:
Advanced Metering Infrastructure
Smart Meters
Data Collectors
Attack Vectors
Targets
Functionality
Attacks
Impacts

ABSTRACT

An advanced metering infrastructure is an integrated system of smart meters, communications networks and data management systems designed to support the safe, efficient and reliable distribution of electricity while providing advanced functionality to energy customers. Unfortunately, sophisticated cyber attacks on advanced metering infrastructures are a clear and present danger. The most devastating scenario involves a computer worm that traverses advanced metering infrastructures and permanently disables millions of smart meters.

This paper presents a security analysis of an advanced metering infrastructure comprising more than one million smart meters, 100+ data collectors and two meter data management systems. Specifically, it provides detailed evaluations of the attack surface, targets – especially the critical data collectors – and their functionality, and possible attacks and their impacts. The systematic identification of each target and its functionality, and possible attacks and their direct impacts, are essential to understanding the security landscape as well as specifying and prioritizing mitigation efforts as part of a robust risk management program. Although this work is based on an analysis of one large advanced metering infrastructure, strong attempts have been undertaken to extract and articulate the commonalities when describing the attack surface, targets, possible attacks and their impacts. Thus, the results presented in this paper can be used as a foundation upon which the unique aspects of an advanced metering infrastructure can be added to create a robust risk management program geared for the specific deployment.

1. Introduction

The U.S. power grid is vulnerable to cyber attacks [17]. Nation states and other malicious entities are believed to have gained persistent access to power grid assets [7]. This access could be leveraged during times of conflict to cause widespread power disruptions that affect millions of people.

On December 23, 2015, the Russian hacker group, Sandworm, attacked the Ukrainian power grid [12]. The hackers used spear phishing to compromise corporate computers. They then pivoted to the control network and remotely opened substation breakers. Overall, the attacks targeted substations at three electric utilities and the resulting blackout affected more than 225,000 customers [10,24]. Despite the large geographical area that was affected, services were restored within six hours by plant operators who had to manually reset the circuit breakers. If this attack had targeted many more nodes across the grid, the recovery time would have been much longer.

Over the past several years, many U.S. electric utilities have leveraged Department of Energy stimulus grants to modernize their electricity distribution systems [29]. Most of the modernization efforts have involved upgrading legacy distribution

[*] *Corresponding author.*
E-mail address: sujeet@utulsa.edu (S. Shenoi).

http://dx.doi.org/10.1016/j.ijcip.2017.03.004
1874-5482/© 2017 Elsevier B.V. All rights reserved.

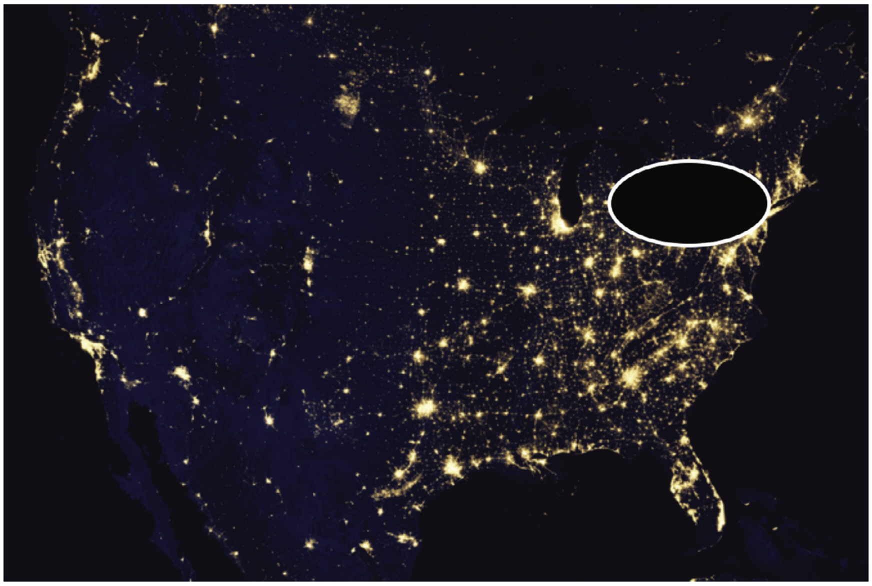


Fig. 1 – Northeast blackout of 2003.

infrastructures to advanced metering infrastructures. An advanced metering infrastructure comprises management systems, databases, data collectors and smart meters installed at customer premises. St. John [29] estimates that more than 50 million smart meters are in use across the United States, the vast majority of them in large metropolitan areas. Approximately 43% of U.S. households currently have smart meters installed.

Sophisticated cyber attacks on advanced metering infrastructures are a clear and present danger. The most devastating scenario involves a computer worm that traverses advanced metering infrastructures and permanently disables or "bricks" millions of smart meters in major metropolitan areas.

Fig. 1 shows a simulated depiction of the famous 2003 blackout in the Northeastern U.S. and Canada. The blackout was initiated by transmission lines in Ohio that were damaged by overgrown tree limbs [25]. Software problems that delayed or prevented alarms from reaching utility operators contributed to the cascading failure that affected 508 generating units at 265 power plants, leaving 50 million people without electricity for seven hours to two weeks.

Fig. 2 shows the potential impact of smart meter bricking attacks on fifteen of the largest U.S. metropolitan areas. The total population in the affected metropolitan areas is approximately 110 million, more than twice as many people as were affected by the 2003 blackout. But much more significant is that the attacks would result in, not a few or even hundreds, but tens of millions of points of failure. Power to each customer premises would not be restored until the damaged smart meter is replaced, which typically takes a technician approximately 30 minutes. What is truly scary is that the limited inventories of smart meters due to production capacity and the inadequate number of trained technicians available to replace the damaged smart meters would result in outages lasting several months to more than one year. How would America cope with extended blackouts of its major cities?

The criticality of advanced metering infrastructures to modern society has resulted in a large body of work on securing advanced metering infrastructures (see, e.g., [4,6,13,19,21,33]). However, missing are detailed empirical evaluations of large fielded advanced metering infrastructures. In particular, evaluations of the attack surface, the targets – especially the critical data collectors – and their components and functionality, and possible attacks and their impacts. This paper attempts to address the gap by presenting the results of a security analysis conducted of an advanced metering infrastructure with more than one million smart meters, 100+ data collectors and two meter data management systems. The attack surface of the advanced metering infrastructure comprises the attack vectors that can be leveraged to target smart meters and/or data collectors and impact the security goals of confidentiality, integrity and availability. The focus is on attackers who would use physical and/or cyber means to gain access and privileges to the devices and networks, following which key assets in the advanced metering infrastructure would be targeted by cyber means. Several attack vectors are presented that enable a sophisticated attacker to target advanced metering infrastructure assets and operations to realize five possible outcomes: (i) theft of data; (ii) theft of power; (iii) localized denial of power; (iv) widespread denial of power; and (v) disruption of grid.

Advanced metering infrastructures are massive and complex systems of systems. Typically, a utility works with vendors and integrators to design and provision an infrastructure. The scale, diversity and complexity of the infrastructure coupled with its continuous evolution in terms of scale, topology, hardware/firmware/software, functionality and security controls make it extremely difficult for utility personnel to comprehend the true attack surface and targets, which include cyber-physical assets as well as their communications channels. It is imperative to understand how an attack on a target or its component can impact functionality and, by extension, the safe and reliable operation of the advanced meter-