Chapter 15

Authentication of Smart Grid:
The Case for Using Merkle Trees

Melesio Calderón Muñoz
Cupertino Electric, Inc., USA

Melody Moh
San Jose State University, USA

ABSTRACT

The electrical power grid forms the functional foundation of our modern societies, but in the near future our aging electrical infrastructure will not be able to keep pace with our demands. As a result, nations worldwide have started to convert their power grids into smart grids that will have improved communication and control systems. A smart grid will be better able to incorporate new forms of energy generation as well as be self-healing and more reliable. This paper investigates a threat to wireless communication networks from a fully realized quantum computer, and provides a means to avoid this problem in smart grid domains. We discuss and compare the security aspects, the complexities and the performance of authentication using public-key cryptography and using Merkel trees. As a result, we argue for the use of Merkle trees as opposed to public key encryption for authentication of devices in wireless mesh networks (WMN) used in smart grid applications.

ORGANIZATION BACKGROUND

Cupertino Electric Inc. is a private company founded in 1954 and headquartered in San José, CA. It provides electrical engineering and construction services.

San José State University (SJSU) was founded in 1857 as a normal school and has matured into a metropolitan university in the Silicon Valley. It is one of 23 campuses in the California State University system, offering more than 145 areas of study with an additional 108 concentrations.

DOI: 10.4018/978-1-7998-1763-5.ch015

INTRODUCTION

The electrical power grid has served humanity well up to now, but as we seek new ways to generate energy and improve efficiency, we find that the existing grid will not be able to meet our needs. It is expected that by 2050 worldwide consumption of electricity will triple (Kowalenko, 2010). Furthermore, power grids are still susceptible to large-scale outages that can affect millions of people (U.S.-Canada Power System Outage Task Force, 2004). These are the motivations for the creation of an "advanced decentralized, digital, infrastructure with two-way capabilities for communicating information, controlling equipment and distributing energy" (National Institute of Standards and Technology (NIST, 2010). This infrastructure will be better able to incorporate new forms of energy generation, as well as be self-healing and more robust. Each device in a smart grid will likely have its own IP address and will use protocols like TCP/IP for communication. Thus they will be vulnerable to similar security threats that face present day communication networks (Yan, Qian, Sharif, Tipper, 2012); however, the stakes will be much higher. That is to say, in the information technology industry the highest priority is the confidentiality, integrity and availability of information. In the electrical power industry the highest priority is human safety. For the smart grid cyber security measures must not get in the way of safe and reliable power system operations (NIST, 2010).

Problem Statement

"The smart grid is a long-term and expensive resource that must be built future proof" (NIST, 2014). That is to say it must be designed and implemented to be able to meet future scalability and functionality requirements. At the same time it also needs to be able to survive future malicious attacks. With this in mind, and with our knowledge of the threat posed to some types of public key encryption from the quantum computer, it must be concluded that if the quantum computer is realize and public key encryption is extensively used in the smart grid we will have a very serious situation on our hands.

While many may still think that the era of quantum computing is in the far horizon, according to the Wall Street Journal, China launched the world's first quantum communication satellite in August 16 2016 (Wall Street Journal, August 2016). While this has "set to launch Beijing far ahead of its global rivals in the drive to acquire a highly coveted asset in the age of cyber espionage: hack-proof communications," it has also shown that cyber attacks that are based on quantum computing may be more eminent that what many initially thought. Finding alternatives to public key encryption that is vulnerable to quantum-computing based attacks for smart grid at this stage is therefore timely, and is in line with NIST goals of making the smart grid "future proof."

This chapter looks at the threat to public key encryption systems from the quantum computer in the context of smart grid security. The authors argue for the use of Merkle (Hash) trees as opposed to public key on the smart grid, specifically when used to authenticate devices in WMN. Results of this chapter have been presented as a poster (Muñoz, Moh, & Moh, October 2014) and a conference paper (Muñoz, Moh, Moh, December 2014). This is a continuation of our research effort in smart grid (Kapoor & Moh, 2015) and in mobile network and cloud security (Wong, Moh, & Moh, 2012; Yang, & Moh, 2012; Gaur, Moh, & Balakrishnan, 2013).

For this chapter a Merkle tree authentication scheme is implemented, and incorporated into the ns-3 Network Simulator. It is then compared to the performances of a publicly available version of RSA, a public key encryption system. The goal is to show that Merkle trees are a reasonable alternative to public key cryptography system for smart grid networks.