PNNL-24641

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Increasing the resilience and security of the United States' power infrastructure

August 2015

SF Happenny

U.S. DEPARTMENT OF
ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

PNNL-24641

Increasing the resilience and security of the United States' power infrastructure

SF Happenny

August 2015

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Abstract

The United States' power infrastructure is aging, underfunded, and vulnerable to cyber attack. Emerging smart grid technologies may take some of the burden off of existing systems and make the grid as a whole more efficient, reliable, and secure. The Pacific Northwest National Laboratory (PNNL) is funding research into several aspects of smart grid technology and grid security, creating a software simulation tool that will allow researchers to test power infrastructure control and distribution paradigms by utilizing different smart grid technologies to determine how the grid and these technologies react under different circumstances. Understanding how these systems behave in real-world conditions will lead to new ways to make our power infrastructure more resilient and secure. Demonstrating security in embedded systems is another research area PNNL is tackling. Many of the systems controlling the U.S. critical infrastructure, such as the power grid, lack integrated security and the aging networks protecting them are becoming easier to attack.

Acknowledgments

The labor for all of my contributions to this work was funded by the U.S. Department of Energy through the Pacific Northwest National Laboratory's National Security Internship Program. Further, all work was conducted at PNNL. I would like to thank my mentor, Sean Zabriskie; project team leads, Thomas Edgar and David Manz; and my team members and colleagues. I would not have had such a successful internship experience if not for the eager assistance offered by my colleagues at PNNL. They have helped immensely with my project work, becoming familiar with the various aspects of PNNL, and my development as a professional. I look forward to continuing my work at the Lab.

Acronyms and Abbreviations

ns-3: Network Simulator 3

Contents

1.0 Introduction

According to Edwin Hill, president of the International Brotherhood of Electrical Workers, "the average age of power transformers in service is 40 years, which also happens to be the average lifespan of this equipment."[1] In addition to the age of U.S. infrastructure, the amount of investment in the current grid infrastructure is significantly less than what its maintenance requires and is just a fraction of the amount needed to grow it to meet the increasing demands we place on it. These factors, plus the increasing sophistication and proliferation of cyber attacks, puts the United States' power grid at risk of massively impactful cyber attacks. The risk is so great that the head of the National Security Administration and U.S. Cyber Command, Michael Rogers, said in November 2014 that it is "only a matter of the when, not the if, that we are going to see something traumatic" happen to the U.S. power grid.[2] In particular, Rogers said that China and "one or two" other nation states are capable of launching a cyber attack that could shut down the entire U.S. power grid in addition to other critical infrastructure.

Fortunately, work on improving the U.S. power infrastructure has begun with the development of smart grid technologies that will help upgrade the power grid into the 21st century and increase the efficiency, resilience, and security of these critical power systems. PNNL has many research programs to support the development of smart grid technologies and help secure U.S. critical infrastructure. One project aims to develop software that will more easily allow researchers to investigate ideas in simulated power grids utilizing smart grid technology. Another project will demonstrate the use of a cheap and common microchip to provide security to the embedded computing systems controlling the physical systems that make up the power and other critical infrastructure. Both of these projects will be discussed in detail in the following sections.

2.0 Integrated power grid simulator

2.1 Overview

As part of PNNL's goal to improve the reliability and security of the nation's power infrastructure, PNNL researchers wish to investigate new distributed control paradigms under realistic conditions. However, to simulate all of the relevant domains and technologies involved in the power grid, multiple simulators must be integrated and executed together. The smart grid technologies used in these new distributed control paradigms include Internet-connected power meters that can decide automatically, based on energy price, when to consume energy and communicate these decisions to other power meters, distribution systems, and customers. This level of communication will enable more efficient transmission of electricity, reduce peak demand, and improve grid resilience and security.[3] Our team is developing a modeling language that encompasses the attributes of interest across all the simulators. This reduces the burden of understanding all of the details of each simulator configuration language, eliminates errors of mapping items between simulators, and makes researchers more efficient.

2.2 ns-3

The Network Simulator 3 (ns-3) is a free, open-source discrete-event network simulator aimed at educational and research use.[4] ns-3 can be used to simulate many different network protocols, including Ethernet, LTE, Wi-Fi, and 6LoWPAN, a wireless device-to-device standard developed for low-power Internet of Things devices.[5] ns-3 can also connect to arbitrary data sources, such as a real networking device like a physical router or a virtual source like Internet traffic from another simulator, and can record information about the simulated network's performance. This combination of free access and versatility makes ns-3 an appealing choice for use in projects like ours where our modeling language will be used to test many different technologies and hypotheses.

The purpose of using ns-3 in our project is to provide a high-fidelity, configurable virtual network over which the smart grid devices can communicate. Without a network simulator, communication between smart grid devices was instantaneous and perfect. This may not sound like a problem, but networking in the real world is far from instantaneous and definitely not perfect. Data takes time to move along physical media and can get bogged down in traffic, adding latency to the data transfer. Also, data are lost all the time in physical networks, necessitating a resend of the original data or some error management on the receiving end, thus adding additional delay and complexity to the communication channel. ns-3 accounts for these delays and imperfections, providing a more accurate representation of physical network conditions. This increased accuracy provides researchers with a truer idea of how the smart grid technologies they are testing will respond in the real-world.

2.3 Progress and outcome

Our team recently demonstrated the basic functionality of our modeling language and is moving towards releasing an initial version to researchers at PNNL. At the demo, we compared code written in the simulators' native languages to the modeling language we have developed to show how simple our language is compared to the native simulators'. We know researchers will most likely not have a strong background in computer programming or networking, so simplifying the creation of the simulated power grid and network is critically important. Our goal is to allow the researchers to focus as much of their time as possible on answering the questions they have, not configuring the tools to do so. We also demonstrated the execution of a power grid model written in our modeling language that researchers developed previously with the discrete simulators. Overall, the demo was a success and secured the continued support for this project.

Before the demonstration, we initialized a major restructuring of the inter-simulator communications and the networking simulator in order to unify the syntax used in our modeling language and provide a more intuitive user interface. Restructuring the networking component was my responsibility and resulted in a much cleaner, simpler public interface for the ns-3 component. In addition to improving the usability of the modeling language, working on this project has taught me more about good software design and coding practices. These skills will be incredibly useful in my future career at the Lab or elsewhere. Moving forward, we will continue to add new features to our modeling language, including support for LTE, point-to-point, and Wi-Fi networks in the networking component. We will also work to make the networking modeler more flexible to allow researchers to create whatever network configurations they require to test their hypotheses.

3.0 Embedded systems security

3.1 Overview

Much of the hardware that runs the United States' critical infrastructure—including power, water, and communication systems—is decades old and has few, if any, built-in security provisions. Once a cyber attacker penetrates the security of the control system network that houses the embedded cyber-physical devices, they generally have full access to these devices that run physical systems like fans, pumps, and more. Therefore, building security into these embedded systems is crucial. One way to provide some security is through a Trusted Platform Module (TPM), a cheap microchip that contains dedicated cryptographic processors and secure storage, which has been used in enterprise-class computers for over a decade. TPMs can provide several processes for providing different types of security and authentication. Measured boot, for example, uses the TPM to check that the pre-boot environment has not been modified by malware and creates a chain of trust that successively verifies that each software layer running on the device has also not been modified.[6] After the values obtained by hashing each piece of software have been verified as correct, they are sealed in a storage unit on the TPM to preserve a signature of the valid state of the software stack. This storage is also used to store securely the keys used for encryption/decryption and signing of certificates. Another example of a function a TPM can provide is attestation, "the process by which a platform can cryptographically prove to another platform that it is in a particular state."[6] Attestation can be used to ensure that a device has not been tampered with before authenticating the device on a network.

For this project, we are using two BeagleBone Black development boards and two CryptoCapes that adds a TPM, among other cryptoprocessors, to the BeagleBone base board.[7, 8] The goal of the project is to demonstrate the ease of setting up and using a TPM to help protect embedded systems. Specifically, we want to use the TPM to certify that software installed on the BeagleBone to emulate the programmable logic controllers (PLCs) that control the physical devices in the power grid has not been modified before performing critical tasks, such as opening a breaker switch. The plan to achieve this goal is to document the setup of the TPMs and use them to attest the integrity of the software installed on the BeagleBones.

3.2 Progress

Work on this particular project has been limited due to demands from the power grid modeling language project. Currently, the BeagleBone boards and TPMs have been configured and are bootable and useable. The next step is to setup trusted boot with the TPMs, an involved process that requires the installation of a bootloader and other software specifically designed to allow trusted boot. After this is accomplished, we will install the PLC emulation software and add this software to the stack verified by the TPM. This will allow the system to verify that any changes made to the PLC emulation software, such as an operator sending instructions to reduce power production, are valid and not due to a malicious hacker inside the system.

4.0 References

1. Edwin D. Hill, EnergyBiz (September/October), (2007).
2. Amelia Smith, China Could Shut Down U.S. Power Grid With Cyber Attack, Says NSA Chief, (2014), (http://www.newsweek.com/china-could-shut-down-us-power-grid-cyber-attack-says-nsa-chief-286119).
3. U.S. Department of Energy, The Smart Grid, (https://www.smartgrid.gov/the_smart_grid/smart_grid).
4. NSNAM, What is ns-3, (2015), (https://www.nsnam.org/overview/what-is-ns-3/).
5. Carsten Bormann and Zach Shelby, 6LoWPAN: The wireless embedded Internet - Part 1: Why 6LoWPAN?, (2011), (http://www.eetimes.com/document.asp?doc_id=1278794).
6. Justin D. Osborn and David C. Challener, John Hopkins APL Technical Digest 32 (2), 8 (2013).
7. J. Kridner, BeagleBone Black, (2015), (http://beagleboard.org/black).
8. SparkFun, CryptoCape, (https://www.sparkfun.com/products/12773).

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by **Battelle** *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov