INL/RPT-22-66768-Revision-0

CyOTE ASSET OWNER ENGAGEMENT SIDE CHANNEL POWER ANALYSIS PROTOTYPE

March 2022

Michael George Durller, Victor Costanza, Joseph Cummings, Jeremy Michael Jones

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/RPT-22-66768-Revision-0

CyOTE ASSET OWNER ENGAGEMENT SIDE CHANNEL POWER ANALYSIS PROTOTYPE

Michael George Durller, Victor Costanza, Joseph Cummings, Jeremy Michael Jones

March 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CyOTE ASSET OWNER ENGAGEMENT – SIDE CHANNEL POWER ANALYSIS PROTOTYPE

MARCH 31, 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

This document was prepared by Idaho National Laboratory under an agreement with and funded by the U.S. Department of Energy.

INL Idaho National Laboratory

Table of Contents

EXECUTIVE SUMMARY

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), through the Cybersecurity for the Operational Technology Environment (CyOTE) Program, worked with energy sector asset owners and operators (AOOs), partners, and Idaho National Laboratory (INL) to develop capabilities for AOOs to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. The CyOTE methodology[1] seeks to identify adversarial techniques within an AOO OT environment that could result in physical disruptions to energy flow or damage to equipment. CyOTE provides a general roadmap for AOOs, starting from a triggering event, or the point in time and space they perceive an anomalous event or condition meriting investigation, and culminating when the AOO has sufficient confidence to make a business risk decision on the appropriate resolution.

CyOTE supplemented these capabilities with engagements with AOOs to assist them with applying the CyOTE methodology in their own OT environments. By participating in these engagements, AOOs were shown how to apply the methodology to identify triggering events of interest. They worked with the CyOTE team to better leverage existing data that aided in the development of capabilities to detect triggering events. In doing so, AOOs will be able to make better informed risk decisions and implement appropriate, prescribed, and timely actions.

This paper outlines the results of one such engagement with the New York Power Authority (NYPA), where the CyOTE program partnered with an AOO to develop a design specification for a power side channel detector to identify anomalous changes to device load. It describes the goal of developing this capability, the development process, the challenges the technical teams faced and the future steps an AOO will need to take to install and use this detector in its OT environment.

[1] Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Methodology for Cybersecurity in Operational Technology Environments*, September 23, 2021, https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf

INTRODUCTION

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), through the Cybersecurity for the Operational Technology Environment (CyOTE) Program, works with energy sector asset owners and operators (AOOs), partners, and Idaho National Laboratory (INL) to develop capabilities for AOOs to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. Unlike the approach taken with commercial security solutions, CyOTE seeks to tie anomalies to early indicators of a cyber-attack.

This paper describes the work the CyOTE research team conducted in their engagement with New York Power Authority (NYPA). The NYPA engagement's goal was to improve internal capability to perceive anomalies related to power flow from devices. AOOs gather volumes of operational data from the OT environment, and most (if not all) of that data is used in support of safe, reliable control of energy systems. The experience of CyOTE's AOO partners demonstrates that operational data alone may be insufficient to perceive malicious cyber activity.[2] Detection of adversarial behavior may require additional data, which strategically placed sensors or detectors can provide. Used together with additional information from non-standard data sources, the capabilities of the CyOTE program enable greater perception and comprehension of anomalous observables.

This paper draws from the CyOTE program's history and NYPA's experience participating in the engagement. The goal is to share information about this capability as an example of the type of capability that other AOOs can develop to enhance the perception and comprehension of cyber and physical anomalies. The paper reflects on the design specifications for this power side channel detector and concludes with next steps that an AOO can take to further the development of this detector for future implementation in their OT environment.

BACKGROUND

Since 2016, the CyOTE program and INL have partnered with industry to develop targeted strategies to increase the cybersecurity and resiliency of America's energy sector. The NYPA is the largest state public power utility in the country, operating 16 generating facilities and more than 1,400 circuit-miles of transmission lines.[3] As one of the nation's largest AOOs, NYPA possesses a large ICS environment to effectively service its customers.

NYPA began working with the CyOTE team in 2020. This reflected NYPA's Vision 2020 Strategic Plan to become the first end-to-end digital utility, by providing greater insight into energy supply and demand levels, reducing operational costs, and improving energy efficiency.[4]

---

[2] For additional information, or to learn more about the CyOTE program, visit https://inl.gov/cyote, or email CyOTE.Program@hq.doe.gov

[3] "About NYPA," New York Power Authority, accessed November 2, 2021, https://www.nypa.gov/about/the-new-york-power-authority.

[4] "New York Power Authority: Vision 2020 Building an End-To-End Digital Utility," New York Power Authority, January 2018, https://www.nypa.gov/-/media/nypa/documents/document-library/isoc/vision2020-digital-utility-roadmap.pdf.

SIDE CHANNEL POWER ANALYSIS

ENGAGEMENT GOAL

The goal was to demonstrate how an AOO can leverage the CyOTE methodology with existing commercial monitoring capabilities and to gain a better understanding of an anomaly within their operational environment. NYPA and the CyOTE research teams created the design specifications to develop a prototype for a novel detector to provide additional information so that the AOO could determine if there was a potential cyber incident or configuration change to a critical industrial control system microprocessor/programmable component using power side channel means. In this case, the power supply's residual noise from the switching power supply present in computers and router equipment is measured to develop a fingerprint of the computing activity happening on that device.

A no-load situation (e.g., when the device is powered down) is easy to detect, but the research team was interested in whether it is possible to detect other load situations, such as when the device is highly loaded with compute activity, or if it is doing a memory check, such as a reboot or reset condition. Additionally, the research teams wanted to discern if a noticeable pattern or electromagnetic noise residual could be used to establish a baseline for the activity of the power drawn from mains when these sorts of actions are being performed by the device.

The ability to detect a change out-of-band from the baseline and classify it as an abnormal condition would essentially prevent a potential adversary from having any visibility or knowledge over what the sensor is reporting—and would give them very little, if any, control over it—as the sensor is not running on the machine itself and cannot be masked by the adversary. This would be the case in a traditional anti-virus or intrusion detection program that runs on the attacked platform, for example.

SENSOR PROTOTYPE SPECIFICATIONS

To develop the design specifications for the prototype sensor, the research teams chose to focus on the alternating current (AC) line input of the machine, which is 120 volts AC in the U.S. The implementation measures the current with a medium speed Analog-to-Digital Converter (ADC) at just under 1 mega-sample per second. For the purposes of the prototype, the CyOTE program chose a single board computer (SBC) popular with the Do-It-Yourself (DIY) and cyber prototype community – the BeagleBone® Black. The BeagleBone® uses an ARM processing unit with roughly the same power of a low-end smart phone.

The BeagleBone® runs Linux as the primary operating system, but two other dedicated Programmable Realtime Unit (PRU) microcontrollers connected to the IO pins will handle the high-speed serial communications (Serial Peripheral Interface [SPI] bus) to the ADC and the 60 Hz zero crossing detection and filtering. The latter part is particularly important, as the operating system typically cannot receive data at a 16MHz clock data rate, which the dedicated PRU microcontrollers can, without some issues of overhead. Thus, the PRUs can run at full capacity forever, as this is their only dedicated (real-time) tasking.

The first PRU will handle the communications interface and the timing of each frame of data sent to the second PRU for packing into two buffers. This is called a ping-pong buffer scheme. The data transfers between the PRUs with an interface that Texas Instruments (TI) calls "broadside

data transfer," where an interrupt can allow an entire processor register set to be transferred to the other processor in a very short period of time.

After the second processor packs the data alternately into the two ping-pong shared memory buffers, the operating system (OS) will run a user program that picks the data up from the buffers when a special tag indicates the data is ready. The shared memory segment of RAM between the PRU and the main processor is specially set aside at boot time using a mechanism called the Device Tree Binary Overlay (DTBO) system, which the Linux Bootloader (u-boot) can understand. This mechanism also reserves some of the general-purpose IO (GPIO) pins on the chip for the three devices and allows the ADC to physically connect to the BeagleBone® SBC.

In support of this research the CyOTE program developed a software flow diagram showing how this process functions on the prototype. These are included in Appendix A.

DEVELOPMENT CHALLENGES AND SOLUTIONS

The CyOTE program overcame several challenges during the development of the design specifications for the sensor prototype, which are described below along with the team's solutions or workarounds.

Cross-Compilation Versus Native Compilation Toolchains for the TI Sitara Processor

The capability to build the PRU and ARM-based binary files is no longer supported on the native (ARM Linux) system, so the research team needed to instead use TI's development environment and install Ubuntu 18, which TI recommends as a base operating system for a cross-compiling toolchain. A new install of Ubuntu 18 was added as a guest OS in VirtualBox.

Another challenge was with the Make utility in Ubuntu, which the research teams did not have experience using. Makefiles could not be pulled outside the example source tree without two environment variables being set up. The deep paths that the Makefiles needed for these tools were printed out via the echo command, later in the main build system. When these environments are fully set up, the toolchain can be run outside the main source tree for the TI toolchain. The toolchain ships with a Git repository already set up for source control.

Device Tree Load at Runtime

The research teams discovered that while the ability to build the PRU and ARM-based binary files was supported by the Linux kernel in the past, it now seems to have been deprecated or is not supported in the more modern (4.19.94-ti-r64) Linux kernel, and the uEnv.txt file is modified to load the overlay modules at boot time from u-boot instead. Uboot_overlay_addr0 and uboot_overlay_addr1 were used to load the overlay files for the DTBO for the Reserved Data Ram Space from the Linux kernel, and the GPIO modes select routine with the interrupt enable routine for the PRU processors. Many of the older TI examples use a different setup for the Device Tree Source files, so these had to be ported over to the device tree overlay format.

Interrupts presented an additional consideration. Interrupts must be enabled on the PRU subsystem to get broadside transfers to work between the two PRUs. Broadside data transfers cannot occur if the interrupt subsystem is not enabled in the DTBO, but they will still compile and look like they are working. This is not well documented by the vendor, especially in troubleshooting. The remote processor will never get the data without the interrupt on the current TI development environment. This is enabled through the DTBO configuration. The

default load for the PRU subsystem brings up the interrupts in question, so this is required in the compiled DTBO file.

Shared Memory

There is a lack of support for an untouched memory segment by the device tree compilers used for this research effort. Version 1.4.7 (and potentially higher) of the device tree compiler must be used to compile properly with the Linux kernel used. This version safely sets aside a high-memory segment that the Linux kernel does not use and is verified to work as a data buffer to transfer data between the PRU and the Linux user space program via direct pointer access. Multiple odd-looking warnings are created on the compilation of this Linux kernel module, but they can be safely ignored.

SPI Digital Noise

Since an evaluation board was used for the ADC that is external to the BeagleBone® and connected by a ribbon cable, some capacitive loading effects can be observed on the SPI bus—especially considering that the IO voltage leveler is only 3.3V at low voltage transistor-transistor logic (LVTTL) signal standards. The research team consider this as a development artifact and should not be an issue when an actual backpack circuit board is designed for the BeagleBone® to mate directly in a backpack fashion.

The SPI driver is synced directly to the external temperature compensated crystal oscillator (TCXO) clock. Because of this, the edge detection in the PRU is not tolerant of glitching, reflections, or noise in the framing of an ADC word with the 3.3V LVTTL signals; the SPI master does not create the clock signal itself and is not acting like a master clock.

FURTHER DEVELOPMENT

To fully implement this prototype into the OT environment, it is recommended that AOO takes the following actions:

1. **Debug and enable coherent sampling**—Coherent sampling, with the same number of AC waveforms per sample window (60Hz in North America) will improve ADC results with the fast Fourier transform (FFT) algorithm by reducing the spectral leakage of each identified frequency bin.
2. **Implement a zero-crossing detector lowpass filter**—Since the sample rate is much higher than the 60Hz signal, a zero-crossing detector lowpass filter will be needed to cut the higher frequency components of the signal and allow the detector to perform the 60Hz zero crossing detection without interference.
3. **Implement FFTW software library**—Since the device is intended to use a FFT algorithm to detect higher frequency signals, the Fastest Fourier Transform in the West (FFTW) library is recommended. The ARM NEON (single precision acceleration) works with this library and the SBC.
4. **Develop classifier algorithm**—Once there is a robust set of FFT data, a classifier algorithm will allow real-time detection. This would operate on the FFT output bins and would likely be functional programming on the Linux OS side.

CONCLUSION

The CyOTE program's goal is to assist AOOs in developing capabilities to detect, investigate, and mitigate malicious activity. If there is sufficient belief the anomalies perceived and comprehended indicate possible malicious cyber activity, the appropriate organizational action is to initiate their cybersecurity incident response process according to organizational policy and procedures. This research assists AOO by incorporating physical properties into the analysis to determine whether an incident is a malicious cyber event or non-malicious failure. The results of the CyOTE program's work with NYPA demonstrated that a power side channel detector could be used to identify potential anomalous changes to device load, which would provide increased visibility into power loads in a manner that an adversary would not be able to detect or control.

AOOs can refer to the CyOTE methodology for more information on identifying anomalies in an OT environment. DOE would like to thank and recognize NYPA for taking part in this discussion and sharing their experience with other industry partners. The CyOTE team hopes that collaboration activities such as this will benefit the industry as a whole in the protection of the flow of energy.

Click for More Information	CyOTE Program || CyOTE Fact Sheet || CyOTE.Program@hq.doe.gov

APPENDIX A: SOFTWARE FLOW DIAGRAMS

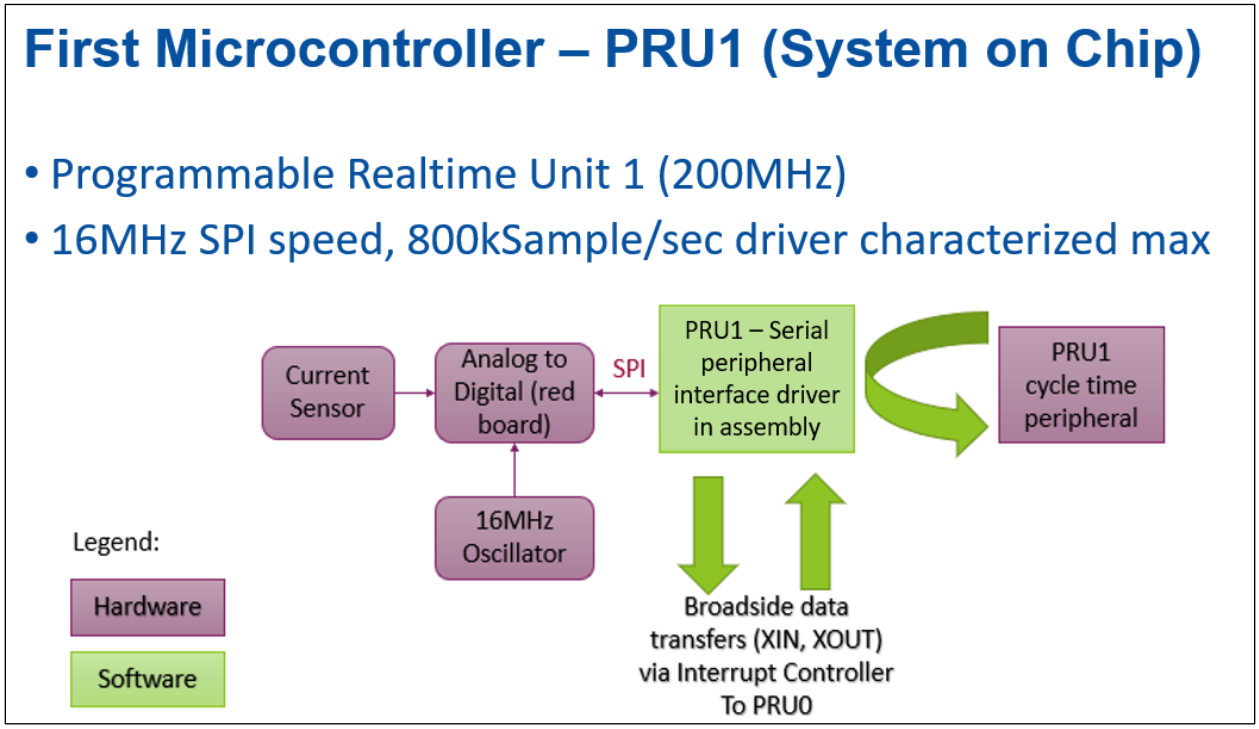

Figure 1: Model of First Microcontroller

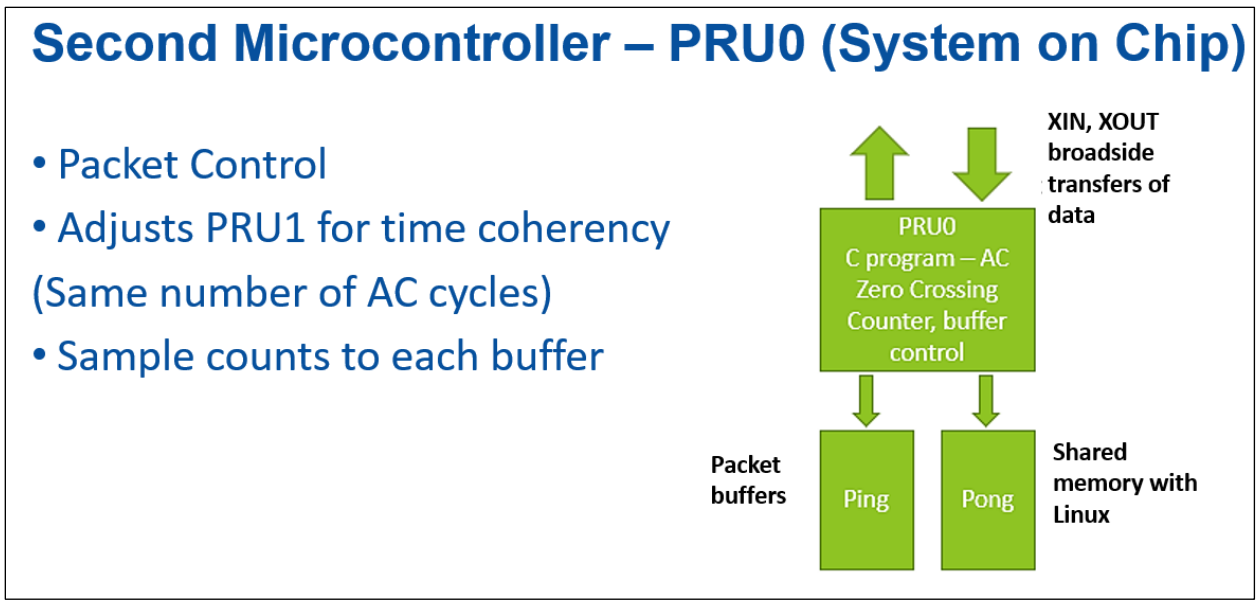

Figure 2: Model of Second Microcontroller

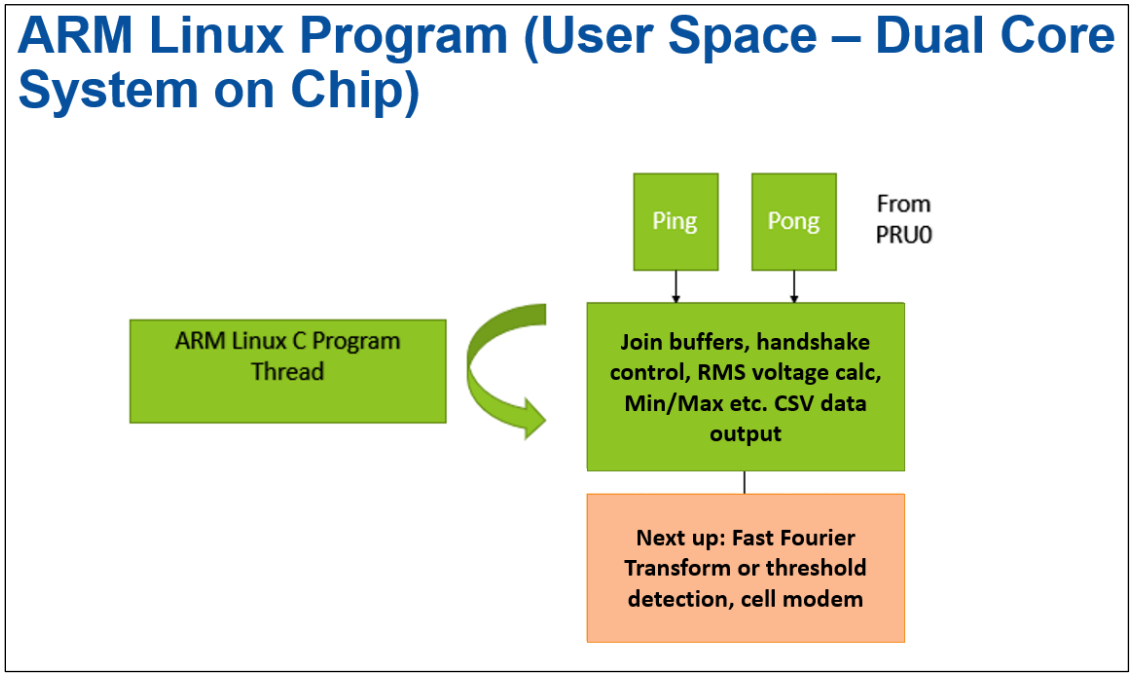

Figure 3: ARM Linux Program