SAND2016-0125R

Emulytics for Cyber-Enabled Physical Attack Scenarios

Interim LDRD Report of Year One Results

December 08, 2015

John Clem, Vincent Urias, William Atkins, and Chris Symonds

ABSTRACT

Sandia National Laboratories has funded the research and development of a new capability to interactively explore the effects of cyber exploits on the performance of physical protection systems. This informal, interim report of progress summarizes the project's basis and year one (of two) accomplishments. It includes descriptions of confirmed cyber exploits against a representative testbed protection system and details the development of an emulytics capability to support live, virtual, and constructive experiments. This work will support stakeholders to better engineer, operate, and maintain reliable protection systems.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2016-0125 R

This page left blank intentionally.

Introduction

This report describes the interim results of research and development (R&D) efforts by a multidisciplinary team investigating the effects of cyber exploits on physical protection systems (PPS). The purpose of the multi-year project is to develop a new modeling and simulation-based capability to support hands-off cybersecurity testing and training for owners and operators of high-consequence PPS. The project enables the confirmation and evaluation of credible cyber threats to the reliability and performance of high-consequence PPS.

Background

The nuclear security community designs and evaluates the performance of physical protection systems using methods that presume the PPS network is isolated, operating as expected, and not itself a target. The National Academies criticized DOE for failing to account for attack scenarios with imaginative elements,[1] and adversaries have compromised critical cyber-based components in similar systems. To date, decision makers lack understanding and quantitative evidence of potential cyber threat impacts on PPS performance, and are not making strategic investments to stay ahead of such emerging threats. Finally, current nuclear security community methods and tools for physical security, such as simulations, do not provide enough fidelity to answer cyber misuse-cases.

Because their activities could be detrimental to the performance of operational PPS, cyber assessment teams that employ adversarial methods (i.e., cyber red teams) are not permitted to connect to, and then explore, test, and evaluate the cyber elements of operational, high-consequence PPS. Sandia National Labs (SNL), however, maintains a real-world PPS testbed that mirrors the general architecture of operational PPS. The testbed is complete with each of the principal *detection, delay, and response* technologies and capabilities found in production PPS. This includes sensors, access control, video surveillance, tampers, alarm communications and display (AC&D), lighting, communications, and many other functional elements. It also includes the PPS network, operator workstations, backend servers, and PPS software used to manage the system. This unique resource, along with SNL's vast experience in the design, engineering and operation of PPS, expertise in cyber threats and vulnerabilities, and knowhow in the development of modeling and simulation is the foundation on which this R&D is built.

High-level R&D Plan

The R&D plan is summarized as a two-part effort:

1. Develop tools and methodology to create high-fidelity models of PPS in an emulation environment. This will enable the development, testing, and assessment of systems in a cost-effective fashion.

[1] Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex, *Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex*, National Research Council, Washington, DC, November 2010.

2. Identify and experimentally execute credible cyber-enabled attacks against elements of a real PPS, and derive design principles that make PPS more robust and resilient against cyber-enabled attacks.

Key Term: Emulytics™

Emulytics is a term coined by SNL that merges the concepts of system emulation with associated analytics. Emulytics blends simulation, virtualized hardware and software, emulated devices, and direct deployment of actual hardware and software to create live-virtual-constructive (i.e., real-emulated-simulated) environments. Emulytics enables rich analyses through scalable infrastructures deployable with great efficiency. The development of an emulytics capability to explore the effects and impacts of cyber interactions for PPS is the end goal of this R&D.

Year One R&D

Summary of Accomplishments

The major accomplishments in year one of this R&D include:

- The testbed PPS network was fully enumerated (mapped by cyber methods);
- Network scans were completed and vulnerabilities discovered;
- A critical protection subsystem was selected for exploitation;
- Cyber exploits against the real-world testbed PPS were developed, successfully tested, recorded, and documented;
- The R&D team successfully concluded an NDA with a global vendor of advanced physical protection systems to enable efficient development of the emulytics framework (team members trained in the vendor's test software);
- Overview briefings were provided to DOE and DoD stakeholders with strong interest in this R&D; and
- The R&D approach and UUR progress to date were presented at the IAEA Conference on Computer Security in a Nuclear World (June 04, 2015).

Year one R&D Focus

The R&D emphasis for year one included two principal elements:

1. Identification and demonstration of a credible cyber-enabled physical attack scenario in the testbed (one that leverages actual vulnerabilities in the PPS testbed and is reasonable to believe would be representative of discoverable scenarios in operational PPS), and
2. Initial research and development of emulytics for PPS. Basic questions driving the emulytics R&D team were:

    - Which PPS elements/components can and cannot be emulated given complexity and other attributes (such as encrypted communications)?

- What communication types are employed in these systems (i.e., serial, Ethernet, fiber, wireless, etc.), and what is their architecture?
- What is the associated tooling needed to allow an automated deployment of emulated components?
- What is the footprint of the real-world system, and what can it be reduced to on an emulytics platform for effective representation?
- Is it possible to develop a fully portable, live-virtual-constructive representation of an actual PPS?
- Can the emulation be sufficiently faithful to allow security researchers to explore attacks and mitigations?

Attack Scenario 1: Hacking the Access Control System from a Remote Bunker

The R&D team's cyber attacker discovered a vulnerable communications box at the testbed remote bunker site. With this discovery, the attacker was able to insert low-cost, off-the-shelf, consumer-grade wireless networking gear into the communications box.[2] Next, the attacker moved well away from the remote bunker site to conduct the actual penetration (using wireless communications), so as not to draw unwanted attention from security personnel. The attacker parked his vehicle approximately one kilometer away from the remote bunker and its now compromised communications box. Next, the attacker connected wirelessly to the gear he inserted at the remote bunker. Once he was connected to his gear in the communications box, he was able to access the PPS network remotely. The attacker discovered the access control server and found it configured with weak administrator credentials, and was able to guess the system administrator login. Additional, straightforward steps were taken using publicly available attack software. The attacker was able to access the system's access control management software used to manage testbed site access authorization. He enrolled a blank access card that can be obtained easily and set a PIN for the card. He gave himself site-wide access privileges. Later, the attacker walked up to the facility and entered the protected area uncontested, using his recently enrolled access credential.

To complete the attack scenario, the cyber attacker used a laptop computer, publicly available no-cost attack software (Metasploit), and less than $400 of additional equipment.[3] It is important to note that no changes to any system configuration were made to facilitate attack success. Finally, vulnerabilities in the PPS architecture and implementation enabled the attacker to easily avoid detection at the remote bunker.

---

[2] The attacker effectively performed a Man-in-the-Middle attack by rerouting the PPS communications from the bunker through his gear and back to the PPS wireless communications tower. In addition, the gear the attacker inserted served as an unauthorized wireless access point to which he could connect, and thus he could then connect to the PPS subnet that serves the remote bunker.

[3] The additional equipment consisted of commercial off-the-shelf (COTS) consumer-grade wireless network router and small switch, fiber to Ethernet adapters, and wireless range-extending antenna.

In summary, the R&D team used an adversarial attack methodology to successfully:

1. Discover testbed PPS vulnerabilities;
2. Leverage vulnerabilities in the PPS architecture and implementation to connect to the PPS network;
3. Exploit weaknesses in the PPS network and backend servers to hack the access control system;
4. Enroll a blank physical access card in the access control database; and then
5. Walk into the protected area undetected, using the attacker's unauthorized credential.

A high-quality video presentation was recorded that documents the main features of the attack scenario and follows the attacker from the beginning of the attack to its completion.

Cyber Exploitation of Central Alarm Station AC&D System

Beyond the completed access control attack, the R&D team also developed a flexible system attack targeting the Central Alarm Station (CAS). If implemented, the attack would enable the attacker to remotely disable the CAS AC&D software or potentially lock out the operators from their consoles for a significant period of time. The developed test code includes a general-purpose system attack against the Windows operating system on which the AC&D software runs. The attack can be delivered in such a way as to cause an extended denial of service causing the CAS to lose the AC&D system for however long it would take for technicians to find and mitigate the problems (attacker access to network, lockout of operators and local administrators, repeated exploitation of vulnerable systems).

Initial Emulytics R&D

Approach

The development of the PPS emulytics leverages existing capabilities to shorten the R&D lifecycle. Figure 1 shows the relationships between the key modeling and simulation software and the emulated system. Dante, a physical security modeling and simulation software tool, is being federated with the new PPS emulytics instantiation. Dante will drive the overall physical security simulation and support system-level analysis of PPS security scenarios that involve cyber exploits. This will enable the quantification of impacts from cyber exploits on PPS performance. In order to bridge the Dante simulation (i.e., mathematical models) to the PPS emulation, SCEPTRE[4], another modeling and simulation framework, will manage system events and effects in the emulation. SCEPTRE integrates the different emulation pieces (hardware in the loop, emulated/simulated sensors, virtualized elements). Both Dante and SCEPTRE were previously developed at SNL under LDRD funding.

[4] SCEPTRE is the name of the modeling and simulation software previously known as VCSE: Virtual Control Systems Environment.

Figure 1: PPS Emulytics software relationships

An important early step in the LDRD was the formation of a partnership with a major vendor of PPS hardware and CAS software. The successful conclusion of a non-disclosure agreement (NDA) enabled the R&D team to acquire proprietary vendor software tools and training.

In order to test the functionality and performance of their software and hardware, the vendor requires a scalable testing environment (one that does not require a large physical infrastructure). Thus the vendor has created software-based tools and models of some of their PPS components. The vendor's developers use these for bug identification, integration testing, and release testing. These activities require reasonably faithful emulators. Fortunately, the vendor's development team shares similar requirements for software fidelity with the emulytics R&D team:

- A scalable system that is hardware-independent;
- The modeled system will respond like the real system;
- Abstraction at an extreme-level of fidelity is not needed for certain components because they are not critical to achieve real world system performance (such as the communications layer between the controller and sensors); and
- A sensor-agnostic implementation (i.e., it does not matter if it is a tamper, microwave, or balanced magnetic switch, rather that the sensor is either tripped or not in the software).

Two members of the R&D team spent several days training at the vendor's headquarters, working with the developers to learn how their system software and hardware are architected. In addition, the vendor supplied the team with proprietary software models useful for laboratory testing and development of the security R&D emulytics system.

Data Collection/Survey

Before the development of the emulytics could begin, it was essential to understand what the emulated system must do, where data flows in the real-world system, and what inputs/outputs are in the real-world system. The R&D team conducted a detailed mapping/survey of the testbed PPS. Two key areas were surveyed:

1. The logical and physical connections of the devices were mapped: how they are interconnected, what communications protocols are used, and the makes/models of the physical components; and
2. The geospatial information of the sensor locations, their fields of view, and the physical distance between the different elements.

The sensor information the R&D team collected is important to support faithful emulation in Dante-driven simulations. It is needed to model physical attacks against the testbed areas protected by its Perimeter Intrusion Detection and Assessment System (PIDAS).

Development

After the site survey and system inventory were complete, and once the R&D team had a solid understanding of the software test platform provided by the vendor, development of the emulytics platform was initiated. Faithful emulation of the components colored red in Figure 2 was achieved. This includes the:

- CAS software hosted on Windows platforms that comprises the infrastructure to monitor and process alarms, set policies, etc.;
- Controller, which collects the sensor and event information and transmits it to the CAS;
- Sensors input tamper sensors, microwave sensors, and badge readers; and
- Communications between the CAS and the controller.

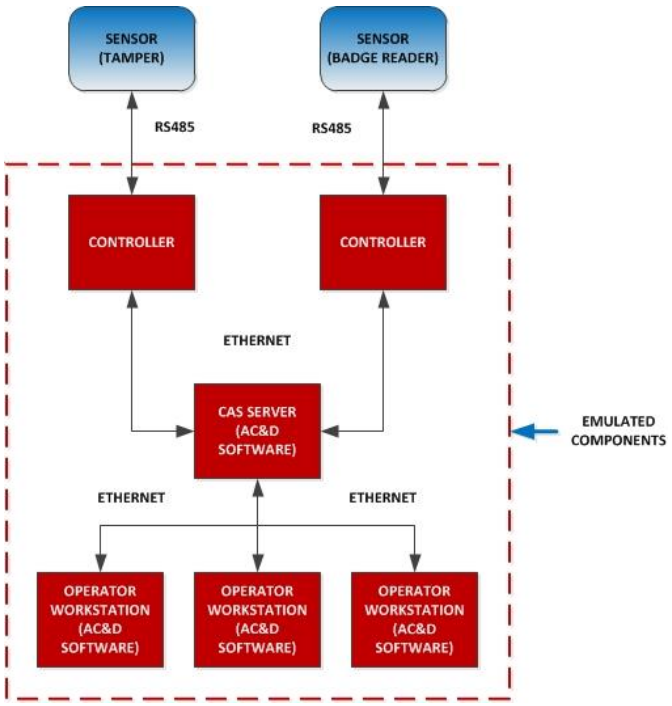

Figure 2: Emulation model

Two key areas were not emulated:

1. Serial communications (RS485) between the sensors and controller, and
2. The actual implementation of every sensor.[5]

Table 1 is an inventory of system elements, including devices, buses and protocols that can be brought into the emulation. These devices can all be provisioned and deployed now with current resources.

Devices, protocols, and buses	Notes/Comments
Controller	Runs on Windows XP Embedded
Bus2 Reader	
Bus2 IO Board	
Bus2 Taut Wire Sensor	
Bus2 Terminal	
Bus1 URI	Universal reader interface
Bus1 HD IO Board	
Bus1 Fence Controller	
Bus1 RAT	Remote arming terminal
Plugin Module	Supports hardware scaling
Reader Type A	For credentials (badges)
Reader Type B	For credentials (badges)
MIFARE Encoder	Wireless proximity chips (badges)
Elevator	(not included in current R&D)
AC&D Module	Part of the AC&D software
Camera Control	
DVR System	Digital Video Recorder
AC&D Software	

Table 1: List of emulatable devices with the vendor's test harness

Creation of the initial emulytics framework (PPS) is largely manual to this point in time. A deep understanding of how to provision the PPS components (implement and configure: badge readers, zones, doors, alarm responses, etc.) is needed to achieve a functional emulation.[6]

The first step to achieve an alpha-grade emulytics package was manual provisioning of CAS and PIDAS systems. That encompassed provisioning the controller, sensor, sensor names, alarms policy, IO boards, Bus1/Bus2, device network addresses, etc.

[5] The vendor's system provides the ability to create events and trip "sensors" on the IO board, but we are unable to implement an exact make and model microwave sensor for example, rather only model the effects of the device tripping or changing voltage.

[6] Naturally, the vendor's AC&D software and test harness do this. One of the year two R&D objectives is to determine the portability of the specification and intermediate representation of PPS data.

After that was built, the emulated system was connected to the AC&D software. However, without additional software, the developer/tester would have to manually connect everything to the controller each time the emulation is instantiated. In order to reduce deployment time and complexity, the development of an IronPython binding to the vendor's software simulator was begun. This software binding will enable the automatic connection and provisioning of logical elements such as MAC addresses, serial IDs, etc. Several other small applications are also in development that, when complete, will result in a turnkey "PIDAS-in-a-box" that automatically starts all of the emulated devices and the AC&D software without requiring any user interaction. Several scenarios have already been developed in order to test the provisioning:

- Simple toy topology with a small number of doors, alarms and sensors;
- Simple toy topology with a badge reader;
- As-is-deployed PIDAS with Bus1; and
- As-is-deployed PIDAS deployed with Bus2.

Figure 3 shows a small, but typical, snippet of the AC&D screen used to support manual configuration of real world PPS elements.

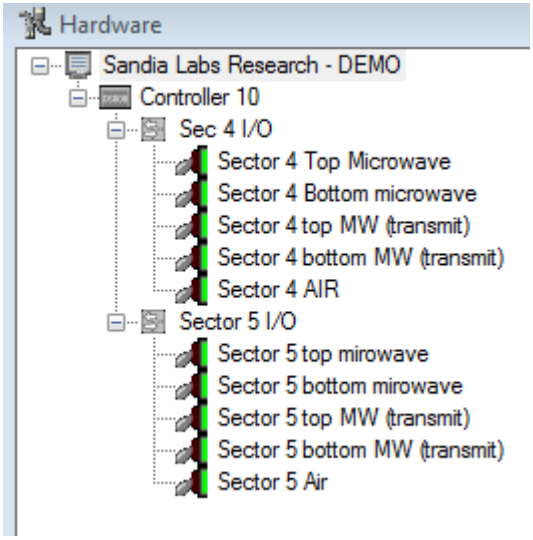

Figure 3: AC&D software configuration screenshot

Besides the software development work described above, a small command-line interface application was developed to allow users to create system stimuli (trip specific sensors, badge-in, badge-out, etc.). This enables the emulytics system to interact with event triggers and support basic testing, alarm verification, and scripted scenarios.

Accomplishments from the Dante portion of the R&D include:

- Integration of a Dante simulation into SCEPTRE to supply data to PPS vendor device models;

- Realization of the ability to run offline simulations of PPS using faithful simulation models without the need to run at the facility;
- Completion of gathering sensor information, such as location, viewing frustum, and specifications, to create an improved Dante model of the real-world testbed; and
- Walk-through of a simple attack scenario that will support validation of the simulated model.

Summary and Year Two Plan

Year One R&D met key milestones, most importantly the:

1. Cyber mapping of the real-world PPS testbed;
2. Identification and demonstration of a credible, repeatable cyber attack against a PPS that highlights modern cyber threats and inherent weaknesses in human-engineered, operated, and maintained systems comprised of COTS components; and
3. Initial development of the emulytics framework, including the reduction of key PPS systems to virtualized instances for use in the emulytics platform.

Multiple briefings were provided to stakeholders from the Departments of Defense and Energy, which generated enthusiastic responses and support for this research. In addition, a technical paper and briefing were authored and accepted for publication/presentation by the International Atomic Energy Agency in its International Conference on Computer Security in a Nuclear World, held in Vienna, Austria, in June, 2015.

The year one creation of a partnership with a global provider of PPS systems supports a stronger, more efficient development of the emulytics capability. Incorporation of Sandia's Dante physical security modeling and simulation software is enabling a more complete emulytics capability for project stakeholders. The use of SCEPTRE represents the modeling and simulation glue to bind together the PPS emulation with the physical security modeling and simulation software.

Year Two Plan

- Q5: Validate system models and the emulation topology for correctness;
- Q5: Demonstrate fidelity of the emulation environment;
- Q6: Conduct vulnerability discovery, modeling, and testing in the emulation environment;
- Q6: Develop and validate exploits by test in both the emulation and real-world environments, compare differences and refine;
- Q6: Demonstrate attacks;

- Q7: Confirm the emulation environment satisfactorily emulates its real-world counterpart, compare existing physical only scenarios to the same scenarios with one or more cyber exploits using current best PPS performance evaluation methods; and
- Q8: Issue the final SAND Report.

Conclusion

Year one R&D has successfully demonstrated the severity of consequences that could arise if an adversary is able to compromise a PPS through cyber exploitation/attack. It is an early confirmation that the concerns the cybersecurity community has raised are valid and need full exploration to ensure that PPS continue to operate robustly. What is not yet known is the breadth of the problem, the prioritization of specific issues that will be discovered, and what solutions will be needed for the future. The work performed under this LDRD represents critical first steps to investigate cyber vulnerabilities in PPS, and develop a novel capability to conduct cybersecurity analyses of PPS. This work will support a needed long-term program to improve the security, and thus reliability, of our nation's and the world's PPS.