Padlock Project

October 22, 2014

Secure Control Systems for the Energy Sector

Funding Number: DE-OE0000538

Project Director:	Rhett Smith, SEL
Principal Investigator:	John Stewart, TVA
Principal Investigator:	Adrian Chavez, SNL
Schedule Status:	Complete
Report Type:	Final Technical Report

Project Team:

Schweitzer Engineering Laboratories, Inc.
Tennessee Valley Authority
Sandia National Laboratories

Executive Summary

The Padlock Project is an alliance between Tennessee Valley Authority (TVA), Sandia National Laboratories (SNL), and Schweitzer Engineering Laboratories Inc. (SEL). SEL is the prime contractor on the Padlock project. Rhett Smith (SEL) is the project director and Adrian Chaves (SNL) and John Stewart (TVA) are principle investigators. SEL is the world's leader in microprocessor-based electronic equipment for protecting electric power systems. The Tennessee Valley Authority, a corporation owned by the U.S. government, provides electricity for 9 million people in parts of seven southeastern states at prices below the national average. TVA, which receives no taxpayer money and makes no profits, also provides flood control, navigation and land management for the Tennessee River system and assists utilities, and state and local governments with economic development.

The Padlock Project addressed *Area of Interest 6: Remote Access*, by protecting the control system stand-alone field devices that are part of an automation control scheme. The Padlock Project built on the firmware platform developed in the Lemnos Project (DOE-Funded Project started in 2007) and developed a commercial solution for an Ethernet Security Gateway with the functionality required to mitigate the threats to a single device out on a pole or in a metal cabinet. The Padlock Project also integrated the results from the Exe-Guard Project (DOE-Funded project started in 2010) for whitelist malware protection. This means the Padlock Project merged the cybersecurity protection of three DOE-funded projects and built the physical tamper sensors to protect distribution automation systems.

As automation and communications expands in the distribution network, cybersecurity needs grow. Many smart grid projects focus on bringing the automation and communications advances from which transmission and generation control systems have benefited to localized installations such as pumps or reclosers. These advances increase reliability, shorten out-of-service times for customers, and bring distributed system awareness to the operators. Security needs in this environment are very different from those transmission or generation entities. The main difference is that this equipment is usually a single device (or low number of devices) located outdoors within a populated area. The risk model points out that physical protection of these devices is the highest priority. This means that a cybersecurity countermeasure needs to focus on identification of physical compromise and then on safeguarding against cyber exploitation propagating beyond the field device that was physically tampered with.

For example, as seen in the picture to the left, a recloser on a pole is only protected by a padlock. Once communications are added to the device, the threat is that if a recloser is physically compromised the perpetrator could use cyber means to expand access back to the substation, or worse, to the control room.

The Padlock Project security gateway was designed to detect physical compromise and alert operators to take action on blocking communications from that device till it can be inspected and brought safely back into service. Building this gateway on the Lemnos project firmware platform

allowed the same interoperable cryptographic communication between central stations and field devices to be established without violating the Electronic Security Perimeter (ESP) requirements of NERC-CIP, which include: strong access control, access logging, and alarming.

Additionally, the Padlock Project gateway serves as a demarcation point between the utility network and the "Smart Meter" network in the case of a smart grid. The "Smart Meters" now can tie into the rest of the substation security model.

The Padlock gateway provides the first line of cybersecurity protection to field devices that are installed separately out in the system and communicate back to a concentration point such as a substation or control center.

The Padlock team researched and developed the SEL-3622, a product based on the SEL-3620 Ethernet Security Gateway developed under the Lemnos Project (DOE-funded project) and combine that with the malware protection technology developed under the Exe-Guard Project (DOE-funded project). The commercialize product details for the SEL-3622 can be found here https://www.selinc.com/SEL-3622/ including datasheets, instruction manuals, delpoyment guides, application notes, and DOE project flyers. The SEL-3622 has already been a huge commercial success with thousands of devices purchased and deployed on power systems all over the world.

The industry requirements gather included:

- Small form factor
- Low power
- 4 serial ports, to support two devices and have two serial ports for each device one for SCADA and one for Engineering Access
- All the logical security in the Lemnos Project Ethernet Security Gateway that is commercialized in the SEL-3620
- Physical security tamper awareness
- Easy to use (configure, update, patch, maintain)
- Low cost
- Interoperable with trust management and cryptographic communications already used at the utility
- Capable of being used in a NERC CIP-compliant way

The Padlock Project was a two phase project, and totaled $1,389,568 with $425,776 provided as cost share in funds over a forty eight month period.

1) Research, develop, and commercialize the SEL-3622 distribution automation security gateway with integrated physical tamper sensor and string cybersecurity for the best situational awareness
2) Laboratory test, field test, and demonstrate the technology in real world control system installations and publish best-practice guides for testing, deployment, and long term management of the technology

Estimated vs. Actual Accomplishments

The Padlock Team established the Statement of Project Objectives and built the research and development plan around accomplishing these tasks on time and on budget. There was two no cost extensions to the project. These were due to two main factors.

1) The industry requested that SEL commercially release the SEL-3622 faster than originally scheduled. This was accomplished by breaking the SEL-3622 commercial release into three releases, this reduced the overall scope of each release accelerating the first release but did cost the project team more work due to the need to test the product three times, once on each release, rather than just once at the end of the full scope for the Padlock project. This is a positive response and allowed the technology to be integrated into the US power system over a year earlier than originally planned. It also spotlighted the industry need for such cybersecurity technology and allowed the Padlock team to get a much broader and more accurate feedback from end user testing and deployment much earlier in the project reducing risk.

2) The second contributor was the industry request to integrate the Exe-Guard whitelist malware protection technology into the Padlock project product, the SEL-3622. Originally this was not planned because the Padlock Project and the Exe-Guard project were parallel projects and the Exe-Guard technology was not going to be completed but with the extension of breaking the overall project into three smaller sections allowed the team to pull this into scope. It is great to see the DOE-funded projects merging for the overall system cybersecurity solution.

The SOPO is listed below with results under each task. The Padlock team accomplished all tasks successfully and the result of the Padlock project is a commercial technology that has already be integrated into many power systems across the world.

TASKS TO BE PERFORMED

Task 1.0: Project Management & Planning: The recipient will revise the version of the Project Management Plan that was submitted with the application by including details from the negotiation process. The Project Management Plan will be updated as the project progresses and the recipient will use this plan to report schedule and budget variances.

Results 1.0: The team developed a project management plan that focused on the R&D completion of the advanced cybersecurity technology and was tracked, updated and followed throughout the project. This PMP was used to track the accomplishments and status of the project on every quarterly report.

Task 2.0: The recipient will complete the research into the field device network communication needs and develop all possible use cases for the Padlock technology. These use cases are the ways that the energy sector will deploy and use the technology, which will drive the specifications of the product.

Results 2.0: The Padlock team developed these use cases starting with an interview of the TVA power system engineers and then SEL was able to host similar interviews with eight other major utilities across the USA. This allowed the team to have solid use cases for distribution automation projects and resulted in the industry requesting a faster commercialization plan so they could use the product in their current projects.

2.1: The recipient will identify communication performance needs by collecting the control system communication requirements and overlay use cases (see task 2.4) to provide worse-case burden.

Results from 2.1: The Padlock team discovered the need for four serial ports and three Ethernet ports for this product. Typical installations could have two IEDs and they want SCADA and engineering access for both resulting in four serial ports. Then on the Ethernet side the installations wanted a bridged Ethernet side for the ring topology for reliability and a third Ethernet port for local access.

2.2: The recipient will complete hardware requirements specifications.

Results from 2.2: The team developed the hardware to comply to IEEE 1613 environmental requirements same as protection relays.

2.3: The recipient will verify open source technology, leveraged from the Lemnos project, is able to handle the worst case burden based on selected hardware requirements.

Results from 2.3: The Padlock team started with the Lemnos firmware foundation

2.4: The recipient will author all uses cases that fulfill a utility partner's technical and business objectives for a managed switch and the security requirements for protecting the remote field devices.

Results from 2.4: Accomplished and proven with end user validation testing and deployment. The SEL-3622 has been in service in some locations for over a year and successfully completing the business requirements desired.

2.5: The recipient will author the technical specifications for the hardware and software

Results from 2.5: Completed and tested to during unit tes, functional test, and validation testing.

2.6: The recipient will complete the top level system requirements specification that combines the use cases and technical requirements. This document will lead the development of all software and hardware designs.

Results from 2.6: This was completed and circulated to the project team for confirmation. This is the top level spec that drive functional scope. This was successful due to the commercial success of the product.

2.7: The recipient will design user interface control system environment

Results from 2.7: This was successful and takes very little technical training to understand the settings. The physical tamper sensors have "High" "Mid" and "Low" settings for sensitivity keeping them simple to use and understand.

Task 3.0: The recipient will develop the commercial distribution automation security gateway.

Results from 3.0: This is completed and the product released as the SEL-3622 and all the sales and customer service backing of SEL including the 10 year warranty. Details can be found at www.selinc.com/sel-3622

3.1: Perform hardware prototype 1 and environmental testing.

Results from 3.1: Completed and hardware changed discovered then sent to prototype two

3.2: Perform hardware prototype 2 and environmental testing.

Results from 3.2: Completed and no need for prototype three

3.3: Perform hardware prototype 3 and environmental testing.

Results from 3.3: Not needed so not performed

3.4: Complete remaining firmware, hardware, and software development activities.

Results from 3.4: Completed and commercially released

Task 4.0: The recipient will complete robust laboratory testing that model the live system with a utility partner and demonstrate the commercial product in real world control system installations and prepare best-practice guides for testing, deployment, and long term management of the technology

Results from 4.0: SEL established a validation test bed that modeled a substation and a utility cabinet on a pole mount and tested all cybersecurity and physical tamper sensors successfully. See picture of pole mount testing below.

4.1: The recipient will perform laboratory testing with a utility partner

Results from 4.1: SEL was able to perform end user testing with many utilities due to the commercial success for the product. There were many utilities that wanted to integrate this product into existing projects and testing started as soon as the commercial release happened. With the tiered release this end user testing happened multiple times as the new features were released and firmware upgrades could be done. All were successful.

4.2: The recipient will perform field testing with a utility and national laboratory partners

Results from 4.2: Same results as 4.1 with success and many SEL-3622 are in service protecting our power systems today.

4.3: The recipient will perform security robustness testing led by a partnering national laboratory

Results from 4.3: Sandia performed this twice and the first time the results were addressed and integrated into the next release. The second test didn't yield any findings to warrant changes concluding the product security profile is solid.

Task 5.0: Best Practices Guide. Once field test is complete, all participating organizations will contribute to a best-practices guide and draft best-practice guide explaining how to test, deploy, and manage the technology for the long term.

Results from 5.0: SEL published many materials on the SEL-3622 detailing specifications, training, testing, and deployment practices. These can all be publically found on the product page listed above.

DELIVERABLES

Reports and other deliverables will be provided in accordance with the Federal Assistance Reporting Checklist following the instructions included therein.

In addition, the following deliverables are required to be submitted and shall be developed in accordance with written instructions provided by the DOE Project Officer.

Project Management Plan (PMP) Update – Due 30 days after award and resubmitted as necessary throughout the Performance Period.

Briefing/Presentation Materials - A copy of all briefing/presentation materials shall be provided prior to the event date.

Topical Reports – Due within 30 days after the completion of appropriate task

1. Topical report on open source code/technology.

2. Topical report on system functionality and specifications

3. Topical report on commercial product development and release

4. Topical report on the test plan

5. Topical report on test results

Results from all deliverables: All deliverables were authored and submitted to DOE. These deliverable reports helped the project team stay focused and on task. Below is a list of milestones for the project and their planned vs completion dates.

Milestone Description	Planned Completion	Actual Completion
Project Start Date	12/2010	12/2010
Complete revision of the project management plan.	*1/2011*	1/2011
Identify communication performance needs	5/2011	3/2011
Biannual Review #1	*6/2011*	6/2011
Complete review of Lemnos open source technologies	7/2011	6/2011

Milestone Description	Planned Completion	Actual Completion
Topical report on open source technology to be employed on the product.	8/2011	8/2011
Complete authorship of use cases that fulfill TVA's technical and business objectives.	10/2011	10/2011
Complete hardware and software technical specifications	10/2011	10/2011
Biannual Review #2	*12/2011*	12/2011
Provide Topical report on system functionality and specifications describing the commercial product and its use on the system level.	12/2011	12/2011
Complete the design of the user interface of the commercial product.	2/2012	2/2012
Gate 1 Exit - Go/No-Go Decision Point	**2/2012**	2/2012
Biannual Review #3	*6/2012*	6/2012
Hardware prototype 1 and environmental testing complete.	7/2012	7/2012
Interim release available for early industry deployment	11/2012	10/2012
Biannual Review #4	*12/2012*	1/2013
Firmware drivers for physical security tamper detection and 3rd Ethernet port written	5/2013	5/2013
Biannual Review #5	6/2013	6/2013
Firmware initial product code complete and unit tested	8/2013	8/2013
Biannual Review #6	12/2013	12/2013
Complete the development and release of the commercial product.	2/2014	6/2014
Gate 2 Exit - Go/No-Go Decision Point	**2/2014**	6/2014
Topical report on the commercial product development and release	3/2014	7/2014
Topical report on the test plan detailing tests to be run at TVA's facilities.	3/2014	7/2014
Biannual Review #7	*6/2014*	8/2014 Peer Review
Complete prototype lab testing at TVA to make sure the team is on track to accomplish the technical and business requirements.	6/2014	9/2014

Milestone Description	Planned Completion	Actual Completion
Completed execution of field demonstration of the commercial product at TVA.	7/2014	9/2014
Topical report on test results	7/2014	9/2014
Complete security robustness testing at Sandia National Labs	7/2014	10/2014
Gate 3 Exit - Go/No-Go Decision	**8/2014**	10/2014
Complete authorship of best practice guide explaining how to test, deploy, and manage the technology long term.	9/2014	7/2014
Project Closeout Review	*9/2014*	10/2014

Summarization of Project Activities

The Alliance team built on the solid relationship of the PIs that started under the Lemnos project and developed the Padlock project. The product development life cycle procedures of SEL guided the R&D, the technology deployment experience of TVA guided the functional scope and the negative testing experience of Sandia guided the security robustness. The assumptions were that merging the physical awareness into the cybersecurity infrastructure would be desirable and beneficial for the industry. This quickly became true when utilities requested a fast commercialization of the SEL-3622 to integrate into current projects. No major adjustments happened throughout the project and the top level spec once authored did not get revised. The idea, plan and execution of the Padlock project were all solid and accomplished their goals. The budget was accurate and the only major adjustment that was made was the schedule and the reasons for that are described above.

Publications, Technology, and Patents

No patents were filed.

Technology was commercially released in the SEL-3622.

The project team published many documents including datasheets, instruction manuals, and application notes on the specifications and how to use the technology commercially released in the SEL-3622 and can all be found at https://www.selinc.com/sel-3622/

Conclusion

The Padlock team has completed all tasks for Phase 1 and Phase 2. The team stayed on budget. The schedule did get pushed out twice with no cost extensions. These were due to two main factors.

3) The industry requested that SEL commercially release the SEL-3622 faster than originally scheduled. This was accomplished by breaking the SEL-3622 commercial release into three releases, this reduced the overall scope of each release accelerating the first release but did cost the project team more work due to the need to test the product three times, once on each release, rather than just once at the end of the full scope for the Padlock project. This is a positive response and allowed the technology to be integrated into the US power system over a year earlier than originally planned. It also spotlighted the industry need for such cybersecurity technology and allowed the Padlock team to get a much broader and more accurate feedback from end user testing and deployment much earlier in the project reducing risk.

4) The second contributor was the industry request to integrate the Exe-Guard whitelist malware protection technology into the Padlock project product, the SEL-3622. Originally this was not planned because the Padlock Project and the Exe-Guard

project were parallel projects and the Exe-Guard technology was not going to be completed but with the extension of breaking the overall project into three smaller sections allowed the team to pull this into scope. It is great to see the DOE-funded projects merging for the overall system cybersecurity solution.

Overall the best measure of success for this project is the success of the commercialization. The power industry has voted with their wallet that they approve of this project results and is buying the technology that resulted from it. Bottom line is the power systems are safer today because of this project and its results and helps the industry get one big step closer to provide resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functionality.