Appendix B
SEEDS Project Proposal
Award Year 3

Executive Summary

Current Project 1.7 – Detecting Compromised Devices in the Smart Grid – FIU Uluagac

The smart grid vision depends on the secure and reliable two-way communications between smart devices (e.g., EDs, PLCs, PMUs). Nonetheless, compromised smart grid devices constitute a serious threat to healthy and secure distribution of data in the grid. Consequences of propagating fake data or stealing sensitive smart grid state information via compromised devices are costly. Hence, early detection of compromised smart grid devices is critical for protecting the smart grid's components and data.

To address these concerns, in this project, we aim to design and implement a system-level configurable framework capable of monitoring and detecting compromised smart grid devices. Specifically, our framework aims to combine system call tracing (i.e., ptrace, library interposition) and statistical and machine learning techniques (basic and advanced) to monitor and detect compromised device behavior.

In Year 1, the project team have successfully built a representative small smart grid testbed environment to evaluate the security challenges associated with compromised devices. The testbed performs essential operations conforming to the IEC 61850 protocol suite, which defines the communication standards for electrical substation automation systems. The testbed includes both resource-limited (e.g., Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs)) and resource-rich (e.g., Phasor Measurement Units (PMUs), Intelligent Electronic Devices (IEDs)) devices. Moreover, the devices in the testbed use open source libiec61850 libraries to exchange smart grid time-critical device messages using the GOOSE messaging format. As part of the evaluation process, we identified six different types of compromised devices with different computing resources and hardware capabilities. This adversary model also complies with the security requirements defined by the US National Institute of Standards and Technology (NIST) for the smart grid. Finally, we built effective algorithms in our framework to detect the different compromised devices. We also evaluated the performance of our framework using the testbed against these adversaries. Our initial experimental results demonstrated an excellent detection rate for the compromised smart grid devices.

The project has also been well-received by the scientific community, yielding fruitful results. It has successfully generated 2 patent filings, 2 Journal articles (under review), 1 Conference paper, 1 poster, 2 live demo, 2 industry talks. Of these, the PhD Student working on the project, Leonardo Babun, received two best demo awards in two different events in January and March 2017. Our technique, methods, and software tools being developed for this project are very unique and can directly be utilized in the industry. Given the initial progress, we are confident that the project will benefit the needs of the industry. Moreover, this project module has direct impact on four (Thrusts 1, 2, 3, and 4) of the thrusts of the SEEDS Center. The success of this module will be one of important pillars of the SEEDS Center’s collective effort not only to secure delivery of the energy system’s data, but also defend against malicious players.

In Year 3 and beyond, the project team aims to continue to work on improving the framework by analyzing the efficacy of other detection algorithms such as machine learning and automating the process of the framework. More importantly, in Year 3, the project team aims to test the developed tools and algorithms in real industry settings, if possible, as part of the alpha and beta testing steps. While working on improving the framework, the project team will also diligently work on identifying an industry partner, who would be interested in trying the developed solutions in this project.
Appendix B
SEEDS Project Proposal
Award Year 3

Project Details

1. Project Description and Objectives

The success of the smart grid depends on the integration of electrical distribution systems with communication networks. Because of the critical role of the smart grid communication devices, the use of untrusted compromised devices could negatively impact the smart grid performance. Such devices can also bring catastrophic consequences for the integrity of the power grid data. In this project, the project team focuses on how to monitor and detect compromised devices in the smart grid architecture.

To achieve the goals of the project, the PI and his team aim to build a configurable framework that is capable of detecting compromised devices which are performing unauthorized operations inside the critical parts of the smart grid architecture such as leaking information, poisoning measurements, or storing-and-sending valuable power status information to unauthorized entities. Specifically, the proposed framework effectively utilizes system call tracing, library interposition, and statistical and machine learning techniques to monitor and detect compromised devices’ behavior. In order to test our proposed framework, we implement a realistic smart grid scenario which performs essential operations under IEC 61850 protocol [1]. The proposed testbed includes both resource-limited (e.g., Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs)) and resource-rich (e.g., Phasor Measurement Units (PMUs), Intelligent Electronic Devices (IEDs)) devices that follow the GOOSE publisher-subscriber configuration using open source libiec61850 libraries [2].

2. Background and Evaluation of State of the Art

Security testbeds for the smart grid: There are some interesting works focused on the development of security testbeds for the smart grid. In [3], the authors present an overview of a generic smart grid security testbed. They also include the set of control, communication, and physical system components required for accurate cyber-physical environment. In [4] PowerCyber, a remote-accessed and experimental smart grid testbed, is presented. In both cases, the testbed implementations are useful, but are different from our work since they both focused on system functionality rather than the behavior of individual smart grid devices. A more comprehensive survey of smart grid testbeds can be found in [25].

Smart grid compromised device detection: In general, the topic of compromised devices has not been extensively studied in the literature. In most cases, researches focus on proposing anomaly detection mechanisms [5] for different types of attacks in the smart grid [6]–[9] without focusing on the attack sources (e.g., compromised devices). In few cases, however, the behavior of the smart grid device is considered. In [10], the authors study the minimal number of compromised sensors in order to manipulate a given number of smart grid states. Intelligent secure packaging, outbound beaconing, and better tracking systems are some of the countermeasures that are being proposed to fight against compromised devices in the supply chain [11], [12]–[14]. However, skilled attackers could have remote access to legitimate devices (e.g., RTUs, PMUs, IEDs, etc.) and create opportunities for tampering smart grid devices outside the smart grid supply chain. And, our proposed work is focused on the possible compromised devices inside the smart grid architecture.

Function and system call tracing techniques for security applications: Since function and system call tracing techniques constitute a powerful method for regulating and monitoring applications behavior [15], they have been largely used in security applications [16]. Specifically, we can find system call tracing techniques in applications like intrusion detection and confinement [17], binary detection of OS functions [18], sandboxing [19], and software portable packages [20]. Specifically in [21], authors use system calls tracing for implementing intrusion detection systems (IDS). Also, in [22] and [23], the authors proposed anomaly detection mechanism based on information obtained from analyzing system calls behavior. In these cases, the implementation of the monitoring tools resulted in too heavy in terms of system overhead. One similar application with improved system overhead can be found in [24]. However, in [24], the tool
is required to run continuously and serves the purpose of complementing antivirus software. Our work is also different from these approaches as it is lightweight and resource-utilization aware in its design.

3. Proposed Novel Approach

Our framework is different from other discussed solutions which, in most cases, focus on specific threats to the smart grid instead of considering different types of threats (e.g., poisoning real smart grid data, stealing information from the smart grid, etc.) acting on different types of devices (resource-rich and resource-limited). There are cases where different approaches are being used for the detection of compromised devices and/or monitoring application behavior, however, only in few of these cases the solutions are intended to be applied in the smart grid domain. And, in order to succeed, these solutions need to be monitoring constantly-changing environments like network traffic or computational systems. This constitutes a limitation in terms of system overhead and resource utilization. On the other hand, our framework has a simpler model and is lightweight in terms of system overhead while designed to provide excellent detection rate of the compromised smart grid devices. Finally, our work can also complement the existing security mechanisms in the smart grid domain with its open-source and configurable nature. Moreover, the open-source nature of our work makes it an appealing choice for interested industry partners.

4. What will the testing plan be for this project?

In Year 3, the project team aims to test the developed tools and algorithms in real industry settings, if possible, as part of the alpha and beta testing steps. While working on improving the framework, the project team will also diligently work on identifying an industry partner, who would be interested in trying the developed solutions in this project. Since the core concepts have already been developed so far and two patents are filed, the project team will be aggressive in finding a suitable partner for the tools and the solutions will be appealing to the industry. Also, in Year 3 and beyond, the project team aims to continue to work on improving the framework by analyzing the efficacy of other detection algorithms such as machine learning and automating the process of the framework.

5. How does this project address the SEEDS Needs Document and what unique tool or direct solution does this research provide to current industry cybersecurity and grid resiliency needs?

a. Addressing SEEDS Center Needs:

The SEEDS Center has five important industry-identified research thrusts: Thrust 1: Cybersecurity Data Analytics and Visualization. Thrust 2: Detection and Response. Thrust 3: Protection and Security Management Thrust 4: Cybersecurity State Assessment of Common Industry Configurations. Thrust 5: Power electronic control system security. This project module has direct impact on four (Thrusts 1, 2, 3, and 4) of the thrusts. Specifically, the success of the project will contribute to the following needs of the SEEDS Center: 1a: Real-time situation awareness and data analytics to detect abnormal events and malicious activities. 2c: Early threat and lateral threat movement detection. 3b: Mitigation and recovery of smart grid equipment hacks. 3e: Cybersecurity for Transient Cyber Assets. 3h: Secure communication protocols for power system components, services and devices. 4c: Secure the legacy Energy Systems. Because smart grid devices may be compromised through corrupted software components and communicate malicious data, leak sensitive information, corrupt memory, the success of this project will be one of important pillars of the SEEDS Center’s collective effort not only to secure delivery of the energy system’s data, but also defend against malicious players. Moreover, “Develop and Implement New Protective Measures to Reduce Risk” is one of the five key strategies suggested by the Energy Sector’s 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity document. The software tools and algorithms that are being developed with this project is in perfect alignment with the Energy Sector’s roadmap and its scope from prevention and detection perspectives.
b. Potential Impact on Industry:
The main objective of this project is the design and implementation of a system-level framework capable of detecting smart grid compromised devices based on the device behavior. There are some direct benefits from this project to the industry:

- **Excellent detection rate:** our framework is very promising for the detection of compromised smart grid devices with excellent results.
- **Minimum overhead:** based on the experimental results, our framework does not represent significant overhead on the use of computing resources.
- **Specific vs. generic solution:** the proposed framework is designed to address the specific problem of compromised smart grid device detection. However, the approaches used for the compromised smart grid detection are perfectly suitable for other security domains outside the smart grid and they can be used in several different scenarios of other industrial control systems.
- **Comprehensive adversary model:** the adversary model used in our project includes resource-limited and resource-rich compromised devices and three different threats for the smart grid. In total, we consider a very comprehensive adversary model with six different types of compromised smart grid devices.
- **Compromised device diversity:** Our framework is suitable for any type of compromised device. The design of our system level framework makes it also suitable for detecting compromised hardware. System/function call comparison and statistical correlation and machine learning are powerful tools capable of detecting changes in hardware and system configurations. This makes our framework a really appealing solution for monitoring and detecting any type of compromised devices for the needs of the industry.

6. Risks to Project Success

In alpha and beta testing phases of this project in Year 3, we would like to test the developed algorithms on real devices. Having access to real devices in industry and the SEED Center’s labs and understanding their software architecture will help us enormously for further success of the project.

7. Milestones and Deliverables for Mid-Project (Y1) and End of Project (Y2) and Year 3

So far, the project team evaluated the risks associated with compromised devices in Y1 and designed the basic structure of the compromised device detection framework. As listed on Products Section of this document (Page 9), our work successfully generated 2 patent filings, 2 Journal articles (under review), 1 Conference paper, 1 poster, 2 live demos, 2 industry talks. Of these, the work received two best demo awards in two different events recently. Our technique, methods, and software tools developed for this project are unique and can directly be utilized in the industry. The project team plans to work closely with the SEEDS Center management team to identify a company who might be interested in adopting the project into their products. The following milestones and deliverables are planned for the project:

- **Year 1 Q4:** W3.1.7-M1: Assessment of compromised devices on power grid communications. **Status:** Completed.
- **Year 2 Q6:** W3.1.7-M2: Development of software tool and framework to detect compromised devices and analyze of the efficacy of the framework. **Status:** In progress.
- **Year 2 Q8:** W3.1.7-M3: Development of other detection algorithms such as machine learning and analyzing their efficacy. **Status:** In progress.
- **Year 3 Q9:** W3.1.7-M4: Development of software tool to automate the process of the framework in the detection of the compromised devices. **Status:** In progress.
- **Year 3 Q11:** W3.1.7-M5: Alpha testing **Status:** To be completed.
- **Year 3 Q12:** W3.1.7-M6: Beta testing **Status:** To be completed.
Appendix B
SEEDS Project Proposal
Award Year 3

8. References

Appendix B
SEEDS Project Proposal
Award Year 3


Relevant Data and Metrics for Project

A. Personnel

<table>
<thead>
<tr>
<th>Demographics</th>
<th>University</th>
<th>Title/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Leader</td>
<td>Dr. A. Selcuk Uluagac</td>
<td>Florida International University</td>
</tr>
<tr>
<td>Postdoctoral Scholar</td>
<td>Dr. Hidayet Aksu</td>
<td>Florida International University</td>
</tr>
<tr>
<td>Graduate Students</td>
<td>Leonardo Babun</td>
<td>Florida International University</td>
</tr>
<tr>
<td>Undergraduate Students</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

6
### B. Products (Note: included only those that explicitly acknowledge DOE support)

| Patents filed/granted | 1. A Method for Identification and Detection of Counterfeit or Compromised Resource-Limited Devices using Correlation and System/Function Call Tracing Techniques. Submitted to Florida International University. October 2016. (Currently, the PI and the patent attorneys are working on the revisions).  
### Salaries and Wages

<table>
<thead>
<tr>
<th></th>
<th># of mo/yr</th>
<th>Annual or Summer?</th>
<th>Monthly Rate</th>
<th>Fringe Rate (%)</th>
<th>Grant Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lead Investigator:</strong></td>
<td>1</td>
<td>Summer</td>
<td>$10,876.87</td>
<td>33.22%</td>
<td>Salary $10,876.87</td>
</tr>
<tr>
<td>Name: Selcuk Uluagac</td>
<td></td>
<td></td>
<td>Fringes $3,613.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Co-PI:</strong></td>
<td></td>
<td></td>
<td>Salary $-</td>
<td>Fringes $-</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td>Fringes $-</td>
<td>Fringes $-</td>
<td></td>
</tr>
<tr>
<td><strong>Co-PI:</strong></td>
<td></td>
<td></td>
<td>Salary $-</td>
<td>Fringes $-</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td>Fringes $-</td>
<td>Fringes $-</td>
<td></td>
</tr>
<tr>
<td><strong>Co-PI:</strong></td>
<td></td>
<td></td>
<td>Salary $-</td>
<td>Fringes $-</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td>Fringes $-</td>
<td>Fringes $-</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th># of students</th>
<th># of mo/yr</th>
<th>Monthly Rate</th>
<th>Fringe Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graduate Assistant (Ph.D.)</td>
<td>1</td>
<td>12</td>
<td>$2,056</td>
<td>5.82%</td>
</tr>
<tr>
<td>Name:</td>
<td>Fringes $24,676.92</td>
<td>Fringes $1,436.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graduate Assistant (MS)</td>
<td></td>
<td></td>
<td>Salary $-</td>
<td>Fringes $-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th># of employees</th>
<th># of hours/yr</th>
<th>Hourly Wage Rate</th>
<th>Fringe Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly, non-student(s)</td>
<td></td>
<td></td>
<td>Salary $-</td>
<td>Fringes $-</td>
</tr>
<tr>
<td>Hourly, enrolled student</td>
<td></td>
<td></td>
<td>Salary $-</td>
<td>Fringes $-</td>
</tr>
</tbody>
</table>

**Subtotal Salaries**: $35,553.79  
**Subtotal Fringes**: $5,049.49

### Direct Costs:

- **Domestic Travel**: $4,000.00  
- **Foreign Travel**: $2,000.00  
- **Materials and Supplies**: $6,000.00  
- **Services (Consultant/Computer/etc.)**: $-  
- **Facility Usage Fees**: $-  
- **Equipment (Capital Expenses greater than $2500)**: $-  

**Subtotal Direct Costs**: $12,000.00

### Participant Costs:

- **Graduate Assistant Tuition (waiver or payment)**: $9,574.74  
- **Participant Stipend (for example, for an REU student)**: $-  
- **Participant Support (only to support students in Stipend category)**: $-  

**Subtotal Participant Costs**: $9,574.74

**Total Project Direct Cost**: $62,178.02  

<table>
<thead>
<tr>
<th></th>
<th>Rate (%)</th>
<th>Base ($)</th>
<th></th>
<th>Grant Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indirect Costs</td>
<td>46.50%</td>
<td>$52,603.28</td>
<td></td>
<td>$24,460.53</td>
</tr>
<tr>
<td>Unrecovered Indirects</td>
<td>$-</td>
<td>$-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Project Costs**: $86,638.55