OPTIGUARD:
A SMART METER ASSESSMENT TOOLKIT

July 14, 2012

Presented by:

INGUARDIANS, INC.

Don C. Weber, Senior Security Analyst
don@inguardians.com

White Paper

TABLE OF CONTENTS

1.0 ROLE OF SMART METERS

The meter portion of the electrical grids throughout the world is swiftly being converted to Smart Meters. The news is littered with public disclosures of smart meter sales and implementations.[1] Smart Meters, one of the primary components of a utility's Advanced Metering Infrastructure (AMI), play an important role to improving the stability, efficiency, and reliability of the new, smarter electrical grid. Smart Meters accomplish this by providing utilities with accurate, real-time and historical, consumption data. Smart Meters also put in place mechanisms to manage the stability of the grid. They do this by controlling demand with the assistance of their customers. In a world where the demand for electricity is rapidly increasing,[2] the Smart Meter offers one method to provide better management and ensure peak load reductions.[3]

As with all new technologies, Smart Meters are still being evaluated for security risks. For years utilities have been heavily dependent on the stability and resilience of the hardware that comprises their infrastructure. It is not unheard of for electrical equipment to have a forty-year-plus lifespan[4] with twenty years being the "rule-of-thumb" industry standard to even be considered for deployment – the first round of Smart Meters was built with this stability in mind. The hardware engineers focused on reliability issues rather than the impact these design considerations would have on the whole of the AMI implementation.

If Smart Meters only measured and stored data more accurately, security might not be such a concern. However, remote data collection, monitoring, configuration, and troubleshooting goals lead to Smart Meters which include two-way communications. Inclusion of these communication features lead to the installation of components and information that can be abused. The components added to Smart Meters include microcontrollers, data storage, and radios. Outfitting Smart Meters with these capabilities also provides a direct connection from publicly accessible devices to the internal components of the AMI deployment. As the capabilities and access to additional resources and data increased, so has the risk that amateur hardware enthusiasts and criminals will become interested in these devices. Thus, the race to secure Smart Meters from unauthorized manipulation of the hardware and communications has begun.

[1] Conduct an Internet Search for "smart meter deployment 2012"
[2] http://energybulletin.net/stories/2012-03-16/world-energy-consumption-1820-charts
[3] http://energy.gov/node/263269
[4] http://www.transformerlife.com.au/transformer-breakdown.php

2.0 RISK PRESENTED BY THE OPTICAL PORT

The purpose of the optical port on a Smart Meter is to provide a utility's field technicians with a method to directly manage individual meters. This capability is necessary numerous reasons, all of which relate to the need for a utility to achieve its primary goal: reliability. Optical ports provide an easy, tested, and safe method for field technicians to interact with these electrified components during a wide variety of field conditions (i.e. extreme heat/cold, high winds, torrential rains).

To successfully interact with a Smart Meter's optical port, attackers and security researchers must gain access to the maintenance software provided by the meter's vendor or develop specialized software. In either case, successful interaction with a Smart Meter will first require authentication credentials. Smart meters are complicated devices that contain several different components where authentication information can potentially be extracted. Microcontroller firmware, memory components, and the interactions between those components all contain information necessary for communicating to and from the meter. This information includes the authentication credentials necessary for interacting with the meter's optical port.

On January 5, 2009 InGuardians, as a member of the AMI Security Acceleration Project Red Team released the AMI Attack Methodology. This methodology, updated to version two (2) on March 1, 2011, outlined several methods that attackers and security researchers will use to extract information from the hardware components installed in Smart Meters and other embedded devices. The material outlined in this methodology was not new information. This white paper merely consolidated the knowledge involved with analyzing embedded devices and their supporting components.

Valuable data can frequently be extracted from Smart Meters by simply following the steps outlined in the AMI Attack Methodology. The following images are examples of data being extracted from Smart Meter components. Figure 1 demonstrates the method commonly used in order to extract memory from Inter-Integrated Circuit (I^2C) EEPROM components. Figure 2 demonstrates a method commonly used for extracting memory from NAND Flash and other Ball Grid Array (BGA) components.

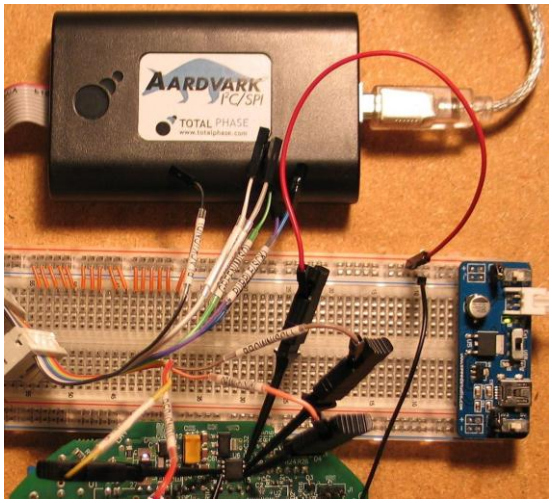

Figure 1Extracting EEPROM Data Using Total Phase Aardvark

Figure 2 Extracting NAND Flash Data using a XELTEK SuperPro 5000

Dumping dumped from these memory components and understanding where the significant information is located are two completely separate issues. Having a prior knowledge of where the data (i.e. security codes and encryption keys) is located can help. This requires initially locating data to use for comparison. Several methods for generating long lists of possible security codes and encryption keys may help in locating this sensitive information. However, this method requires brute force authentication actions to positively identify useful data. These actions can (and should) be detected by proper logging methods.

Other methods, such as component-to-component bus monitoring can be used to detect security codes and encryption keys while they are being used by the Smart Meter. Monitoring communications between components can significantly narrow down the time required to identify this information. Figure 3 is an example of a Smart Meter that has been tapped to detect the signals passing between components. This setup also provides a means for sending signals to individual components in order to elicit responses or respond to requests by the tapped components.

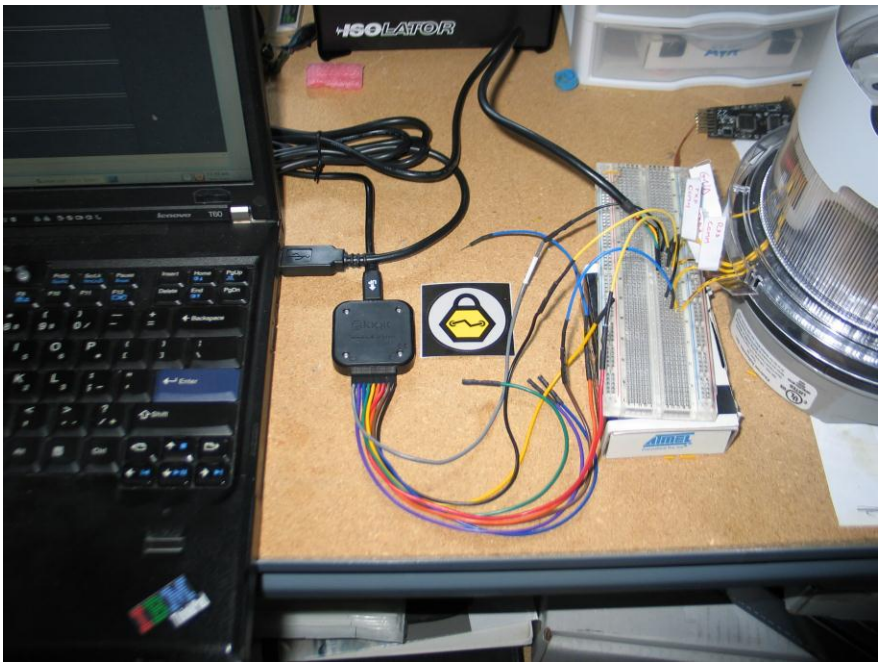

Figure 3 Bus Sniffing and Man-In-The-Middle Attack

In the case that authentication credentials or encryption keys cannot be obtained using hardware extraction methods, an attacker can fall back to time-consuming brute-force methods. If generated properly, security codes implemented by Smart Meters will make straight brute forcing nearly impossible due to the enormous time required to iterate through all of the possible combinations of the twenty byte security code. However, security code dictionaries can be generated with common vendor names, utility names, and the vendor's default Smart Meter passwords to narrow the field of possibilities.

Once a Smart Meter's security code has been identified, communicating with the meter via the Optical Port requires only having the proper software and equipment. Every Smart Meter vendor has a different and specific software package to manage the meter via the optical port. An Optical Probe, such as the one shown in Figure 4, is frequently used to connect field devices and laptops to meters in order to gather information or make configuration modifications. These Optical Probes may vary slightly between meter vendors, but all of the different styles are readily accessible from supply companies on the Internet.

Figure 4 Communicating with a Smart Meter using a Optical Probe

Meter vendors and utilities already understand the accessibility of a Smart Meter's Optical Port. The ease with which attackers may be able to gain access to meters via this publicly accessible interface causes concern. Security teams and assessment teams need to realize there are several primary risks that the Smart Meter's security code is designed to protect. The following list details the primary concerns utilities have regarding unauthorized interaction with a Smart Meter's optical port.

- **Disconnect/Reconnect** - residential meters can, and usually do, provide the ability to disconnect and reconnect the meter remotely and via the optical port.
- **Rate Modification** - meter settings can be modified to reduce or increase the electric consumption calculated by the meter.
- **Attack Platform** – attackers may modify the meter to interact with other meters, aggregators, non-AMI networks, and back-end resources.
- **Brand Impact** - Smart Meter deployment and Smart Grid initiatives are directly impacted by public opinion and perception and may be adversely affected by a successful attack.

3.0 OPTIGUARD

Developing tools to communicate with Smart Meters and other AMI components begins with understanding communications standards. Standards associated with Smart Meter communications have been developed by the American National Standards Institute (ANSI) and the International Electrotechnical Commission (IEC). Smart Meters deployed in North America utilize the standards C12.18, C12.21, and C12.22 that define the communications between resources within an AMI solution.[5] C12.19 describes a protocol for formatting the standard and manufacturer-based information passed within these communications. Similar details for European Smart Meter interactions are outlined by the standards IEC 62056-21, 62056-53, and 62056-61, among other important IEC 62056 standards.[6][7]

The core of the OptiGuard is a collection of Python[8] modules designed to provide C12.18 and C12.19 communication and assessment capabilities. The libraries manage the sending and receiving of C12.18 packets and, in limited cases, can parse C12.19 information. A Python-based serial interface is included to provide direct hardware interactions as well as to leverage optical probes used by field technicians (e.g. the Probe-Tec OptoCord USB Optical Probe).[9] The tool is not designed to replace vendor software necessary for managing Smart Meters. OptiGuard merely provides C12.18 and C12.19 functionality so that more specialized tools can be developed. Such tools may emulate functionality or produce specific communication events necessary for testing and evaluation.

Three communication clients have been included with the OptiGuard toolkit. These clients have been tested with several meters but may need modifications to function properly with all meters depending on the manufacturer and model of the meter.

The "c12_18_hw_client.py" script is used to generate correctly formatted C12.18/19 messages and can send the data across hardware pins or data bus connections in specially timed increments. Although the tool can be updated to understand responses, the client currently requires that all responses are captured via a logical analyzer and parsed to determine the contents of the response messages. To assist with parsing this information, the "c12_18_csv_parser.py" tool has been provided to parse and mark C12.18/19 messages captured by a Saleae Logic Analyzer[10]. The hardware client provides the user with the ability to read and write to all standard and manufacture tables. It also provides the user with the ability to run standard and manufacturer procedures while sending the procedure any amount of data. The following textbox contains the usage data provided by this tool.

```
user$ python c12_18_hw_client.py -h
Usage: c12_18_hw_client.py [-h] [-D] [-P <num>] [-f <file>] [-no] -a <action>
[-t <num>] [-d <num>] [-p <num>] [-s <data>] [-lp <comma separated list>]
   -h: print help
   -D: turn on debugging statements
   -P <num>: Start pause seconds
   -a <action>: Perform specific action:
       test_login
       read_table: requires -t and table number or defaults to 0
       read_decade: requires -d and decade number or defaults to 0
```

[5] http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.+Smart+Grid+Meter+Package
[6] http://webstore.iec.ch/webstore/webstore.nsf/mysearchajax?Openform&key=62056&sorting=&start=1&onglet=1
[7] http://en.wikipedia.org/wiki/IEC_62056
[8] http://www.python.org/
[9] http://www.probe-tec.com/catalog.htm#OptoCord
[10] http://www.saleae.com/

```
        run_proc: requires -p and procedure number or defaults to 0
   -f <file>: select configuration file
   -t <num>: table number
   -d <num>: decade number
   -p <num>: procedure number
   -s <data>: data for sending
   -lp <data>: comma separated list of procedure numbers
   -no: turn off negotiation attempts

NOTE: This tool is fire and forget.  You will need to monitor the hardware
lines
      with a logic analyzer to determine success and failure or to read data.
```

The second and primary client, "c12_18_optical_client.py," provides the user with a menu-based interface to the full functionality of the OptiGuard toolkit. This client communicates directly with a Smart Meter's optical port using a serial-based optical probe. The optical client functions in a similar manager to the hardware client. C12.18/19 messages are built to be sent to the meter and the meter's responses are received and parsed to determine the message data. Users are provided with the ability to read one or more tables at a time, write data to any table, and run all procedures leveraging any data the users decides to provide.

NOTE: Use of the "c12_18_optical_client.py" script REQUIRES a valid C12.18 Security Code of the appropriate security level to make modifications or run procedures[11] on correctly configured Smart Meters.

The optical client parses several standard tables including the Table 00 (Configuration Table) and Table 01 (General Manufacturer Identification Table). Users are also provided with other testing capabilities, such as brute force authentication, table fuzzing, and meter disconnect/reconnect. The strength of this client is its modularity. Users can easily add new functionality to this client and update the menu to provide access to the new capabilities. The following textbox contains the user menu that is used to interact with Smart Meters via the meter's Optical Port.

```
user$ python c12_18_optical_client.py
############################################################
## C12.18 Optical Client - InGuardians, Inc.
## Please review license and Terms of Use before using this software.
############################################################
Start Time: 11:47:55 04/10/12 CDT
########################################
## 0) Quit
## 1) Test Negotiation Sequence
## 2) Test Logon
## 3) Parse Configuration Table
## 4) Parse General Manufacturer Identification Table
## 5) Read Table
## 6) Read Multiple Tables
## 7) Read Decade
## 8) Run Procedure
## 9) Run Multiple Procedures
## 10) Run Multiple Procedures without login
```

[11] Some meters, usually dependent on meter manufacturer, do not require a valid C12.18 Security Code to read some, non-security related, tables.

```
## 11) Write Table
## 12) Brute Force Logon
## 13) Alternate Brute Force Logon (Read Table Verification)
## 14) Fuzz Security code
## 15) Alternate Fuzz Security code
## 16) Read Single Table walking User IDs
## 17) Read Multiple Table walking User IDs
## 18) Write Table 13 Demand Control Table. Table write Proof of Concept
only.
## 19) Run Procedure 21 Direct Load Control and set 0 percent load
## 20) Run Procedure 21 Direct Load Control and set 100 percent load
## 21) Toggle Negotiation
## 22) Terminate Session
## 23) Reset Serial
## 24) Toggle Debug
## 25) Toggle Invert
########################################
Enter Action Selection:
```

The third client is the "client_framework.py" script. This script is a dummy client and is designed to be an easy starting point for new users. It provides the basics necessary to begin developing new functionality. This functionality can be moved to the optical client once it has been developed and tested. The following textbox contains the user menu that is used to interact with Smart Meters via the meter's Optical Port.

```
user$ python client_framework.py
############################################################
## C12.18 Optical Client - InGuardians, Inc.
## Please review license and Terms of Use before using this software.
############################################################
Start Time: 11:49:31 04/10/12 CDT
########################################
## 0) Quit
## 1) Read Table
## 2) Toggle Debug
## 3) Toggle Invert
## 4) Toggle Negotiation
## 5) Terminate Session
## 6) Reset Serial
########################################
Enter Action Selection:
```

All of the clients are augmented by configuration file "c12_18_config.txt" and logging functionality. The configuration file is used to store common values, such as C12.18 security codes, and settings. The logging functionality is necessary to document findings and results of testing. A generic "meter_passwd.txt" has also been included and provides the user with an example password file that could be used for brute force authentication testing. Users can build password files by hand or from data dumped from Smart Meter memory components using the "c12_18_extract_keys.py" script.

4.0 OPTICAL PORT RISK MITIGATIONS

Mitigations of the risks posed by a Smart Meter's optical port depend on the capabilities of the utility's overall AMI solution. The following are a few mitigations that are known to exist in several AMI solutions.

- **Brute Force Authentication** - Most meters log authentication attempts. If these logs are collected by the head-end systems they can be used to detect brute force authentication attempts.
- **Disconnect/Reconnects** - Head-end systems can determine the current state of the meter and compare it to the expected state of the meter. Incident response procedures can be developed and implemented to react to unauthorized meter disconnects or reconnects.
- **Configuration Modifications** - Head-end systems can determine the current state of the meter and compare it to the expected state of the meter. Incident response procedures can be developed and implemented to react to unauthorized meter configuration modifications.

In addition to these mitigations meter vendors and utilities should consider the following points.

- **Meter Deployment Considerations** - Meters that provide disconnect/reconnect functionality should not be deployed at locations responsible for critical infrastructures (e.g. cellular towers, water pumping stations). Identifying a change in a meter's status can take time which could lead to outages at critical times.
- **Meter Passwords** - Utilities should use more than one authentication password for their meters. It is not generally feasible to generate unique passwords for every meter, which could lead to millions of passwords. Utilities can use several methods to make smaller group passwords such: a different password for residential and commercial meters types, a different password for each vendor, passwords computed using the zip code of a meter, etc.
- **Secure Password Storage** - meter vendors should determine ways to secure passwords stored on the meter and to protect them when being communicated between the meter's hardware components.
- **Brand Issues** - By understanding that attacks can occur on meters and successful modifications will become public knowledge, utilities can prepare statements and responses for the media.
- **Service Level Agreements** - Utilities need to learn to develop and modify service level agreements (SLA) with their AMI vendors to ensure that the vendors are identifying and addressing situations which impact AMI reliability, including security, in a timely manner.
- **Incident Response Planning** - Utilities should develop incident response plans associated with AMI resources. Procedures should be developed , tested, and implemented for identifying and responding to unauthorized meter modifications and meter-centric attacks. Solution vendors can begin this process by documenting incident response scenarios and distributing them with the rest of the solution documentation.

5.0 CONCLUSION

The optical ports of Smart Meters are intended to provide utilities with a safe method to directly manage individual meters. This capability is necessary to ensure the reliability of these increasingly complex and widely distributed devices while also protecting the field technicians servicing the meters. The management software developed and distributed by the meter vendors is intended to enable meter management, only. These tools do not provide methods for testing all situations, fuzzing of data and components, or brute forcing authentication mechanisms, nor should they. A separate class of tools to test unusual use cases is necessary. Flexible tools that can provide communications using the protocols outlined by ANSI C12.18, C12.19, C12.21, C12.22, IEC 62056-21, IEC 62056-53, and IEC 62056-61 are critical to ensure that Smart Grid solutions are reliable, effective, and secure.

Tools such as the OptiGuard provide vendors with the ability to test their solutions during development and as new components are integrated into their solutions. These tools also provide utilities and other industries with the capabilities to validate vendor claims, test resource implementations, and determine functionality issues as solutions evolve over time. Open sourcing these tools to security research teams, utility security teams, and embedded device vendors is critical to reducing the costs associated with developing separate tools for the wide variety of AMI solution deployments. The experiences of these separate, and often segregated, testing teams can improve the utility industry's knowledge base and ensure that all Smart Grid vendors and utilities benefit from the time and efforts devoted to similar, or exact, AMI implementations.

6.0 ACKNOWLEDGEMENTS

InGuardians
John Sawyer
Tom Liston
Matt Carpenter
Andrew Righter
Joshua Wright
Justin Searle
Travis Goodspeed
Ed Beroset – Elster Solutions, LLC
Robert Former – Itron, Inc.
Smart Meter and Smart Grid Security staff from various utilities

