



---

# **Smart Meter Hacking Research, and the Related Privacy Issues!**

---

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

# Don C. Weber

---



- InGuardians, Inc. - Senior Security Analyst
- United States Marine Corps 1991 - 1999
- Plethora of Security Positions
  - Certification and Accreditation
  - Security Manager
  - Incident Responder
  - Penetration Tester
- Periodic Blogger
- Python Programmer
- Hardware Smasher



# Agenda

---



- Answer Questions Provided to InGuardians
- Answer Your Questions

# Smart Meters Researched



- What types (manufacturer, model, etc.) of smart meters have you used in your research and hacking activities?

**REDACTED**

InGuardians works with several clients and sees a variety of Smart Meter deployments. Although we have conducted "research" that is not associated with our clients, this has generally occurred merely to facilitate our understanding of hardware assessments. We talk about those methods but we do not mention our clients or the vendors they leverage.

As most of you know, AMI solutions are usually unique to each utility. Although some of the equipment, internal and external, are the same, each utility has their own "method" that best suits their business challenges and perceived risks.

# Smart Meter Data Types



- What types of data did you find in the smart meters?
  - Outlined in ANSI C12.19 Standard
    - Manufacture Tables depend on vendor
    - Mostly configuration information
  - Storage and management are different
  - Security tools help provide insight

Time [s]	Value	Direction	Field
70 635036	0xE	Metro-RODD	stp
70 636078	0x0	Metro-RODD	ident
70 637119	0x0	Metro-RODD	cntl
70 638161	0x0	Metro-RODD	Seq-nbr
70 639203	0x0	Metro-RODD	len0
70 640245	0x0	Metro-RODD	len1
70 641286	0x0	Metro-RODD	identify
70 642328	0x82	Metro-RODD	ctrl0
70 64337	0x70	Metro-RODD	ctrl1
70 696466	0x06	lnG-TXDD	ack
70 727682	0xE	lnG-TXDD	stp
70 728725	0x0	lnG-TXDD	ident
70 729767	0x0	lnG-TXDD	cntl
70 73081	0x0	lnG-TXDD	Seq-nbr
70 731852	0x0	lnG-TXDD	len0
70 732895	0x05	lnG-TXDD	len1
70 733937	0x0	lnG-TXDD	ok
70 73498	0x0	lnG-TXDD	ok
70 736022	0x01	lnG-TXDD	ok
70 737065	0x0	lnG-TXDD	ok
70 738107	0x0	lnG-TXDD	ok
70 73915	0xFF	lnG-TXDD	ctrl0
70 740192	0x42	lnG-TXDD	ctrl1
70 785653	0x06	Metro-RODD	ack
70 790667	0xE	Metro-RODD	stp
70 791709	0x0	Metro-RODD	ident
70 792751	0x0	Metro-RODD	cntl
70 793793	0x0	Metro-RODD	Seq-nbr
70 794835	0x0	Metro-RODD	len0
70 795876	0x05	Metro-RODD	len1
70 796918	0x61	Metro-RODD	negotiate
70 79796	0x01	Metro-RODD	negotiate
70 799001	0x0	Metro-RODD	negotiate



ANSI C12.19-2008

American National Standard  
For Utility Industry  
End Device  
Data Tables

Let's start by saying that interacting with a Smart Meter may or may not require a Security Code. To do any administrative actions the Security Code is required. However, some meter vendors do provide read access to "some" standard and manufacturer tables without the need to authenticate to the meter.

As to the information contained, this is all solution dependent. The information contained in the standard tables are documented in the C12.19 standard document. Manufacturer tables, however, are a different story. Those are proprietary and maintained internally. They may or may not be shared with the utility. This data is generally configuration data and consumption information. Smart Meters are VERY configurable. Utilities might only leverage a small portion of the data and to everything else on the back end. But if they are not worried about data in specific tables, are they managing it?

One of the things that OptiGuard, the optical assessment toolkit developed by InGuardians, provides is an insight into all of the tables. It doesn't know how to specifically parse the data without additional information provided by "someone." But, if the data contains strings or words, rather than just number data, then it might be easy to figure out. Insider knowledge could also help.

# Meter Read Frequency



- What were the range of meter read frequency settings that you have found in the smart meters?
- What is the most common frequency read setting that you found?



Copyright 2012 InGuardians, Inc.

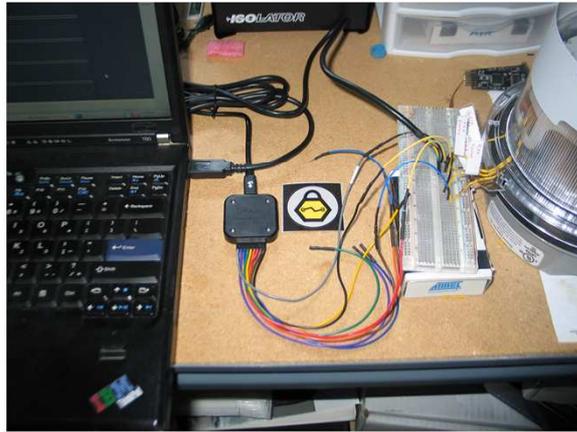
6

Utilities still have to pay for the "data reads" as the data is transmitted across the cellular network they have selected. So frequency is going to depend on their tolerance for paying for that information. Typically a normal meter read is going to happen once per day across a solution. At least that is a good benchmark. Area or individual reads to detect and respond to issues will happen periodically but "generally" not across the entire solution. The size of the utility is going to play a factor in this as well.

# Meters As Attack Platforms



- Were you able to get to any downstream or upstream systems through the smart meter?



Copyright 2012 InGuardians, Inc.

7

I asked on utility security contact "What is your biggest fear?" His response was "That you will be able to leverage the AMI assets (i.e. Smart Meters, relays, aggregators) to jump to the internal network or to other systems such as in a substation." So, that is the question.

In the solutions we have reviewed, InGuardians has not been able to leverage Smart Meters specifically to hop to other Smart Meters or systems on the internal or external networks. Yet. That is the continuous question. Every time a vendor makes a modification to the metrology board or the communications board there is a possibility.

Utilities need to approach AMI and SCADA solutions from the stand point that a resource HAS been compromised. Can that compromise be contained such that it does not propagate through the network? Can you detect anomalous activity and respond quickly? If the solution is provided by a third-party, do they have these capabilities and are the contractually obligated to tell the utility?

# Is HAN a Risk?



- Were you able to get to any home area network (HAN) through the smart meter?
- What specifics and amount of granularity were you able to determine through the smart meter with regard to specific appliances being used, activities in the dwelling, etc.?

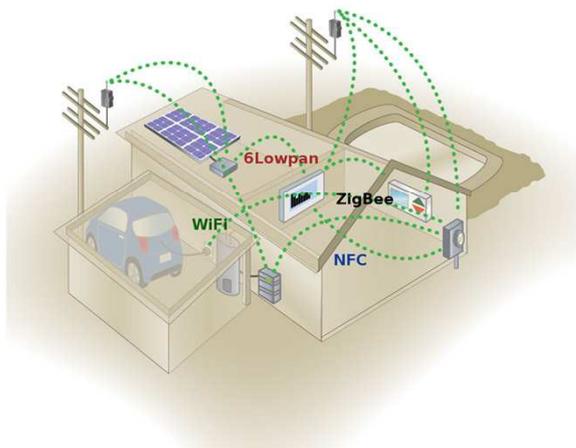


Image Borrowed from: <http://www.trilliantinc.com/products/securemesh-han>

Copyright 2012 InGuardians, Inc.

8

Thus far InGuardians has experienced no AMI solutions where the HAN network has been enabled. Actually, part of our tasks are to ensure the HAN radios are disabled. Of course, most solutions (if they are not implementing them now) are being deployed with the capabilities because the utility needs to think ahead to those programs. But, for now, InGuardians has not experienced issues in this area. This will change as we move forward.

But whose responsibility is that anyway? Do utilities have control over the devices purchased by their customers? Are they going to force their customers to particular solutions? Are they going to configure those solutions for their customers?

The question really boils down to, how is the solution protecting the private keys that enable secure communications between the HAN and the Smart Meter. It is these keys that will permit attackers to mimic Smart Meters and attack the HAN users. This protection is solution dependent and requires consideration of the Smart Meter, key management server, and the solutions encryption management practices.

# Modifying Meter Configuration



```
trunk: python
cutaway> 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: 00:50:36 12/20/11 CST

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

- Was it possible for you to shut off the electricity supply to the dwelling?
- Was it possible for you to copy the data from the smart meters?
- Was it possible for you to change the read frequency settings?

Yes. This "required" having knowledge of the Security Code. Some meters use standard procedures for connects/disconnects. Other meters use manufacturer procedures, and therefore proprietary, and disable the standard procedures. But with procedure fuzzing, if you know the Security Code, you may be able to connect/disconnect the meter without knowledge of the required procedure.

# Shutting Off The Cold Air



- Was it possible for you to shut off or otherwise control specific appliances within the house?

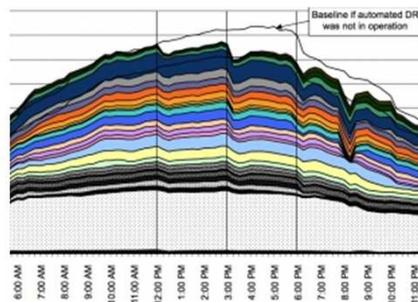


Image taken from: <http://www.greentechmedia.com/articles/read/making-the-case-for-smart-grid-to-shave-peak-power/>

Copyright 2012 InGuardians, Inc.

10

No. Doing this will most likely not come from the actual Smart Meter. More than likely this will occur using tools that leverage stolen HAN keys and third-party or custom tools.

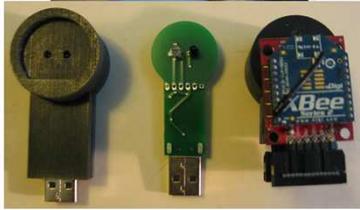
One thing you have to remember is that shutting off an appliance is not necessarily the worst thing that can happen. Another attack scenario involves modifying peak usage time tables. If you make a home's appliances believe that it is not a peak period and they all turn on it is going to have an impact. If you do this on a large number of homes it could have an impact on the whole grid. Other considerations are technologies with HAN capabilities built-in but that are not connected to a HAN network. How does a business know if it is purchasing something with these capabilities? Can somebody impact them even though they are not connected to their Smart Meters and therefore not leveraging the functionality? This is not the problem of the utility, but it should be a concern for the whole industry.

There are probably many more examples people in the industry can come up with.

## Remote Smart Meter Surveillance



- Were you able to attach a monitoring device to the smart meter to enable remote surveillance of the readings?



Top Image taken from: <http://www.bluegiga.com/solution?g=Consumer&n=Probe-TEC>

Copyright 2012 InGuardians, Inc.

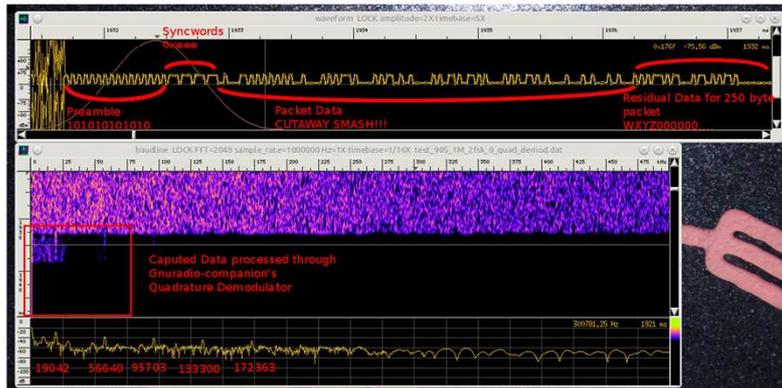
11

InGuardians has not built these capabilities into any tools. But we have talked about it. Several vendors already sell Bluetooth enabled optical probes. You can build one very easily. As the currently available assessment tools speak to a serial port, and can be modified to speak via other methods, they are compatible with these types of technologies.

# InGuardians Research



- What plans do you have to continue this hacking research on other types of smart meters? Which types?



Copyright 2012 InGuardians, Inc.

12

We cannot talk about the solutions we are reviewing now or in the near future. I can tell you that InGuardians is **EXTREMELY** interested in the radio aspects of the external solutions. With the explosion of embedded devices being leveraged by businesses the attackers are going to be studying and developing tools that involve radio communications. This will have an impact on AMI and Smart Grid solutions. The industry should pay attention. We are.

# Questions



- InGuardians, Inc.
  - consulting@inguardians.com
- Don C. Weber
  - don@inguardians.com

