



# Analysis and Defense of Large-Scale Smart Meter Networks

John Ellis, Kaila Perry, Lawrence Livermore National Laboratory, Norfolk State University

Mentors: Jeffrey Duffany, Universidad del Turabo at Gurabo, Puerto Rico; Celeste Matarazzo, Lawrence Livermore National Laboratory, Cyber Defenders



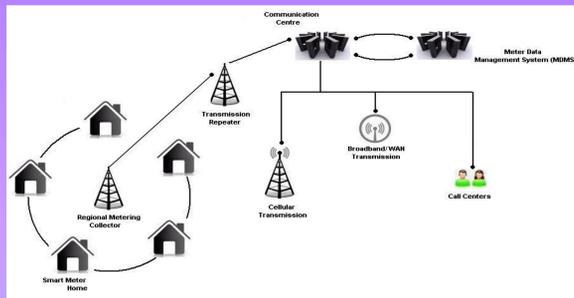
**Abstract:** Over the years, utility companies have transitioned to using smart meters as a means of calculating the energy usage of commercial and residential users. As of now, approximately one-third of U.S. homes have smart meters, but electric companies hope to have 90-95% of homes installed with smart meters by 2015. With well over nine million smart meters deployed thus far in California, the concern about possible vulnerabilities is rapidly rising. In the same way, the vulnerabilities not only affect individual smart meters, but the entire smart grid network as a whole. Because of the importance of the smart grid, it is crucial to determine the vulnerabilities and their potential damages in order to find a better way to secure them.

## Introduction:

Smart meters are electrical meters that record the consumption of electric energy and communicates that information back to the utility company through a network for monitoring and billing purposes. Suppose a large scale attack is coordinated against the smart meter network or the smart grid. What actions could have been taken to prevent the attack in the first place, and what should Lawrence Livermore National Laboratory's role be?



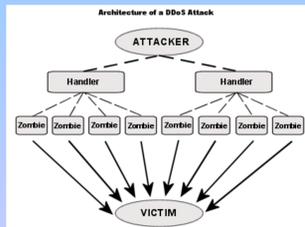
Smart Meter



Smart Meter Network

## Methods:

- Became familiar with smart meters
- Identified smart meter manufacturers
- Determined smart meter vulnerabilities
- Identified smart meter attack methods
- Experimented with the NS-3 simulator
- Explored how other labs are attempting to prevent vulnerabilities



Distributed Denial of Service Attack

## Results:

### Smart Meter Manufacturers:

Smart meters are made by multiple companies. The most popular smart meters are made by Itron, Elster Group, General Electric (GE), Landis + Gyr, and Sensus.

### Vulnerabilities:

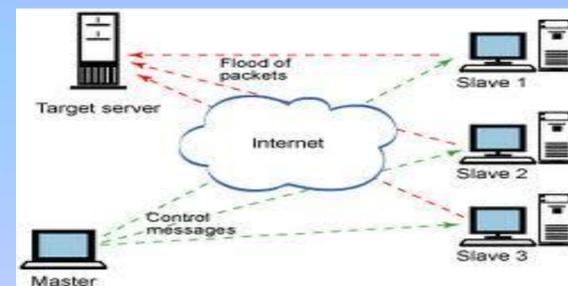
- Smart meters were built on a network that they were not meant to be used on. As a result, hackers are able to wirelessly connect to the smart meter networks allowing them the ability to change, disrupt or disable the network.
- Smart meters can be stolen, reprogrammed, and returned without the owner or company ever noticing because everything is done electronically.

### Attack Methods:

- Identity Theft
- False Data Injection
- Denial of Service
- Weak Key Derivation
- False Operation Signals
- Worms
- Physical Threats (Magnet Attacks)



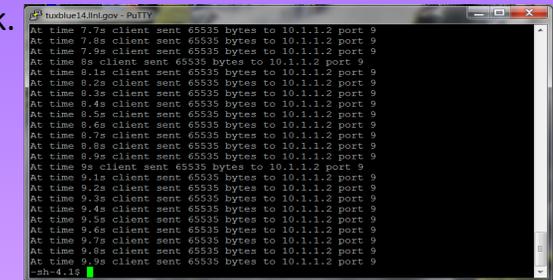
Many oppose smart meters because they are unsafe, and unsecure



Denial of Service (DoS) Attack through packet flooding

## Discussion:

After extensive research, it has been found that smart meter manufacturers make smart meters with little to no cyber security, and it is very possible to hack the smart meter network using various techniques. The most common way to hack a smart meter is by using a magnet to slow the meter readings. However, a Denial of Service attack would be the most likely to occur in a deliberate widespread attack.



Attempting DoS attack by packet flooding using NS-3

<sup>3</sup>Oak Ridge National Lab has partnered with Sensus and EnerNex to improve the software of smart meters. In addition, Idaho National Lab is working on improving the SCADA\* security in an effort to make the smart grid more secure.

Based on what other labs are doing and the research compiled, LLNL should simulate large scale attacks using NS3, analyze the data, and find a solution to prevent smart meter vulnerabilities from being exploited.

## References:

1. "Quizlet." Smart Meter Vulnerabilities Flashcards. N.p., n.d. Web. 10 June 2012. <<http://quizlet.com/11918325/smart-meter-vulnerabilities-flash-cards/>>.
2. Peisert, Sean "Insiders, Forensics, IDS, BFT, Elections, Ants, Turtles, and the Smart Grid" Seminar. June 2012.
3. "Sensus Joins EnerNex and Oak Ridge National Lab to Heighten Cyber Security in Smart Meters." Sensus. July 2012.

\* Supervisory Control and Data Acquisition