Security of the Smart Grid
Reza Motamedi*

Scribed by Dan Ellsworth
March 7, 2012

*Reza has requested that clarifications be directed at Kofi

Preamble
On March 7, 2012, Reza Motamedi presented "Security of the Smart Grid". This presentation focused on privacy issues with smart grid technology and primarily based on the paper "Protecting Consumer Privacy from Electric Load Monitoring".

What is the SmartGrid
The SmartGrid comes from the Energy Independence and Security Act of 2007. The vision is to add smart agents to the power grid to improve power transmission, reduce outages, support green power, and other public goods. A SmartGrid uses the existing generation, transmission, and distribution components of the power grid while enhancing communications and operation as well as introducing new end-user applications.

Attacks on the SmartGrid
Two major threats to the smartgrid were given; tampering and disclosure. Tampering would allow the attacker to defraud the grid by potentially reducing or otherwise changing the amount billed to the customer improperly. Privacy would allow an attacker to glean detailed information about a location. This talk looks primarily at attacking privacy.

Privacy can be breeched non-intrusively by recovering the power usage data. The SmartGrid agents, basically, collect detailed information on power usage, known as the usage profile. Mining the usage profile, an attacker can infer what is happening within a building. The usage profile is converted to a load profile, which can be paired with appliance profiles to produce a behavior profile. Changes in load profile are "sister events" to those in the behavior profile (i.e. turning on a TV creates a sudden increase in load).

Defense
The defense must not require modification to the monitor and must report accurate usage. Load leveling is the suggested defense to reduce the amount of information leakage. Basically, an appliance is placed in the home that uses batteries to even out
or smooth the load to the grid. The authors estimated that Deep cycle lead acid battery technology is suitable for this setting, with a half-life of 1 to 2 years.

The complexity for such an appliance is in the control system. Slide 10 contains the definitions and constraints for such a system. At a conceptual level, the system charges when load is light and supplements when load is high such that the load remains constant. However, as formulated, the system does not work due to the magnitude of load changes over short intervals. To address this defect, the signal state solution has a low recovery state and high recovery state added. Slide 11 contains a formula used to help tune the state transitions.

**Evaluation**
System evaluation was done using SmartGrid data captured in spring 2010. Gaps existed in the data that were patched (there was no discussion in the presentation of how the patching was done). A TED device was used for data collection; providing the usage profile graphs shown in the presentation. The collected data was then processed through a simulation environment in MatLab (see slide 14).

By applying the load leveling algorithm, many features in the initial usage profile are lost. Peaks are still present since the some events are too large for the batteries to compensate for. 91-97% of the initial features were removed using the technique. The majority of the information leaked is during the low state, when the batteries don't have much stored energy to help smooth load.

- Small variations in load can be effectively hidden.
- Large transient variations can't be protected against due to limited battery power.
- Legitimate loads in the low state are a problem since there we can normally hide these but they leak when the system is in this state.

  **Kevin:** What are we able to prevent? Can we still stalk the people? It looks like that still works?
  **Reza:** So, these are all the features in the signal. Not all are legitimate. The amount of time they are leaking is low. Raw features are reduced 99%, 65-85% of the simulation time is leveled.

**Future work**
Future work is suggested for optimizing the parameters to improve battery life and generating additional noise in the usage profile based on the knapsack problem. There were also points raised about high frequency monitoring being able to defeat
the system (not possible with current monitors). Cost savings (estimated at 1-5%) were also cited as a potential side-effect from how power used is smoothed.

**Seminar Discussion**

**Hannah:** If the battery is charging and offloading doesn’t this change the cost scheme?  
**Reza:** Basically you’re not being charged the same through out the day. If you time shift the charging you might save. Businesses may see the opposite effect since they

**Reza:** Adam, do you have a question?  
**Adam:** No.  
**Reza:** Thank you.

**Joe:** Do they try to charge during non-peak  
**Reza:** No, they didn’t charge based on time of day.

**Paul:** I don’t see the point. I’m still going to leak things I care about; like being home or not.  
**Reza:** Though the important stuff still leaks through sister events, they are removing many of these events.  
**Joe:** I think Paul is saying is that we are still leaking the most important information.  
**Reza:** You can still tell that there are breaks. Yeah, this is what it is.  
**Kevin:** Is that true?  
**Joe:** A bigger battery allows you to smooth more. How much is your privacy worth?  
**Reza:** Don’t want to level more than consumption.  
**Joe:** I disagree with Paul. I can look at the power or watch the lights; way easier than looking at the power. What is important is what I can’t see the easy way. They are successful in removing that information.  
**Paul:** I agree, I just didn’t know what I wanted to gain.  
**Kevin:** Sure but I can mine remotely; maybe the power company would sell the information.  
**Joe:** I’m not thinking about the power company, I’m thinking of an adversary that might plug in a physical monitor. Still easier than owning the grid.

**Kevin:** Successful paper? Are you ready to put $200 on batteries?  
**Dan:** I don’t know what I want from this. What information would I want to protect.  
**Joe:** Filled under when I go crazy and wear a tinfoil hat all the time. If someone wants a profile on me they can just watch my laptop connections; clearly I’m not worried about that information.  
**Kofi:** Seems like all of the behavioral information is already being sold and is already present to various degrees.  
**Nick:** I’m on twitter; I advertise it.  
**Kofi:** Sure take out the middle man.
**Kevin:** I think it is surprising the amount of information you can infer; it seems like a lot of information you can glean.
**Reza:** At the same time, on the attacker side; how much do you want to spend on getting the load profile.
**Adam:** I don't think you should discount not wanting the power company to find out.
**Joe:** Oh yeah, I wouldn't want to disclose it but the cost.
**Kevin:** Near real-time tracking with additional data, what does this mean for inferring behavior? Think about the recent Target article on knowing when your pregnant.
**Joe:** Fight the good fight, but the game is already up. If I had the $200, I'd do it.
**Paul:** I like the idea of saving money by using the charging time.

**Kevin:** Do we have smart meters in OR?
**Kurt:** There's debate. Lots of radiation concerns.

**Reza:** Why should it be so fine grain?
**Dan:** Timeliness is important
**Reza:** Why would I want to know so fast? What is an additional 30 minutes?
**Paul:** In Alaska, power out in 20 minutes can lead to deaths.
**Reza:** Granular data doesn't make sense in residential context.
**Kevin:** This could be a monitoring service offering. Fast detection of brownout and overload conditions; those cascading failures can happen pretty quickly.