Hacking the Smart Grid
OWASP Tampa
Presenter

» Tony Flick

» Principal, FYRM Associates

» Over 6 Years in Information Assurance

fyrmassociates.com
Agenda

» What is the smart grid?
» Known problems
» Security initiatives
» Timeline
» History repeating
» Web Application Interfaces
» Recommendations

fyrmassociates.com
What is the Smart Grid?

- Current infrastructure
- Future infrastructure
What Makes up the Smart Grid?

» Devices
» Network infrastructure
» Bi-directional communication
Problems

» Physical security

» Bi-directional communication introduces attack vectors

» Same problems as every other type of network/application
Implications

» Privacy Concerns
» Denial-of-Service
» Electricity theft
Security Initiatives

» The Energy Independence and Security Act of 2007
» NIST Interoperability Framework
  » Advanced Metering Infrastructure System Security Requirements (AMI-SEC)
» NERC CIP 002-009
Timeline - Part 1

Examples of Integrating Security from the beginning (2006 - 2009):

» NIST Smart Grid Interoperability Framework
  » Initial list of standards for inclusion in version 1.0 released on May 8, 2009.
» Advanced Metering Infrastructure (AMI) System Security Requirements v1.01
  » 2007 - 2008
» NERC CIP
  » 2006, 2009
» Critical Electric Infrastructure Protection Act (CEIPA) - (HR 2195)
  » 2009

fyrmassociates.com
Timeline - Part II

» Design and implementation of the smart grid

» 2002 actually occurred before 2006

» Anyone have a flux-capacitor?

» Austin - 2002

» Salt River Project - 2006

fyrmassociates.com
Timeline Repercussions Example

- Oncor Energy Timeline
- Purchase 900,000 smart meters
- State issues operating standards
- Replace non-compliant smart meters
- Who do you think is paying for the old and new smart meters?
  - Early Adopter fee?

fymassociates.com
Low Hanging Fruit

- Eight Utility Company Web Sites
  - Sensitive information over clear-text protocols
    - What amount of security is in a name?
  - Cross Site Scripting
  - Information Leakage

fyrmassociates.com
The Major Players

- iGoogle (PowerMeter)
- Microsoft Live (Hohm)
We Have an App For That

- Monitor Usage - Current Majority
- Control Appliances
  - iTunes App Store
  - Energy UFO

fyrmassociates.com
Social Networking

» Do you want everyone to know how much electricity you are using?
  » The power of groups

» Twitter now

» Facebook in the works

fyrmassociates.com
Social Networking

Hey there! [username] is using Twitter.
Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? Join today to start receiving [username]'s tweets.

Currently using 29.4 Watts, 2084 Wh in last 24hr, 0 Wh previous day -
10:29 PM Aug 5th from API

Currently using 91.1 Watts, 4233 Wh in last 24hr, 3660 Wh previous day -
6:45 AM Jul 18th from API

Electricity meter reading: 31400 KWH
About 11 hours ago from web

outside lights turned off about 18 hours ago from web
outside lights turned on about 18 hours ago from web
outside lights turned off about 18 hours ago from web
outside lights turned on about 18 hours ago from web
phone is ringing about 21 hours ago from web
power consumption has been reduced (16p per hour for 30 min) about 21 hours ago from web
"unusually" high electricity use (46p per hour for 30 min) about 21 hours ago from web

fyrmassociates.com
Social Networking

Lyceum's Notes

Lyceum at University of Mississippi for Sep 7 2009
Sun at 10:00pm

(1025.82 kWh usage, 12.24 kWh peak) Give yourself a hand – we were down ~51.27% in electricity usage and ~88.73% in peak, too!

Updated on Sunday

Lyceum at University of Mississippi for Sep 7 2009
Sun at 10:00pm

(1024.82 kWh usage, 12.24 kWh peak) Give yourself a hand – we were down ~51.27% in electricity usage and ~88.73% in peak, too!

Updated on Sunday

fymassociates.com
Consumer Perspective

- You don’t have to sign up for these services
  - ...but then what’s the point?
Duck and Cover?

» Fix the low hanging fruit

» Opportunity missed at the beginning, but we can still do some good

» Allow security to mature

» Innovation vs. Security/Regulation

fyrmassociates.com
General Discussion

If you have any followup questions:

» Email me: tony.flick at fyrmassociates.com