

Hacking the Smart Grid

OWASP Tampa



Presenter

- » Tony Flick
 - » Principal, FYRM Associates
 - » Over 6 Years in Information Assurance



Agenda

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



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 I

- » Examples of Integrating Security from the beginning (2006 - 2009):
 - » Energy Independence and Security Act of 2007
 - » 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



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



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?



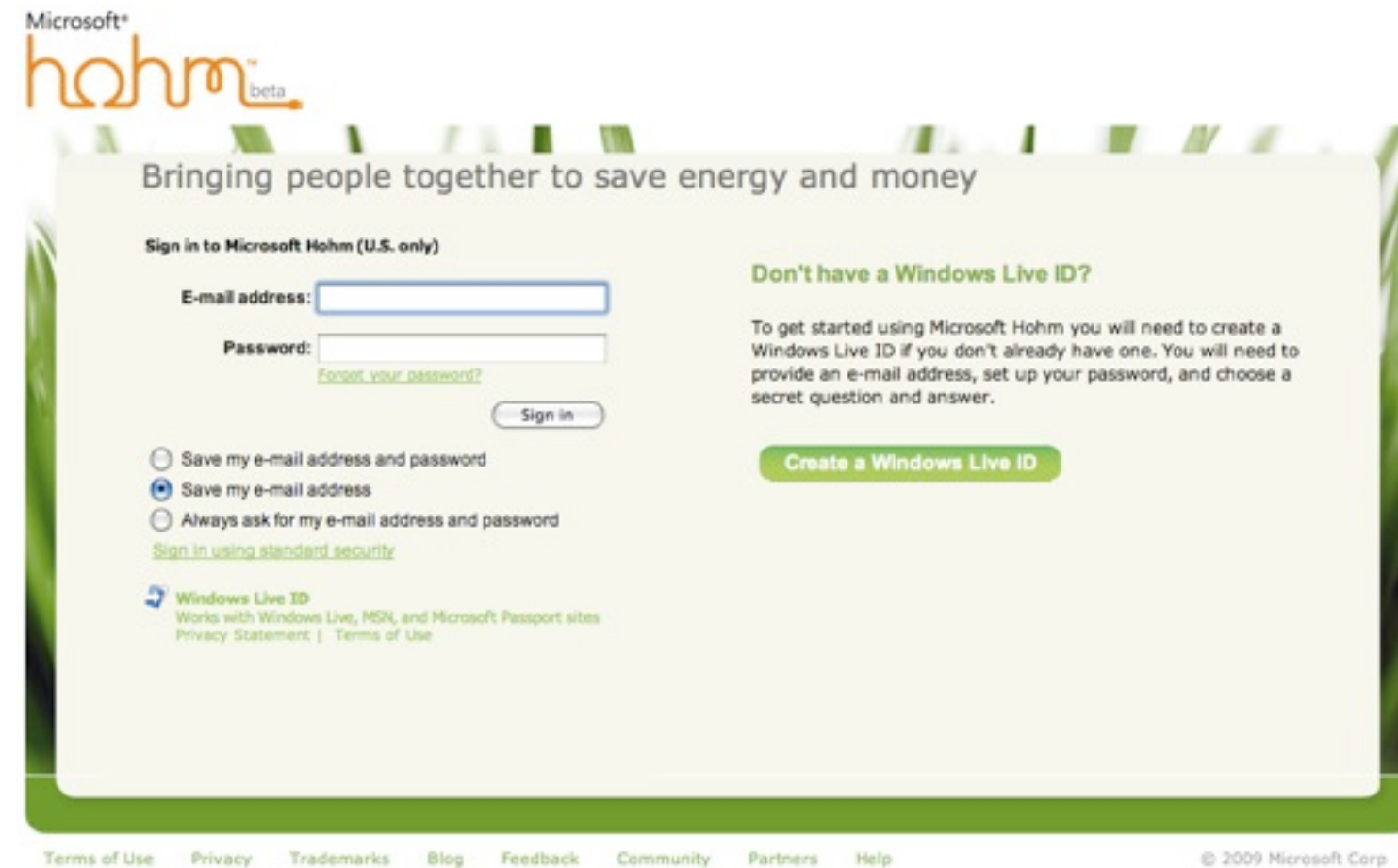
Low Hanging Fruit

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



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



Social Networking

- » Do you want everyone to know how much electricity you are using?
 - » The power of groups
- » Twitter now
- » Facebook in the works



Social Networking

Hey there! [redacted] 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 [redacted] tweets.

[Join today!](#)

Already using Twitter from your phone? [Click here.](#)



Currently using 29.4 Watts, 2084 Wh in last 24hr, 0 Wh previous day - [redacted]

10:29 PM Aug 5th from API

Currently using 91.1 Watts, 4235 Wh in last 24hr, 3660 Wh previous day - [redacted]

6:45 AM Jul 18th from API

24 following 554 followers

Tweets 309

Favorites

Following

twitter

Name or location search or Login / Join Twitter!

Select Language

Hey there! [redacted] is using Twitter.

Twitter is a free service that lets you keep in touch with people using the web, your phone, or IM. [Join today](#) to start receiving [redacted] updates.

[Join today!](#)

Already using Twitter via SMS or IM? [Finish signing up.](#)

electricity meter reading: 31400 KWH

about 11 hours ago from web

Previous With Others

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

the phone is ringing [redacted] about 21 hours ago from web

power consumption has been reduced (16p per hour) about 21 hours ago from web

"unusually" high electricity use (46p per hour for 10 mins) about 21 hours ago

About

Name [redacted]

Location [redacted]

Stats

Following	1
Followers	35
Favorites	0
Updates	1,363

Following



Social Networking

facebook Remember Me Forgot your password?
Email Password
 Facebook helps you connect and share with the people in your life.



Lyceum's Notes

[Back to Lyceum](#)

Lyceum's Notes

View: [Full](#) | [Compact](#)

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

(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

Subscribe to these Notes

 [Lyceum's Notes](#)
[Subscription Help >](#)



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



General Discussion

- » If you have any followup questions:
 - » Email me: [tony.flick at fyrmassociates.com](mailto:tony.flick@fyrmassociates.com)

