



WELCOME

TO *Hacking the*

SMART GRID

DEFCON

Presenter

- » Tony Flick
 - » Principal, FYRM Associates
 - » Over 6 Years in Information Assurance
 - » Many DEFCONS / First presentation



Agenda

- ❖ What is the smart grid?
- ❖ What makes up the smart grid?
- ❖ Known problems
- ❖ Security initiatives
- ❖ Timeline
- ❖ History repeating
- ❖ 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



Implications

- » Google Maps art
- » Denial-of-Service
- » Electricity theft



Security Initiatives

- ❖ The Energy Independence and Security Act of 2007
- ❖ NIST Interoperability Framework
- ❖ Advanced Metering Infrastructure (AMI) System Security Requirements v1.01
- ❖ Critical Electric Infrastructure Protection Act (CEIPA)
– (HR 2195)



Fluffy

- » Using security fluff words to make people feel warm and fuzzy
- » Security integration from the beginning
- » CIA



Timeline - Part I

- » Examples of Integrating Security from the beginning (2007 – 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
 - » Critical Electric Infrastructure Protection Act (CEIPA) – (HR 2195)
 - » 2009



Timeline - Part II

- » Design and implementation of the smart grid
 - » 2002 actually occurred before 2007
 - » Austin – 2002
 - » Salt River Project – 2006



History Repeating

- » PCI DSS
 - » “Self-policing” and SAQs
- » NERC and FERC
 - » NERC – Utilities under reporting
 - » NERC and FERC – Aurora vulnerability



Duck and Cover?

- ❖ Opportunity missed at the beginning, but we can still make good
- ❖ Allow security to mature
- ❖ More stringent security requirements
 - ❖ Compliant vs. Secure
- ❖ Tighter regulation



Questions?

- » If we run out of time:
 - » I'll be here until Sunday evening
 - » Email me: tony.flick@fyrmassociates.com

