Smart Grid Cyber Security
How Smart is the Threat?

Simone Riccetti,
IT & SCADA Security Consultant
Where are the specific areas of security and privacy concerns?

Emerging Smart Grid Issues
- Millions of new end points
- Massive amounts of data

System security
- Vulnerable software
- Lack of access control
- Mis-configuration of options

Data Vulnerability
- Weak/No encryption
- Inappropriate storage
- Installation of malcode

Potential Fraud
- Invalid credentials
- Weak authorization
- Insufficient tamper protection

Downtime
- Denial of service risk
- System corruption

“The Smart Grid scares the hell out of me. It's not the new capabilities; it's the amount of interconnectedness it brings.”  - Joe McClelland, Director, FERC Office of Electric Reliability

Img courtesy: www.smartgrid.epri.com
A Smart Grid needs security enforcement at multiple points:

- SCADA network systems
- Advanced metering data management system
- Substation Remote Monitoring equipment
- Meter to Cell Relay

IP addressability and use of open standard protocols for the control grid necessitates it to be securely protected at multiple points.
Challenging exploits: more vulnerabilities in sophisticated category

- 24 X-Force alerts and advisories in H1 2011

- 12 high value, cheap-to-exploit
  - Publicly available exploits for 9 of them

- 9 harder to exploit but high value
  - This is a higher number than in previous years
Proliferation of “Smart” Networked Devices

- Switch from analog to digital controls
- Incorporation of network standards
  - TCP/IP communications
  - Wireless communications
- Replacement SKU parts include new features “free”
  - Additional features may be “on” by default
  - May be turned on by engineers

From analog to digital (+ networked)
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) ha emesso un alert riguardo al motore di ricerca SHODAN, che può essere utilizzato per identificare i sistemi SCADA che sono connessi a Internet. Questo può essere sfruttato da parte di attacker per compromettere questi sistemi. ICS-ALERT-10-301-01 descrive una serie di raccomandazioni per ridurre questo rischio.
Internet Intelligence Collection

– Scan the corporate website, Google, and Google News
  • Who works there? What are their titles?
  • Write index cards with names and titles

– Search for Linkedin, Facebook, and Twitter Profiles
  • Who do these people work with?
  • Fill in blanks in the org chart

– Who works with the information we’d like to target?
  • What is their reporting structure?
  • Who are their friends?
  • What are they interested in?
  • What is their email address?
    At work?
    Personal email?
Hacktivists are politically motivated

A member of Anonymous at the Occupy Wall Street protest in New York*

One self-description is:
“We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.”**

"The world's leaders in high-quality entertainment at your expense."

*Source: David Shankbone  
**Source: Yale Law and Technology, November 9, 2009
Zeus Crimeware Service

© 2011 IBM Corporation
Grazie!

simone.riccetti@it.ibm.com