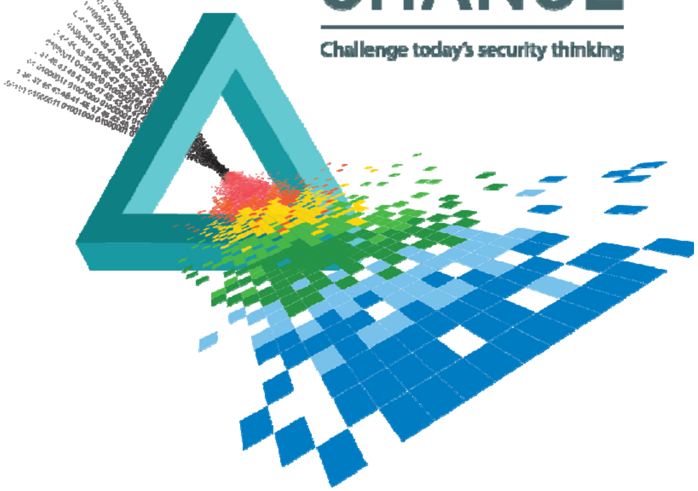
RSA®Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking



SESSION ID: SSC-W08

Smart Grid Security: A Look to the Future

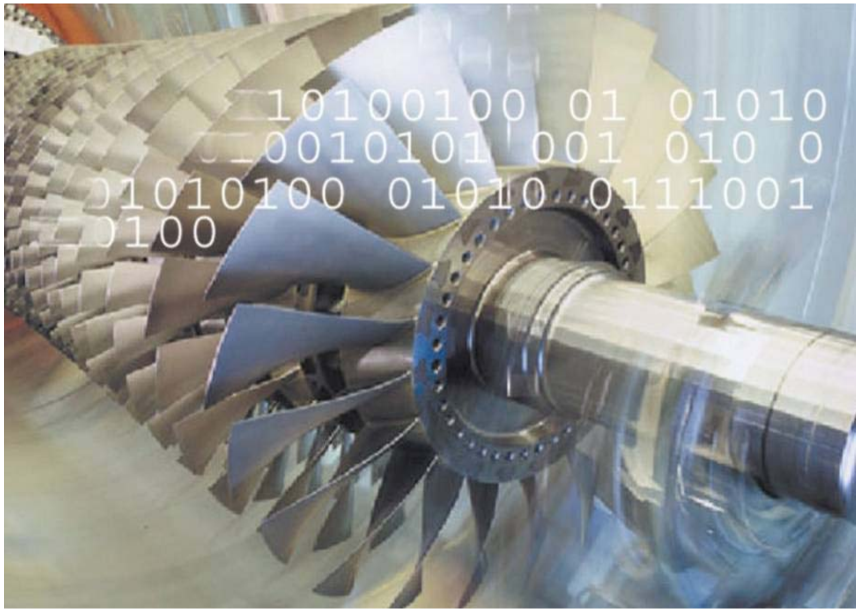
Gib Sorebo

Chief Cybersecurity Technology
Leidos
@gibsorebo

#RSAC

Overview

- Distributed Energy
- Plug-in Vehicles
- Evolving Threats: Market Manipulation, Cascading Failure Modes

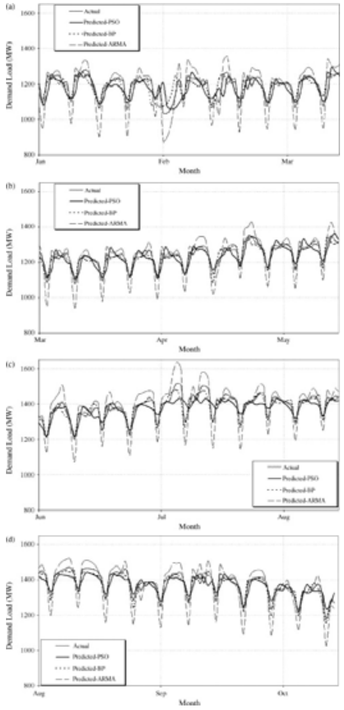


Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Depends on a sophisticated communications infrastructure to be always available
  - Needs instantaneous information
  - Often widely dispersed
  - May leverage public networks

Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Integrity of Information is Critical
  - Using complex algorithms
  - Tampering with or errors in algorithms can lead to power outages
  - Protection of the software supply chain will be critical



Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Do-It-Yourself Generation
  - Not really new
  - Potential for manipulation
  - Analogous to BotNet networks

Plug-In Vehicles: Grid to Vehicle

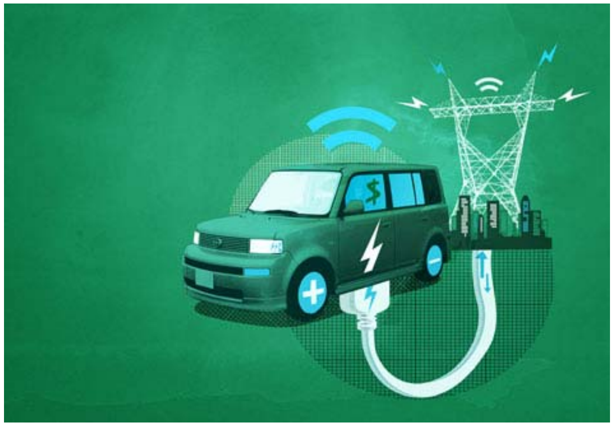
- Plug-in vehicles will require significant instrumentation and data reporting
  - Utilities will need feedback from vehicles to predict demand
  - Privacy concerns
  - Charging stations need trusted communications
  - More monitoring of traditional grid components
  - Communication with vehicle over home area network (HAN)

Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Public Charging and Roaming
  - Payment systems for charging
  - Should someone be able to roam and use their vehicle's identification number like cell phones or simply pay owner of facility without utility involved?
  - Potential for fraud and privacy issues; tax collection

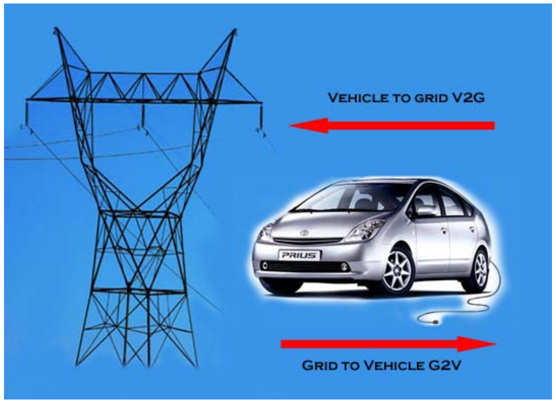
Plug-In Vehicles: Vehicle to Grid

- The Potential for Energy Storage
  - Potential boon for utilities
  - Sell back electricity
  - Need strong analytics

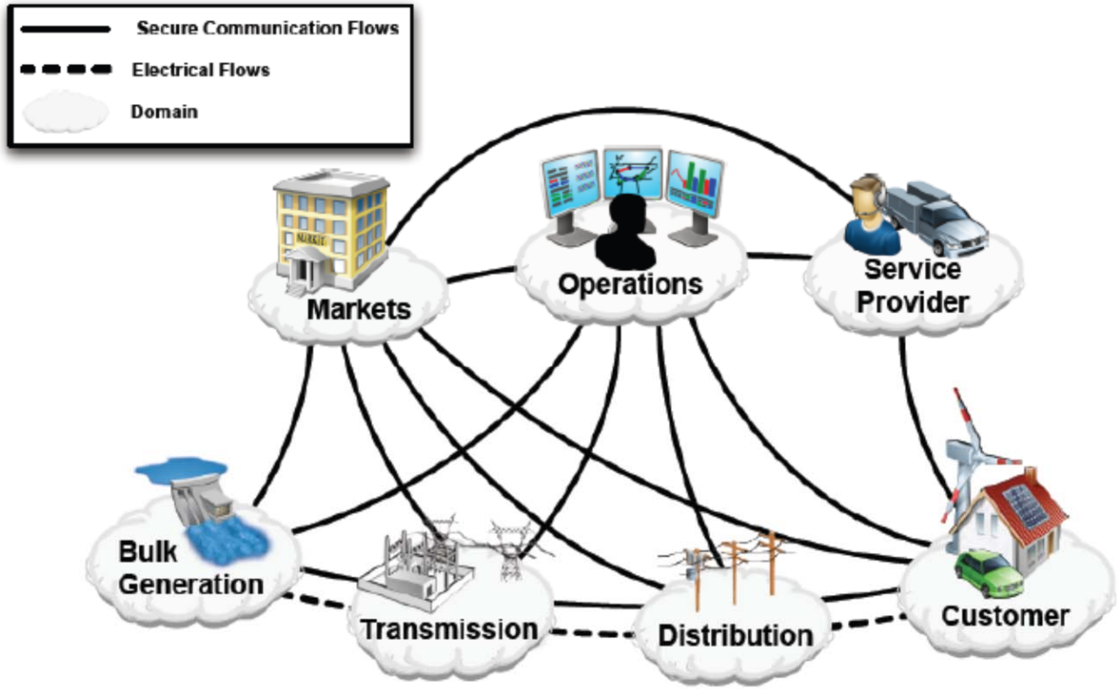


Plug-In Vehicles: Vehicle to Grid

- Cybersecurity Challenges
  - Similar to “do-it-yourself generation”
  - Vehicle identifiers
  - Privacy
  - Potential for malfunctioning vehicles to disrupt grid
  - Need a mini balancing authority



Evolving Threats: Market Manipulation, Cascading Failure Modes



NIST Smart Grid Framework 1.0 January 2010

NIST = National Institute of Standards and Technology

Evolving Threats: Market Manipulation

- Market Manipulation
  - With distributed energy resources come exchanges to buy and sell energy
  - Markets can be manipulated by obtaining generation capabilities and demand data before it is available to the general market
  - Data can be manipulated to influence markets
  - Keeping humans involved is critical

Evolving Threats: Cascading Failure Modes

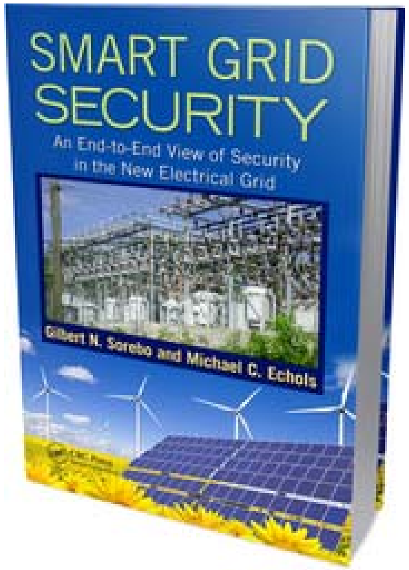
- Cascading Failure Modes
  - We have limited information of the failure modes
  - Can sensor feeds, at a high enough volume, overwhelm a system?
  - Will automation and safety protocols lead to unintended consequences
    - Yuma, Arizona, incident
  - Automated controls often need human sanity checks

Key Takeaways

- For Utilities
  - Build your architecture to support cybersecurity for future innovation
  - Assume manufacturers of consumer products won't build in adequate security
  - When creating new markets, assume someone will look to exploit them
  - Be prepared to operate in a world where you have less control
- For Residential and Business Customers
  - Don't assume the utility can protect you from whatever you connect to the grid
  - Demand that product vendors spell out how security is implemented
  - Always have a manual override and analog gauges available

Questions?

Thank You.


SMART GRID SECURITY
An End-to-End View of Security in the New Electrical Grid
Gilbert N. Sorebo and Michael C. Echols
CRC Press

Gib Sorebo

Chief Cybersecurity Technologist

tel: 703-676-0269 | *email:* sorebog@leidos.com