RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Smart Grid Security: A Look to the Future

SESSION ID: TECH-W03A

Gib Sorebo

Chief Cybersecurity Technologist
Leidos
@gibsorebo

Overview

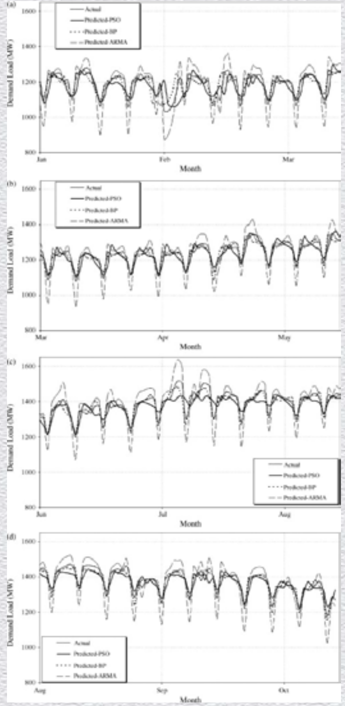
- Distributed Energy
- Plug-in Vehicles
- Evolving Threats: Market Manipulation, Cascading Failure Modes

Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Depends on a sophisticated communications infrastructure to be always available
  - Needs instantaneous information on status of generation resource, particularly wind and solar
  - Often widely dispersed from control centers and vulnerable to cable cuts and radio frequency interference
  - May leverage public networks that are more vulnerable to infiltration or bandwidth limitations

Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Integrity of Information is Critical
  - Using complex algorithms, renewable resources such as solar and wind can be dispatchable
  - Tampering with or errors in algorithms can lead to power outages when an expected power resource is not available
  - Protection of the software supply chain will be critical



Distributed Generation: Cybersecurity Threats and Vulnerabilities

- Do-It-Yourself Generation
  - People have been able to sell back power to utility for decades, but not at any scale
  - Potential for manipulation of generation data or even intentional disruption of grid
  - Analogous to BotNet networks; if malicious actors can control thousands of micro-generation sites, the consequences could be significant

Plug-In Vehicles: Grid to Vehicle

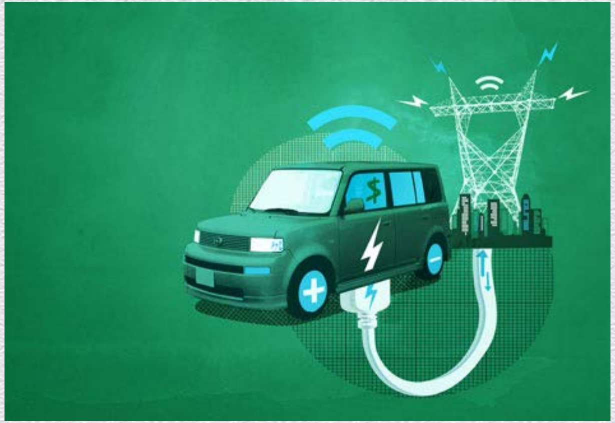
- Plug-in vehicles will require significant instrumentation and data reporting
  - Utilities will need feedback from vehicles to predict demand
  - Potential privacy concerns will need to be addressed
  - Charging stations need trusted communications infrastructure and data reporting
  - More monitoring of traditional grid components
  - Communication with vehicle over home area network (HAN) needs higher level of protection

Plug-In Vehicles: Grid to Vehicle

- 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

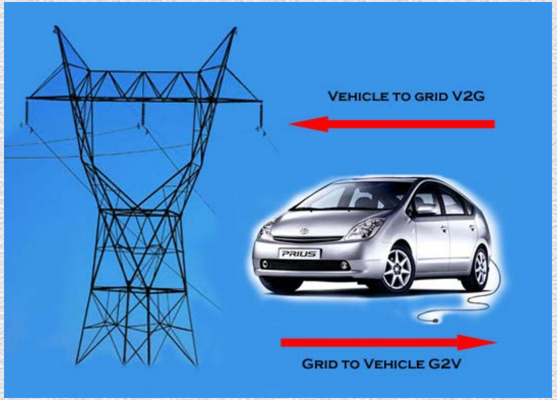
Plug-In Vehicles: Vehicle to Grid

- The Potential for Energy Storage
  - Utilities can draw from potentially thousands of energy storage resources without having to pay for the capital costs
  - Vehicle owners have option to sell back electricity during peak times and charge during low peak
  - Requires vehicle owner to accurately predict driving habits and for battery technology to inform the utility of the available power in real time

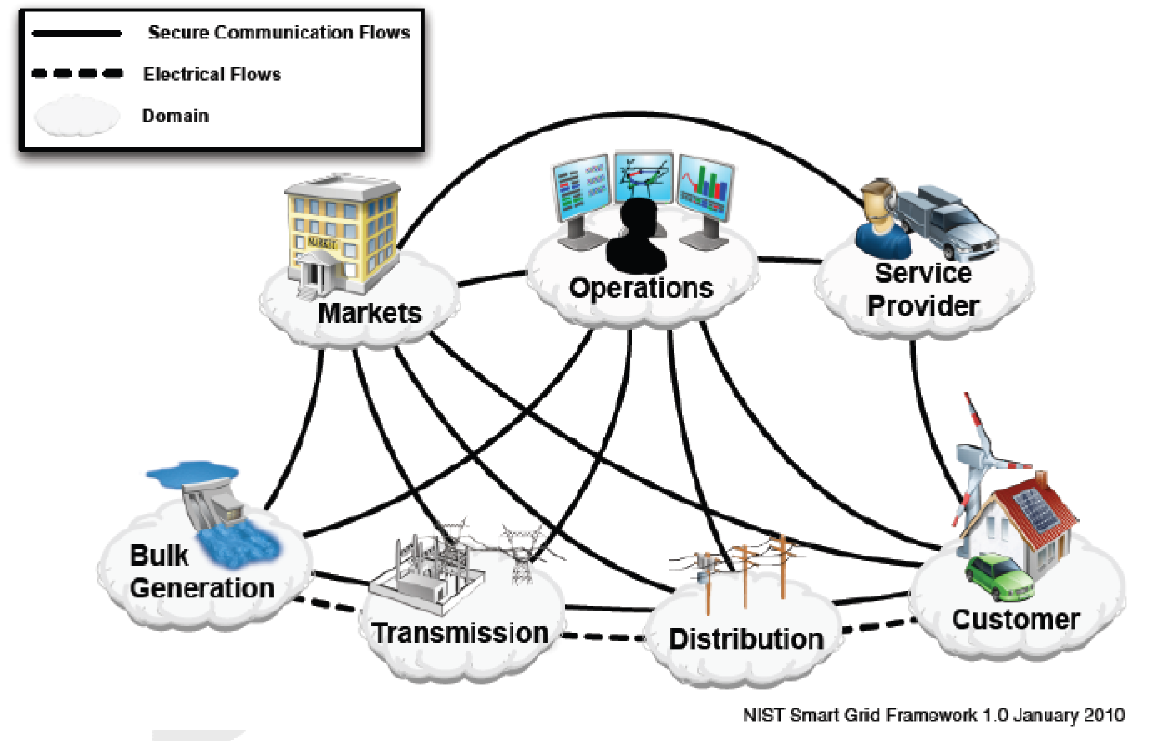


Plug-In Vehicles: Vehicle to Grid

- Cybersecurity Challenges
  - Similar to “do-it-yourself generation;” people can send false information to manipulate how much a utility thinks it is paying for
  - Someone else’s vehicle identifier could be stolen or hacker could manipulate whose power is used
  - Potential for privacy issues
  - Potential for malfunctioning vehicles to disrupt grid
  - Need a mini balancing authority for vehicles and a reliable system for detecting abuse



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

Evolving Threats: Cascading Failure Modes

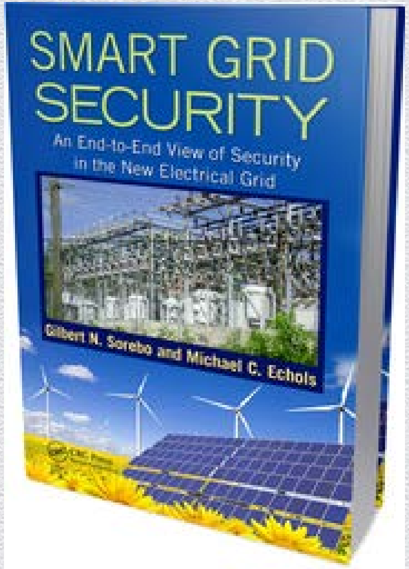
- Cascading Failure Modes
  - We have limited information of the failure modes of many new and critical devices on the distribution and transmission side
  - Can sensor feeds, at a high enough volume, overwhelm a system?
  - Will automation and safety protocols lead to unintended consequences such as the Yuma, Arizona, incident; protection devices seek to prevent further damage but cause more
  - 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

Available at the RSA Bookstore

Gib Sorebo

Chief Cybersecurity Technologist

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