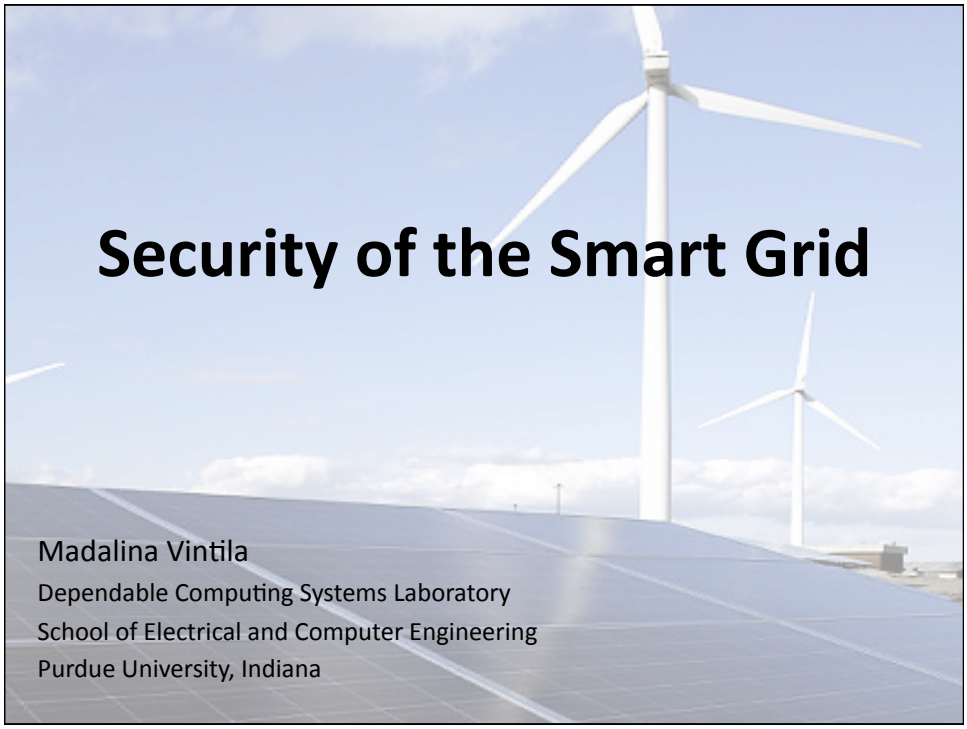


Security of the Smart Grid

Madalina Vintila
Dependable Computing Systems Laboratory
School of Electrical and Computer Engineering
Purdue University, Indiana

Overview

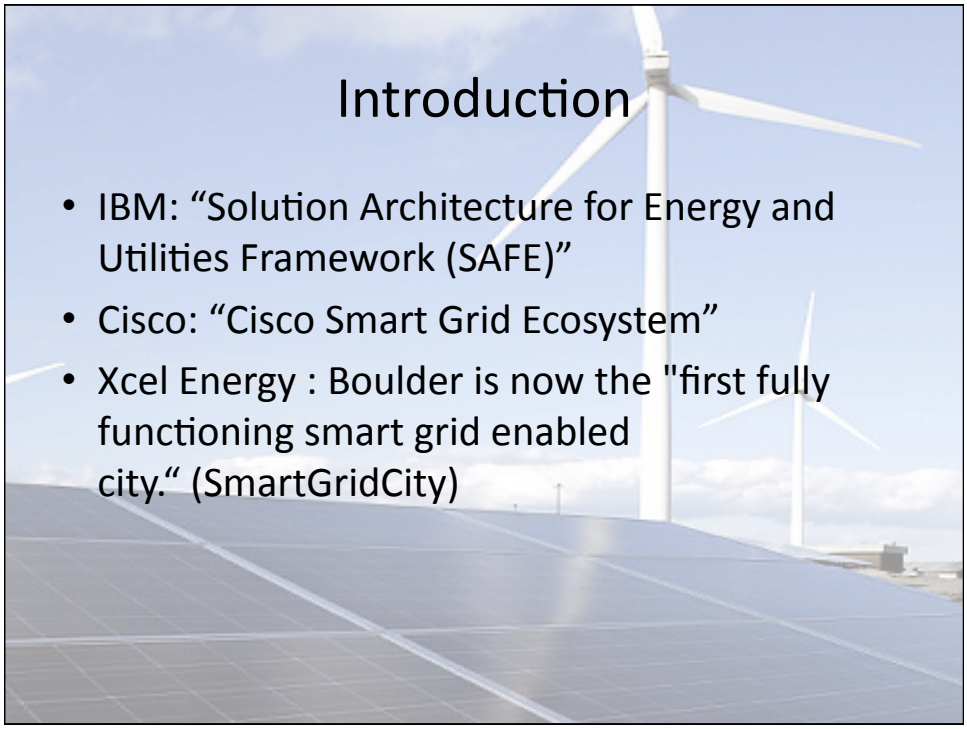
- Introduction
- Security Insights
- Smart Grid Security
- Conclusions

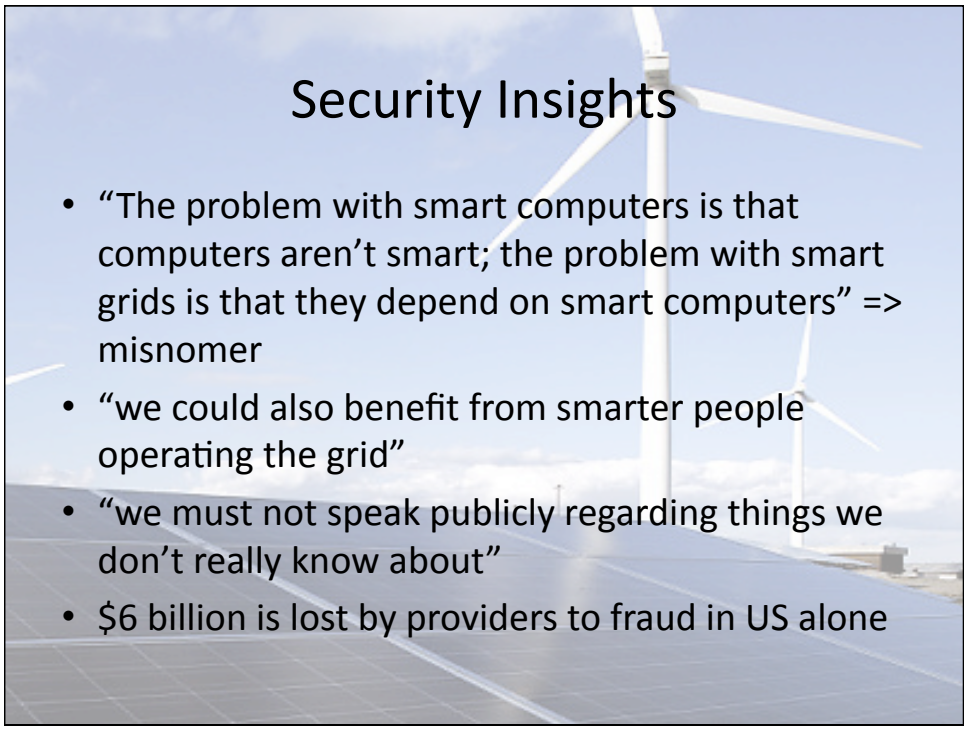
Introduction

- What is a Smart Grid?
  - A **network** which delivers electricity using digital technology with two-way communications
  - SCADA: supervisory control and data acquisition (every 1-2 min)
  - PMUs: phasor measurement units (30-60 /sec)
  - A neighborhood collector device <-> wireless mesh network of individual home devices
  - $4.5 billion for smart grid technology development

Introduction

- Why a Smart Grid?
  - For consumers:
    - Consumer appliances can be controlled to save energy, reduce cost
    - Increased delivery reliability
    - Better transparency
  - For providers:
    - Time-of-use pricing
    - Track usage as a function of time of day
    - Disconnect customers via software
    - Alarms in case of problems


Introduction
• IBM: “Solution Architecture for Energy and Utilities Framework (SAFE)”
• Cisco: “Cisco Smart Grid Ecosystem”
• Xcel Energy : Boulder is now the "first fully functioning smart grid enabled city.“ (SmartGridCity)

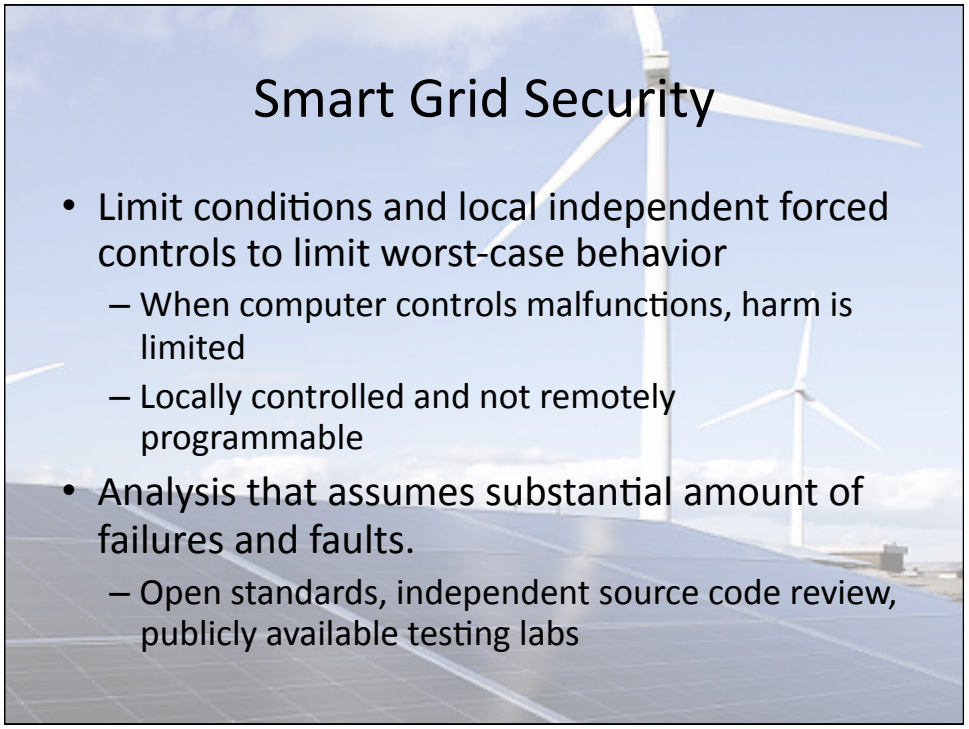

Security Insights
• “The problem with smart computers is that computers aren’t smart; the problem with smart grids is that they depend on smart computers” => misnomer
• “we could also benefit from smarter people operating the grid”
• “we must not speak publicly regarding things we don’t really know about”
• $6 billion is lost by providers to fraud in US alone

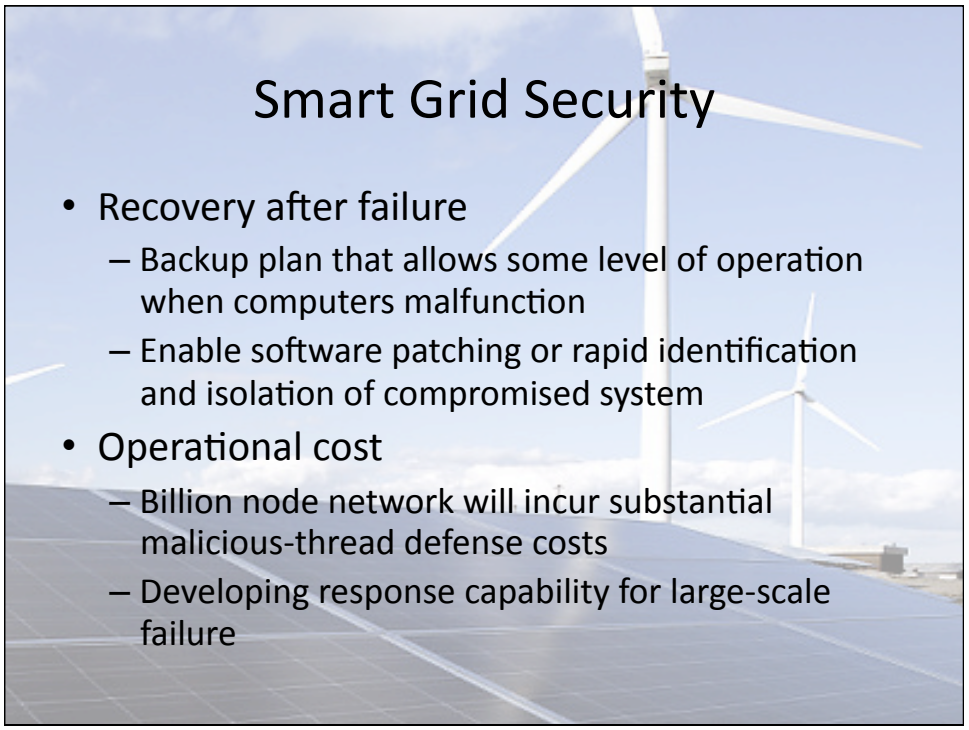
Security Insights

- Home attack scenarios:
  - Detection of when occupants are not home (privacy)
  - Power down alarm systems
  - Slowly alter environmental conditions to defeat sensors
  - Shut down airflow and turn gas on a stove
- System-wide attacks:
  - Routing infrastructure attacks
  - Denial-of-service attacks
  - Cascade failures

Smart Grid Security

- Reverse current trend of controllers to become increasingly general-purpose:
  - General-purpose computer is an enabler for new functionality (including unintended)
  - Murphy's Law
- Limit system interfaces
  - Examine input and allow only within safety boundaries of current state


Smart Grid Security
• Limit conditions and local independent forced controls to limit worst-case behavior
– When computer controls malfunctions, harm is limited
– Locally controlled and not remotely programmable
• Analysis that assumes substantial amount of failures and faults.
– Open standards, independent source code review, publicly available testing labs


Smart Grid Security
• Recovery after failure
– Backup plan that allows some level of operation when computers malfunction
– Enable software patching or rapid identification and isolation of compromised system
• Operational cost
– Billion node network will incur substantial malicious-thread defense costs
– Developing response capability for large-scale failure

Smart Grid Security

- Government regulations for consumer protection
  - Similar to Health Insurance Portability and Accountability Act (HIPAA)
  - Guide for how consumer data is collected and to whom it may be exposed
- Cryptographic key management
  - X.509 certificate for device identification (currently lifetime value, should periodically update)
  - Current servers cannot support computation necessary for periodic cryptographic key updates

Smart Grid Security

- Effective Cybersecurity Solutions
  - Confidentiality, integrity, **availability**
  - Efficiency and scalability
  - Adaptability and evolvability
- Transmission substations – 4 ms delivery requirement
  - Efficient authentication algorithms
  - Avoidance of buffering packets
  - Packet-loss tolerance, small communication overhead

Smart Grid Security

- Policy-based data sharing
  - Wide-area measurement systems
  - GPS-clock-synchronized fine-grained measurements to provide stability and reliability
  - Securely sharing measurements (trusted third parties)
- Attestation for constrained smart meters
  - Ensure that software is authentic
  - Cost, power, memory and computational limitations

Conclusions

- Several open-ended questions remain
- Much research is still needed in this area

- "The security community must become well informed on electrical-power-system and power infrastructure issues, and
- The power engineering and operations community must welcome the security community and its vast body of knowledge of what can go wrong and how to drive security into the grid"

Sources

1) Cohen, F.; , "**The Smarter Grid**," Security & Privacy, IEEE , vol. 8, no.1, pp.60-63, Jan.-Feb. 2010.
2) McDaniel, P.; McLaughlin, S.; , "**Security and Privacy Challenges in the Smart Grid**," Security & Privacy, IEEE , vol. 7, no.3, pp.75-77, May-June 2009.
3) Khurana, H.; Hadley, M.; Ning Lu; Frincke, D.A.; , "**Smart-Grid Security Issues**," Security & Privacy, IEEE , vol.8, no.1, pp.81-85, Jan.-Feb. 2010.