Security Considerations for the Smart Grid

Carl A. Gunter
University of Illinois
Trustworthy Cyber-Infrastructure for Power (TCIP)

- NSF “center-scale activity” awarded in 2005 to the University of Illinois
- General coverage
  - Devices
  - Networks
  - Load control
  - Modeling and simulation
- Renewed with DoE support in 2009 as TCIPG
Sample TCIP Research Projects

**Automatic Assessment**
- Zahid Anwar, Ravinder Shankesi, Roy. H. Campbell
- DSN 2008
- A collection of models and tools to enable quantitative analysis of trade-offs for security protections especially for power grid operations.

**Attested Meter**
- Michael LeMay, Carl A. Gunter
- ESORICS 2009
- An architecture and prototype for practical remote attestation for residential power meters.
Automatic Assessment Tool Chain

Module 1: Converting CIM XML to Prolog Tool
- CIM to Prolog Tool
- Security Enhanced CIMXML

Graph Generation
- Network Model
- Prolog Rules
- ConstructAttackGraph

Module 2: Representing Recovery Activities as YAWL Workflows
- Grounded? Yes
- Energize Transformer
- No
- Ground Transformer

Module 3: Converting YAWL XML to Maude
- XML to Maude Tool
- Maude Workflow

Module 4: Advisory Generation
- YAWL Model Checking

Module 5: Updating Attribute State from PowerWorld
- Event Aggregator
- EvaluateAttackRisk
- Risk Calc
Cumulative Remote Attestation

<table>
<thead>
<tr>
<th>Data Acquisition</th>
<th>Local Storage on Sensor</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data may not be accurately recorded.</td>
<td>Stored data may be corrupted or deleted.</td>
<td>Data may be withheld or misreported.</td>
</tr>
</tbody>
</table>

Attacks detected by normal attestation

Attacks detected by cumulative attestation
Some Research Issues for the Future

- Managing keys for large numbers of small processors
- Providing an integrated model for the power network and the data network
- Real time security
- Outlier detection with malicious intruders
The Internet in the Smart Grid

• How is it possible to assure reliable power systems when using the Internet?

• Are the Internet protocols appropriate for use in the Smart Grid?

• Given a clean slate for networking, is the Internet architecture the best choice for the Smart Grid?
What to Look Out For

• New ideas, some silly but some potentially transformative. Keep an open mind on research ventures.

• The next generation of students.