Information Security and the Electric Power Industry

A Presentation to the Fourth Workshop on Computer Misuse and Anomaly Detection (CMAD-IV)

Ab Kader

Ron Skelton

Electric Power Research Institute (EPRI)

Presentation Overview

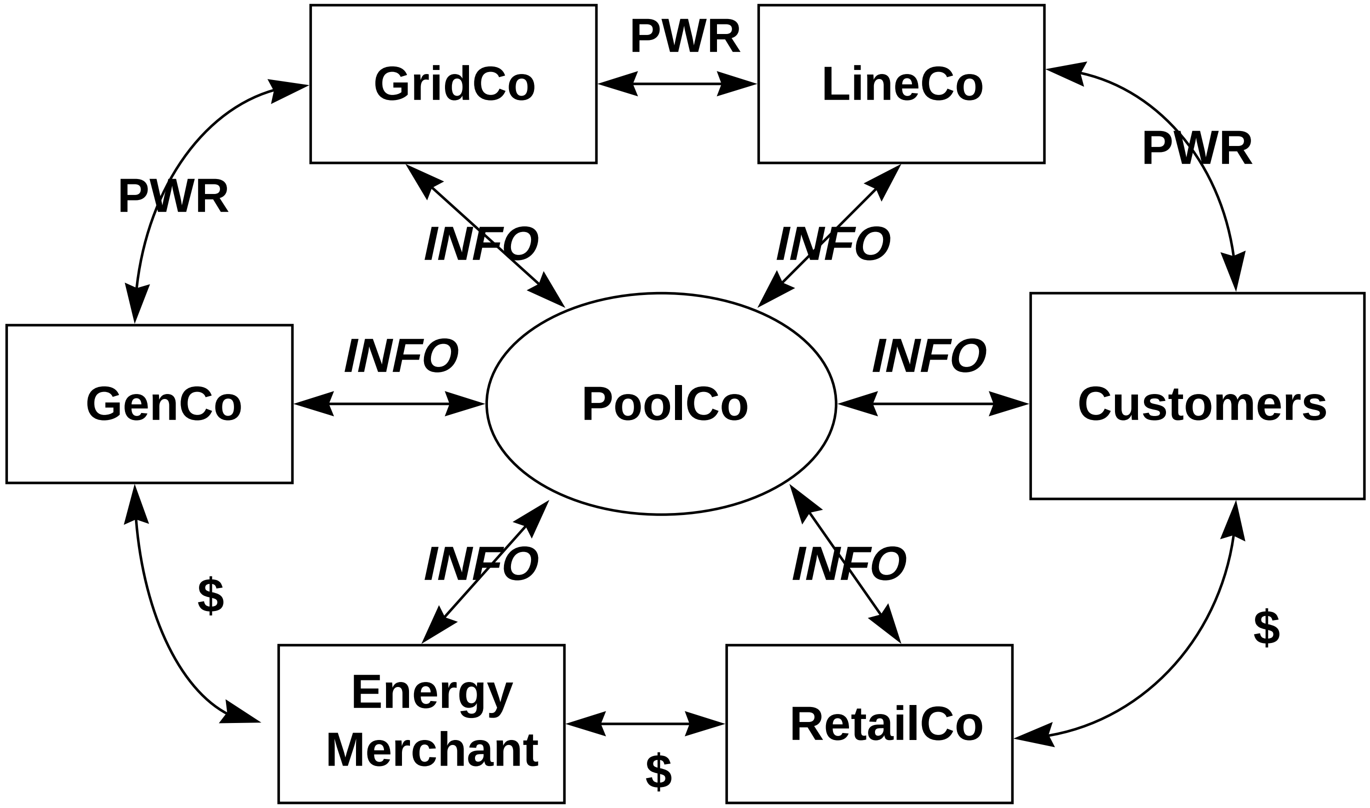
- The Challenge
  - Why do Electric Utilities have a security problem?
- The Response
  - What is EPRI doing about it?
- Future Work
  - Where do we go from here?

Utility Information Networks

Utility Information Networks

- Corporate: generic (& utility specific) back office processing.
- Power Plant: generation control & communication systems.
- Control Center: interface between generation & transmission.
- Transmission: SCADA and EMS.
- Distribution Automation: remote monitoring and control of distribution substations.
- Customer Interface: remote communication with devices at customer sites.
- External: other utilities, power pools, vendors etc..

Utility Industry “Future”



Richard Abdoo, CEO WEPCo
Public Utilities Fortnightly, 2/15/95

“Future” Is At Hand

- Federal Energy Regulatory Commission (FERC) 889
  - information on transmission availability and prices.
  - equal access for wholesale sellers and purchasers.

EPRI ⇓

- Open Access Same Time Information Systems (OASIS)
  - internet based information system.
  - encryption and digital certificate based security.

OASIS Nodes

EPRI Security Initiatives

- Information Security Workshop
  - Utility Security Survey (NSTAC)
  - Utility Security Assessment (Battelle)
  - Utility Security Policies (EPRI)
  - Security Tutorial (MIS Training)

- Information Security Applications
  - Power System Security (LANL)
  - Residential Customer Security (LANL)

Security Survey Highlights

- Willing to share security incident information.
- Believe “private nets” are secure.
- Trend towards less secure “public nets”.
- Concerned more about internal threats.
- Widespread lengthy electric grid disruptions unlikely.
- Security protection and audit practices inadequate.
- Internal priorities limiting attention to security concerns.
- 90% expressed a desire of ongoing EPRI involvement.

Security Assessment Conclusions

- Growth and reliance on information technology increases security threats.
- Business climate does not foster adequate security protection measures.
- Electric utility industry trends introduce new ill understood security vulnerabilities.

Security Policies Universe

Inter Control Center Communications Protocol (ICCP)

Internet Based Home Energy Management Pilot

Next Steps

- Real time intrusion detection
  - research techniques for protecting power dispatching and trading, utility customer communications....

- Incident response handling
  - security incident reporting, resolution, and information dissemination (anonymously, if so desired).

- Security testing center
  - penetration testing and security auditing services customized for electric utilities.