Smart Grid Security: Build in Now or Blackout Later

Presented by: Ernest Wohnig

November 3, 2009

Booz | Allen | Hamilton

delivering results that endure

Discussion Themes

- Current Detect / Protect model breaks down when Assurance and Resilience are preeminent objectives
- New Governance, Software, and Data Analytic Models/Methods will be Key to a Secure Grid
- Layered Grid Architecture Roadmap is Required
- Summary
- Q&A

Threats / Vulnerabilities in a Smart Grid Environment

- **Threats**
  - The usual (but ever evolving) suspects: Nation States, Organized Crime, Hacker Groups, Lone Wolf, Insider
  - The not so usual suspects: the Backhoe Terrorists, Suicide Squirrels, Rouge Routers
- **Vulnerabilities**
  - Environmental Threats: Blurred Boundaries, Grid Maturity Stratification, and Data Volume / Data Flow
  - Inadequate Protocols: Configuration Management, Asset Identity Management, Data Integrity

Security Needs Survivability

Current paradigm for security: detection + reaction

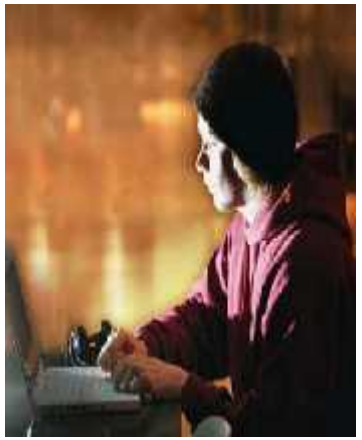
- **Detect:**
  - Logging (events)
  - Auditing (usage)
  - Sensing (anomalies, intrusions)
  - Monitoring (functioning)
- **Protect: "defense in depth"**
- **Respond:**
  - Minimize extent, intensity, duration of impact, and likelihood of recurrence by:
    - Blocking certain types of inputs
    - Terminating user sessions
    - Shutting down some or all functionality
    - Terminating some or all network connections
    - Assessing damage; attempting to recover to pre-incident state

* Unavoidable: response/recovery affects dependability

Security needs survivability cont'd

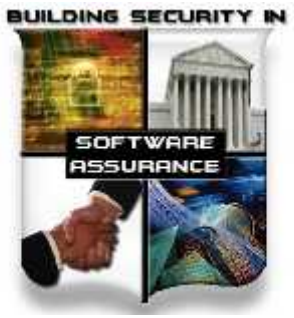
Why detect-protect-respond model is "broken"

- Adversaries are becoming:
  - Too skilled
  - Too expert
  - Too quick: new attack strategies and mechanisms are emerging faster than countermeasures
- Delivery systems have little tolerance for delays associated with post-incident recovery
- Systems and software must have the ability to "fight through"—and *survive*—intrusions and attacks



Retro fitting an old security paradigm into a new smart grid compromises the future.

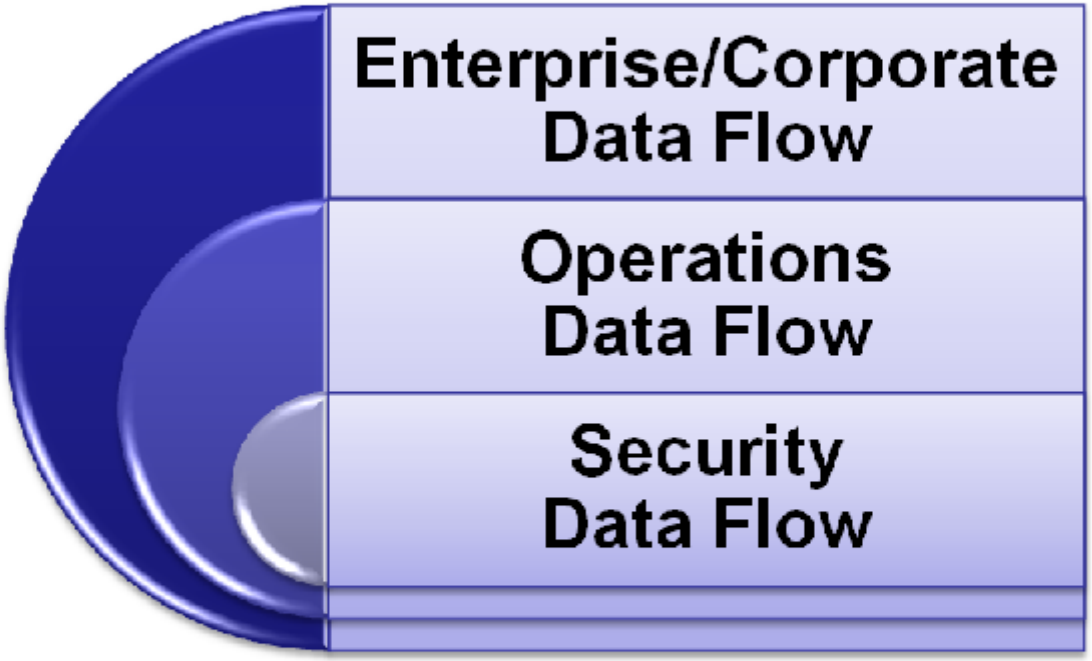
IT/Software Supply Chain Management is Critical to the Grid



- Adversaries can gain “intimate access” to target systems, especially in a global supply chain that offers limited transparency
- Advances in computer science and technology will always outpace the ability of government and industry to react with new policies and standards
  - National security policies must conform with international laws and agreements while preserving a nation’s rights and freedoms and protecting a nation’s self-interests and economic goals
  - Forward-looking policies can adapt to the new world of global supply chains
  - International standards must mature to better address supply chain risk management, IT security, systems, and software assurance
- IT/software suppliers and buyers can take more deliberate action to enhance the security of their processes and practices to mitigate risks
- Government and industry have significant leadership roles in solving this issue

Governance – Multiple Data Flow within a Multi-Ownership Environment

- Multi-Data Flow Issue
  - Operational and Corporate
  - Increase bandwidth requirements for Security Component ?
- The legacy (Geological) Issue
  - Not starting from a green field
  - How do we manage the migration and integration?
- The Multi (1000s) Ownership Issue
  - Existing stakeholders
  - Renewable Suppliers
  - Household generators

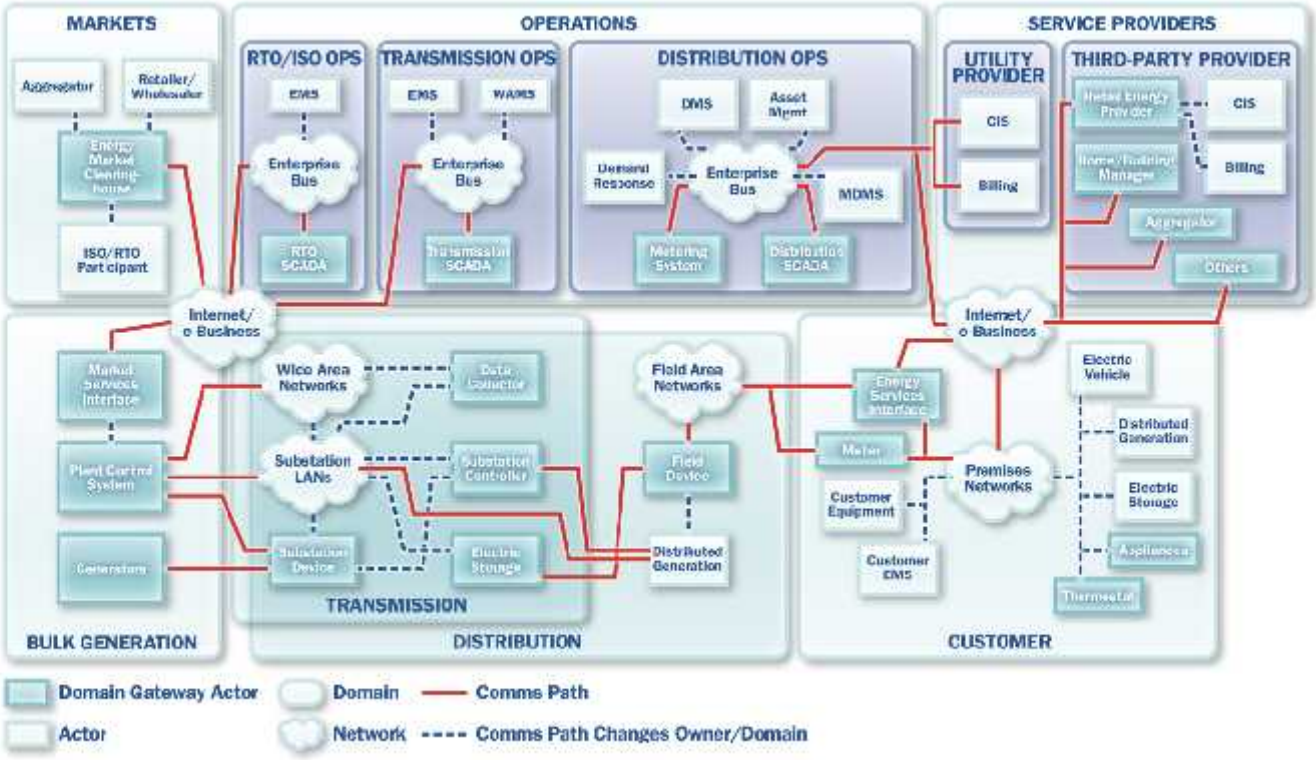


What happens if billions of dollars in investment are ungovernable ?

Need a data tiering and aggregation strategy across the Grid

Trouble Shooting and Incident Response Complexities in a Smart Grid Environment

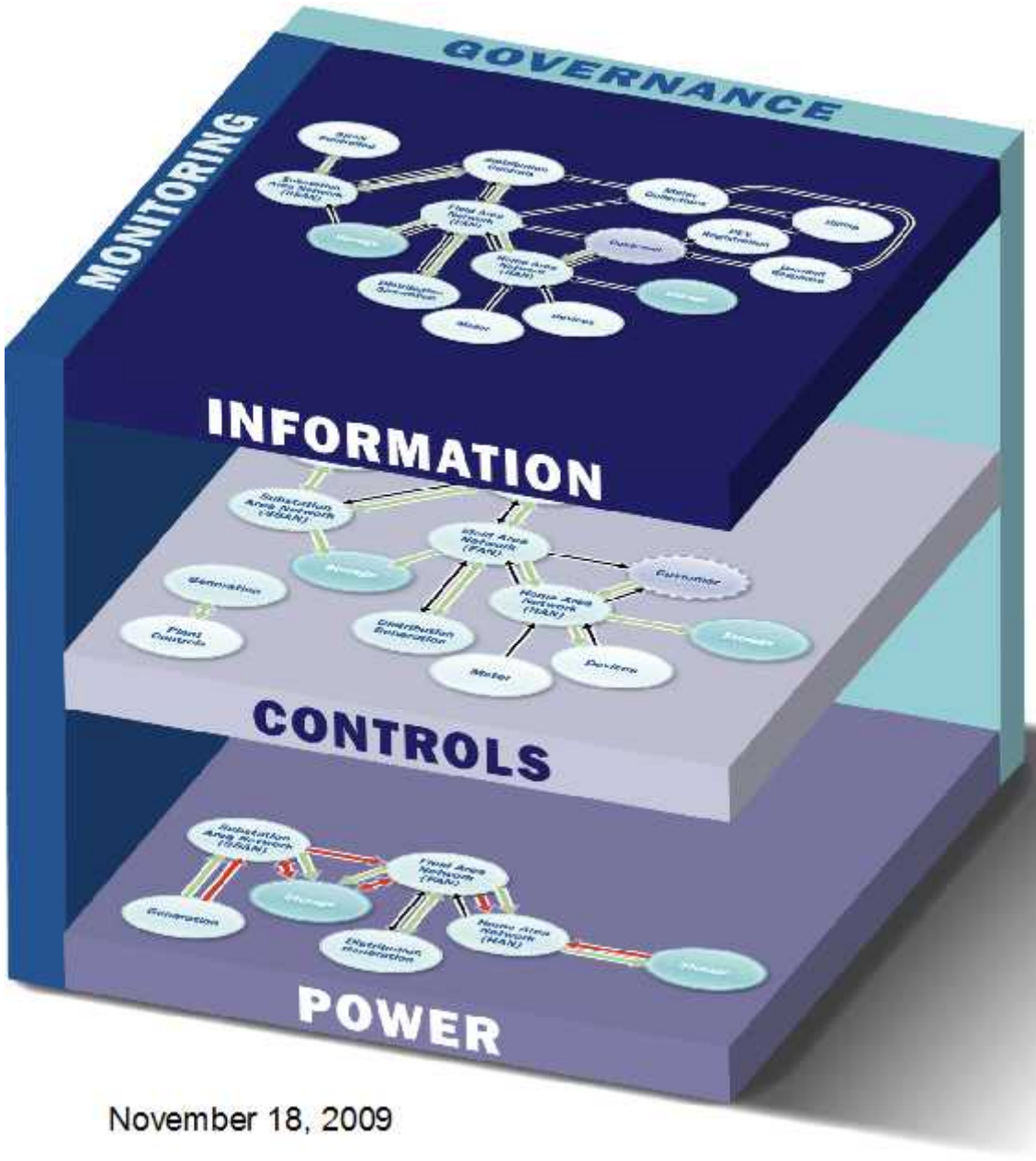
- Trouble Shooting
  - New requirements/uses
  - Across network and physical asset components
  - Across boundaries
  - Legacy interconnect issue
  - Minimizing impact of software/hardware changes
- Incident Identification & Response (Who/What/ Where)
  - Legislation/ Regulation/ Standards
  - Stakeholders
  - Diverse Technology Ecology
  - Boundary/jurisdiction issues



Architecting in an Assurance & Resilience Environment

- Security Needs Survivability
- System vs. Software-Level Security Focus
- Software Security Design Considerations
- Software Engineering to Achieve Survivability
- Injecting Security Into the Reliance-Critical Smart Grid Life Cycle

Layered, Secured, and Evolving Architecture Does Not Occur Without a Plan



- The blueprint for the Grid architecture needs to be established
- A strong governance process needs to be in place to manage change
- Layered and segmented architecture is a critical success factor
- Proper continuous monitoring of component behavior must be incorporated into each device added to the Grid
- An evolving trust model for security based on behavior is required to secure the Grid

Architecture Roadmap Sets the Course for the SmartGrid in Terms of Design Principles

- **Evolving Layered Architecture**
  - No single point of failure
  - Comprehensive defense-in-depth/breadth design
  - Simplified component design
  - Secure/trusted messaging between components

- **Security and Resilience-Based Design**
  - Governance-controlled technology vetting process
  - Evolutionary trust model
    - Grant trust based on capability and capacity
    - Trust independently identifiable devices
    - Monitor device behavior
    - Behavior-based access controls: enable verifiable trust

In Summary…

- SmartGrid governance involves more than standards
- Smart Grid security threat environment will grow in complexity, intensity, proliferation, and unpredictability; therefore, a behavior-based evolving trust model is required to maintain security
- Current detect-protect-respond paradigm is inadequate
- The SmartGrid imperative is the need for an architecture that can “fight through” security threats for survival rather than depending on point-level security solutions
- Elements of the SmartGrid architecture roadmap:
  - A layered security-in-depth/breadth strategy
  - Information at the right levels in the right quantity
  - Advanced analytics
  - Simplicity must be maintained where ever possible

SmartGrid is a MegaCommunity challenge requiring MegaCommunity thinking and solution development