Informal briefings organized by the American Association for the Advancement of Science (AAAS) Center for Science, Technology and Security Policy at the U.S. Capitol for Homeland Security Committee members and staff of the United States Senate and the House of Representatives, Washington DC, 14 February 2008

International and Domestic Defenses Against Cyber Attacks

Seymour Goodman, Ph.D., Professor of International Affairs and Computing at Georgia Tech and recent chair of the National Research Council's Committee on Improving Cybersecurity Research in the United States

Stephen Lukasik, Ph.D., former Director of DARPA, Chief Scientist of the FCC, and vice president of several major high tech companies

Anthony Rutkowski, JD, Vice President for Regulatory Affairs and Standards at VeriSign, and a former senior staff member at the FCC and the International Telecommunication Union (Geneva)

Dependencies, Vulnerabilities, Risks

- The United States, and many other countries, are extensively and increasingly dependent on the internet and other internet-like networks (collectively referred to as "cyberspace") to enable and support innumerable economic, social, and government activities
- Cyberspace has become a critical global infrastructure in its own right and an important component of most other critical infrastructures and sectors including electric power, transportation, banking and finance
- The networks of cyberspace are deeply riddled with flaws and vulnerabilities that are being, or could be, exploited by an unprecedented spectrum of malicious parties
- These flaws are also the basis of accidents and irresponsible actions by non-malicious parties, further raising issues of safety and reliability, not just security
- Almost everyone, and every place, in the U.S. is thus subject to disruptions that range from identity theft and other massive low-level economic impacts to those that could have major national and homeland security consequences
- The increasing use of internet IP based networks as a replacement for protected legacy telecommunication infrastructure and services makes the potential adverse consequences even more severe

Trends and Deficiencies

- **The overall security situation is bad and getting worse**
- **New technology is helpful, but is not being introduced as extensively and effectively as we might hope and is not enabling the great majority of the user and provider populations to keep up with increasingly potent threats**
- **Markets are pushing people to greater dependencies, but not to comparably greater security**
- **The nature and extent of the problems are such that we do not see any magic bullets from new technology or from the market**
- **Slowing and reversing the current situation and trends is going to be a long, perhaps endless, battle requiring an ongoing infusion of new technology and evolving market pressures**
- **New government interventions will also be necessary, and they will need to be aggressively considered and pursued**

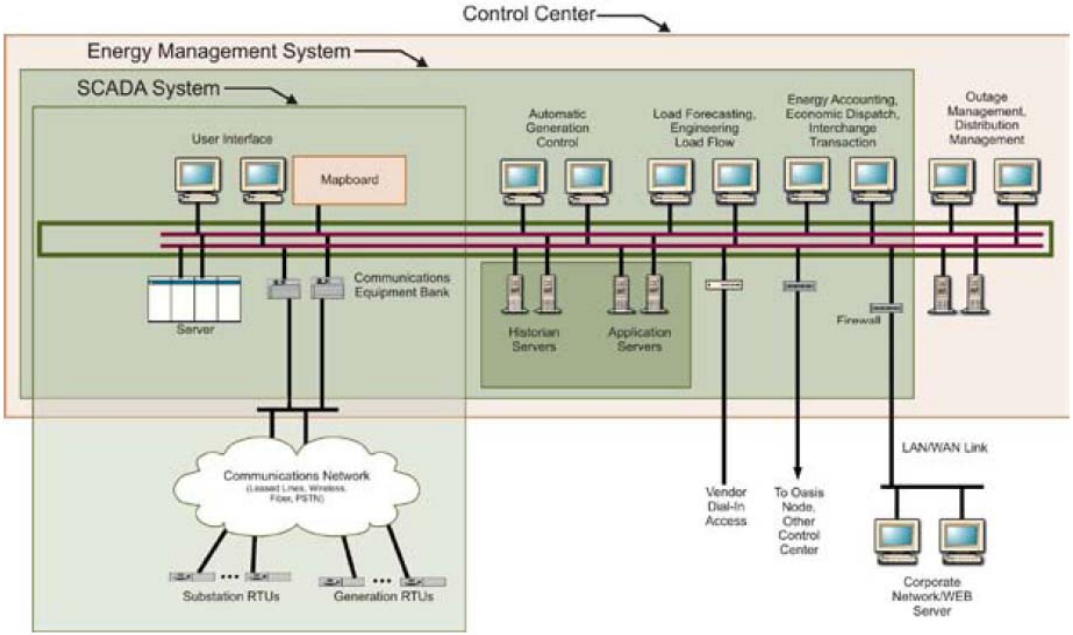
Examples of Interventions or Requirements Already Considered

- Required reporting of data breaches
- Limited liability for fraudulent credit card charges
- Anti-SPAM efforts
- Halting system vulnerabilities in new aircraft
- Regimes for international cooperation

Some cyber environments are more important than others

- Electrical power infrastructures
  - Cyber access to control rooms provide paths for outsider attack directly and through control nodes
  - Large components (e.g., generators and transformers) which are difficult to replace can be completely destroyed
  - Attack modes are low-risk, high-yield
  - Effects on society are significant
- Financial and telecommunication infrastructures
  - Have even greater vulnerabilities due to increased use of common open Internet platforms
  - Information-telecommunication infrastructure management is increasingly being outsourced offshore
- Military and government network infrastructures
  - Constantly being probed for entry points to yield intelligence

Electrical power infrastructures have multiple vulnerable points of entry



- Connections of remote operating devices (SCADA)
- Energy management – the real control system
- Emergency outage management
- Energy trading system (OASIS)
- Vendor and support contractor systems
- Corporate enterprise management systems
- Other control centers networked together

One Solution – Limit Access

Create a cyber "air gap" and apply "two-man" rule

- Defense against cyber **Outsiders**
  - Separate control centers and nodes of the operational power grid from the information internet
  - Eliminate all connections between operational grid and enterprise management systems, vendors, and contractors
  - Eliminate wireless connections between nodes and control centers
  - Enforce regulations through live testing

- Defense against cyber **Insiders**
  - Operator vetting
  - Fault-tree models to determine actions designated for monitoring and two-man rule
  - Two-man rule on predetermined actions
  - Automated monitoring of control room actions
  - Collection of forensics and development of behavior models

Significant infrastructure protection model action recently taken

- ***Mandatory Reliability Standards for Critical Infrastructure Protection***, Federal Energy Regulatory Commission, Final Order 706, 18 January 2008
  - http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf
  - Substitutes mutual distrust for trust
  - Defense-in-depth security architecture mandated
  - However, it fails to deal with managed mutual distrust among interconnected control centers and early warning opportunities through analyses of probes
  - Associated Cyber Security Standards,
    - http://www.ferc.gov/industries/electric/indus-act/reliability/cip.asp#skipnavsub
    - CIP-002-1 Critical Cyber Asset Identification
    - CIP-003-1 Security Management Controls
    - CIP-004-1 Personnel & Training
    - CIP-005-1 Electronic Security Perimeters
    - CIP-006-1 Physical Security of Critical Cyber Assets
    - CIP-007-1 Systems Security Management
    - CIP-008-1 Incident Reporting and Response Planning
    - CIP-009-1 Recovery Plans for Critical Cyber Assets
- See also
  - **Trust in Cyberspace**, Fred B. Schneider, (Ed.), National Academy Press, Washington, D.C. 1999
  - **Roadmap to Secure Control Systems in the Energy Sector**, Energetics, January 2006
    - http://www.energetics.com/csroadmap/index.aspx

Where is trust and security in telecommunication – IP networks?

- Threats and Abuses Abound
  - Cybersecurity threats, identity theft, attacks on government and utility networks, SPAM, large scale fraud, loss of emergency network capabilities, cyberstalking, CallerID spoofing, etc.
  - In U.S. alone for 2006, FBI reported 200,000 complaints with $200M loss - for consumer fraud alone
  - Doesn't even begin to deal with threats to national network infrastructure and security
- How We Got Here
  - Historically trust was provided by closed, fixed networks with Title II regulation
  - In the 1990s, the "perfect storm" for infrastructure and consumer vulnerability struck
    - Open public networks (e.g., Internet) without security, ubiquitous wireless, nomadicity, globalization, and abandonment of Title II regulation without a common trust infrastructure
- Action Needed Now
  - Situation is now exponential; the consequences will get much worse without effective remedy
  - Threats are global and governments worldwide want solutions

Fixing the trust challenge

- Develop a Flexible, Universal, Global Means for Provider Trust
  - Focusing on providers enables concentration on achievable solutions
  - All parties (government, business, and consumers) have a shared interest in implementing provider trust capabilities
  - Enables trust and effective compensation among all providers and enhances efficiency
  - Potentially enhances privacy and other consumer needs
- Government Involvement is Key
  - Regulatory, contract, tort, copyright, treaties plus the marketplace worldwide can drive common trust solutions
  - Marketplace/industry, technology, R&D, or national action alone, will NOT solve the problem
  - Criminal law and voluntary guidelines do not solve the underlying problems
  - The technology exists. Leadership commitment, cooperation, and implementation are the problems.
  - ITU Radio and Telecom Regulations mandate infrastructure protection capabilities
- Broad government-industry cooperative action nationally and globally are essential

ProviderID: a solution for enabling trust

- Trusted Service Provider (SPID) initiative emerged recently under global intergovernmental-industry auspices (ITU-ISO)
  - Followed more than a year of meetings and collaboration among scores of different organizations dealing with Identity Management
  - SPID standards and demonstration slated for 2008
- Capability also a DOD Global Information Grid (GIG) architecture mandate that may serve as the model for national infrastructures
- SPID is simple, stable, open, low-cost, self-funding, regulatory-minimal
  - Assign a SPID identifier to every provider worldwide, together with implementing a trusted registry based SPID Name System that allows instant lookup of "trust resources" concerning the provider
  - Enables all other providers and users to make trust decisions when relying on a provider's identity and assertions
  - Fosters a means for trust resource services innovation and development
  - Built on existing, distributed, robust, open "resolver" platforms (no centralized databases) using network of trusted SPID registrars worldwide who are also part of the trust system
  - Allows a universal, global, identifier to be used for providers – itself a significant value
  - Trivial costs the can be covered in existing agency programs and user self-funding mechanisms

- ProviderID Act of 2008. Congress should require FCC, FTC and other agencies institute a universal global Trusted SPID capability in appropriate legislation
  - Consider a section addition to the *CallerID Act of 2007* now in the Senate