Towards a Healthy Cyber Ecosystem

Workshop Proceedings

Session Overview

On June 30, 2010, the Office of the Deputy Undersecretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security sponsored a workshop to explore ways to build a fundamentally more secure cyber ecosystem for users, machines, and applications. A draft white paper entitled "Towards a Healthy Cyber Ecosystem: Enabling Cyber Defense through Automated Coordinated Action" was circulated before the workshop. The workshop was co-chaired by DHS Officials Philip Reitinger and Bruce McConnell, and participants included White House and Congressional staffers and representatives from thirteen federal departments and agencies. (See attached list of participants).

In a series of presentations and group discussions, participants reviewed technical models and incentives that could lead to an increase in the adoption of more secure cyber capabilities.

Among the key themes discussed were healthy cyber ecosystem attributes and building blocks, the business case, economic incentives and adoption, the role of outsourcing and cloud computing and next steps. The workshop proceedings, reported herein, are organized around these five themes.

Summary of Discussion

Healthy Cyber Ecosystem Attributes and Building Blocks

Participants thought that an expression of preferred ecosystem attributes would be most useful for engaging industry. To that end, they explored attributes of an ecosystem that would indicate or be fundamental to "good health." They discussed what a "healthy" cyber ecosystem might look like:

- Inclusive– encompassing capabilities embedded in an ever-widening web that extends far beyond traditional notions of the public Internet or of information technology (IT) and services. The ecosystem would include the Smart Grid, with its energy-controlled home networks and IP addressable appliances; the next generation of the National Airspace System, which takes advantage of satellite capabilities; and the large number of legacy devices and control systems which must interoperate with the newest technologies.
- Effective – able to defend against all types of cyber threats – including supply chain attacks, remote or network-based attacks including those launched by sophisticated and well-resourced attackers using persistent methods, proximate or physical attacks or adverse events and insider or disgruntled employee attacks – while preserving privacy and civil liberties.
- Smart (or Sentient) – able to sense the environment, recognize patterns, and share information in near real time across sectors and communities at both the human and machine levels in order to assure authorized transactions, prevent the most serious

security breaches and increase response effectiveness when breaches or other adverse events do occur. One participant noted, "DoD has a saying that every gun is a sensor. In cyberspace, every machine or device can be a sensor if we want to use them that way – and they can be authenticated."

- Barrier-free – having security choices instantiated in configurable digital policies rather than being "hardwired" in network or system designs or imposed by technology limitations or shortfalls. In the words of participants: "We should design with the assumption that everything will be shared with everyone" and "The only barriers to collaboration should be those we impose by policy."
- Optimized – having capabilities and decision making allocated among humans and machines to best leverage the strengths and cycle-times of each. Further, having cyber defense organized so that machines defend against machines and people defend against people.
- Understandable – having security expressed in user or stakeholder terms rather than in specialized security "jargon" and recognizing that "everyone is a cybersecurity stakeholder whether they know it or not." Participant examples of how security might be expressed in stakeholder terms: visibility into the cyber environment, ability to query the environment and get back a high fidelity answer, and the ability to rationalize costs.
- Assured -- able to sustain consumer confidence over time. This was characterized as extending beyond traditional security notions of "preventing unwanted transactions" to "ensuring the right transactions occur", which would contribute more broadly to a sense of consumer safety and trust in sector operations for transportation, energy, health, etc.
- Usable – having assembly, configuration, operational, and performance properties that are straightforward and well-behaving, rather than overwhelmingly complicated, brittle, and error-prone.

They also discussed what such an ecosystem might provide as a value add, that is, what would be different in a healthy ecosystem:

- Greater network reach or extent, including powerful new ways to work across multiple classification or trust levels
- Rapid or "viral" and essentially universal learning with potential to minimize niches ("no Galapagos Islands in cyberspace")
- Information connected across space and time
- New kinds of analytics
- New defensive tactics – dynamic networking, uncertainty (see the discussion on , Moving Target Defense in the Federal Cybersecurity Game-change R&D Themes at http://cybersecurity.nitrd.gov/page/federal-cybersecurity-1)

- Ability to close the loop for cybersecurity by feeding operational learning back into the early part of system and technology life cycles.
- Trusted transactions and greater attribution (see the discussion on Tailored Trustworthy Spaces in the Federal Cybersecurity Game-change R&D Themes at http://cybersecurity.nitrd.gov/page/federal-cybersecurity-1)

Participants noted that moving target defense and tailored trustworthy spaces work together. For example, the ability to make dynamic adjustments to configuration controls in response to trust choices is a form of moving defense. Further, together they help address the full spectrum of threats. A self-defending ecosystem with human involvement could force attackers to take more risks and be more exposed. This combined with greater attack attribution would enable law enforcement or other deterrence to be more effective. The key is a balanced approach – a comprehensible level of effort to have reasonable individual security supplemented by government capabilities.

Participants discussed some of the essential elements of a healthy cyber ecosystem, and thought they might include:

- Authentication of machines and operators. In addition to providing users with confidence in a given device, person, or process, including control system transactions, authentication provides identity attribution for law enforcement, intelligence, and defense related deterrence activities.
- Automation at the machine and application levels to improve prevention and reaction time
- Implementing seamless interoperability among machines, systems and agencies through the development and enforcement of (1) standards that separate security information or content from delivery, and (2) processes that manage security information as an asset.
- Training to ensure users understand systems and their capabilities
- Sound or trustworthy devices at creation, which might require specifying design, development, and attestation criteria for soundness and guaranteeing the trustworthiness of suppliers and service providers. Criteria for soundness might include systems as well as devices. Ideally, criteria and associated metrics would inform real decisions and be internationally accepted.
- Architectural practices that include principles of security and resilience (DoD term is “mission assurance”), guidelines for tailoring to critical capabilities or assets, planning for graceful degradation (e.g., operating with less than full capability), and advanced use of modeling and simulation.

Participants considered automation and interoperability to be tightly bound and essential to creating the glue to link security with existing infrastructure components, e.g., network management and trouble ticketing, in a way that lets security functions be performed faster, across larger populations, and more holistically. They also considered that some building blocks such as sound or trustworthy devices and systems might be more long term as they might require basic research.

Making the Business Case

Participants discussed persistent difficulties in being able to:

- Establish the level of harm (e.g., loss of intellectual property, loss of privacy, loss of confidence) that actually results from a cyber incident
- Show how investments in cyber health can reduce operating costs
- Show how investments in cyber health can improve business agility and enable other decisions, e.g., new business partners, outsourcing
- Show how early investments to buy down security risk can avoid the larger costs of clean-up or mitigation (example: the cost of data leakage protection software compared to the cost of mitigating large-scale identity information disclosure)
- Compare returns on security investments with returns on other business investments so trades can be made. One participant noted, "An airplane crash makes video. A Google crash doesn't."

Participants brainstormed ideas that might help:

- A clearing house that can collect incident and mitigation data, aggregate it to develop actuarial type information, and share the actuarial data anonymously with the government. An example of similar ongoing activities: the collection, aggregation, anonymization, and reporting of aviation safety data using a Federally Funded Research and Development Center (FFRDC) as the neutral intermediary.
- Better, more objective ways to measure or validate extant cybersecurity capabilities and posture
- Better methods for evaluating initiatives relative to the three elements of the cyber risk model – vulnerabilities, consequences, and threats
- Cost models that incorporate resilience into critical infrastructure

Economic Incentives and Adoption

Participants noted that best practices and current security technologies are not being implemented, indicating an imbalance of incentives. They considered incentives to include policy and legal frameworks (including regulation), social forces, and technologies, and they noted, "Defenders are not incented, but attackers are."

Participants engaged in a rich discussion on the role of cyber insurance and liability regimes. They noted some characteristics of the cyber insurance market:

- Market is small (less than 20 companies actively engaged worldwide) with slow growth
- Corporate risk managers cite discrepancies between insurance company offerings and corporate needs
- Insurance works well for random, independent risk than is widely spread across, but not for large-scale, correlated risk (e.g., a large scale cyber event).

- Cyber insurance companies are willing to work with the federal government on a way forward

Examples where insurance has facilitated standards adoption:

- Aviation safety
- OSHA

How cyber ecosystem activity might stimulate growth of the cyber insurance industry or other liability regimes:

- Help with collection of incident and mitigation data and development of actuarial data
- Help with underwriting standards
- Help with metrics

How the federal government might stimulate adoption of security technologies and best practices:

- Target the development of standards and repositories that have the potential to change business models. For example, the creation of the Common Vulnerability and Exposure (CVE) standard and the National Vulnerability Database (http://nvd.nist.gov/) changed the business model for vulnerability management vendors because they stopped competing on the number of [self-identified] vulnerabilities they could find (content) and they started competing on quality of service and usability (delivery). The time is right for this to happen with threat information and signatures. For example, standard enumeration of malware and attack patterns and a national database of threat information would allow vendors to compete on quality of detection, prevention and reporting rather than on the number of signatures they can amass.
- Be demanding consumers, and include standards-based security automation in Requests for Proposal.
- Promote and showcase security automation and interoperability through events such as Advanced Concept Technology Demonstrations (ACTDs), pilots, and tradeshows. For example, Interop events were instrumental in helping mature TCP/IP (http://www.interop.com/).
- Engage the [Lead] System Integrators to see how they can influence the market.
- Pursue enterprise procurement vehicles and licenses for all federal departments and agencies.

The Role of Outsourcing and Cloud Computing

Participants discussed whether the advent of clouds would impact the ecosystem vision or help with legacy systems. They concluded that clouds present both risks and opportunities.

Risks	Opportunities
✓ A cloud composed of fundamentally insecure devices	✓ A cloud that is an enterprise with moving target defense is fundamentally more secure.

and systems is insecure. In the words of one participant, "Virtualizing bad systems in other bad systems is bad."

- ✓ Flat aspect increases the reach or consequences of exploited vulnerabilities
- ✓ Clouds increase the importance of authentication
- ✓ Homogeneity simplifies management and control and provides potential for strengthening system administrator competencies
- ✓ Clouds can ease delivery of authentication mechanisms
- ✓ Clouds introduce service providers, which may shift liability away from individual hardware and software vendors
- ✓ Consolidation may simplify measurement and validation of security capabilities and posture, which could help with actuarial data and business cases

Next Steps

Considerations for next steps included:

- Clearly defining the roles and responsibilities of the federal government in developing a more secure online environment.
- A full-on national discussion of the cyber ecosystem vision and priorities.
- Instantiation of the vision in national strategy.
- A forum for identifying and collaborating on near-term activities the federal government can use to promote better awareness and adoption of existing security configurations, technologies and best practices
- Broader engagement in identifying new standards that are strategic and federal collaboration to fund and develop them
- Identification and promotion of standards drivers. For example, the Federal Desktop Core Configuration (FDCC) helped drive version 1 of Security Content Automation Profile (SCAP).
- Development and implementation of international standards as a basis for capabilities that help meet national and homeland security needs

Workshop Participants

Sorted Alphabetically by Organization

Defense Advanced Research Projects Agency	Howie Schrobe
Department of Commerce	Dawn Leaf
Department of Defense	Anne Neuberger
Department of Defense	Cheryl Roby
Department of Defense	Orlie Yaniv
Department of Education	Bucky Methfessel
Department of Energy	Bill Hunteman
Department of Homeland Security	Brian Morrison
Department of Homeland Security	Bruce McConnell
Department of Homeland Security	Earl Crane
Department of Homeland Security	John Burns
Department of Homeland Security	Kim Johnson
Department of Homeland Security	Mike Brown
Department of Homeland Security	Phil Reitinger
Department of Homeland Security	Robert West
Department of State	John Streufert
Federal Aviation Administration	Jim Williams
Federal Bureau of Investigation	Steve Chabinsky
Federal Communications Commission	Jeffery Goldthorp
Homeland Security Systems Engineering & Development Institute	Gary Gagnon
Homeland Security Systems Engineering & Development Institute	Glenda Turner
Homeland Security Systems Engineering & Development Institute	Margie Zuk
National Institute for Standards and Technology	Curt Barker
National Science Foundation	José L. Muñoz
National Security Agency	Tony Sager
National Security Staff, Executive Office of the President (EOP)	Chris Painter
Nuclear Regulatory Commission	Patrick Howard
Office of Science and Technology Policy, EOP	Chris Greer
Office of the Director for National Intelligence	Jason Kerben
Senate Armed Services Committee	Kirk McConnell
US Senate Homeland Security & Governmental Affairs Committee	Adam Sedgewick