Government-University-Industry Research Roundtable

February 2011

Chris Greer

Assistant Director for Information Technology R&D

White House Office of Science & Technology Policy

America's economic prosperity in the 21st century will depend on cybersecurity

- President Obama, May 2009

President's Cyberspace Policy Review

May 2009

Themes:

- Lead from the top
- Build capacity for a digital nation
- Share responsibility for cybersecurity
- Create effective information sharing and incident response
- Encourage Innovation

President's Cyberspace Policy Review

May 2009

Themes:

- Lead from the top
- Build capacity for a digital nation
- Share responsibility for cybersecurity
- Create effective information sharing and incident response
- Encourage Innovation

Encouraging Innovation

Provide a framework for research and development strategies that focus on game-changing technologies that will help meet infrastructure objectives, building on the existing NITRD strategies …

Interagency Coordination

- NITRD: Networking and Information Technology Research and Development Program
  - CSIA: Cyber Security and Information Assurance Working Group
  - SSG: Senior Steering Group for Cybersecurity
- SCORE: Special Cyber Operations Research and Engineering

Strategy Overview

- Near Horizon
  - Moving Target Defense
  - Tailored Trustworthy Spaces
  - Cyber Economic Incentives
  - Assumption Busters
- Over the Horizon
  - Science of Cybersecurity
- Research for Results
  - Translation to practice

Near horizon – Change the Game

- The cost of attack is asymmetric and favors the attacker – Moving Target
- The cost of simultaneously satisfying all the cybersecurity requirements of an ideal system is prohibitive – Tailored Trustworthy Spaces
- The lack of meaningful metrics and economically sound decision making in security results in a misallocation of resources – Cyber Economic Incentives

Moving Target

Examples of MT goals:

- Design resilient systems that operate reliably in a compromised environment
- Shift from reactive security postures to active preemptive postures
- Create and develop MT mechanisms that are internally manageable, creating disruption for the adversaries, but not for legitimate users
- Analyze the effectiveness of MT mechanisms against various attacks and disruptions, in relation to applicable environments
- Increase the ability to observe, shape, and expose the actions of adversaries as they attempt to break MT mechanisms

Tailored Trustworthy Spaces

Examples of TTS goals:

- Trust negotiation tools and data trust models to support negotiation of policy
- Type-safe languages and application verification, tools for establishment of identity or authentication as specified by the policy
- Data protection tools, access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire transaction path
- Hardware mechanisms that support secure bootload and continuous monitoring of critical software
- Least privilege separation kernels to ensure separation and platform trust in untrustworthy environments

Cyber Economic Incentives

Examples of CEI goals:

- Explore models of cybersecurity investment and markets
- Develop data models, ontologies, and automatic means of anonymizing or sanitizing data; provide methods to support personal data ownership
- Define meaningful cybersecurity metrics and actuarial tables
- Improve the economic viability of assured software development methods
- Provide knowledge in support of laws, regulations and international agreements

Science of Cybersecurity

Examples of SC goals:

- Science of composition; Composability and modularity; Complex systems; Techniques for component, policy and system composition
- Control theory for maintaining security in the presence of partially successful attacks
- Behavioral factors in security and insecurity; Game theory; Integrating the human in the system; Usability and security; Modeling adversaries
- Economics of security; Market externalities; Incentives frameworks; Risk management

Translation to Practice

Examples of Goals:

- Link researchers, venture capitalists, entrepreneurs, and adopters
- Test and evaluation
- Government as early adopter
- Standards origination, evolution, and integration
- Testbeds and pilot projects

Assumption Busters

Examples:

- Defense-in-depth is a means to achieve robust security
- Trust anchors are invulnerable
- Distributed data schemes provide security
- Abnormal behavior detection finds malicious actors.

First Workshop:

- March 22, 2011
- Defense in Depth
- Information: cybersecurity.nitrd.gov

.

Strategy Overview

- Near Horizon
  - Moving Target Defense
  - Tailored Trustworthy Spaces
  - Cyber Economic Incentives
  - Assumption Busters
- Over the Horizon
  - Science of Cybersecurity
- Research for Results
  - Translation to practice

"*We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time*."

-President Obama on Securing our Nation's Cyber Infrastructure
May 2009

Contact:

CGreer@ostp.eop.gov

Information Web Site:

Cybersecurity.nitrd.gov