Weaving a National Initiative?

Source: NSF Security Program Overview, 2009
Motivators for CNCI R&D

- Attackers Rule, Disasters are Likely
- Short-term Measures Essential but Insufficient
- Market Forces Will Not Change the Balance
- New Technology Can Catalyze Major Changes
- **Only a National Initiative Will Make a Real Difference**

-- National Cyber Defense Initiative activities
Background: CNCI

Comprehensive National Cybersecurity Initiative

U.S. Computer Emergency Readiness Team (US-CERT)

DHS National Cybersecurity Center

Trusted Internet Connections Initiative

EINSTEIN Program

Cyber education

Supply chain defense

National Cyber Investigative Joint Task Force (NCIJTF)

Increasing funding for IT security

National Infrastructure Protection Plan (NIPP)

Leap-Ahead R&D & Coordination

National Cyber Leap Year FY 2009
(Coordination) A high-priority, high-intensity, focused, and coordinated set of Federal government activities over the next 10 years

(Leap-Ahead Program) Expanding cyber research and development into high-risk, high-return areas

“to transform the cyber infrastructure so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances”
National Cyber Leap Year Background

- **NCLY Authority**
  - Spring of 2008, OSTP tasked NITRD Program to devise plans to execute the CNCI Leap-Ahead Program Directive
  - NITRD Senior Steering Group (SSG) for Cybersecurity was formed to provide senior leadership and coordination with classified initiatives

- **NCLY Strategy: Game-Change Framework**
  - Morph the Board (changing the terrain, ex. non-persistent virtual machines, adaptive networks)
  - Change the Rules (rules that favor society’s values, ex. accountability, attribution, anonymity)
  - Raise the Stakes (increase risk and cost for attackers, ex. charging for spam email)

- **NCLY Phases**
  - Gather concepts: October 08 – April 09, SSG directed 3 public RFIs to obtain input; 238 submissions
  - Develop best concepts: NCLY Summit, August 09; 3-day summit in Washington DC with 150 security experts from industry, academia, government
SSG synthesis of submissions to the NCLY identified following prospective game-changing directions

- Basing trust decisions on verified assertions (digital provenance)
- Attacks only work once if at all (moving-target defense)
- Knowing when we’ve been had (hardware-enabled trust)
- Move from forensics to real-time diagnosis (health-inspired network defense)
- Crime doesn’t pay (cyber economics)

NCLY Summit August 09

- Explored the game-changing concepts
Cyberspace Policy Review

- Announced by President Obama on May 29, 2009
- Recommends that: “Federal government should provide a framework for R&D strategies that focus on game-changing technologies ... building on the NITRD strategies”
National Cyber R&D Framework: Changing The Game

- **Trusted Tailored Spaces**
  - Capabilities to create virtual spaces tailorable by stakeholders to meet their needs
  - Basing trust decisions on verified assertions
  - End-to-end platforms of trust and trustable digital provenance

- **Maneuverability and Diversity**
  - Develop and deploy diverse and mutating systems to enable Moving Target Defense
  - Attacks only work once if at all
  - Reverse the cost model: attacks become expensive (must do new recon for each attack)

- **Cyber Incentives**
  - Explore economic incentives and means frameworks (cyber insurance, cyber public health, shareable data)
Enable Sub-spaces in Cyberspace

- **Enable trust fabrics**
  - Establish a rich set of trust fabrics and the analytic and risk management technology needed to support decisions in a complex trust environment

- **Enable sub-spaces**
  - Support different security policies and different security services for different types of interactions

- **Provide transparent, secure modes of operations suited to a variety of cyber interactions**

- **Challenges:**
  - Separation and isolation
  - Software and hardware assurance
  - Policy framework
  - Protocol design
  - Negotiation mechanisms
Moving target defense

- Resilience and redundancy
- Limit the span of exposure to vulnerabilities
- Systems must remain dependable and easy to use and manage despite added complexity

Challenges:
- Low cost, high processing capacity
- Virtualization and workload migration
- Adaptive network connectivity
- Address space randomization
- Methods to reduce exposure time with no interruption of service
- Just-in-time compilers

Explore cybersecurity technologies based on our understanding of natural immune systems
- Awareness of self and foreign
- Pathogen pattern recognition
- Multi-layered protection
- Decentralized control
- Diversity
- Signaling
Economic Incentives

- Provide a scientific framework for economic incentives to cybersecurity
- Provide sound metrics
- Provide processes that enable assured development
- Develop cost/risk analysis methods
- Foundation for an effective cybersecurity insurance market

Challenges
- Gathering meaningful data
- Establishing standard extensible metrics
Where does your research fit?

Can your research contribute?

Do you have ideas or results to share?
Contact Information

Tomas Vagoun, PhD
Technical Coordinator

National Coordination Office for Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230

Tel: (703) 292-4873

vagoun@nitrd.gov