Challenges of Engineering
Cybersecurity: Government Perspective

Tomas Vagoun
Cybersecurity R&D Coordinator
NITRD (Program)

❖ **Purpose**
   - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
   - Supports NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
   - Established by the High-Performance Computing Act of 1991

❖ **Scope**
   - Approximately $4B/year across 16 agencies, seven program areas
   - Cyber Security and Information Assurance (CSIA)
   - Human Computer Interaction and Information Management
   - High Confidence Software and Systems
   - High End Computing
   - Large Scale Networking
   - Software Design and Productivity
   - Social, Economic, and Workforce Implications of IT and IT Workforce Development
## CSIA R&D Budgets (Unclassified) in NITRD

<table>
<thead>
<tr>
<th>Selected Agencies</th>
<th>Cyber Security &amp; Information Assurance (CSIA) R&amp;D (Unclassified)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FY 2014 Actual</td>
</tr>
<tr>
<td>DARPA</td>
<td>$265M</td>
</tr>
<tr>
<td>OSD, DoD Service</td>
<td>$182M</td>
</tr>
<tr>
<td>Research Organizations</td>
<td></td>
</tr>
<tr>
<td>NSF</td>
<td>$103M</td>
</tr>
<tr>
<td>DHS</td>
<td>$78M</td>
</tr>
<tr>
<td>NIST</td>
<td>$62M</td>
</tr>
<tr>
<td>DOE</td>
<td>$31M</td>
</tr>
<tr>
<td>Total</td>
<td>$721M</td>
</tr>
</tbody>
</table>

Challenge

Given limited/finite financial resources, what should be the goals for Federal Government’s basic research in cybersecurity?
Underlying Cybersec Deficiencies

- Systems are static and homogeneous → Great ROI on attack reuse
- Users take actions in absence of verified trust → We don’t know when we’ve been had
- Weak capabilities to measure, assess, and maintain SW security → Security fix-loop is slower than attack development-loop: always one (n) steps behind attackers
- Cybersecurity is substantially an economic, social, and behavioral issue → Technical fixes may not be the most effective solutions

Need game-changing, not incremental solutions
Federal Cybersecurity R&D Strategic Plan

- Research Themes
  - Tailored Trustworthy Spaces
  - Moving Target
  - Cyber Economic Incentives
  - Designed-In Security
- Science of Cyber Security
- Support for National Priorities
- Transition to Practice

Moving Target
  – Providing resilience through agility

Tailored Trustworthy Spaces
  – Supporting context specific trust decisions

Designed-In Security
  – Developing secure software systems

Cyber Economic Incentives
  – Providing incentives to good security

Science of Security
  – Improving our understanding of fundamentals that underpin cybersecurity
Moving Target Defense

Monoculture Problem
• Identical systems → same attack disables all systems
• Unchanging systems → same attack works repeatedly

Need dynamic diversity that makes systems unique and increases work for attackers

Long Repair-Cycle Problem
• Long lead time to patch
• Patch cycle is slower than attack development cycle

Need adaptation

Biology to the rescue?
Biology Inspiration for Security

<table>
<thead>
<tr>
<th>Fortress</th>
<th>Biological</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impenetrable (hopefully) barrier with unprotected inside</td>
<td>Many partial and overlapping barriers</td>
</tr>
<tr>
<td>Monolithic</td>
<td>Heterogeneous</td>
</tr>
<tr>
<td>Rigid</td>
<td>Adaptation is a core mechanism</td>
</tr>
<tr>
<td>Need perfect components</td>
<td>Fallible components</td>
</tr>
<tr>
<td>Design reflects scarcity of resources</td>
<td>Abundance of resources</td>
</tr>
<tr>
<td>Evolutionary pressure: price-performance tradeoff</td>
<td>Evolutionary pressure: survivability</td>
</tr>
<tr>
<td>No system-wide survivability</td>
<td>Diversity for population survival, evolution</td>
</tr>
</tbody>
</table>
Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) Program

- Rethink computing systems → immune systems inspiration
- Design systems that can adapt and continue providing services after an attack, learn from attacks, and repair themselves

Rethink
- Hardware
- Programming languages
- Operating systems
- Architecture

Tag every piece of data and enforce access restriction on data in HW

Incorporate rules about information flows and access rights

Enforce security properties specified in the code

Redesign OS as independent modules suspicious of each other
<table>
<thead>
<tr>
<th>Cybersecurity Problem</th>
<th>Biological Approach</th>
<th>DARPA CRASH</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems are easily penetrated</td>
<td>Innate immunity: fast reacting defenses to known pathogens</td>
<td>New hardware and OS that eliminate common vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Repair is costly</td>
<td>Adaptive immunity: slower reacting defenses to unknown pathogens + Adaptation</td>
<td>Adaptive software that determines causes of vulnerabilities and dynamically repairs flaws</td>
<td></td>
</tr>
<tr>
<td>Computing homogeneity: large pool of targets, large ROI for attackers</td>
<td>Diversity: sustains population survival</td>
<td>Techniques that increase entropy, make systems unique, and raise work factor for attackers: instruction set randomization, address space randomization, functional redundancy</td>
<td></td>
</tr>
</tbody>
</table>
DARPA CRASH Innate Immunity: An Example Hardware Solution

Conventional Computer

Meta-computing System

Source: DARPA CRASH Program
Dynamic diversification techniques make systems look the same to the users but vary low-level details that attackers exploit, making each system look different to the attackers.
### MTD Dimension | Examples of MTD Techniques
--- | ---
Systems of Systems | Virtualization, Cloud Computing, Machine Rotations
Data | Secure Distributed Data Chunking, Self-aware Data
Networks | IP Hopping, Dynamic DSN, Dark IP Space
Software | Diversity in Software, Just-in-time Compiling
System | Instruction Set Randomization, Address Space Layout Randomization, OS Diversity
Hardware | Hardware Diversity, Multi-core Processing

---

**Agility**  
Diversity  
Redundancy  
Complexity Support overhead

---

Decreased attack ROI  
Additional work for attackers

---

= Better Security

---

Do we understand:  
- Costs (complexity) vs. Benefits (security)?  
- Measurements of security benefits?  
- Provable security properties?
FROM: Patch & Pray

TO: Standardized metrics
Repeateable experiments
Hypothesis testing
Engineering
Science
Need Focus on Science of Security

Priority Goal: Developing Scientific Foundations

How to nudge the creation of a science?

NSA Science of Security Initiative
CMU, UIUC, NC State, UMD

5 Hard Problems
- Resilient Architectures
- Scalability and Composability
- Secure Collaboration
- Metrics
- Human Behavior

Other examples:
AFOSR: Science of Cyber Security MURI
ARL: Science for Cyber Portfolio program
OSD: Cyber Measurement Campaign
Advancing Science of Security

Annual NSA Competition

http://cps-vo.org/group/SoS
I Want You To Help Build Game-Changing Cybersecurity Solutions

Identify Problems
- Systems are static and homogeneous
- Users take actions without verified trust
- Security is often added-on, not built-in
- Cybersecurity is also an economic, social, and behavioral issue

Execute USG R&D Strategy
- Moving Target (Defense)
- Tailored Trustworthy Spaces
- Designed-In Security
- Cyber Economic Incentives

Innovate

Strengthen Science and Engineering
Some Useful Links


- Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (2011)

- NITRD Supplement to the President's Budget (FY 2016)
Contact Information

Tomas Vagoun, PhD
Cybersecurity R&D 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

http://www.nitrd.gov