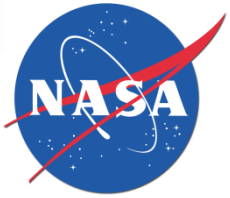
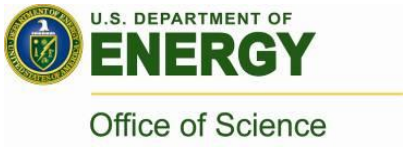
US Federal Cybersecurity R&D Strategic Plan





NITRD (Program)

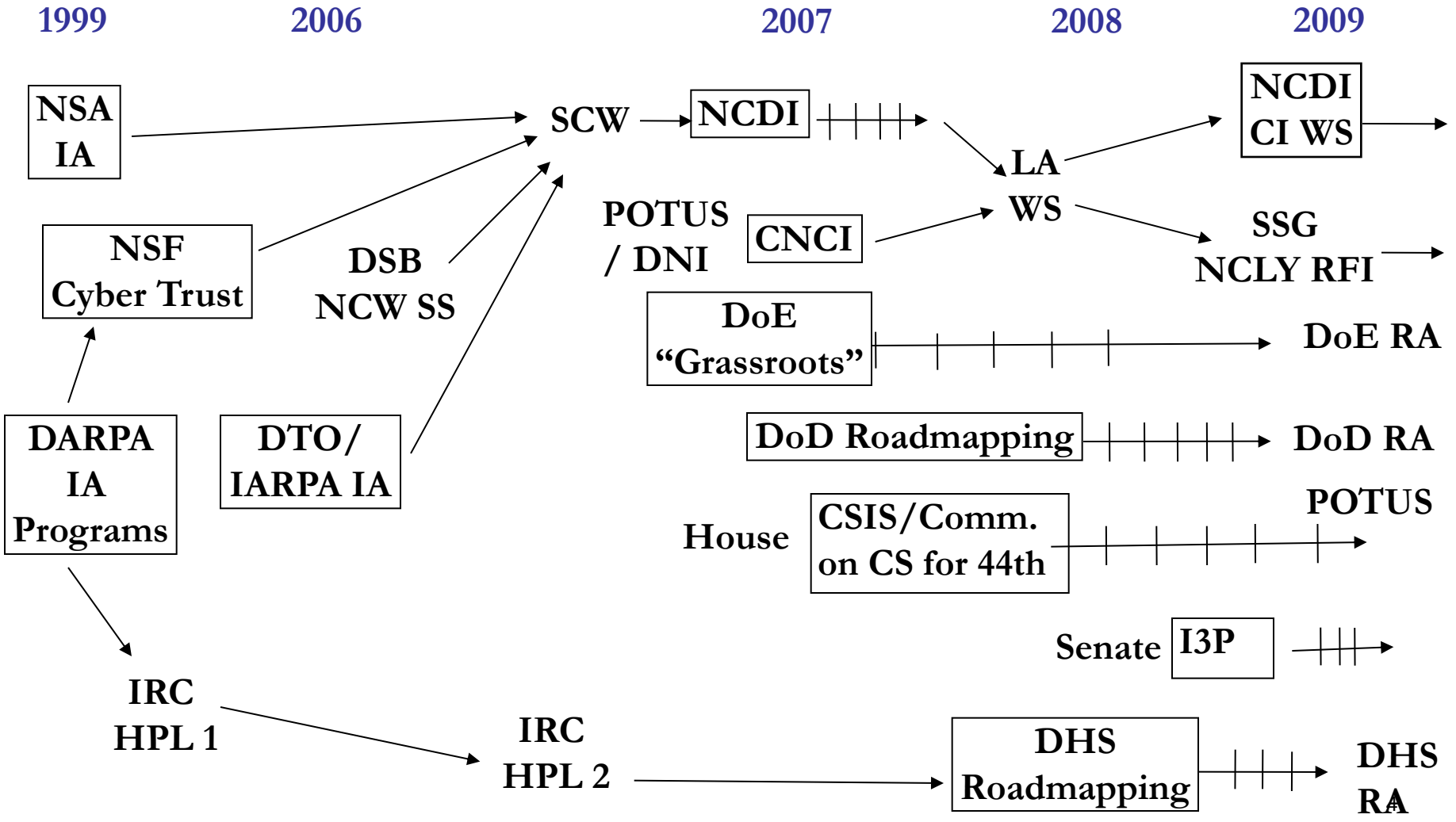
- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Supports NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
  - Established by the High-Performance Computing Act of 1991
- Scope
  - Approximately $4B/year across 16 agencies, nine program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT (SEW)
  - Big Data
  - Cyber-Physical Systems

Selected NITRD Agency Budgets in CSIA R&D

Selected Agencies	Cyber Security & Information Assurance (CSIA) R&D (Unclassified)	
	FY 2012 Actual	FY 2014 Request
DARPA	$223M	$266M
OSD, NSA and DoD Service Research Organizations	$204M	$243M
NSF	$99M	$114M
DHS S&T	$49M	$70M
NIST	$45M	$68M
DOE	$33M	$41M
Total	$653M	$802M

Source: "NITRD Supplement to the President's Budget FY 2014," http://www.nitrd.gov/pubs/2014supplement/FY2014NITRDSupplement.pdf

Federal Cybersecurity R&D: National Dialogue



Vision of R&D under CNCI

Comprehensive National Cybersecurity Initiative (CNCI), Presidential Directive, 2008

"to initiate coordinated set of Federal government activities over the next 10 years to:
to transform the cyber infrastructure so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances."

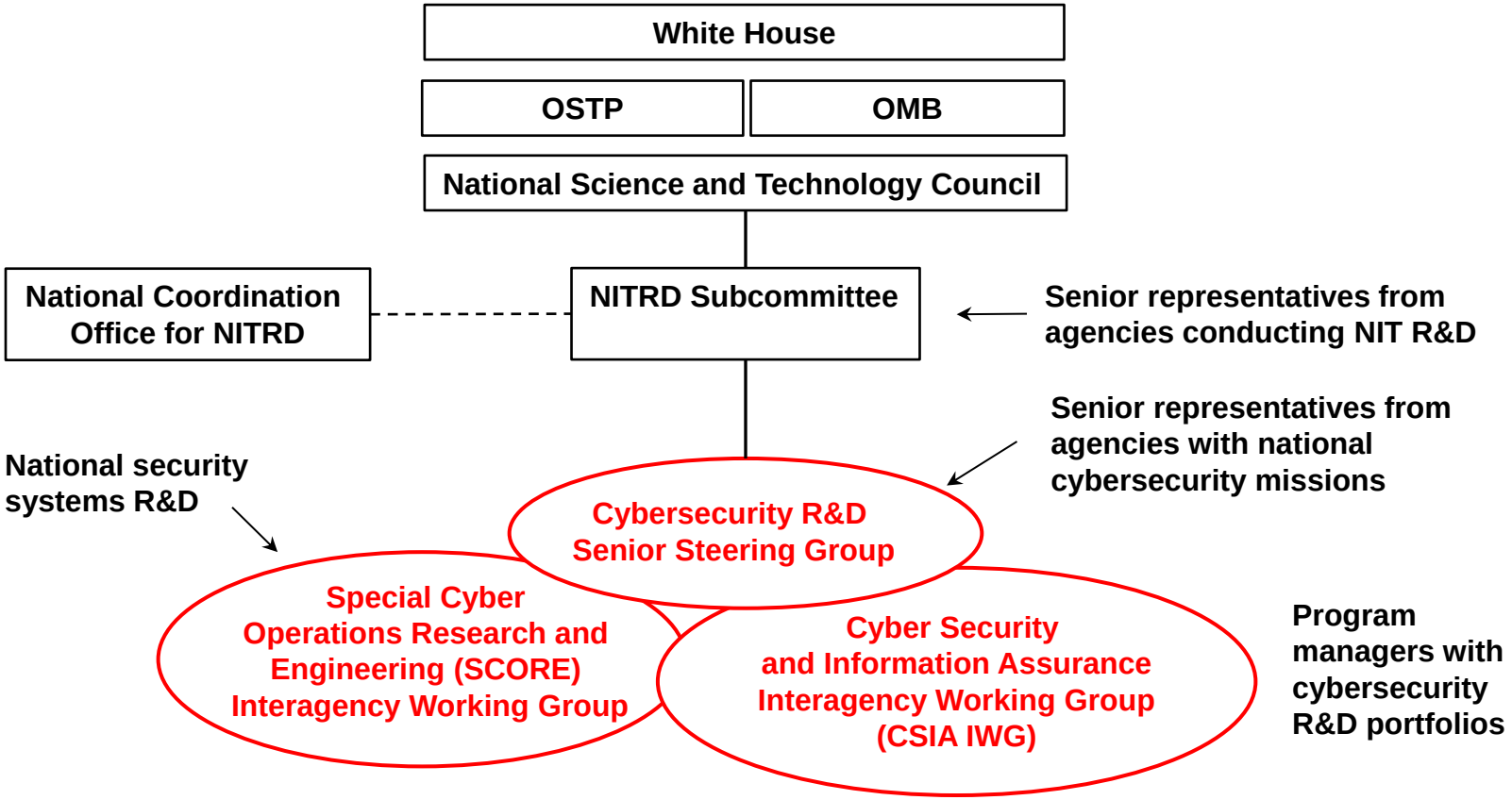
<u>Leap-Ahead/Game-Change R&D</u>
Expand cybersecurity R&D in high-risk, high-return areas

<u>Coordination</u>
NITRD
CSIA R&D SSG
CSIA IWG
SCORE

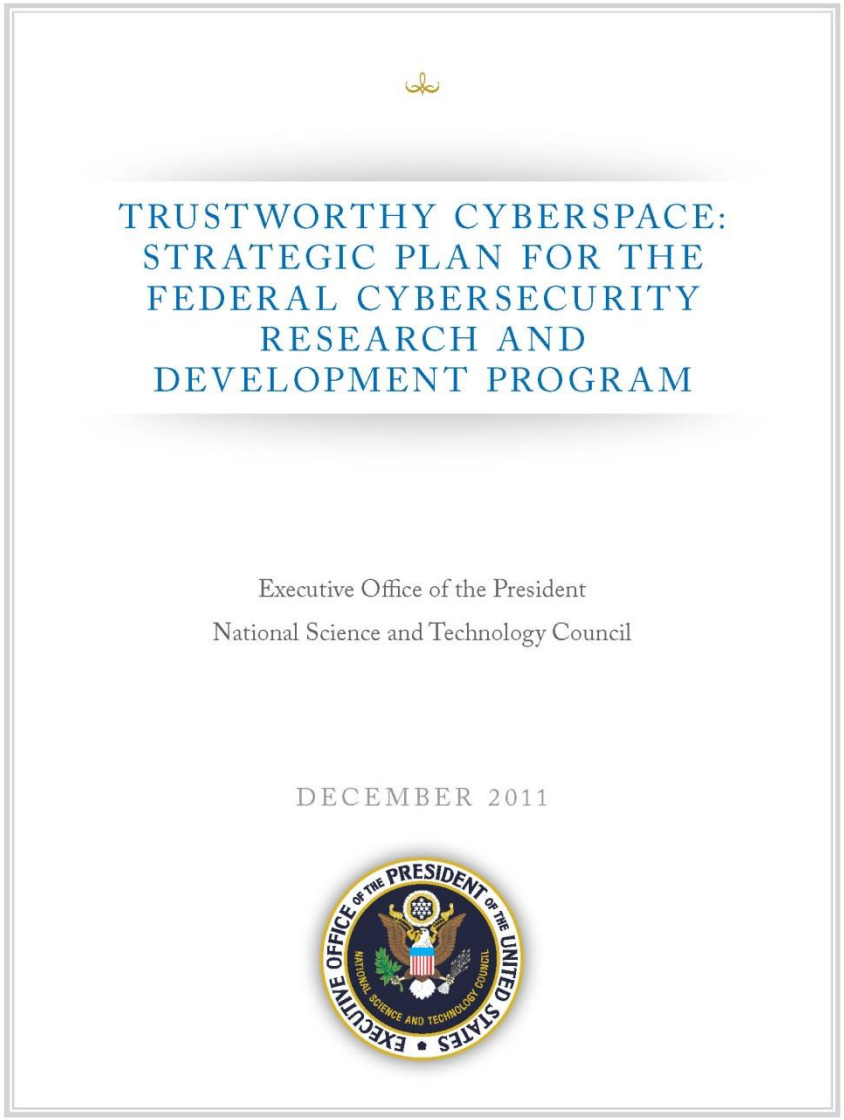
Coordinated Effort on Game-Changers

- It's about trustworthiness of digital infrastructure
  - Security, reliability, resiliency, privacy, usability
- Strong commitment to focus on game-changing technologies for coordinated cybersecurity R&D agenda
  - Comprehensive National Cybersecurity Initiative
  - Presidential Cyberspace Policy Review
  - President's Chief Technology Officer
  - White House Cybersecurity Coordinator
  - NITRD Cybersecurity R&D Senior Steering Group

NITRD Structure for US Federal Cybersecurity R&D Coordination



Federal Cybersecurity R&D Strategic Plan



- Research Themes
- Science of Cyber Security
- Support for National Priorities
- Transition to Practice

http://www.whitehouse.gov/blog/2011/12/06/federal-cybersecurity-rd-strategic-plan-released

R&D Coordination Through Themes

- Hard Problem Lists ≠ Research Strategy
- Federal research strategy focuses on underlying causes of cyber in-security
- Themes provide shared vision of desired end state
- Themes compel a new way of operating / doing business
- Established through robust community discussion of what matters
- Themes recognize that independent thinking is vital to good research

Research Themes

- Tailored Trustworthy Spaces
  - Supporting context specific trust decisions
- Moving Target
  - Providing resilience through agility
- Cyber Economic Incentives
  - Providing incentives to good security
- Designed-In Security
  - Developing secure software systems
- Annually re-examine themes
  - Enrich with new concepts
  - Provide further definition or decomposition

Tailored Trustworthy Spaces Paradigm

- Users can select/create different environments for different activities satisfying variety of operating capabilities
  - Confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to dynamically create new environments with mutually agreed characteristics and lifetimes
- Users can base trust decisions on verifiable assertions

TTS Research

- TTS Characterization
  - Identify and specify elements that describe TTS
  - Translate operational requirements into policies
  - Define tailoring requirements
  - Translate tailoring requirements into executable rules
- Trust Negotiation
  - Frameworks, methods, techniques to establish trust between system components
- TTS Operations
  - Dynamically create, tailor, join, split, merge, dismantle TTS
- TTS and Privacy
  - Fine-grained tailoring to support establishing the context for interactions

TTS R&D Program Examples

- NIST Security Content Automation Protocol (SCAP) Program
  - Common framework and language for specifying instructions for security-related configuration
- ONR FABRIC Program
  - Software development environment for establishing security guarantees based on explicitly stated security policies for distributed systems with complex and changing trust between participants

TTS R&D Program Examples (2)

- Trusted foundation for cyberspace operations [OSD and Service Labs]
- Content and Context Aware Trusted Router (C2TR) [AFRL]
- Access Control Policy Machine [NIST]
- Trusted Hardware/Secure Processor Program [AFRL]
- Trust Management for Optimal Network Performance Program [ARL]
- Hardware-Enabled Trust Program [DHS]
- Security and Privacy Assurance Research (SPAR) Program [IARPA]

TTS R&D Program Examples (3)

- Security and Privacy Assurance Research (SPAR) Program [IARPA]
  - Develop techniques for exchanging data that protect security & privacy interests of each party
  - Application areas include database queries, publish/subscribe systems, outsourced data storage systems
  - Follow up to IARPA Automatic Privacy Protection (APP) program

Moving Target Paradigm

- All systems are compromised; perfect security is unattainable
- Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure
- MT provides controlled change across multiple system dimensions to:
  - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
  - Increase resiliency and fault tolerance within a system

Moving Target Research

- Frameworks
  - Novel approaches for managing systems employing MT mechanism
- Techniques
  - Techniques that modify system characteristics in one or more dimensions, e.g. policies, system of systems, data, networks, software, system, hardware
- Scientific Foundations for MT
  - Analysis of the effectiveness of MT mechanisms

MT R&D Program Examples

- DARPA Clean-slate design of Resilient Adaptive Secure Hosts (CRASH)
  - Computer systems that are resistant to cyber-attacks, adaptive, and self-repairing
  - Clean-slate, biologically-inspired thrusts
    - Innate Immunity: eliminate common technical vulnerabilities; focus on HW, OS, middleware, formal methods
    - Adaptive Immunity: identify, diagnose, and recover from new attacks
    - Dynamic Diversity: diversity across computers and diversity in each computer over time
- DARPA Mission-oriented Resilient Clouds (MRC) Programs
  - Detect, diagnose, respond to attacks in cloud computing systems
  - Use cloud resources to
    - Relocate computations
    - Induce artificial diversity across hosts
    - Group resources to provide collective defense
    - Automatically develop workarounds and patches

MT R&D Program Examples (2)

- ONR Robust Autonomic Host Program
  - Develop computing systems that are self-healing, able to operate under attack with reduced capabilities, employ artificial diversity to increase resilience, and engage in disinformation
  - Research in efficient and adaptive data acquisition and monitoring, machine intelligence, machine reasoning and strategic planning, automated diagnostic, artificial diversity, and automated strategic deception

MT R&D Program Examples (3)

- IARPA Securely Taking On New Executable Software Of Uncertain Provenance (STONESOUP) Program
  - Automate detection and mitigation of security vulnerabilities in software applications
  - Diversify the program code, so that any residual vulnerabilities are harder to exploit
  - Develop novel techniques for randomizing, rewriting, and monitoring software application code so that an adversary will not be able to predict the location of instructions or data needed to launch exploits

MT R&D Program Examples (4)

- AFRL Polymorphic Machines and Enclaves Program
  - Develop techniques to continuously change computer, system, and network characteristics, presenting a shifting target space to an attacker
- AFRL Active Repositioning in Cyberspace for Synchronized Evasion (ARCSYNE) Program
  - Employ IP address hopping to create an agile and stealthy network where the network identity of hosts changes rapidly
  - DHS-funded expansion of the technology
    - Network appliance unit operating at 10 Gbit/sec
    - IP address changes in the network at 10 times/sec

MT R&D Program Examples (5)

- Self Regenerative, Incorruptible Enterprise that Dynamically Recovers with Immunity [AFRL]
- Cyber Camouflage, Concealment, and Deception [DARPA]
- Morphing Network Assets to Restrict Adversarial Reconnaissance (Morphinator) [Army]
- Defensive Enhancements for Information Assurance Technologies (DEFIANT) [Army]
- Moving Target Defense Program [DHS]

Designed-In Security Paradigm

- Designing and developing SW systems that are resistant to attacks
- Require verifiable assurance about system's attack-resistance to be natively part of the SW lifecycle
- Enable reasoning about a diversity of quality attributes (security, safety, reliability, etc.) and the required assurance evidence
- Stimulate further developments in methods and tools for detecting flaws in SW

Designed-In Security Research

- Software Development and Verification Environments
  - Automatically recognize vulnerabilities in code; suggest corrections; generate SW without code-based vulnerabilities
- Assurance Evidence and Synthesis
  - Synthesis of system functional specifications, safety and security policies, resource constraints, HW specification, and operational environmental descriptions to develop systems with provable security properties
- Tools
  - Secure coding standards, compilers, etc.

DIS R&D Program Examples

- ONR Software Efficiency Reclamation Program
  - Enhance software execution security and efficiency by reducing unnecessary SW complexity while preserving programmer's productivity
  - Reduce indirection, perform automatic program de-layering and program specialization, resulting in a compact and efficient codes/executable, with much reduced attack surface

DIS R&D Program Examples (2)

- DARPA High-Assurance Cyber Military Systems (HACMS) Program
  - Construct high-assurance, cyber-physical systems via a clean-slate, formal methods-based approach that enables semi-automated code synthesis from executable, formal specifications
  - Develop a synthesizer capable of producing a machine-checkable proof that the generated code satisfies functional specifications, and security and safety policies
  - Develop techniques to ensure that proofs are composable, allowing the construction of high-assurance systems out of high-assurance components

DIS R&D Program Examples (3)

- Secure Coding Initiative [OSD/SEI]
- Survivable Systems Engineering [OSD/SEI]
- Trusted Computing [DARPA, NSA, OSD, NIST]
- META (flows, tools, and processes for correct-by-construction system design) [DARPA]
- Software Assurance Metrics And Tool Evaluation (SAMATE) [DHS, NIST]

Cyber Economic Incentives

- A focus on what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - Promotion of science-based understanding of markets, decision-making and investment motivation
  - Theories and models of the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models

CEI R&D Program Examples

- NSF Secure and Trustworthy Cyberspace (SaTC) Program (FY12 Solicitation)
  - NSF Computer & Information Science & Engineering Directorate + NSF Social, Behavioral & Economic Sciences Directorate; 18 CEI awards
- DHS Cyber Economics Incentives Program (2011 BAA)
- ONR Infiltration of BOTNET command-and-control and support ecosystems MURI
  - Techniques for infiltration of botnet command and control structures
  - Automated analysis of malware binaries
  - Natural-language processing of human communications that support the botnet ecosystem

Strategic Thrusts

- Research Themes
  - TTS, MT, DIS, CEI
- Science of Cyber Security
- Support for National Priorities
- Transition to Practice

Science of Cyber Security

- A major research initiative on the *science of security* that
  - Organizes the knowledge in the field of security
  - Investigates fundamental laws
  - Results in a cohesive understanding of underlying principles to enable investigations that impact large-scale systems
  - Enables repeatable experimentation
  - Supports high-risk explorations needed to establish such a scientific basis

Science of Security Program Examples

- AFOSR 2011 Science of Security MURI
  - Stanford, Berkeley, Cornell, CMU, U of Penn
- NSA Science of Security Lablets
  - UIUC, NC State, CMU
- ARL Science for Cyber Portfolio Program
- NSF TRUST Program components
  - Berkeley, CMU, Cornell, San Jose SU, Stanford, Vanderbilt

Science of Security Examples (2)

- OSD Cyber Measurement Campaign
  - Develop a suite of metrics to define hypothesis-driven experiments that measure key cyber security capabilities
- AFRL Foundations of Trust and Assurance Program
  - Develop mathematical algebra to represent missions, applications, and cyber infrastructure for provably correct mission characterizations in contested environments

Maximizing Research Impact

- Goals
  - Maximize cybersecurity R&D impact to support and enable advancements in national priorities
- Support for National Priorities (examples)
  - Health IT
  - Smart Grid
  - Financial Services
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)
- Integrating Research Efforts (examples)
  - OSD Cyber Applied Research and Advanced Development Program
  - Journal of Sensitive Cybersecurity Research and Engineering (JSCoRE) by ODNI

Maximizing Research Impact International Cooperation Examples

- DOD The Technical Cooperation Program (TTCP)
  - MOU among Australia, Canada, New Zealand, UK, and US
  - Command, Control, Communications, Information Systems (C3I) Group / Technical Panel 11 focus on information assurance and defensive information warfare
- DoD Network and Information Sciences International Technology Alliance (ITA)
  - research alliance between the UK Ministry of Defense and US ARL
- ONR Global Division
  - International science and technology office, Prague, Czech Republic, 2010
- DHS S&T 2011 Cyber BAA
  - Includes jointly-funded projects with US partners: Australia, UK, Canada, Netherlands, Sweden, Germany, and Israel
- US-Israel Binational Science Foundation
  - NSF support for US-Israel collaborative research in computer science and cybersecurity

Transition to Practice

- Concerted effort to get results of federally funded research into broad use
  - Integrated demos
  - Conferences and workshops
  - “Matchmaking” efforts
    - Among Agencies
    - Between research and product
  - Potential funding for last mile

Transition to Practice Examples

- DHS S&T Transition to Practice (TTP) Program
- DHS S&T Integrator and IT Company Forums
- NIST National Cybersecurity Center of Excellence (NCCoE)
- NSA's Applied Research Prototypes Program
- NSF SaTC Program Transition to Practice Perspective
- AFRL Next-Generation Cyber Warriors Initiative

Drivers for game-change solutions

- Basing trust decisions on verifiable assertions
- Shifting burden of processing onto attackers
- SW (system) lifecycle must natively incorporate verifiable assurance about system's attack-resistance
- Facilitating sound cybersecurity incentives and enabling effective business & personal cybersecurity decisions

“It advanced the technology, but it’s not a game changer.”

Credit:
Lee Lorenz
The New Yorker

Contact Information

Tomas Vagoun, PhD
Cyber Security and Information Assurance IWG 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
http://cybersecurity.nitrd.gov

Examples of Trust Research

- Tailored Trustworthy Spaces Theme
  - Trust Evidence as a critical enabling element
- OSD/ASD(R&D) Cyber Research Program
  - Foundations of Trust research area
- AFRL Cybersecurity S&T Strategic Goals
  - Strategic Goal #4: Invent Foundations of Trust and Assurance
- AFRL Trusted Hardware/Secure Processor Program
- ARL Trust Management for Optimal Network Performance Program
- DHS Hardware-Enabled Trust Program

OSD/ASD(R&D) Cyber Research Program

- Program Areas
  - Assuring effective missions
  - Cyber agility
  - Cyber resilience
  - Foundations of trust
  - Modeling, simulation, and experimentation
  - Embedded, mobile, and tactical

OSD/ASD(R&D) Foundations of Trust

- Develop foundational trust services to assess, compose, and deploy cyber elements with known and predictable confidence in their identity, functionality, and content
- Cyber elements include hardware and software; users and their roles; processes, data, interconnections, and services
- Measurable and predictable levels of trust to enable a quantitative approach to design, tradeoff analysis, and risk mitigation

AFRL Cyber S&T Strategic Goals

- Assure and Empower the Mission
- Create Next-Generation Cyber Warriors
- Enhance Agility and Resilience
- Invent Foundations of Trust and Assurance

AFRL Invent Foundations of Trust and Assurance Cyber S&T Strategic Goal

- Areas of emphasis
  - Scientific Foundations of Mission Assurance
    - Develop mathematical representation of functions within a mission, and algebra to reason about the security properties of information handling within each function across the information lifecycle
  - Scientific Foundations of Trust
    - Develop capabilities to quantify the security, reliability, and assurance of complex interconnected systems
  - Supply Chain Trust

ARL Trust Management for Optimal Network Performance Program

- Understand the role trust plays in networks of large systems with complex interactions between communication, information, and social networks
- Quantify and model the dynamics of trust in networks
- Explore socio-cognitive models of trust for achieving fast trust emergence, propagation, and high sustainability
- Initial application in areas such as traffic routing through nodes with varying levels of trustworthiness, or detection of cyber-compromises by collaborative assessment of trust by multiple nodes in the network