FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN

ENSURING PROSPERITY AND NATIONAL SECURITY

National Science and Technology Council

Networking and Information Technology Research and Development Program

February 2016

Table of Contents

Executive Summary

Computers and computer networking provide major benefits to modern society, yet the growing costs of malicious cyber activities and cybersecurity itself diminish these benefits. Advances in cybersecurity are urgently needed to preserve the Internet's growing social and economic benefits by thwarting adversaries and strengthening public trust of cyber systems.

On December 18, 2014 the President signed into law the *Cybersecurity Enhancement Act of 2014*. This law requires the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development (NITRD) Program to develop and maintain a cybersecurity research and development (R&D) strategic plan (the Plan) using an assessment of risk to guide the overall direction of Federally-funded cybersecurity R&D. This plan satisfies that requirement and establishes the direction for the Federal R&D enterprise in cybersecurity science and technology (S&T) to preserve and expand the Internet's wide-ranging benefits.[1]

This strategic plan updates and expands the December 2011 plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. The 2011 plan defined a set of interrelated breakthrough objectives for Federal agencies that conduct or sponsor R&D in cybersecurity. This Plan incorporates and expands the priorities in the 2011 plan and adds a strong focus on evidence-validated R&D. Evidence of cybersecurity efficacy and efficiency, such as formal proofs and empirical measurements, drives progress in cybersecurity R&D and improves cybersecurity practice.

Four assumptions are the foundation of this plan:

Adversaries. Adversaries will perform malicious cyber activities as long as they perceive that the potential results outweigh the likely effort and possible consequences for themselves.

Defenders. Defenders must thwart malicious cyber activities on increasingly valuable and critical systems with limited resources and despite evolving technologies and threat scenarios.

Users. Users—legitimate individuals and enterprises[2]—will circumvent cybersecurity practices that they perceive as irrelevant, ineffective, inefficient, or overly burdensome.

Technology. As technology cross-connects the physical and cyber worlds, the risks as well as the benefits of the two worlds are interconnected.

The plan defines three research and development goals to provide the science, engineering, mathematics, and technology necessary to improve cybersecurity in light of these assumptions. The science and engineering advances needed are socio-technical in nature, and vary from foundational to applied over a range of time scales:[3]

Near-Term Goal (1-3 years). Achieve S&T advances to counter adversaries' asymmetrical advantages with effective and efficient risk management.

Mid-Term Goal (3-7 Years). Achieve S&T advances to reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation.

Long-Term Goal (7-15 years). Achieve S&T advances for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution.

While near-term goals are frequently focused on developing and refining existing science, medium- and long-term goals require both refinement and improvement of existing science, and fundamental research, which has the potential for identifying transformative new approaches to solve problems beyond the current research areas.

To achieve these goals, the Plan focuses on developing S&T to support four defensive elements:

Deter. The ability to efficiently discourage malicious cyber activities by measuring and increasing costs to adversaries carrying out such activities, diminishing the spoils, and increasing risks and uncertainty for potential adversaries.

Protect. The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability, and accountability.

Detect. The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.

Adapt. The ability of defenders, defenses, and infrastructure to dynamically adapt to malicious cyber activities, by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration, and adjusting to thwart similar future activity.

After a description of each element and associated research challenges, the Plan identifies research objectives to achieve in each element over the near-, mid-, and long-term. The objectives are not comprehensive but establish a basis to measure progress in implementing the Plan. These elements are applicable throughout cyberspace, although some objectives are most meaningful in particular contexts, such as cloud computing or the Internet of Things (IoT).

The Plan identifies six areas critical to successful cybersecurity R&D: (1) scientific foundations; (2) enhancements in risk management; (3) human aspects; (4) transitioning successful research into pervasive use; (5) workforce development; and (6) enhancing the infrastructure for research.

The Plan closes with five recommendations:

Recommendation 1. Prioritize basic and long-term research in Federal cybersecurity R&D.

Recommendation 2. Lower barriers and strengthen incentives for public and private organizations that would broaden participation in cybersecurity R&D.

Recommendation 3. Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient cybersecurity research results into adopted technologies, especially for emerging technologies and threats.

Recommendation 4. Expand the diversity of expertise in the cybersecurity research community.

Recommendation 5. Expand diversity in the cybersecurity workplace.

Implementing the Plan and these recommendations will create S&T for cybersecurity that effectively and efficiently defends cyberspace and sustains an Internet that is inherently more secure.

[1] "S&T" refers to a broad set of disciplines in Science, Technology, Engineering, and Mathematics (STEM).

[2] Non-malicious.

[3] "Socio-technical" refers to the human and social factors in the creation and use of technology. For cybersecurity, a socio-technical approach considers human, social, organizational, economic and technical factors, and the complex interaction among them in the creation, maintenance, and operation of secure systems and infrastructure.

Detect: Challenges & Objectives

- Challenge: Establishing and maintaining situational awareness and understanding in real time
- Challenge: Human understandable and actionable presentation of all components and interactions of a network, IT enterprise, or cyber ecosystem
- Challenge: Differentiating malicious cyber activity from authorized operations
- Challenge: Differentiating malware from legitimate software
- Challenge: Assessing the limits of the protection element as deployed in a system or network
- Near: Discover and apply automated tools to map networks, including entities, attributes, roles, and logical relationships between processes and behaviors.
- Near: Develop usable presentation interfaces that allow operators to better anticipate incidents, discover them in progress, and achieve better post-incident response.
- Mid: Use data analytics to identify malicious cyber activities and differentiate them from authorized user behavior with low false positive and false negative rates.
- Mid: Apply predictive analysis techniques across a range of potential cyber-threat vectors (e.g., via software or hardware) and determine the probable course of action for each threat method. Predictive analysis supports all four defensive elements: Deter, Protect, Detect, and Adapt.
- Long: Develop automated tools for cyber threat forecasting in order to assess the limitations of protective measures and better inform sensor deployment.

Adapt: Challenges & Objectives

- Challenge: Responses often have unforeseen dependencies and coupled interactions
- Challenge: Modern design principles
- Challenge: Increasingly autonomous cybersecurity systems
- Challenge: Multi-scale risk
- Challenge: Faster decision cycles
- Near: Develop the technologies and techniques that enable critical assets to adjust and continue operating acceptably, despite adversary actions.
- Mid: Establish methods to achieve the timely recovery of functionality of inter-dependent systems even while adversary activity continues.
- Long: Build adaptive effective collective defenses informed by predictive analysis that minimize adversary-imposed effects, as well as unintended effects caused by defender actions.

Fundamental Challenge

Make cybersecurity less onerous while providing more-effective defenses

Deter: Challenges & Objectives

- Challenge: High-confidence attribution in real-time
- Challenge: forensic techniques robust enough to preserve evidence suitable for use in legal proceedings, while also bolstering immediate detection and cyber analytical abilities
- Challenge: Quantifying the resources an adversary would require to successfully breach or evade cybersecurity controls or detection.
- Near: Establish quantifiable metrics of adversary level of effort needed to overcome specific cybersecurity defenses; assess the viability and cost of alternative courses of action to achieve the same or similar objectives.
- Near: Determine what probability of attribution and criminal or economic sanctions would be necessary to deter various types of malicious cyber activities and adversaries.
- Mid: Automatically extract information about malicious cyber activities to document, verify, and share among law enforcement agencies and other partners to support attribution in near-real time.
- Long: Accurately and efficiently attribute malicious cyber activities to specific actors, companies, or nation states, with sufficient precision to support imposition of costs or economic sanctions and sufficient probability to deter malicious activities.

Protect: Challenges & Objectives

- Challenge: Limiting Vulnerabilities
- Challenge: Enforcing Security Principles
- Near: Develop secure update mechanisms that support the full range of product formats (i.e., proprietary and open source), applications (e.g., enterprise services and IoT), and lifecycles.
- Near: Develop tools and techniques for evidence-based assessment to determine the efficacy and efficiency of widely-available protection technologies.
- Near: Make cryptographic tools and techniques available for constrained environments (e.g., lightweight cryptography), privacy-preserving applications (e.g., private databases), and long-term confidentiality (e.g., quantum-resistant cryptography).
- Mid: Create tools for static and dynamic analysis that reduce vulnerabilities in traditionally developed code bases to one defect per ten thousand lines of code (reducing the number of vulnerabilities in new and legacy code bases by a factor of ten).
- Mid: Develop automated tools and techniques to derive fine grained security policies implementing least privilege from high-level, mission-oriented policy.
- Mid: Develop tools and techniques to verify authenticity and provenance of software and firmware with 98 percent accuracy.
- Long: Create tool chains that support development of software with one defect per hundred thousand lines of code with a relative efficiency metric of 90 percent for productivity and system performance (i.e., systems with 1 percent of the defects in current systems that take no more than 10 percent longer to implement and run up to 10 percent slower than unprotected systems).
- Long: Enhance efficacy and efficiency of security controls, as demonstrated by evidence-based assessment tools and techniques, by two orders of magnitude over 10 years.
- Long: Demonstrate repeatable methodologies for correct computation.