Excerpted from the 2016 Federal Cybersecurity Research and Development Strategic Plan

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.

Excerpted from the 2016 Federal Cybersecurity Research and Development Strategic Plan

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.

Critical Dependencies: Challenges in Scientific Foundations

- Formal frameworks and definitions for threats, measurable security assumptions, and guarantees
- Efficient formal methods for evaluating compositions of systems, defenses, and adversaries
- Principled design techniques to construct security ecosystems with provable or measurable verification and validation of security properties, and characterizations of efficiency
- Reasoning frameworks to anticipate evolving and disruptive technologies and threats