Cyber, Space & Intelligence Association and the Cyber Threat Alliance

Recommendations for Federal Funding for
R&D Relating to Improving Security of Computer Code
November 30, 2017

Executive Summary:

Several systemic weaknesses make IT systems inherently difficult to defend from a cybersecurity perspective. These weaknesses include vulnerabilities in computer code, misaligned incentive structures, a lack of understanding of critical interdependencies, and difficulties in managing the supply chain for both hardware and software. Although current cybersecurity practices can reduce the risk from these threats, substantially altering the balance between intruders and defenders will require sustained research and development (R&D) activity. In many cases, due to the fundamental, broad, long-term nature of the problem, the Federal government is the right sponsor for such R&D. Research and development funding in any or all the following areas would help address a critical systemic weakness: supply chain; secure coding practices; automation, artificial intelligence and machine learning; incentives; encryption and key management; understanding interdependencies and incentives; defenses against data manipulation; and workforce training.

Problem

Although we have made significant advances in cybersecurity practices over the past few years, almost IT systems suffer from a set of systemic weaknesses that render them vulnerable to malicious actors and make securing them extremely challenging. These weaknesses include:

Code vulnerabilities: based on the work of several computer science researchers, code produced using the best-known practices still results in a fairly high exploitable error rate. This high error rate means that opportunity for intruders to find zero-day vulnerabilities remains high, even years after the code is produced. Yet, we do not know how to reduce the error rate to an acceptable level.

Critical dependencies: at almost every level from within IT sub-systems to between critical infrastructures society-wide, systems and process depend on each other to keep functioning properly. However, we do not understand these relationships and so when a process, sub-system, system, or critical infrastructure fails, it can create unexpected security problems. Since these systems are often chaotic and complex (in the formal uses of those terms), understanding these critical dependencies will require substantial R&D efforts.

Misaligned incentive structures: although we know what actions and behaviors reduce cyber risk, we are not very good at getting individuals and organizations to implement those best practices. Since we know that people do not want to suffer cyber intrusions, the incentives for implementing these best practices must be misaligned.

Supply chain: the supply chain for both hardware and software is long, complicated, and almost impossible to have complete situational awareness about. Given this length and complexity, it is impossible right now to ensure the integrity of the entire supply chain, providing ample opportunity for malicious actors to introduce vulnerabilities and malware.

Recommendations:

We have identified seven research initiatives that could reduce the risk associated with these systemic weaknesses. Although the private sector is investing in these areas, the benefits would often accrue broadly across multiple companies and sectors of society, so the private sector is likely under-investing relative to what we from a society-wide perspective. As a result, the participants believe the following areas would benefit from additional Federal R&D spending and would materially improve our overall cybersecurity posture:

- Better code creation (e.g., security, quality) – R&D activities would seek to reduce the number of exploitable vulnerabilities per line of code. Research topics could include how to:
    - Develop and implement secure coding requirements and standards
    - Implement Formal Methods for source code development so that code does only what we want it to do
    - Develop safe programming languages to ensure performance
    - Develop, implement, and standardize code testing capabilities (e.g., functionality testing, penetration testing, vulnerability scans)
    - Validate adherence to secure code practices
    - Automate more of the software development process to reduce human error
    - Develop a "fail to safe mode" for hardware and software and ensure that safe mode is noncorrupted
    - Deal with maturation of code and code libraries
    - Integrate traceability analysis between requirements/user stories, code that implements those functions, and execution traces (looking for mis-matches)

- Cybersecurity economics – R&D in this area would seek to understand how to:
    - identify or create incentives for individuals and organizations to adopt, implement, and maintain good cybersecurity practices
    - model connected systems to identify critical interdependencies and single points of failure
    - Induce additional people to enter the cybersecurity workforce

- Supply chain – R&D activities would seek to enable vendors or 3rd party reviewers to verify hardware and software security, whether developed internally or via a 3rd party, throughout the acquisition and systems engineering life cycle. Topics could include how to
    - Ensure integrity and functionality throughout every milestone stage, including:
        - Design
        - Development
        - Production

      Operations
    - Address the risk of companies that enter the U.S legitimately but pose security risks to software systems

- Secure communications – R&D in this area would seek to reduce the weaknesses inherent in the software protocols that make the Internet function. Potential topics include:
    - Creating an easy-to-use security protocol library that operates securely while still conforming with the protocol standards
    - Designing modular library that can support cryptologic algorithm replacement
    - Improving the use and verification of cryptographic systems

- Artificial Intelligence and Machine Learning -- R&D in this area would seek to understand how AI/ML could be used to enhance both offensive and defensive cybersecurity capabilities. Topics could include how to:
    - Develop self-healing code
    - Predict the evolution of malware and develop risk mitigation scenarios
    - Combat homogeneity of source code
    - Understand the vulnerabilities of ML algorithms to manipulation
    - Automate and continually scan IT elements (hardware and software) on a network
    - Detect elements (hardware and software) of an IT system that are not abiding by the organization's cybersecurity policies
    - Automate adherence to policies of IT elements
    - Perform real-time detection of malicious activity on a network
    - Develop real-time automated response to detected malicious activity
    - Provide training data among organizations to continually improve the performance of the learning algorithms

- Spoofing, data manipulation, and data corruption defenses: R&D in this area would seek to develop the capability to defend against spoofing, data manipulation, and data corruption across any kind of IT system. Potential topics include learning how to:
    - Use encryption could reduce risk
    - Harden software against these threats
    - Ensure that the wrong material does not get delivered to the wrong person at the wrong time

- Cybersecurity workforce: R&D in this area would aim to improve cybersecurity training for the workforce, and improve methods for identifying, reporting, and tracking suspicious behavior. Topics could include how to:
    - Develop and implement effective education and training programs at the federal, state, and local levels
    - Standardize cyber capabilities within the educational system. Application should include all levels of education and should seek to inform and teach students all aspects of coding including:
        - Develop secure applications and software from the perspective of a hacker
        - Determine software threats and vulnerabilities
    - Recruit and retain a qualified cybersecurity workforce
        - Verify sufficient security staff
        - Recruit, hire, and retain necessary personnel
        - Guarantee that personnel have the necessary skills and expertise to address challenges

Contributors

This white paper was produced under the auspices of the Cyber, Space, & Intelligence Association and the Cyber Threat Alliance. The majority of the content came from an in-person discussion under Chatham House rules on September 26, 2017. Participants included experts from across the cybersecurity field.