2004 Research & Development Exchange Workshop:

A Year Later:
Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness

Cyber/Software Security Session

Background

In its seminal report *Trust in Cyberspace*, the National Research Council framed a set of issues related to the trustworthiness of the Nation's telecommunications network. Specifically, the report focused on the correctness, security, reliability, safety, and survivability of the public switched network (PSN) and the Internet; the logical elements of computer networks; and the systems, devices, and applications employed by end users. To protect against the threat of malicious software and distributed denial of service attacks, an array of technologies such as firewalls, intrusion detection systems, and virtual private networks have been researched, developed, and fielded. The effectiveness of those technologies, however, is limited by several factors, including the inability to keep pace with attack profiles, interoperability issues between proprietary solutions, inconsistent patch implementation, and the increasing complexity of the telecommunications network as a result of convergence activities.

Network trustworthiness may be defined as the expectation that systems on that network will do what they are supposed to do and not do what they are not supposed to do. As such, software plays an integral role in achieving trustworthiness, as it is the software that integrates and customizes general-purpose system components to accomplish any given task. Consequently, inadequate software security can have many far-reaching negative consequences that detract from the overall trustworthiness of information systems. Factors related to software that can affect the trustworthiness of systems include, but are not limited to: (1) complex source code that could contain millions of lines of code to be tested and evaluated in short time periods; (2) the connection of legacy systems to more current, diverse systems; (3) the movement toward using commercial off the shelf software, which in many cases causes developers to become dependent on third party vendors for the design and security of important components; (4) the inability to ensure that system administrators are updating system software patches in a timely manner; and (5) other influences, such as standards and/or regulations that compete with efforts to develop trusted systems.

These security issues have considerable impact for national security and emergency preparedness (NS/EP) stakeholders and the technologies upon which they rely. Additionally, of increasing concern to the NS/EP community during recent years is the growing prevalence of spyware, which represents a significant challenge for industry and Government because of a number of associated security implications: loss of sensitive and/or proprietary information, loss of privacy, loss of bandwidth, loss of system integrity, and loss of resources.

Many advances have been made in the arena of cyber and software security, including the creation of the National Cyber Security Division within the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate to address the concerns related to the Nation's cyber security posture and the National Security Agency's recent proposal to create a government-funded research center devoted to improving the security of commercial software. However, new technological advancements and the increasing global access to the Internet only serve to increase the difficulty of ensuring network trustworthiness. As the nature of the network continues to change, so too will the discussions related to trustworthiness.

2003 RDX Workshop Results

At the RDX Workshop at the Georgia Tech Information Security Center at the Georgia Institute of Technology in March 2003, participants determined that protecting NS/EP mission-critical systems and ensuring their reliability had become a responsibility not only of the U.S. Government but also that of the private sector, the primary owner and operator of critical infrastructure. Participants emphasized the Nation needed to expect and, in turn, develop strategies to eliminate more sophisticated threats likely to be unleashed in the future. They noted today's security practitioners were responding to hackers defacing websites or stealing credit card numbers. In the future, however, highly organized terrorist organizations (and possibly hostile foreign countries) might launch more sophisticated, widespread, and debilitating attacks, exploiting vulnerabilities in the information infrastructure.

Several participants noted how R&D investments in cyber security were minimal in the 1980s, and how the results of that neglect were visible today. They stated the increasing reliance on commercial off-the-shelf products had reduced overall cost, but also caused users to become dependent on third party vendors for the design and security of important components. Others stated the U.S. Government, reluctant to regulate the Internet to avoid stifling competition, had mainly delegated the responsibility to protect the Nation's critical telecommunications infrastructure to the private sector. They noted, however, that market objectives and national security concerns were not always harmonious. They stated the primary motivation for a company was to increase profitability and market presence. Therefore, most participants agreed that reliance on pure market forces was unlikely to produce a business case conducive to spending valuable resources on security protections. The group also expressed an overall sense of frustration at the political and bureaucratic processes driving research in cyber security technologies, noting many of today's security vulnerabilities were identified more than a decade ago, but little progress had been made in eliminating them.

As a result of the discussion, participants recommended that the Office of Science and Technology Policy focus on R&D activities in two dimensions: (1) *short-term research* that could improve the trustworthiness of software and cyber systems in the near future and (2) *long-term research* that could embed the concept of trustworthy computing in the design of future systems. These priorities are summarized below:

Cyber Security and Software Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Economic Incentives	• Develop and encourage the creation of market incentives designed to stimulate research in security technologies. Those incentives could include, but not be limited to, tax breaks and credits, subsidies, or any other monetary incentives
Vulnerabilities	• Develop methods and tools to eliminate vulnerabilities in software during the design and development phases, particularly with source code • Develop techniques to automatically test for vulnerabilities in COTS • Develop validation and quality assurance techniques to ensure that appropriate software patches are installed • Develop and deploy computer security embedded measures (e.g. trustworthy code, secure default mechanisms)† • Design compilers to scan source code and identify, if not remove, vulnerabilities†
Secure Protocol Design and Development	• Promote secure protocol design by analyzing current routing and signaling protocols (e.g. BGP) and incorporating findings into the design of future protocols
Legacy System Security	• Implement techniques to strengthen the security of legacy systems
Priority Routing	• Develop a GETS-like program for priority packet routing in all networks with assured quality of service for use during emergency situations
Modeling and Simulation Mechanisms	• Develop modeling, simulation, and analytic techniques and mechanisms to pinpoint systemic weaknesses and better prepare for and respond to emergencies • Model and simulate networks to map network topologies and monitor Internet traffic

	• Develop early warning systems to prevent and respond to cyber attacks†
System-wide Recovery and Remediation	• Improve system-wide recovery and remediation to create more robust network systems that respond more quickly to attacks
Intelligent Agents	• Research methods, such as intelligent agents, to monitor traffic electronically, configure systems, and enforce security policies automatically
Information Sharing	• Determine what information should be shared amongst infrastructure owners • Create data collection system to help generate a business model for sharing
Risk Assessments	• Promote the development of risk assessment methodologies to help analyze the costs associated with implementing/not implementing security mechanisms
Best Practices	• Conduct impact analyses to assess the efficacy of best practices and evaluate how they are implemented
Cyber Security Research	• Support basic research in the science of cyber security to include building and deploying inherently secure architectures; testing and evaluating large-scale systems; defining rules of composition for large-scale systems; and defining and developing technical metrics that measure the strength of security† • Design compilers that eliminate or (at least) identify vulnerabilities during compilation of software applications
Embedded Systems	• Promote the security of "embedded systems" where old architectures have been integrated into new, more security oriented architectures†
Advanced Investigative Tool Development	• Develop tools for authentication, forensics, and attribution to facilitate international investigations and foster cooperation†
System Criticality	• Determine the criticality of specific systems to better understand the potential impact of specific system vulnerabilities and to rationalize and prioritize investments to protect, mitigate, and eliminate those with the greatest potential economic/performance impact
Security Metrics	• Develop and verify security metrics for use on a national level to create a much-improved environment and common format for sharing intrusion information
Information Assurance Decision Making	• Develop decision support tools to help organizations better understand how security products and applications might impact system performance and assess economic impacts (e.g., return on investment)
Internet System Dynamics	• Develop a clearer understanding of the Internet's system dynamics including reconciling the security roles, responsibilities, and relationships between the "end-nodes" and the intermediaries • Create a national cyber command and control system to develop and implement a national process for cyberspace indications and warning and develop national benchmarks for trustworthiness of NS/EP telecommunications systems based on different levels of criticality that would improve the health of the Internet
Well-Trained Workforce	• Promote the development of a more well-trained workforce for research, development, and operation • Increase emphasis on security, trustworthiness, and cyber ethics at academic and training institutions
Trustworthiness	• Improve the "building blocks" of trustworthiness – better attribution and damage prevention/limitation
Policy Development	• Develop policy fostering cooperation, collaboration, and prosecution for the mutual protection of national and international infrastructures

† Denotes Long-Term Focus

Questions to Address

- What progress has been made, if any, in trustworthiness R&D since March 2003 when the last RDX Workshop was held?
- What critical challenges remain for ensuring network trustworthiness? Are these challenges the same as those raised at the last RDX Workshop? What other areas deserve consideration? Are there new challenges and issue areas not previously discussed? Are there events that have occurred since March 2003 (e.g. the Northeast blackout) that underscore additional issues to consider?

- How can the R&D community work collaboratively to effectively share information and capitalize on collective advancements that relate to trustworthiness as communities of interest shift?
- What roles should industry, Government, and academia (e.g., OSTP, DHS/S&T, etc.) play in advancing the trustworthiness issue? Who is responsible for leading the way and implementing past and future recommendations? Which other partners are essential or desirable to effect the recommended changes? What funding is likely necessary? From what sources?
- Based on the session discussions, what input would you provide to OSTP in its preparation of the President's research agenda and budget requests? What are the underlying policy issues that should be studied by the President's NSTAC or other body?
- What would be your three to four key points related to developing an agenda for action on trusted NS/EP telecommunications?