



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

Human Factors Breakout Session

Background

The efficacy of any technology is directly dependent upon the ability of humans to configure, implement, and manage it as it was designed. Various factors—user awareness, organization policies and procedures, legal issues, and business pressures, among others—all shape how trust is instilled in systems. Poor user awareness or inadequate policies, for example, can manifest two problems. First, users unfamiliar with key technologies designed to engineer trust into networked information systems can inadvertently expose those systems to risk through poor configuration, implementation, or management. Second, insiders authorized to use systems they later employ for illicit purposes remain a vexing problem in terms of building trustworthy systems. Without strong protections (such as background checks, access controls, and multi-layered defenses), insiders may be able to exploit what might be technically considered a “trustworthy system.”

Recent publications focused on insider activities, including the U.S. Secret Service and CERT® Coordination Center’s *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, acknowledge that many reported incidents are technically unsophisticated, and thus require organizations to concentrate on their overall business processes rather than focusing narrowly on technical solutions. Additionally, as today’s virtual organizations expand to include networked associates (such as vendors, trading partners, and customers), the definition of “insider” evolves to encompass a far greater number of users necessitating increased focus on information security policies. The *Insider Threat Study* discusses the importance of strengthening business practices and organization policies by creating a culture of security. The study recommends that all users (from individuals responsible for data entry to system administrators to senior management) are aware of the value of security and are endowed with responsibility for responding to and reporting on suspicious behavior. In today’s environment there are limited guarantees that the integrity of software assets for national security and emergency preparedness (NS/EP) communications have not been compromised, suggesting the need for increased non-intrusive surveillance techniques to defend against malicious interference from insiders.

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 emphasized the fact that human factors pervade all aspects of trustworthiness in NS/EP telecommunications and information systems. Even the best technical solution can prove vulnerable to intentional (e.g., external attack, insider threat) or unintentional acts (e.g., defective software, inadequate system configuration, non-compliance with security policies). Participants identified seven broad areas shaping the operating environment focused on efforts to minimize the risk of inadvertent failures and malicious acts: education, training, and awareness; policy development, dissemination, and enforcement; human processing and decision-making; anomaly detection; insider threats; cultural shifts; and supply source identification.

As a result of the discussion, participants developed the following list of research priorities.

Human Factors Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Human Processing and Decision-Making	<ul style="list-style-type: none"> Leverage knowledge accrued from other risk management disciplines (e.g., banking, transportation, public health) to minimize biases and risks related to information security Enhance tools and technologies to improve human decision-making under conditions of ambiguity or uncertainty Reduce impact of human factors (e.g., number of humans interfacing with key systems) by making security transparent
Anomaly Detection	<ul style="list-style-type: none"> Research automated tools/techniques to detect anomalies (both physical access and cyber) across an entire enterprise Research tools to better visualize/interpret outputs in real or near real-time from highly complex detection/anomalous activity systems (e.g., replace audit logs)
Education, Training, and Awareness	<ul style="list-style-type: none"> Educate, train, and increase awareness of security issues (e.g., conduct market research on effective techniques to raise awareness across demographic divides)
Insider Threats	<ul style="list-style-type: none"> Investigate true prevalence of insider incidents (e.g., frequency, impact) Research cultural, psychological, technical, and organizational factors that both motivate and deter insiders (e.g., what motivates an insider to act; what prevents others from exploiting known vulnerabilities) Research tools and techniques to better combat insider threats Translate insider threat research (existing/ongoing) into useful techniques and policies
Supply Source	<ul style="list-style-type: none"> Explore multiple, distributed venues for checking source code (e.g., coordination with IA Centers of Excellence) Validate distribution processes Prioritize what code needs to be checked

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?

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering