



2004 Research and 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

Physical Security Session

Background

Recognized as the “backbone” for all other critical infrastructures, the telecommunications sector is heavily relied upon by the United States Government, other critical infrastructures, and the general public. Consequently, threats against key telecommunications facilities could adversely affect not only the day-to-day operations of the many residential and commercial customers who rely on the networks but also the national security and emergency preparedness (NS/EP) services that run across the network. Although industry and Government have made progress in protecting the infrastructure, vulnerabilities still remain with regard to physical security at critical telecommunications facilities. Trusted systems may be compromised via damage to and/or infiltrations of the facilities in which critical telecommunications systems are housed. Significant concern arises around the structural elements of the facility as well as the trusted physical access granted to individuals requiring entrance to sites where telecommunications assets are concentrated.

The physical design of a facility may leave the key elements of the telecommunications infrastructure vulnerable to a variety of environmental and human factors. The southeastern United States is struggling to recover from an arduous hurricane season and the telecommunications infrastructure and those that rely on it are still learning critical lessons from the September 11 terrorist attacks. With the threat of both natural and man-made disasters ever looming, the telecommunications industry has sought new ways to build physical protection technologies into its networks and facilities and to identify which technologies – both new and old – provide the right combination to create a more secure environment.

In addition to the physical protections built into the structure and design of a facility, a second physical security concern relates to procedures for granting trusted access. While many facilities currently address, to some degree, the concern that unauthorized persons with malicious intent could gain access to the facility, the fear also exists that legitimate personnel with authorized access to critical facilities can have malicious intent for a variety of reasons. This type of threat is both difficult to detect and defend against. Employees, contractors, maintenance and supply workers require access to facilities housing sensitive or critical elements of the infrastructure on a regular basis. However, many facilities cannot guarantee that those granted access are trusted individuals, though they are often given unsupervised access.

Protection efforts must also consider emergency incident response situations, such as earthquake-related disaster areas and access to national special security events (NSSE), such as national political conventions and Presidential inaugurations. Communications are critical to the successful execution of both situations and telecommunications personnel will be utilized in various stages of such events. The identification of fluid methods of involvement for personnel from the telecommunications sector (and other critical infrastructures) in the continued heightened security alert state, including access to those emergency and special security events and the networks they rely on, are critical issues for industry and Government to resolve to ensure the continued trustworthiness of the network.

While industry and Government have made significant progress in their efforts to identify mitigation strategies related to both design and access related vulnerabilities, communications technologies continue to permeate the reaches of the U.S. infrastructure, pushing the issue of physical security at telecommunications facilities into

new territory. Though physical security efforts have traditionally focused on the physical protection efforts related to the facilities where infrastructure components are housed, the issue has branched into the arena of logical access to critical information and networks as well. As more of the communications infrastructure becomes networked, and a greater portion of critical assets are stored in cyberspace. Consequently, those addressing the issue of physical security at telecommunications facilities are faced with the additional concern of protecting and restricting “cyber” access to their critical networks.

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 agreed on the importance of several overarching themes to characterize the state of physical security. First, they stated there were not defined or Government-validated threat scenarios or adversary attack plans against which to build measures for protecting facilities. Second, they noted the difficulty for telecommunications companies to first determine what threats existed to the industry and then protect against all feasible attack techniques. Participants also noted a lack of widespread understanding and appreciation within the industry for the sophistication of threats they face on a day-to-day basis. Finally, participants emphasized the importance of considering physical security in the context of protecting human capital, in addition to the more obvious and visible threats to physical assets. In considering R&D issues related to physical security, participants identified physical access control, information control, architectural integrity, and education and awareness as key issues in the discussion.

As a result of the discussion, participants developed the following list of research priorities they believe should be further examined through industry/Government/academic partnerships.

Physical Security Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Modeling and Simulation	<ul style="list-style-type: none"> Undertake advanced modeling and simulation activities for NS/EP events that include virtual attack/defense of facilities/networks Develop a “SimFacility” simulation tool (based on SimCity-like capabilities) to better understand vulnerabilities and potential threats to physical infrastructures housing critical network components
Vulnerability Analysis	<ul style="list-style-type: none"> Develop better vulnerability analysis to understand critical single points of failure and interdependencies
Biometrics	<ul style="list-style-type: none"> Develop industry standards for and implement a biometrics based national standard industrial identification card Utilize biometric technologies (e.g., iris scanning, hand geometry, facial recognition) to enhance access control processes
Critical Infrastructure Standards	<ul style="list-style-type: none"> Investigate standards for the diversity of critical infrastructures
Automated Defenses	<ul style="list-style-type: none"> Develop a system(s) for automatic defense of cable routes from backhoes, etc
Background Checks	<ul style="list-style-type: none"> Provide better background checks for people with access to critical facilities
Anomaly Detection	<ul style="list-style-type: none"> Develop a process to analyze patterns of facility use (e.g., social engineering, data mining)
Information Availability	<ul style="list-style-type: none"> Research the possibility of withdrawing critical vulnerability information from the public domain
Immune Buildings	<ul style="list-style-type: none"> Research and develop “immune” building technologies to better secure facilities against biohazard attacks

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?