CSIIR Workshop Theme

This document is meant to help focus the CSIIR workshop participants in developing their individual presentations as well as to give context toward the common goal of developing our near term research goals aimed at finding/building a tangible doable foundation that can help expand our collective capabilities and broaden our opportunities for future collaborative (i.e., summer research visitations and beyond) R&D success in Cyber Security and Information Infrastructure.

Forward

The information infrastructure consists of technologies and capabilities for gathering, handling, and sharing information that are accessible to, or commonly depended upon by, multiple organizations, whether within a single enterprise, a critical infrastructure sector such as banking and finance, the U.S. Government, the nation as a whole, or transnationally. The information infrastructure includes well-engineered systems as well as poorly configured systems in businesses and homes.

In the United States, the private, academic, and public sectors invest significant resources in cyber security. The commercial sector primarily performs cyber security research as an investment in future products and services. While the public sector also funds R&D in cyber security, the majority of this activity focuses on the specific missions of the government agency funding the work. Thus, broad areas of cyber security remain neglected or underdeveloped. Therefore, the following agenda identifies the highest-priority gaps, i.e., R&D problems of significant value to the security of the information infrastructure that are either not funded or under-funded within the collection of private sector and government-sponsored research in the U.S., but are expected to become significant foci in the future based on thrusts currently being promoted by the I3P (http://www.thei3p.org).

Agenda

1. **Enterprise Security Management:** Each piece of the information infrastructure may be owned by individuals or enterprises, but we are all interconnected. Therefore, the enterprise security management (ESM) challenge is to integrate diverse security mechanisms into a coherent capability for managing access to and use of enterprise resources, monitoring behavior on enterprise systems, and detecting and responding to suspicious or unacceptable behavior. While the marketplace offers product suites under the rubric of ESM, the problem area is broader than the fragmented capabilities provided by existing products. Research needs remain in the areas of enterprise policy definition and management, definition and maintenance of a targeted risk posture, and definition of, and protection at, security boundaries. IT-based collaboration with partner organizations, and increased services to home users make these boundaries more complex and extend the definition of "insiders." Further research is needed to address the insider threat.
2. **Trust Among Distributed Autonomous Parties:** In cyberspace, entities –individuals, organizations, software, and devices –need to establish relationships dynamically and without recourse to a central authority or previously determined trusted third party. Existing research, particularly in terms of the techniques entities use to establish trust in the security of other entities, is expected to address many of the needs articulated by enterprise users. However, solutions are needed that address the autonomy, scale, complexity, and dynamism of critical infrastructures. Research needs exist for trust models for autonomous entities that are geographically or organizationally distributed, definition and management of dynamic security relationships in peer-to-peer settings, techniques for developing trust relationships between systems and end-user devices such as cell phones or laptops, and approaches to establish trust in data.
3. **Discovery and Analysis of Security Properties and Vulnerabilities:** The information infrastructure has a large number and variety of components, in different forms: hardware, firmware, software, communications media, storage media, and information. Frequently, the properties of these components are poorly understood, due to undocumented functionality, flaws in their design or implementation, or unanticipated uses. Products and systems commonly include vulnerabilities and inadequately understood security properties. Moreover, the security properties

of a system or subsystem cannot be derived or deduced from those of its components, and emergent properties of large-scale systems are difficult to describe, much less predict. Considerable effort has been applied to the problem of ensuring the presence of desired security properties and preventing (or determining the presence of) vulnerabilities. The need is acute for ways to determine, throughout a product or system's life cycle (development, integration, update and maintenance, decommissioning, or replacement of components), whether exploitable defects have been introduced or unanticipated security properties have emerged or escalated. Research is needed into techniques, embodied in tools to ensure their utility, to analyze code, devices, and systems in dynamic and large-scale environments.

4. **Secure System and Network Response and Recovery:** The proliferation of numbers and types of computing devices has resulted in the increasing size and complexity of the information infrastructure. Response to and recovery from attacks against such multifaceted systems are hindered by this inherent complexity. As a result, response across a set of organizations is often uneven and difficult to coordinate, and reconstitution to a secure state can be difficult. The potential for survivability from attacks and in making intrusion detection systems more proactive has driven research into secure response and recovery. Current research, however, does not adequately address the issues of scale, coordination across different administrative and policy domains, or coordination across the highly diverse systems that are the hallmarks of information infrastructure protection. Research needs remain in the areas of prediction or pre-incident detection, as well as recovery and reconstitution for systems of systems.

5. **Traceback, Identification, and Forensics:** During and after an attack, responding organizations must have prompt and reliable information to determine and implement an appropriate response. Current capabilities are oriented toward enabling the enterprise to detect and respond internally to suspected attacks. Research is needed into capabilities that enable responders to trace back, or identify the source location of the attack; to identify the individual, group, or organization originating the attack; and to determine the actual nature of the attack.

6. **Wireless Security:** Wireless technologies are increasingly crucial to enterprise systems and across critical infrastructure sectors. Wireless networks include not only wireless telecommunications per se, but an increasingly diverse set of end devices, such as sensors, process controllers, and information appliances for home and business users; in some cases, end devices may also provide wireless telecommunications services. Many security concerns for wireless networks mirror those for the wired world; however, in practice, solutions developed for wired networks may not be viable in wireless environments. Private sector concern, and thus investment, focuses on proprietary or enterprise solutions. Research is needed to make security a fundamental component of wireless networks, develop the basic science of wireless security, develop security solutions that can be integrated into the wireless device itself, investigate the security implications of existing wireless protocols, integrate security mechanisms across all protocol layers, and integrate wireless security into larger systems and networks. In particular, research is needed into security situation awareness techniques for wireless networks and strategies to address distributed denial-of-service attacks.

7. **Metrics and Models:** Individuals, organizations, and critical infrastructure sectors bear the risks of relying on the information infrastructure. For organizations to manage cyber security risks–to accept a given level of risk, transfer or externalize risk, or apply resources to decrease the level of risk to an appropriate balance–decision makers need a clear and defensible basis for making investment decisions that can be related to organizational missions and strategies. That basis should be founded on rigorous and generally accepted models and metrics for cyber security. Research is needed to provide a foundation of data about the current investment and risk levels. Research is also needed to define metrics that express the costs, benefits, and impacts of security controls from multiple perspectives–economic, organizational, technical, and risk–so that the dynamics at work in making security decisions can be better understood. Research is needed into techniques for modeling the security-related behavior of the information infrastructure and predicting consequences of risk management choices.

Frequently noted are the importance of education, training, and awareness; quality assurance methodologies; information sharing and coordination; practicable procedures; and physical security. These areas are important considerations for researchers who seek ultimately to affect the practice of cyber security. Similarly, technology transfer is frequently identified as problematic, highlighting the need for cyber security R&D programs to explore innovative strategies for improving the flow of ideas and technologies between researchers, product developers, system integrators, and end user organizations.

March 14-15 Workshop Focus:

Insider Threats: Develop outside-of-the-box concepts for near-term capabilities in identifying, defending against, and countering insider who attempts to abuse his or her computer privileges. The potential for damage from insider threats can be potentially catastrophic. Insider threat is defined as the potential damage to the interests of an organization, a company, or a corporation, done by a person regarded as loyally working for or on behalf of the organization, company, or corporation. The insider threat focus is limited to threats posed to devices connected to a network. This can be simply inadvertent violation of security policy or overt attempt at defeating the security systems from within the network.

Life Cycle Threats:
There is not a means for automated testing of large software, both static and mobile code, to detect, identify malicious code, sleeper codes, and exploitable vulnerabilities and to determine and understand the potential impact on the life-cycle of the codes. Current testing approaches are largely manual rather than automated.

Distributed Ad Hoc Trust/ Multi-Level Trust:
A mobile ad hoc network (MANET) is a network formed in a spontaneous manner without any central administration or with few connections to other fixed networks (i.e., an autonomous system of mobile nodes). The absence of the pre-existing knowledge between the nodes and no trusted central server make traditional trust establishment mechanisms and assumptions inappropriate. The communication among nodes is prone to security attacks and nodes can be easily compromised. Attacks such as wormhole and DoS can compromise routes through spoofing ARP or IP packets (passively or actively). Threshold cryptography is an example of one solution but suffers in cases of bandwidth constraints and energy conservation so an efficient implementation of the scheme is critical. A multi-level trust model is needed, in which a device's capabilities in the network are determined by the level of trust assigned to them and the trust level is determined by the certificates issued by their peers.