NISSC OCTOBER 5-8, 1998
R & D TRACK

IMPROVING NETWORKED INFORMATION SYSTEM TRUSTWORTHINESS: A RESEARCH AGENDA

Introduction to *Trust in Cyberspace*, Fred B. Schneider (Chair)
The operation of our nation's critical infrastructures is becoming increasingly dependent on vulnerable networked information systems (NISs). Improving the trustworthiness of these NISs is difficult given the limitations of available knowledge and technologies. A broader range of choices is needed, and new research is essential for that. Such a research agenda is proposed in *Trust in Cyberspace*, the final report of the Committee on Information System Trustworthiness of the National Research Council's CSTB. This panel will present the principal findings, conclusions and recommendations from that study.

Network Trustworthiness: The Public Telephone Network and the Internet, Steven M. Bellovin
Many of the technical problems faced by developers and operators of future NISs can be anticipated by examining the public telephone network (PTN) and the Internet. Besides being large and complex NISs, the PTN and Internet are likely to provide communications services for most other NISs. Yet today, the PTN and Internet are vulnerable to environmental disruption, operational error, hardware and software design implementation errors, as well as malicious attacks; and both are evolving in ways that affect these various dimensions of their trustworthiness.

Software and Architecture Issues, John C. Knight
When implementing an NIS, the well-known difficulties associated with software development are compounded by the need to integrate legacy systems and by the realities of COTS (Commercial Off the Shelf) components. Moreover, the assurance question takes on an entirely new character with systems that are large, geographically distributed, grow by accretion, and are not completely under control of developers either before or after deployment. Ideally, a discipline would enable system developers to build trustworthy systems by combining untrustworthy components according to engineering principles. Clearly, there are many other opportunities for research here.

Networked Information Systems and Security, Stephen T. Kent
Although today attacks are responsible for relatively few NIS outages, attacks are the fastest growing source of NIS disturbances and are potentially the most destabilizing form of trustworthiness breach. The limited utility of extant security models, products, and services can be a starting point for identifying future directions for security research. The trustworthiness implications of anticipated developments in hardware and software, such as the increasing use of mobile code, also must be considered.

Economic and Public Policy Context for Trustworthiness, Fred B. Schneider
The viability of technological innovation is invariably determined by economic and political realities. How do consumers decide what level of investment to make in trustworthiness? What are the important forces in the market for trustworthiness products and services? Government policies, such as those relating to cryptography, are also strong influences on consumer and producer decision making. As the major supporter of research relating to NIS trustworthiness, the role, priorities, and management of the federal funding agencies will be discussed, with recommendations for improving the process of research funding.