Panel

Technologies/Procedures Needed to Enhance the Assurance of the Telecommunications Infrastructure

Panelist:

Dick Brackney (**Panel Chair**)
National Security Agency
email: rcbrackney@aol.com

Nancy Wong
President's Commission on Critical Infrastructure Protection
nancy.wong@pccip.gov

Teresa Lunt
Defense Advanced Projects Agency (DARPA)
email: tlunt@darpa.mil

Steve Kent
BBN
email: kent@bbn.com

John Kimmins
BELLCORE
email: jkimmins@notes.cc.bellcore.com

Ted Humphreys
XiSEC Consultants (UK)
email: ted@xisec.demon.co.uk

Panel Summary

Civilian and military leaders as well as policy makers have all recognized the growing dependencies between the telecommunications infrastructure and national security objectives. For example, the vast majority of DOD's communications relies on the public telephony and data networks for connectivity. Furthermore, the U.S. Department

of State relies on the same public telecommunications infrastructures for the transfer of diplomatic information. In other words, these public, open systems based communications networks, provide the transport layer for many governmental activities and other infrastructures such as power and utility distribution, financial and banking, and transportation systems. Consequently, the Government is particularly concerned about denial of service attacks to public communications in times of crisis.

This Panel will discuss a number of issues that are related to the technologies and procedures that are needed to increase the level of assurance in the telecommunications infrastructure. Experts from the Government, telecommunications service providers, and the standards community will share their views on the kinds of technologies and technological as well as procedural advances that will be necessary to significantly increase the assurance of the current and emerging national and global telecommunications infrastructure.

Internet Routing Infrastructure
Steve Kent, BBN

The Internet routing infrastructure, especially BGP route advertisements, is vulnerable to a variety of attacks that can severely degrade or deny service to large numbers of subscribers. In fact, accidental configuration errors have resulted in such "attacks" during 1997. BGP peer authentication and integrity facilities have been defined, but are rarely deployed due to the lack of a suitable key management infrastructure. Even if these security mechanisms were widely deployed, the lack of a corresponding authorization infrastructure means that errors (or attacks) could still create routing "black holes," and similar problems on a large scale. The work described here is an ongoing project to create an authorization and key management infrastructure for use with BGP, and to add mechanisms to BGP to support checking and enforcement of route authorization information.

Intrusion Detection: Technology Gaps and Research Investments

Teresa F. Lunt, DARPA

Today's intrusion detection systems attempt to detect attacks on individual end systems rather than on networks or network elements, and too many of them are Unix-specific and Internet-specific. They focus on penetrations rather than on detecting attacks intended to disrupt or manipulate the infrastructure. They are knowledge-based, looking for strings associated with known intrusions, which means that they can detect

only what they know to look for. Most systems look for only a dozen or so intrusion types, whereas serious IW adversaries can be expected to use "surprise" attacks we haven't seen before. Today's systems have a high number of false alarms, with most of the
flagged activity being of little concern (e.g., password guessing). This results in an extremely large numbers of alarms, which must be investigated manually. There is no ability for cooperating intrusion detectors, which could filter events of lesser or only local concern to facilitate scaling. Moreover, these systems cannot deal with missing, incomplete, untimely, or otherwise faulty data.

Under investigation at DARPA are methods to detect highly unusual events or combinations of events. These include statistical methods, neural networks, and machine learning. We are also investigating methods to detect activity outside prescribed bounds. We still do not have answers to questions such as detection performance in realistic settings with single methods and combinations of methods, detection performance with faulty data, false positive and false negative rates, and time to detection. We also need efficient and effective methods for peer-to-peer cooperative problem solving to be applied to the detection problem.

There is also a need for operational deployment of advanced intrusion detection prototype systems. We need to learn how advanced systems will behave in an operational environment, especially of an interesting scale. We expect such experience
to provide valuable feedback to the research community, as we learn through experience what works and what doesn't.

SECURING THE EVOLVING PUBLIC TELECOMMUNICATIONS NETWORKS

J. KIMMINS, BELLCORE

The current public telecommunications infrastructure in the United States is going through
massive changes. These changes have serious security impact if they are not properly planned, implemented and managed. Some of these high-impact changes are the open interfaces to network elements and support systems, distributed switching architectures, mobile user services, customer network management capabilities and the insertion of new technologies, like broadband, into the network infrastructure.
All of these changes create multi-dimensional security issues as well as the need for different types of solutions. They include changes in policies, methods and procedures, adaptable security architectures and integrated and interoperable security technology. There are also problems, like software integrity, that need further study before the appropriate controls can be developed and

implemented to effectively deal with the major issues.

GII Security - Research, Technical Developments and Standards
Ted Humphreys, XiSEC (UK)

The Global Information Infrastructure promises to revolutionize electronic commerce, revive and energize government, and provide new and open access to the information society. Consequently security for GII is of critical importance to individuals, businesses and governments: both for privacy protection, and security and reliability, to provide the right levels of confidence and assurance in using this information infrastructure.

Work is being undertaken at different levels:

- standardization effort is being applied within ISO/ISE and ITU-T, and at national levels (e.g. the ANSI IISP);
- research is being carried at the national, regional and global levels (e.g. global interoperability of broad networks, global emergency response networks, telecoms networks for government on-line, trans-European networks in telecommunications);
- pilot projects (e.g. the G7 Pilots).

There are many security issues to be consider and many areas of research into the security and assurance of telecoms networks to be covered. This presentation reviews some of the requirements and topics for research and standardization currently being discussed for GII Security.

Technology Research

Nancy Wong, PCCIP

From my professional experience and perspective, technology and tools are only as effective as the processes and mind-set/culture which are in place that uses them. Information assurance consists of a system of processes, technology/tools which support those processes, and an organizational framework of accountability. Assurance can only be as strong as the weakest element in that system.

Implementation of information assurance technology can facilitate effective processes and sustain a supportive mind-set for information assurance when they are:

- Easy to install, maintain, and use;
- Transparent to the end user of the business asset the assurance tool was designed to protect;
- Integrated, compatible, and delivered as part of the system they are to protect, not a separate add-on, which the customer must monitor for interoperability through following upgrades.