NISSC Panel: Preparing for Internet Threats in the Years 2001 to 2010

Panel Chair: Barbara Y. Fraser

Panelists:

Dr. Steven Lucas
Senior Vice President and CIO
Privaseek, Inc.

Ken Fong
Senior Security Analyst
IBM Security and Privacy Services
IBM
Fong, Ken" klfong@us.ibm.com

Lawrence R. Rogers
Senior Member of the Technical Staff
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University

Description:

As computers networks have expanded over the last few years and interconnectivity of these networks has increased, critical information resources and business activities have moved to the Internet. In the past ten years, we've seen the Internet grow from under 100,000 hosts to tens of millions of hosts, and hundreds of millions of users. Increasingly, valuable assets are being stored, processed, and transmitted across these networks. In the civilian agencies alone, several notable examples can be seen. Law enforcement officials rely on the FBI's computerized databases, the IRS relies on computers to process and store taxpayer data, and the Customs Service depends on computer systems for the processing and inspections of billions of dollars worth of imported goods. Financial institutions are providing more online services to their banking customers and power companies rely on computer system and networks to control the distribution of power throughout the United States.

All of this growth means that there are more and more valuable assets supported by these computer networks, and the Internet in particular. As the value of available information and services increases, there will be a corresponding increased interest by criminals and other hostile entities to harvest these assets for their own benefit and profit.

In the past 10 years, the CERT Coordination Center has handled over 15,000 computer security incidents. The results of these incidents have included the modification and loss of information, the disclosure of sensitive information and

the disruption of services. Today, the gains to be had through exploitation of security weaknesses are staggering, and the potential damages that can be wrought, catastrophic.

This panel of experts will discuss current intruder trends and what they view are the most serious emerging threats that will affect Internet-connected systems and networks over the next 10 years. In addition, the panel will present their views on what the community needs to do now to prepare for those threats.