President’s Information Technology Advisory Committee

Subcommittee on Cyber Security

Update

F. Thomson Leighton, Chair

January 12, 2005

National Science Foundation

Arlington, VA

Charge to the Subcommittee

- How well is the Government targeting the right research areas?
- Is there a good balance between short-term and long-term research?
- Have the research programs been successful?
- What can be done to improve technology transfer?
- Are we well prepared to respond to the cyber security challenges of the future?

Subcommittee Members

- ***F. Thomson Leighton***, Ph.D., ***Chair***, Chief Scientist, Akamai Technologies and Professor of Applied Mathematics, M.I.T.
- ***J. Carter Beese***, Jr., President, Riggs Capital Partners
- ***Patricia Thomas Evans***, President and CEO, Global Systems Consulting Corporation
- ***Luis E. Fiallo***, President, Fiallo and Associates, LLC
- ***Harold Mortazavian***, Ph.D., President and CEO, Advanced Scientific Research, Inc.
- ***David A. Patterson***, Ph.D., Professor and E.H. and M.E. Pardee Chair of Computer Science, University of California, Berkeley
- ***Alice Quintanilla***, President and CEO, Information Assets Management, Inc.
- ***Eugene H. Spafford***, Ph.D., Professor and Executive Director, Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University
- ***Peter S. Tippett***, M.D., Ph.D., CTO and Vice-Chairman, TruSecure Corp.
- ***Geoffrey Yang***, Managing Director, Redpoint Ventures

Subcommittee Activities (1)

- PITAC meeting on 4/13/04
  - Presentations from representatives of DHS, NSF, and DARPA, and an academic technical expert
  - Included a public comment period
- Administrative meeting on 4/14/04
  - Organizational session for the subcommittee
- PITAC meeting on 6/17/04
  - Status update
  - Included a public comment period

Subcommittee Activities (2)

- Information gathering meeting on 7/29/04
  - Presentations from Federal agency representatives: ODDR&E, DHS, NSA, ARDA, NIST, and NIJ; and from several industry experts
- Town hall meeting at GovSec on 7/29/04
  - Presentations from Harris Miller, President, Information Technology Association of America, and Joel Birnbaum, Chair, NRC/CSTB Committee on Improving Cyber Security Research in the United States
- Formal request to agencies (late July)
  - Asked for written response to questions about an agency’s cyber security R&D activities

Subcommittee Activities (3)

- Analysis of data from RAND and Federal agencies
  - Technical support from PITAC member Peter Tippett and OSTP
- OMB data call
- Review of findings and recommendations of past reports

Subcommittee Activities (4)

- Conference calls with senior agency officials
- PITAC meeting on 11/19/04
  - Provided update and presented draft findings and recommendations
  - Deliberated on draft findings and recommendations
  - Solicited further input from the public

Subcommittee Activities (5)

- Extensive revisions and editing of draft report based on input from PITAC members and the public
- Vetting of data
- PITAC meeting on 1/12/05
  - Provide update on final draft of report
  - Solicit further input from the public
  - Deliberate on draft report

Next Steps

- Discuss today’s inputs and make revisions in the report as appropriate
- Obtain approval from PITAC
- Perform final editing
- Release report to the President and the public

President’s Information Technology Advisory Committee

Subcommittee on Cyber Security
Presentation of Draft Report:

Cyber Security: A Crisis of Prioritization

F. Thomson Leighton, Chair

January 12, 2005
National Science Foundation
Arlington, VA

Report Outline

- Executive Summary
- Cyber Security: A Problem of National Importance
- Federal Cyber Security Research and Development: Current Priorities, Future Impacts
- Findings and Recommendations

Statement of the Fundamental Problem

The information infrastructure of the United States, which is now vital for information, communication, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of the cyber security technologies that underpin these products and practices. The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security in order to fulfill its responsibilities in this regard.

Background

- There has been explosive growth in the use of networks to connect IT systems.
- It is now relatively easy to obtain information, to communicate, and to control IT systems across great distances.
- Because of the tremendous productivity gains and new capabilities enabled by networked systems, they have been incorporated into virtually every aspect of the Nation’s critical infrastructure—including the communications, utility, financial, transportation, and defense sectors.

Background (2)

- Ubiquitous interconnection is central to what makes IT important to society.
- BUT ubiquitous interconnection is also a primary source of widespread vulnerability.

Societal Consequences of Information Technology Vulnerabilities

- Past Examples include:
  - Distributed denial of service attacks
  - Theft of financial and personal data
  - Failures of major networks
  - Loss of control of utility SCADA systems

- Future Threats:
  - Disruption of telecommunications
  - Attacks on the Global Information Grid

The Problems are Growing at a Dramatic Rate

- The number of new vulnerabilities discovered in software is growing at 140% per year, and is now in excess of 4000 per year (CERT).
- The average time between disclosure of a vulnerability and release of an associated exploit has dropped to 5.8 days (Symantec).
- The percent of PCs infected per month has grown from 1% in 1996 to over 10% in 2003 (ICSA Labs).
- The rate at which new hosts are “zombied” rose from 2,000 per day to 30,000 per day during the first 6 months of 2004 (Symantec).

The Problems are Growing at a Dramatic Rate (2)

- 92% of organizations experienced “virus disasters” in 2003 (ICSA Labs).
- 83% of financial institutions experienced compromised systems in 2003, more than double the rate in 2002 (Deloitte).
- Hostile (worm) traffic originated from 40% of networks controlled by Fortune 100 companies in 1H04, despite the fact that these companies have taken a variety of protective measures (Symantec).

The Problems are Growing at a Dramatic Rate (3)

- 17% of 100 companies surveyed reported being the target of cyber extortion (CMU-Information Week)
- The number of unique phishing attacks is doubling every month with 2000 different attacks perpetrated against millions of users in July alone (Anti-Phishing Working Group).
- 1% of U.S. households fell victim to phishing attacks in early 2004, at a cost of over $400M in direct monetary losses (Consumers Union).

The Problems are Growing at a Dramatic Rate (4)

- Cyber security is not just about email being slow or your favorite E-commerce site being down.

- Viruses, worms, Trojan horses, spoofing attacks, cyber extortion, and other kinds of cyber attacks are like a rapidly spreading cancer in the IT and networking world.
  - They are largely invisible to the lay person but alarming to those who know how to diagnose a dangerous condition.
  - The threat they pose is rapidly growing.
  - To combat the problem, we must establish a foundation of knowledge and skill that will assist the cyber security professionals of tomorrow.

How Did We Get Into this State?

- The network protocols used today are based on those used 30 years ago, which were developed in an environment of trust.
- The vast majority of R&D has been devoted to building new functionality and not on securing that functionality.
- Traditional notions of security rely on border defenses, which are not sufficient in today’s Internet-based world.

How Did We Get Into this State? (2)

- Cyber security is a very difficult problem, and the Nation was reluctant to make the necessary investment.
  - Although there have been many warnings, we have only recently begun to suffer substantial cost.
- There are no quick fixes—retrofitting security into our networked IT infrastructure will require many years of work.

What Must be Done
to Improve Cyber Security

- Funding of Basic Research
  - Basic research is needed to move us from a model of “plugging holes in the dike” in response to each new vulnerability to a model where the system as a whole is secure against large classes of current and future threats.
  - Basic research is the responsibility of the Federal government.

What Must be Done to Improve Cyber Security (2)

- Development and Technology Transfer
  - Effective development needs supporting mechanisms such as testbeds and metrics.
  - The Federal government has a critical role to play in the development of metrics, testbeds, and best practices.
- Market Adoption of Products and Best Practices by Government and Industry
  - Very important but not the primary focus of this report.

Cyber Security R&D Activities in Federal Agencies

- Multiple agencies are involved in cyber security R&D.
- Primary focus of the Subcommittee has been on NSF, DARPA, and DHS.
- Also of note: NIST, NSA, and ARDA.
- Others: ODDR&E, DOE, FAA, NASA, NIJ, and uniformed services.

National Science Foundation (NSF)

- Only Federal agency with substantial activity that focuses on basic research for the civilian sector.
- Much of NSF’s cyber security activity takes place within its Cyber Trust Program.
- Construes “cyber security” very broadly
- FY 2004: $76 million total; $37 million for research grants (which includes $5M from DARPA)
  - Funded about 8% of proposals (6% of requested dollars); about 25% worthy of funding

Defense Advanced Research Projects Agency (DARPA)

- Military focus: Some emphasis on networking systems that find targets and systems that kill targets.
- Short-term time horizon: departure from historical support of longer-term research.
- Programs are increasingly classified, thereby excluding most academic institutions--also a departure from historical support of university researchers.
- Assumes other agencies, especially NSF, will fund basic research—DARPA’s (new) strategy is to incorporate pre-existing technology into products for the military.

Department of Homeland Security (DHS)

- Much of the DHS cyber security activity takes place within its S&T Cyber Security R&D Program.
  - Focus on cooperative efforts, infrastructure such as metrics and testbeds, and technology transfer. Some efforts to improve Government adoption of new products.
- FY 2004 budget (and FY 2005 as well) is $18 million for cyber security; about $1.5 million directed to basic research. Most funding for short-term activities.
- WMD is primary priority. Assumes NSF and industry are responsible for basic research.

National Institute of Standards and Technology (NIST)

- Focus on standards, metrics, guidelines, testing, security checklists, and research.
- Research program is primarily near-term.
- Cyber security budget is approximately $10 million in FY 2004.

National Security Agency (NSA) & Advanced Research and Development Activity (ARDA)

- NSA
  - Focus on high-end threats.
  - Almost all cyber security research is directed towards the military and intelligence communities.
- ARDA
  - Focus on high-risk, high-payoff sponsored research.
  - Almost all research is directed towards the intelligence community.

Cyber Security R&D Expenditures

Preliminary PITAC Analysis

(Based on FY 2004 Data)

	Military and Intelligence	Civilian	Totals
Short Term	$136+ million	$38 million	$174 million
Long Term	$27 million	$37 million	$64 million
Totals	$163 million	$75 million	$238 million

Findings and Recommendations

Issue 1: Federal Funding Levels for Basic Research on Civilian Cyber Security

- Finding: The Federal R&D budget provides inadequate funding for basic research in civilian cyber security.

- Recommendations:
  - The NSF budget for cyber security should be increased by $90 million annually.
  - Funding for basic research on civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA.
  - Funding should be allocated so that ten specified areas of cyber security research are addressed.
  - Further increases in funding may be necessary depending on the Nation’s future cyber security posture.

The Need for a Long-term Focus

- Most cyber security funding addresses immediate needs.
- These needs must be addressed, but such activities generally do not contribute toward long-term solutions.
- The diversity and magnitude of future vulnerabilities frame a formidable challenge that is not being addressed adequately.
- The present funding situation forces tomorrow’s cyber security efforts to be reactive rather than proactive.

Avoiding Incrementalism

"We have virtually no research base on which to build truly secure systems…. When funds are scarce, researchers become very conservative, and bold challenges to the conventional wisdom are not likely to pass peer review. As a result, incrementalism has become the norm."

Wm. A. Wulf, President
National Academy of Engineering

Civilian Cyber Security Research

- Refers to unclassified R&D associated with systems and networks used by civilian Federal agencies, utilities, corporations, universities, and the population at large.
- Does not include research targeted exclusively at military or intelligence contexts, which is often ultimately classified.

The Importance of Civilian Cyber Security Research

- Classified cyber security R&D is, of course, needed for numerous purposes.
- However, classified work tends not to benefit generic cyber security products—which are used throughout society (including the military and intelligence communities).

The Amount Needed for Research

- Cyber Trust
  - Provides approximately $37 M in research grants.
  - The Cyber Trust success rate (8.2% of proposals and 6.1% of requested funds) is approximately a factor of 3-4 lower than the NSF average.
  - An approximate quadrupling of the Cyber Trust budget could be productively used by the cyber security R&D community that focuses on civilian work.
  - NOTE: Reallocations within CISE are not desirable:
    - Low success rates within CISE as compared to other NSF directorates.
    - Reductions in other areas of IT R&D may also inhibit cyber security R&D.

The Amount Needed for Research (2)

- Military and intelligence R&D funded at $136+M vs. $75 M for civilian R&D.
- Sponsor agency diversity is desirable, so increased funding for cyber security R&D should include NSF and other agencies.
- Significant reductions in support for cyber security R&D at DARPA and low prioritization at DHS intensify demands on NSF funding.

Areas in Need
of Increased Support

- Computer Authentication Methodologies
- Securing Fundamental Protocols
- Secure Software Engineering and Software Assurance
- Holistic System Security
- Monitoring and Detection

Areas in Need of Funding (2)

- Mitigation and Recovery Methodologies
- Cyber Forensics and Technology to Enable Prosecution of Criminals
- Modeling and Testbeds for New Technologies
- Metrics, Benchmarks, and Best Practices
- Societal and Governance Issues

Areas in Need of Funding: Summary

- There is no silver bullet or small set of silver bullets.
- It is not a matter of “tweaking” in the Internet—there is no foundation of security to tweak.
- The existing Internet was built based on assumption of trust: it was assumed that no one would harm the infrastructure, even by accident.

Issue 2: The Cyber Security Basic Research Community

- Finding: The Nation’s cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States.
- Recommendations:
  - The Federal government should intensify its efforts to promote recruiting and retention of cyber security researchers and students at research universities, with a goal of doubling the size of the civilian cyber security basic research community by the end of the decade.
  - Specifically, the government should
    - increase and stabilize the funding for civilian cyber security basic research,
    - support programs that enable researchers to move into cyber security research from other fields, and
    - emphasize the importance of unclassified cyber security basic research.

The Cyber Security Research Community Today

- Cyber security has historically been the focus of a small segment of the computer science research community.
- There are fewer than 250 active research faculty in cyber security or cyber assurance in the U.S., of which only a fraction have formal education or substantial professional experience in cyber security or cyber assurance.

Issue 3: Translating Research Into Better Cyber Security for the Nation

- Finding: The PITAC finds that current cyber security technology transfer efforts are not adequate to successfully transition Federal research investments into civilian sector best practices and products.
- Recommendations:
  - The Federal government should strengthen its cyber security technology transfer partnership with the private sector.
  - Specifically, the Federal government should
    - place greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated,
    - jointly sponsor with the private sector an annual inter-agency conference at which new cyber security R&D results are showcased,
    - fund technology transfer efforts (in cooperation with industry) by researchers who have successfully completed a research grant, and
    - encourage Federally-supported graduate students and post-doctoral researchers to gain experience in industry as researchers, interns, or consultants.

Discussion

- In most areas of IT, there is a long and successful history of Federally funded IT R&D efforts
- Cyber security is different: Market forces have been less forceful and added value is ‘negative’—the absence of bad things happening.
- Another obstacle: the consequences of increasing classification of Federal government research.
- Making progress: Information transfer and people transfer

Issue 4: Coordination and Oversight for Federal Cyber Security R&D Activities

- Finding: The Federal cyber security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight.

- Recommendation: The Interagency Working Group on Critical Information Infrastructure Protection should become the focal point for coordinating Federal cyber security R&D efforts. It should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.

Existing Coordination Mechanisms

- Interagency Working Group on Critical Information Infrastructure Protection (IWG/CIIP),
  - reports to the Committee on Infrastructure of the National Science and Technology Council (NSTC)
- Interagency Working Group on Information Technology Research and Development (IWG/ITRD)
  - coordinates the NITRD Program and reports to the NSTC Committee on Technology, and its Coordinating Groups, especially the:
    - High Confidence Software and Systems Coordinating Group
    - Large Scale Networking Coordinating Group
- Infosec Research Council

What’s Missing?

- No entity within the Federal government charged with awareness of security needs, funding, and setting standards and direction for agencies.
- No overall oversight to ensure that the most critical research topics receive funding.
- No systematic effort to operationalize the results of R&D.
- Lack of a single authoritative source that could itemize spending categories and provide basic budget information

Coordination Should Include:

- Making decisions about Federal cyber security R&D activities cognizant of private sector efforts in this area.
- Meeting with private sector representatives responsible for deployed cyber security to better understand the implications of their needs for the research agenda to be pursued.
- Convening forums or roundtables in which participants from university, government, and industrial settings could meet to exchange information about high-level architectural issues and strategies to better meet the growing cyber security challenge.

Coordination Should Include:

- Supporting mechanisms, such as seminar series, for the informal exchange of information about ideas in cyber security R&D.
- Actively coordinating research priorities in different agencies so that unnecessary duplication is avoided and jointly supported work is undertaken when appropriate.
- Collecting data on cyber security R&D efforts throughout the Federal government on a systematic basis.

Question and Answer Period

- Public comments
  - From NSF in Arlington, VA
    - Queue behind the microphone for public comment.
    - State your name and affiliation.
    - Limit your remarks to 3 minutes.
  - On WebEx:
    - Using the chat feature, send a question to all participants. Co-Chair Edward Lazowska will read your question as time allows.
- Discussion by PITAC members