President's Information Technology Advisory Committee

Subcommittee on Cyber Security

Update

F. Thomson Leighton, Chair

November 19, 2004

Grand Hyatt Washington at Washington Center

Washington, D.C.

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
- Subcommittee 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)

- Subcommittee 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 Cybersecurity 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
  - Provide update and present draft findings and recommendations
  - Deliberate on draft findings and recommendations
  - Solicit further input from the public

Next Steps

- Discuss today's inputs and make revisions in the draft report as appropriate
- Generate remaining text
- Verify and vet data
- Complete draft report for consideration at the January 12, 2005 PITAC meeting

President's Information Technology Advisory Committee

Subcommittee on Cyber Security

Presentation of Draft Findings and Recommendations

F. Thomson Leighton, Chair

November 19, 2004

Grand Hyatt Washington at Washington Center

Washington, D.C.

Outline

- Chapter 2: Cybersecurity: A Problem of National Importance
- Chapter 3: Cyber Security Research and Development Activities Within the Federal Government
- Chapter 4: Findings and Recommendations

Chapter 2: Cybersecurity: A Problem of National Importance

Societal Consequences of Information Technology Vulnerabilities (1)

- IT is at the heart of society; IT runs critical infrastructures: electric power grid, financial systems, air traffic control, food distribution, defense networks, etc.
- The use of IT (and the faith in it) has had enormous positive impact on productivity, with tremendous remaining potential (e.g., see PITAC Health Care report).

Societal Consequences of Information Technology Vulnerabilities (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 (3)

- 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
  - The Global Information Grid

The Problems are Growing at a Dramatic Rate (1)

- 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 US 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)

- Cybersecurity is not just about email being slow or your favorite E-commerce site being down.
- Viruses, worms, Trojan horses, spoofing attacks, extortion, and the like are 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.

What Must be Done to Improve Cyber Security (1)

- 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.

Chapter 3: Cyber Security Research and Development Activities within the Federal Government

Activities in Federal Agencies

- Cyber security R&D takes place in a number of agencies.
- 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 substantial program to focus 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: $64 million total; $31 million for research grants (which includes $5M from DARPA)
  - Funded about 8% of proposals (6% of requested dollars); about 25% worthy of funding
- Other activities include scholarship support and initiatives that involve other NSF programs.

Defense Advanced Research Projects Agency (DARPA)

- Military focus: Some emphasis on networking systems that find targets and systems that kill targets.
- Short/middle-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) mission is to incorporate pre-existing technology into products for the military.

Department of Homeland Security (DHS)

- 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 $15 million in FY 2004 (which includes $5 million in reimbursements from other agencies).

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 Analysis)

	Military and Intelligence	Civilian	Totals
Short and Medium Term	$80 million	$43 million	$123 million
Long Term	$27 million	$31 million	$58 million
Unidentified Term	$115 million	$0	$115 million
Totals	$222 million	$74 million	$296 million

Chapter 4: Findings and Recommendations

Statement of the Fundamental Problem

The information infrastructure of the United States, on which we depend both directly and for control of our physical infrastructure, is vulnerable to terrorist and criminal attacks. The private sector has a key role to play in securing the nation's IT infrastructure, by deploying good security products and adopting good security practices. But the Federal government also has a key role to play in providing the intellectual capital and evaluation infrastructure that enables these good security products and practices. The committee finds that the U.S. government is largely failing in its responsibilities in this regard.

Issue 1: Funding Levels for Civilian Cyber Security Research

- Finding: The Federal R&D budget provides severely insufficient funding for civilian basic research in cyber security.
- Recommendation: The overall funding for civilian basic research in cyber security should be substantially increased, i.e., by an amount of at least $90 M annually. Further increases may be necessary depending on the Nation's cyber security posture in the future.

Issue 1: Discussion (1)

- Reversing the focus on near-term applications
  - 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.

Issue 1: Discussion (2)

- Avoiding incrementalism (1)

"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

Issue 1: Discussion (3)

- Avoiding incrementalism (2)
  - Non-incremental cyber security research is necessary because tweaking existing technologies is inadequate for needs of tomorrow.
  - In general, basic research takes longer and is riskier than applied research. Research programs need to accommodate longer time periods and some “failures.”

Issue 1: Discussion (4)

- Importance of civilian cyber security research (1)
  - Civilian cyber security R&D:
    - Refers to unclassified R&D associated with systems and networks used by civilian Federal agencies, corporations, universities, and the population at large.
    - Primary target user of the results from such R&D is the vast IT marketplace, which includes the commercial Internet and most private computing systems and networks connected to the commercial Internet, although users with specialized needs, such as the control of electric power generation and distribution, also benefit from civilian cyber security research.

Issue 1: Discussion (5)

- Importance of civilian cyber security research (2)
  - Civilian cyber security R&D does not include research targeted exclusively at military or intelligence contexts, which is often ultimately classified.
  - 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).

Issue 1: Discussion (6)

- Magnitude of the amount needed for research (1)
  - Cyber Trust
    - NSF is the primary funding agency for basic cyber security research. Its Cyber Trust program provides approximately $31 M in research grants.
    - The Cyber Trust success rate (8.2% of proposals and 6.1% of requested funds) is approximately a factor of 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.

Issue 1: Discussion (7)

- Magnitude of the amount needed for research (2)
  - 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.
  - 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.

Issue 1: Discussion (8)

- Magnitude of the amount needed for research (3)
  - Military and intelligence contexts funded at $220 M + vs. approximately $70 M for civilian contexts.
  - Cyber security R&D community is small. Future increases may well be justified. (See Issue 2)

Issue 1: Discussion (9)

- Magnitude of the amount needed for research (4)
  - Areas in need of funding:
    - Computer Authentication Methodologies
    - Securing Fundamental Protocols
    - Secure Software Engineering
    - End-to-end System Security
    - Monitoring and Detection

Issue 1: Discussion (10)

- Magnitude of the amount needed for research (5)
  - Areas in need of funding (2):
    - Mitigation and Recovery Methodologies
    - Cyberforensics and Technology to Enable Prosecution of Criminals
    - Modeling and Testbeds for New Technologies
    - Metrics, Benchmarks, and Best Practices
    - Societal and Governance Issues

Issue 1: Discussion (11)

- Magnitude of the amount needed for research (6)
  - 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 cyber security basic research community is too small, considering the importance of the work it undertakes, and fails to adequately engage the range of intellectual talent needed for genuine progress.
- Recommendation: The Federal government should aggressively seek to strengthen and enlarge the cyber security basic research community by supporting mechanisms aimed at recruiting and retaining current and future academic researchers in research universities.

Issue 2: Discussion (1)

- Cyber security has historically been the focus of a small segment of the computer science research community.
  - Probably only 200-300 significant, active research faculty in cyber security or cyberassurance in the U.S.

Issue 2: Discussion (2)

- Growing the community (1)
  - Increasing Federal funding for basic civilian cyber security research.
  - Providing stability of Federal funding.
  - Supporting mechanisms that enable researchers to move into cyber security from other fields.
  - Helping researchers obtain access to important data.

Issue 2: Discussion (3)

- Growing the community (2)
  - Favoring unclassified basic research.
  - Improving the utility of unclassified research to military programs.
- Issues 1 and 2 go hand-in-hand
  - A more robust research community can better ensure that important new ideas—as opposed to incremental advances—may be generated.

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

- Finding: Technology transfer efforts in the cyber security area are critical to the successful incorporation of Federal government-sponsored research into best practices and products.
- Recommendation: The Federal government should sustain and strengthen its support for technology transfer activities in cyber security.

Issue 3: Discussion (1)

- 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 3: Discussion (2)

- Information transfer
  - Sponsor annual inter-agency workshop/conference where new cyber security R&D results are showcased by federally funded grant recipients.
  - Require grant recipients to describe potential practical utility of their research results.
  - Establish a fund to support technology transfer efforts by researchers that have successfully completed a research grant.
  - Establish and maintain a national database of results from federally-funded cyber security research.

Issue 3: Discussion (3)

- People transfer
  - Give preference to research proposals from principal investigators with a track record of technology transfer efforts.
    - Also provide allowance for first-time cyber security principal investigators.
  - Encourage federally-supported graduate students and post-doctoral researchers to gain experience in industry.
  - Sustain and strengthen support for the development of validated metrics, models, datasets, and testbeds.

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

- Finding: The present Federal cyber security R&D effort lacks adequate coordination and coherence.
- Recommendation: An entity within the National Science and Technology Council should provide greater coordination and monitoring of federal R&D efforts in cyber security.

Issue 4: Discussion (1)

- Benefits of coordination
  - Avoid duplication of effort
  - Leverage efforts of other, related programs
  - Coordinated workshops can save money and participant time
  - Facilitate technology transfer by teaming with other entities

Issue 4: Discussion (2)

- Existing coordination mechanisms
  - Infosec Research Council
  - High Confidence Software and Systems Coordinating Group, Interagency Working Group on ITR&D
  - Interagency Working Group on Critical Information Infrastructure Protection

Issue 4: Discussion (3)

- What's missing?
  - No entity with 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.

Issue 4: Discussion (4)

- What's missing? (2)
  - Lack of a single authoritative source that could itemize spending categories and provide basic budget information.

Issue 4: Discussion (5)

- 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.

Issue 4: Discussion (6)

- Coordination should include (2):
  - 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

- Discussion by PITAC members
- Public comments
  - From the Grand Hyatt Hotel, Washington, D.C.:
    - 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.
  - On the teleconference:
    - Respond when prompted by Dr. Lazowska.