NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

HARDENING THE INTERNET

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

October 12, 2004

GEORGE H. CONRADES
WORKING GROUP CHAIR
CHAIRMAN AND CHIEF EXECUTIVE OFFICER
AKAMAI TECHNOLOGIES

ACKNOWLEDGEMENTS

Mr. George Conrades wishes to thank the members of the Working Group and Study Group who have contributed to this effort, as well as others who have supported us by sharing their wealth of knowledge. These individuals and companies represent some of the luminaries of the Internet industry, and this report would not have been possible without their continuous support.

Contributors:

Working Group Members:
George Conrades, Akamai
John Chambers, Cisco
Margaret Grayson, V-ONE
Alfred Berkeley, Pipeline Trading Systems

Study Group Members:
Bora Akyol, Cisco
Vint Cerf, MCI
John L. Clarke III, US-CERT
Andy Ellis, Akamai
Noam Freedman, Akamai
Adam Golodner, Cisco
Barry Greene, Cisco
Deb Miller, V-ONE
Bob Mahoney, Zanshin Security
J. Scott Marcus, Senior Advisor to FCC
Mike Petry, MCI
Jeff Schiller, MIT
Howard Schmidt, eBay
Marty Schulman, Juniper
Rick Waddell, MSN
Ken Watson, Cisco
Lee Zeichner, GMU

Department of Homeland Security Support:
Gail Kaufman
Brett Lambo
Tim McCabe
Nancy Wong

Additional Study Group Resources:
Pete Allor, ISS
Matt Bishop, UC-Davis
Steve Crocker, Shinkuro, Inc.
Sean Convery, Cisco

Sean Donelan, SBC
Matt Korn, AOL
Charles LeGrand, IIA
Gerry Macdonald, AOL
Paul Vixie, ISC

TABLE OF CONTENTS

Hardening the Internet

Executive Summary:

The Internet was designed 35 years ago as a robust, distributed network without centralized control in order to provide resiliency against a multitude of attacks, including nuclear war. Globally, the Internet has been substantially built out and built up throughout the last decade. The Internet is more than just a network of routers. Across the world, it has a network of computers, ranging from high-end computing environments and server farms in offices to end-user, personal computers in households. This distributed network of systems has proven resilient, especially to point failures such as the 9/11 terrorist attacks, natural disasters, or backhoes. The most consequential events to affect the functioning of the Internet and its dependent businesses have been attacks coming from within the Internet itself (e.g., the spread of worms, such as the Morris and Slammer worms and denial of service attacks against the services and protocols that make up key sections of the Internet).

While education and awareness programs, research and development, and increased law enforcement activities are ongoing to harden the Internet, the Council has developed more effective and efficient recommendations the Federal Government can implement, in partnership with industry to protect the network infrastructure, computers, and other devices attached to the Internet. This has become particularly important because more needs to be done to address the dynamic, changing environment and increasingly new audience of end-users.

Specifically, the National Strategy to Secure Cyberspace, which was released in February 2003, has provided foundational guidance to harden the Internet, providing effective cyber security tools and education to home users and small businesses through many outreach, awareness, and education efforts. The establishment of the US Computer Emergency Response Team (US-CERT) and its National Cyber Alert System provide a step toward a national awareness campaign. The alert system provides periodic alerts, tips, best practices and other guidance for dissemination to all sectors of our society. The Department of Homeland Security (DHS) also provides cyber security tips to home users and small businesses through the National Cyber Security Alliance's *StaySafeOnline* campaign to help educate all users about basic security practices, and to increase overall awareness as well as cyber security tool kits that can be disseminated to both groups.[1]

Despite progress, cyber attacks are costing the government and industry billions of dollars annually, which will likely increase in years to come. To help further progress, the President asked the Council in July 2003, to examine ways to harden the Internet. As a result, the Council created a Working Group to evaluate the work of many organizations and recommend ways for the Federal Government to address the President's request. Such organizations include: the National Security Telecommunications Advisory Council, the National Cyber

[1] According to June 2004 testimony of Amit Yoran, then director of National Cyber Security Division, before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census Committee on Government Reform U.S. House of Representatives.

Security Partnership, and US-CERT. The Working Group relied on the expertise of more than thirty study group participants, including individuals who were involved in designing the Internet 35 years ago.

The Council's report focuses its recommendations in the following three areas:

1) Near-term Approaches: Encouraging the adoption of Best Current Practices (BCPs)[2] as the most effective approach to harden existing defenses against attack. The Council centers these recommendations on education and awareness initiatives and research into the adoption of BCPs;
2) Long-term Approaches: With sufficient time for research and development, additional work on core Internet protocols can be used to harden the Internet and associated networks and devices against malicious attacks. The Council centers these recommendations on more robust research and development;
3) Empowerment: In the near and long term, Internet Service Providers (ISPs)[3] and law enforcement agencies need on-going capabilities to investigate suspicious activity, prosecute cyber criminals, and harden their core operations. The Council centers these recommendations for empowering ISPs and law enforcement agencies on research and policy issues.

The Council recognizes that other NIAC reports have considered a host of other issues surrounding the health of the Internet including:

- Vulnerability disclosure
- Regulatory and proper role of government intervention
- Prioritizing vulnerabilities
- Vulnerability scoring
- Information sharing, and interdependency and risk assessment.

This report does not seek to revisit those issues. Following the Background section are the specific recommendations made by the Council. Detailed discussions of the recommendations are found in the Recommendation Discussion sections. This report concludes with a list of resources the Council found useful and of interest within the Internet security arena.

Background:

One of the major benefits of the Internet is the common infrastructure that provides the core services. Specifically, the exterior routing fabric, BGP[4], and domain name service infrastructure, DNS[5], are the two principal building blocks of the network; the former allows

[2] For a list of BCPs, see the National Reliability and Interoperability Council's Best Practices Selector at http://www.bell-labs.com/cgi-user/krauscher/bestp.pl.

[3] The Council is referring to a broad set of service providers.

[4] BGP is the abbreviation for Border Gateway Protocol. BGP is used to exchange routing information between autonomous systems in the Internet.

[5] DNS is the abbreviation for the Domain Name System. DNS is used to convert human readable hostnames into network readable IP addresses.

the network to build itself and direct data streams in transit, while the latter allows for people to send requests to appropriate locations. Vulnerabilities in these infrastructures tend to be oriented around the ability of attackers to insert fraudulent control messages, with a secondary focus on the survivability of these systems to attack.

In addition to the global Internet, multiple public and private organizations run networks based on the Internet Protocol (IP), and are isolated from global networks. Despite being isolated, networks and the computers attached to them are not immune to threats that exist throughout the Internet today. Threats can vary from a trusted employee compromising corporate networks, to worms and viruses entering and affecting the performance and integrity of the network. Consequently, systems, that control vast network resources in aggregate, when compromised[6] by a malicious adversary, will leave open the possibility for information attack operations against these seemingly isolated infrastructures.

Hardening the Internet is a global, not just a national issue. The Internet infrastructure represents a complex interaction of computers, networks, cables, radio waves, processes, and people. Its use is managed by voluntary adherence to common practices promoted by the Internet Architecture Board, the Internet Assigned Numbers Authority, the Internet Engineering and Planning Group, Internet Engineering Steering Group, Internet Corporation for Assigned Names and Numbers, and the Internet Society. No single government or multi-national entity could accomplish the task of hardening the entire Internet, nor could one effectively harden its own part of the global Internet. The recommendations in this report regarding best practices adoption and research are applicable globally, and their voluntary adoption is highly encouraged. This report also makes specific policy recommendations for the President to help accelerate near-term and long-term hardening activities.

There are two areas of the Internet that could benefit from hardening:

- The core infrastructure -- the routers, name servers, and backbone links that comprise the interconnected network at the heart of the network

- The customer environment -- the personal computers, enterprise networks, and e-business servers that connect to the Internet and support our nation's businesses.

[6] These infected systems can be used for a variety of illegal activities including: Distributed Denial of Service (DDOS) attacks, spam propagation, and for infecting more machines. The DDOS attacks by machines that are owned are harder to filter out and distinguish from DDOS attacks that come from spoofed IP addresses. It is important that steps be taken to ensure end systems are well-protected and incident response mechanisms in place to mitigate compromised machines or botnets. Botnets are openly sold and bought on the markets. The focus of the attackers has shifted from pranks to financial gain. Attacks for financial gain will be harder to defend against than just pranks. They are developed using more advanced codes, which are harder to detect because they typically piggyback on normal Internet traffic.

The Council discovered a wealth of best practice guidelines exist and if implemented, would significantly strengthen the Internet. The Council's recommendations are divided into those which increase implementation of those best practices and those urging new technology areas to improve the environment. Since much of the infrastructure and environment lies in the control of the private sector, policy recommendations reflect what government traditionally does well, to encourage good behavior in the private sector. As a result, the Council suggests the Federal Government should:

- Convene groups of experts to guide hardening efforts
- Use the bully pulpit to educate and advocate for improvements
- Sponsor research to improve security technologies
- Encourage private development of best practices and standards.

SECTION I – RECOMMENDATIONS:

Recommendation Area I

Near-Term Hardening Approaches: Education and Awareness

Overview: Education and Awareness initiatives can provide the impetus for better security among the general Internet computing population, and help to ensure that developers of infrastructure and software systems and maintainers of Internet components implement BCPs. The recommendations regarding awareness focus on ensuring that system owners implement best practices already established for their respective systems, including best practices related to: routers, servers, and home personal computers. The recommendations regarding education focus on ensuring a common level of security understanding among software developers and that security education is readily accessible. These recommendations are a prelude to the work to be conducted by the Council's Workforce and Education and Preparation Working Group, which will delve more deeply into educational parity.

Issue: There is a need to strengthen awareness and adoption of Internet hardening best practices, both within the industry and within the general Internet computing public. Moreover, efforts should be undertaken to better understand the calculus decision makers employ to determine whether, and to what extent, they should invest in security resources.

These recommendations are described in more detail in Section 2, Recommendation Discussion.

Recommendations: Adoption of Security Best Practices

1A. Research the Level of Best Practice Adoption: The Federal Government should sponsor research on obstacles and solutions to the adoption of cyber security Best Common Practices (BCPs).

1B. Adopt Route and Packet Filtering: Industry should adopt and DHS should promote the use of route and packet filtering as important security best practices.

Recommendations: Awareness of Security Best Practices

1C. General Outreach and Awareness Programs: DHS should initiate robust and sustainable partnership programs to increase awareness activities targeted at educating the American public to implement best practices to improve computer security with metrics to monitor progress. While DHS already has programs in place, the Council believes more must be done to address the ever-changing technology and threats.

1D. Industry Education: DHS, software vendors, and academics should work jointly to develop guidelines for Secure Software Development Life Cycles. The Federal Government

should sponsor a research project to determine the effectiveness of the adoption of the Secure Software Development Life Cycle.

1E. Enterprise Board Education: The Federal Government should develop and sustain long-term partnerships with appropriate channels of communication and influence within industry to provide and promote education to boards of companies and universities around information technology (IT) security policy, oversight, and governance. The Federal Government should further promote cyber security policy and education through its appropriate agencies to contractors and government organizations that initiate procurements. The Council believes current approaches to this do not address why certain best practices are or are not followed throughout the government and industry.

Recommendation Area II

Longer-Term Hardening Approaches: Research and Development

Overview: In the near-term, through education and the adoption of BCPs, the resilience of the Internet will be improved. But additional research and development, work on core Internet protocols and a suite of tools and techniques for dealing with scalable monitoring, management of networks, and analysis of data will be essential for long-term Internet hardening. The areas of strategic importance for research and development include: routing registries, scalable management and anomaly detection tools, and network forensic data collection at high data rates.

Issue: While education and the adoption of BCPs are important first steps in improving near-term Internet resilience to ensure longer-term Internet hardening, funding should be made available to support extensive research and development programs. Research and development should be carried out in a number of key areas, including routing registries, scalable management and anomaly detection tools, and network forensic data collection at high data rates.

These recommendations are discussed in more detail in Section 2, Recommendation Discussion.

Recommendations: Research and Development

2A. Develop Route Registry Infrastructures: The Federal Government should establish funding for, and task a federal organization with guiding research – in conjunction with industry – for an automated route registry infrastructure for secure inter-domain routing. This research would address any technical and operational impediments to existing proposals like Secure Border Gateway Protocol (BGP) and Secure Origin BGP.

2B. Develop Management and Anomaly Detection Tools: Funding should be made available to various agencies to develop tools that will help capture malware[7] activity; anomaly detection tools; and standardized reporting tools.

2C. Fund Research for Development of Forensic Capabilities: Federal research funds should be provided to academia and industry to improve network-based forensic data collection, storage, and analysis at high data rates.

2D. Fund Research for Vulnerability and Flow Analysis: The President should encourage DHS to establish a research funding line specifically for improving scalable vulnerability/flow analysis for complex communications and security systems throughout the network.

Recommendation Area III

Empowering Service Providers and Law Enforcement

Overview: Malware costs the U.S. economy billions of dollars a year. Identity theft is the fastest growing and most widespread consumer crime. The Federal Government is taking notice of the increasing number of exposures and threats to critical infrastructure, consumer privacy, and economic interests. The following recommendations regarding increased information sharing within the public and private sectors, reviews of the existing laws and regulations, and funding to combat cyber crime are intended to address these very important aspects of Internet usage.

Issue: A crucial element in protecting the Internet against criminal activity and preventing subsequent damage to critical infrastructures is the increased involvement of Law Enforcement and the empowerment of ISPs to combat cyber crime. Sufficient resources should be made available to Law Enforcement and ISPs, and information sharing activities should be enhanced.

These recommendations are discussed in more detail in Section 2, Recommendation Discussion.

Recommendations: Empowering Service Providers and Law Enforcement

3A. Empower Internet Service Providers: The President should encourage industry to establish an Internet information-sharing mechanism to focus exclusively on Internet reliability and security issues.

3B. Enhancement of Online Law Enforcement: Examine whether there are sufficient law enforcement resources in place to combat cyber crime, given the rapid increase in attacks and sophistication of attacks.

[7] Malicious software is designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

SECTION 2 – RECOMMENDATION DISCUSSION:

Recommendation Area I

Near-Term Hardening Approaches: Education and Awareness

Adoption of Security Best Practices

1A: Measuring Best Practice Adoption

Issue: Network operators, vendors, management practices organizations such as professional auditors and government organizations have developed many recommendations and best practices for improving information infrastructure security. Although there has been significant progress in deploying resources and adopting best practices, this approach is not universal, nor is there a clear view of progress and effectiveness. The calculus decision makers employ to determine whether, and to what extent, they should invest in security technology, processes and people is not well understood. The Council's research indicates that there are no methodologies in place to determine what the return on investment is for software and hardware vendors on making their products more secure. Currently, vendors depend on ad hoc calculations based on consumer confidence and loyalty to determine what improvements have been made to vulnerabilities.

Discussion: The Council suggests new research be conducted to determine who adopts or invests in security technologies, processes, and people; and what their rationale is for making decisions for adoption and implementation. For example, many surveys including the National Cyber Security Alliance and America Online, released in October 2004, highlight the fact that a majority of home computer users mistakenly believe they are immune from online threats. However, the reports stop short of explaining why this is the case. This research should help quantify deployment and adoption rates of best practices, and will provide actionable feedback for private sector and government policy makers to improve the security profile of critical infrastructure sectors and the public. While it is commonly believed education and awareness campaigns do help in the adoption of best practices, researchers should help everyone understand the metrics that drive and quantify investment decisions within critical infrastructure sectors and the public. They should also examine the impact of outreach campaigns that might contribute to those decisions. The development of these metrics will improve the effectiveness of education and awareness programs, and help everyone understand how firms and consumers make decisions about adopting and deploying security technology, processes, and people.

Recommendation 1A: The Federal Government should sponsor research on the obstacles and solutions for adoption of cyber security BCPs. This research should focus on the following areas:

1. Surveys or other techniques to determine adoption and deployment rates of cyber security best practices within the critical infrastructure sectors
2. Investigation into the best-practice adoption and deployment decision process, including perceived costs, benefits, incentives, risks, rewards, competitive advantages, externalities, and other factors influencing decisions
3. Development of metrics to quantify the costs and benefits of implementing BCPs
4. Development of a cost-benefit decision support tool or tools to aid decision makers in determining the most appropriate level of investment in varying kinds of security technologies, security management processes, and corrective actions
5. Explore the potential benefits and risks of using government procurement power to influence deployment decisions by altering perceived costs and benefits associated with deployment of cyber security best practices within the critical infrastructure sectors.

1B: Route and Packet Filtering

Issue: Routing advertisements and filtering packets at edge networks are not universally practiced among ISPs. Without them, networks have open doors for malicious users to inject false messages into control protocols like the BGP. Without proper filtering, ISPs are also unable to validate the source and authenticity of some packets, which could confuse cooperative investigations of suspicious incidents with their peers or law enforcement. According to one major ISP, at any point during a day, 75 percent of the company's transited traffic is either spam or botnet DDOS traffic.

Discussion: Increased adoption of route and packet filtering by all ISPs is clearly an easy way to decrease vulnerabilities at a base level. If these two best practices are widely adopted, there would be a significant decrease in hijacking of routes in BGP. Several cyber security experts interviewed for this report consider BGP the most commonly used entry point for spammers, and denial of service attackers, which use forged or unexpected source IP addresses.

Recommendation 1B: The Council recommends the implementation of route[8] and packet[9] filtering as an important security best practice. Given that best practices exist and are documented for edge networks to filter both routing advertisements and filtering packets from their downstream networks, the Council recommends all ISPs implement such route and packet filtering practices. This will help to prevent hijacking of traffic via the injection of false routing control messages via the BGP. It would also provide real time information for ISPs to validate legitimate messages and will greatly aid in cooperative investigations among ISPs and law enforcement agencies. The Federal Government should advocate ISPs to adopt these BCPs.

[8] http://www.bell-labs.com/cgi-user/krauscher/bestp.pl?number=6-6-8043

[9] http://www.faqs.org/rfcs/rfc2267.html

Awareness of Security Best Practices

1C: End-User or General Public Education

Issue: A major Internet Service Provider, which declined to be named in this report, suggested that the adoption of security patches by the general Internet computing population is as follows:

- 40 percent are aware and adopt security patches **prior** to a vulnerability exploit being released
- 40 percent will become aware and will adopt a security patch **after** a vulnerability exploit has been released
- 20 percent are not likely to become aware or adopt a security patch, unless it is done for them or their system becomes corrupted to the point of being unusable.[10]

The Federal Communications Commission (FCC) has identified 28 million broadband subscriptions in the U.S. as of December 2003. If it is assumed that the 20 percent of these users are vulnerable, then there are approximately 5.6 million defenseless computers that are connected to "always on" networks with an up-link bandwidth in excess of 128 kilobits per second.[11] In actuality, about half of these computers are on at any given time. The number of online compromised computers appears to vary between 2 percent and 8 percent, usually staying under 5 percent, except during major outbreaks like Blaster. The aggregate bandwidth these computers can produce is on the order of 179.2 billion bits per second. It would be very difficult to coordinate these computers in a single attack, due to bandwidth constraints related to the topology of the Internet and the complexity of command and control channels. But, even a small percentage of these networked, "always on" computers, constitute enough capacity to have significant, detrimental impact against specific sites on the Internet.[12] For example, hostile networks comprised of approximately 10,000 devices have already been observed in the Internet according to the FCC's report.

Discussion: While it is possible that a massive outreach effort might not be completely successful in reaching the last 20 percent of users, the value to be gained in reducing the vulnerability window of the middle, 40 percent makes this a worthwhile effort**.** Many private organizations and partnerships[13] are already working to reach out to end-users, but a much broader, far-reaching effort is needed to bring these programs together. The 40 percent of the population identified as people who will update their machines if given a good reason to do so and given an easier way of having updates installed. The education of these people should make the reasons very clear on how their machines (as part of the Botnet farm) are causing issues with the Internet. Also, such efforts must be sustained in order to be more effective. Studies indicate that the private sector and the public sector have not done enough to inform people of their "responsibilities" in being a "good Internet citizen." It's not that these

[10] A major ISP submitted this data from an internal survey. The ISP asked not to be named in the report be used to provide anecdotal information.

[11] FCC fourth report on broadband availability, which was released on September 9, 2004; FCC No. 04-208.

[12] According to the FCC's June 8, 2004 report: "High-Speed Services for Internet Access: Status as of December 31, 2003".

[13] See Appendix A for a list of some of these organizations.

individuals are intentionally trying to cause harm, rather they are uninformed of the consequences of their inaction.[14] Outreach programs in the past have not been successful because they have not been properly sustained over the long-term.

Recommendation 1C: The President should encourage DHS to initiate and sustain longer-term partnership programs to increase awareness activities targeted at educating the American public to implement best practices for improving computer security. These activities require close coordination with the industry consortia to ensure a well-focused campaign is successful in educating the nation's end-users and in driving adoption of best practices and computer security. DHS should hire a professional marketing firm to conduct a targeted campaign, such as the National Advertising Council, to hone in on those who do not take appropriate precautions to help ensure security, promote awareness efforts, and where appropriate, use nationally-sponsored commercials or events. The Council believes many of the awareness programs out there are "pull programs," meaning it is incumbent on the "Internet citizen" to take proactive action to understand their responsibilities. Programs that are being recommended in this report are more of the "push model" to get this information, awareness and education to the consumer. Further, DHS should encourage the IT industry to make applying patches much easier and more publicly known, requiring the user to have less sophisticated knowledge.

1D: Industry Continuing Education

Issue: Despite the existence of quality systems like the Software Engineering Institute's Capability Maturity Model (CMM) for Software and International Standardization Organization (ISO) standards (15408, 17799), many software vendors have not adopted methodologies and processes to ensure security best practices are built into their product development life cycles and releases. The Council did an informal survey of study group participants and found it was clear that hardware and software vendors did not have an engineering excellence program in place to ensure a more secure product development life cycle.

Discussion: Advocating the use of an existing standard increases awareness, but the reluctance of some companies to adopt these process changes indicates that promoting awareness alone is not enough. The possible reasons behind this assessment include: the cost may outweigh the expected benefits, sufficiently trained software developers may not be available, and customers may be demanding new software capabilities that preclude retooling in mid-production cycle. Also, existing methodologies may be too broadly focused. The lynchpin of competitiveness in software is innovation; any best practice must not blunt this innovation.

Recommendation 1D: The Council recommends DHS, representatives from leading software vendors, and academics who teach software development programs to engage in an activity designed to develop and publish guidelines and documentation on a focused Secure Software Development Life Cycle. Further, the Federal Government should sponsor a research project to develop metrics to determine the effectiveness of the adoption of the Secure Software Development Life Cycle in reducing exploitable vulnerabilities in software releases,

[14] AOL/NCSA Online Safety Study, October, 2004.

implementation incentives, and rewards for documenting sound, security software development. This work should be conducted by a combination of a professional research firm, an academic institution, and the National Institute of Standards and Technology (NIST).

1E: Enterprise Board Education

Issue: Despite an increased focus on corporate information security, vulnerable computer systems on enterprise networks still represent a threat to the network as a whole. These systems are managed by larger enterprises, where system users are not necessarily responsible for their own systems. The problem lies not with the education of individual users, but with management models, that do not sufficiently prioritize system security requirements.

Discussion: Enterprises, like consumers, need to ensure they have the right security technology, processes, and people to achieve a reasonable level of security. There are many groups that sponsor education campaigns to highlight best practices and the benefits to the enterprise and networks from adoption and deployment. In many cases, boards of directors and internal audit committees are unaware of the existing processes they can employ to implement IT security policies and monitor and assure compliance. Where boards have awareness, they assure high-level information security policy, but often have no clear means for monitoring and assuring compliance.

Enterprises participate in shared responsibility to protect cyberspace through appropriate policies and procedures. The Federal Government can play an important role in influencing corporate governance by educating corporate boards about the importance of security policies and employment of best practices within critical, corporate networks. In addition, by partnering with groups that have greater influence on board-level actions, the Federal Government can introduce key topics appropriate for policy, oversight, and governance to assure compliance as part of their fiduciary responsibility for managing risk to their business operations. The work done in this area from 2000 to 2002 by the former Critical Infrastructure Assurance Office (now merged with DHS), in coordination with the Audit community and the National Association of Corporate Directors, as well as a segment of the insurance industry, has been very successful in raising awareness by putting foundations for corporate board education in place.[15] Even after the 9/11 terrorist attacks, many boards did not fully appreciate the merit of critical infrastructure and security being part of board-level discussions. In sum, Federal Government-supported outreach/awareness conducted during the last 5 years has accomplished important awareness goals that need to be re-initiated and sustained. This recommendation has two more focused challenges for the government: (1) Focus on raising board-level awareness on hardening the Internet, which means corporate networks/systems and infrastructure, as well as vendors/contractors, etc. and (2) Hone in on identification and integration of best practices.[16]

It is important to recognize the unusual position large academic and research organizations have regarding overall stability of the Internet. These labs and universities can differ from

[15] National Association of Corporate Directors, KPMG's Audit Committee Institute, Institute of Internal Auditors and Critical Infrastructure Assurance Office. Board Leadership Series: Information Security Oversight Essential Board Practices, December, 2001.

[16]The Institute of Internal Auditors' Critical Infrastructure Assurance Project. Information Security Management and Assurance: A Call to Action for Corporate Governance, April 2000.

government and corporate sites in significant ways. Universities often have large and well-connected networks, with a wide range of host types and differing operating systems and hardware deployed. The user population turnover is also consistently high, due to the normal course of student careers, i.e., a large percentage of the systems administration being performed by part-time or research staff. Given the significant resources at the disposal of universities and the decentralized nature of security governance within them, it is important initiatives for security reporting be crafted to include university and research governance bodies, not just corporate entities.

Recommendation 1E: The Federal Government should reinitiate sustainable partnerships with groups, such as: the Institute for Internal Auditors (IIA), Financial Executives International (FEI), and the National Association of Corporate Directors (NACD) to continue providing and promoting education to boards of companies and universities around IT security policy, oversight, and governance. This activity could take the form of providing information on voluntary standards available to organizations that wish to scale security programs against industry best practices and championing stronger cyber security policies and best practices, specifically including board level attention to their company's security practices.[17] The Council further recommends that the Federal Government promote cyber security policy and practice education through its appropriate agencies to contractors and government organizations that initiate procurements. The Federal Government should also evaluate and consider funding a "Mentor-Protégé" program, where large government prime contractors adopt smaller companies to help educate and implement appropriate security policies and practices.

Recommendation Area II

Long-Term Hardening Approaches: Research and Development

2A: Routing Registries for Securing Inter-Domain Routing

Issue: Being able to trace and verify advertised route information to BGP is critical to hardening the Internet beyond what is recommended by existing BCPs. In order to trace route information, the Internet must have a system of registries that formally tie advertised IP address range information to autonomous systems, forming the backbone of the network. This is part of the basic BGP protocol, as defined in the Internet's Request for Comment (RFC) 1771. An autonomous system (AS) originates a route, and this route can not be verified out of band unless there is an existing registry that ties address allocation to AS numbers.

Discussion: This recommendation focuses on establishing research on one of the critical components needed to implement extensions to harden BGP: tying IP address range information to authorized advertisers of that range. The Council discussed various alternatives, which are outlined below, and decided further research is necessary before a solution is recommended.

[17] These generally accepted security best practices are defined by a corporation's information security program. The program needs to be based on an internationally accepted standard such as ISO 17799 or SAS 70.

Recommendation 2A: The President should establish research funding and task a federal organization, such as the National Science Foundation (NSF), in conjunction with an industry coordination body, such as Merit[18], with guiding research for an automated route registry infrastructure that addresses any technical and operational impediments to existing proposals like Secure BGP and Secure Origin BGP. The scope of this work must consider the following:

- Distributed architectures and trust models - centralized models limit scalability, create social engineering vulnerabilities and present issues in the international environment
- Data quality and verification - there is no reliable consensus on the accuracy of existing registries or the minimum requirements needed for a workable system
- Operational cost of implementation - equipment upgrades and additional staffing levels must be understood
- Exception handling – under emergency circumstances, it may be necessary to rapidly propagate temporary or permanent routing changes.

2B: Scalable Management and Anomaly Detection Tools

Issue: The speed of analysis is a critical component for identifying and addressing vulnerabilities in networks. The large number of flows and nodes in the network represents a challenge to the speed and accuracy of existing network analysis and management tools. Additionally, a large number of service providers utilize homegrown scripts that have limited capabilities instead of an extensible, structured, and scalable analysis tools.

A second component of this recommendation is to improve the process for detecting anomalous activity in networks with a large number of flows. By combining scalable analysis and anomaly detection, service providers can better manage the ill-behaved devices on their networks, ultimately improving the security of the Internet. As it exists today, there are no real-time tools for malicious traffic analysis that can be run in large-scale networks. This is market knowledge. If industry had the tools, they could shut down the malicious flows earlier, thereby causing less damage.

Discussion: Currently, standard technologies are applied within the infrastructure environment to ensure packets are appropriately routing traffic. The Council believes it is important to provide a well-developed toolset to replace the homegrown scripts network service providers use today to detect, analyze, and resolve malicious activity. Data must be collected before it can be analyzed. There is a need for sustained and improved funding to analyze flaws in large systems. Networks and the software used are becoming increasingly complex. It is beyond the ability of a developer to immediately recognize or understand the flaws they may have written into their code. Having the tools to intelligently detect flaws in communications infrastructures could prevent the release of flawed infrastructure and protocols before being released to the end-user.

[18] Merit (www.merit.edu) currently runs the U.S. Internet Routing Registry and is highly qualified to act as a conduit for research into routing registries based on both their present and past experience as a routing registry as well as their involvement in NANOG and closeness to the service provider community.

Recommendation 2B: The President should request that funding be made available to the White House's Office of Science and Technology Policy, the DHS's Science and Technology Division (DHS/S&T), the National Institute of Standards and Technology's Computer Security Division (NIST/CSD), the Homeland Security Advanced Research Projects Agency (HSARPA), National Science Foundation (NSF), and the Defense Advanced Research Projects Agency (DARPA) for further research and development in the following areas:

- Security and management tools that allow both large and small service providers and enterprises to transition from large scale network trend analysis to capturing and visualizing individual flows in the network in real time. These tools will help capture malware activity and make it easier to defend networks.
- Anomaly detection systems and algorithms and tools for automated correlation of malicious activity within and across organizational boundaries. The monitoring of malicious activity will result in advanced, early detection capabilities that allow network operators and researchers to gain more knowledge about the anomalies circulating in networks. Existing anomaly detection techniques collect information. However, this information is not correlated and is usually time-consuming to process. The government needs to improve the state of the art in the fields of anomaly detection and correlation of collected data.
- Standardized reporting tools that allow for wide distribution of the results obtained via the Security and Management tools and Anomaly detection systems and algorithms identified, in the bullets above, to network operations, enterprises, law enforcement agencies, and Internet infrastructure vendors.

2C: Forensics at High Data Rates

Issue: Existing devices and software for capturing data that transits a network can benefit from improved throughput and capacity.[19] The storage capacity of these devices is also limited. From a research perspective, ISP representatives interviewed for this report acknowledge it is critical to be able to observe the behavior of malicious software, such as worms or BotNets in a real network to determine their growth pattern. As the network speeds and number of feeds connected to the Internet increase, the existing equipment will not be able to obtain and store this information due to technology constraints.

Discussion: This recommendation completes the longer-term Internet hardening approaches. Funding research in the area of network forensic data collection in high-speed networks[20] and long-term storage of collected data, will allow researchers to:

- Analyze more data and organizations that have been compromised via a variety of means
- Reconstruct the compromise
- Defend networks more effectively.

[19] Current devices tend to operate at about 1 Gbps, while carriers have already demonstrated the ability to transmit data at 40 Gbps rates according to software experts contributing to this report.

[20] High-speed networks can operate at speeds greater than 2.4 Gigabits/sec according to Cisco engineers.

Recommendation 2C: The Council recommends research funds be provided to academia and industry to improve network-based data collection, storage, and analysis at high data rates that can be deployed on high-speed data lines carrying malicious activity. Mechanisms must be developed to determine how such collection can be filtered in real-time to bring it into accord with legal and privacy requirements. The data could be used to analyze malicious activity during and after a compromise, when collected pursuant to law and with regard for the privacy rights of network users.

2D: Scalable Vulnerability and Flow Analysis

Issue: Network elements and hosts, including the host operating systems are growing in complexity at almost the speeds predicted by Moore's law. The fundamental systems engineering and computer science tools that are available to designers and developers are at least a decade behind in analyzing the complexities associated with modern network equipment and hosts today. Computer-aided software engineering tools have not taken hold in the networking industry. They are also not used by major software vendors due to inefficiency, speed, and lack of suitability to the task. The large numbers of interacting components also present a scalability challenge for flow analysis tools. While there may be some academic tools that exist for code analysis, there are not any that can analyze over one million lines of code, document complex relationships including timing and reduce these into legible data in finite time, according to several computer engineers interviewed for this study.

Discussion: This recommendation focuses on research of analysis tools that can be used to build and analyze systems and software with well-defined interfaces, in a structured manner. This is an area that could benefit significantly from research funding and would result in following significant benefits:

- Better understanding of vulnerabilities within existing networks including infrastructure and end users
- Better engineered systems, including the software that runs on it
- Being able to change/rewrite components of the system and having a good understanding of the collateral damage caused by the change.

Recommendation 2D: The President should establish a research funding line specifically for improving the state of the art in scalable vulnerability/flaw analysis for complex communications and security systems throughout the network. The President should encourage DHS to consider research in the areas of automated software analysis tools and techniques for making tools more usable in terms of speed and detection of a wider range of flaws.

Recommendation Area III

Near Term and Longer Term: Empowering Service Providers and Law Enforcement

3A: Empowering Internet Service Providers

Issue: Inter-ISP information sharing continues to be highly dependent on informal and ad-hoc relationships. Existing information sharing structures that have been setup for voice telecommunications do not work well for Internet incident management.

Discussion: Over time, informal channels of communications have been established between ISPs to handle tactical events like virus propagation and Distributed Denial of Service (DDOS) events. These open channels are typically between the Internet security and operations teams of the affected ISPs, and have become a necessity for successful operation of the Internet Infrastructure. In the telecommunication's carrier space, these channels are distinct from the channels that exist for voice operations; a side effect of the unique technology and services the Internet provides.

Efforts by existing information sharing groups have met with mixed success. The multi-sector nature of Internet service usage has not mapped cleanly to existing information sharing mechanisms. Incidents often involve the private and public sectors and call upon resources from the same organizations, including the US-CERT and the National Cyber Security Division.

Recommendation 3A: The Council recommends the President consider stimulating increased information sharing by encouraging the ISPs and vendors to establish an Internet information sharing capability. While an IT information sharing capability exists, the establishment of a discrete Internet information sharing capability to focus exclusively on Internet security should be considered.

3B: Enhancement of Online Law Enforcement

Issue: Crime is a growing problem on the Internet. The federal, state, and local government must have the resources to enforce laws against theft, extortion, fraud, and other illegal activity through and against computers. Criminal behavior is becoming more sophisticated. Sophisticated identity thieves are targeting customers of financial institutions and high-profile sites, such as eBay and Amazon. A recent study by Gartner Research,[21] estimates 76 percent of all known phishing[22] attacks have occurred since December 2003. The Anti-Phishing Working Group also reported 1,125 unique phishing attacks in April, which is up from 402 in March.[23] Security attacks on the Internet have moved from prank driven to money driven. Laws and law enforcement cannot keep pace with this type of crime.

Discussion: As businesses increasingly move commerce activities onto the Internet, the financial threat posed by criminal activity will increase. As the risk to the nation's economy increases, maintaining an equitable protection and enforcement profile is logical to ensure a safe environment in this area of economic growth. Currently, not much is being done in this area in a concerted or collaborative way. Responsibility for this belongs to all participants on

[21] Gartner, Inc. provides research and analysis on the global IT industry.

[22] Phishing schemes are attacks that use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5 percent of recipients to respond to them.

[23] The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing.

the Internet, i.e., consumers, enterprises, vendors, ISP's, transit providers, government, etc. It is obvious that something must be done that most interested bodies are waiting for someone to take the lead, but nothing substantive is happening.

Recommendation 3B: The Council recommends the Federal Government re-examine existing funding resources available to combat cyber crime, given the significant increase in activity, and provide for the following:

- An increase in law enforcement resources at the national and local levels to investigate Internet security breaches in real time. Security breaches and attacks at any level should be investigated. Specific resources for this would be used to track down, investigate, and provide education to affected corporations and end-users.
- Law enforcement training and investigative and forensic capabilities must be enhanced. Law enforcement is challenged by an accelerating race against cyber criminals, with criminal capabilities improving faster than law enforcement's investigative capabilities.
- In order to investigate attacks, greater resources should be devoted to developing: (1) nationally-scalable network investigations and computer forensics training, possibly through the creation of a national computer forensics and network investigations training development center, and (2) investigative tools and techniques that can be deployed broadly to support Internet investigations, especially new tools and techniques that support automated forensic analysis of very large data sets. These should be made widely available to federal and local law enforcement officers.
- Strengthen Law Enforcement capabilities with enhanced coordination efforts between agencies and countries, increased legal capabilities for Law Enforcement, and enabling agencies to communicate in a timely manner.

Appendix A: Organizational Resources:

Financial Executives International (FEI) – an association for senior-level corporate financial executives. The group represents 15,000 individuals.

International Association for Financial Executives (IAFEI) -- an association to build and improve mutual understanding internationally among financial executives through the exchange of financial information, experience and ideas. The group has more than 32,000 members.

Global CSO Council – a think-tank comprising a group of corporate, government and academic security experts dedicated to raising the awareness of online security issues.

International Systems Audit and Control Association (ISACA) – an association started up in 1967 to address critical auditing controls for computer systems. The group has more than 35,000 members worldwide.

National Association of Corporate Directors (NACD) – group published a best practices document several years ago. The group is currently in the process of integrating information systems security controls into their standard professional accounting practices and standards. This organization serves 15,500 board members and customers represent companies ranging from Fortune 100 public companies to small, over-the-counter, closely held, and private firms.

The Institute for Internal Auditors (IIA) -- serves approximately 90,000 members in internal auditing, governance and internal control, IT audit, education, and security worldwide. The Institute serves as the profession's watchdog and resource on significant auditing issues around the globe.

Information Systems Security Association (ISSA) – an international organization of information security professionals and practitioners, which provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

International Information Systems Security Certification Consortium (ISC)^{2} -- a global, organization dedicated to maintaining a common body of knowledge for Information Security. Certifies industry professionals and practitioners under an international Information Security standard.

InfraGard –partnership between Private Industry and the U.S. government (represented by the FBI). The InfraGard initiative was developed to encourage the exchange of information by the government and the private sector members. Private sector members and an FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership. Each chapter is also part of an organization, which is InfraGard. There are 79 active InfraGard chapters, with hundreds of company members across the nation.

Cyberpartnership.org -- The National Cyber Security Partnership (NCSP) is led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet, and the U.S. Chamber of Commerce in voluntary partnership with academicians, CEOs, federal government agencies and industry experts. Following the release of the 2003 White House National Strategy to Secure Cyberspace and the National Cyber Security Summit, this public-private partnership was established to develop shared strategies and programs to better secure and enhance America's critical information infrastructure. The partnership established five task forces comprised of cyber security experts from industry, academia, and government. Each task force is led by two or more co-chairs. The NCSP-sponsoring trade associations' act as secretariats in managing task force workflow and logistics. The task forces include:

- Awareness for Home Users and Small Businesses
- Cyber Security Early Warning
- Corporate Governance
- Security Across the Software Development Life Cycle
- Technical Standards and Common Criteria

FTC Federal Consumer Security Awareness Site found at:
http://www.ftc.gov/bcp/conline/edcams/infosecurity/resources.html
Has links to a number of websites that address cyber security: they include:

StaySafeOnline.info – National Cyber Security Alliance (NCSA's) coalition site and growing outreach activities found at:
http://www.staysafeonline.info/
The NCSA is a cooperative effort between industry and government organizations to foster awareness of cyber security through educational outreach and public awareness.

GetNetWise -- About Security found at:
http://security.getnetwise.org/
The GetNetWise.org security section was established to deliver information and materials to consumers to protect their information and networks from theft, misuse and destruction. The site includes tutorials on how to use common software programs to enhance security and privacy.

Introducing the National Cyber Alert System found at:
http://us-cert.gov
US-CERT, a partnership between the Department of Homeland Security's National Cyber Security Division (NCSD) and the private sector offers the National Cyber Alert System to provide timely information about current and emerging threats to computers and networks. To sign up for alerts from the National Cyber Alert System, click on the US-CERT logo on the right.

The National Strategy to Secure Cyberspace found at:
http://www.whitehouse.gov/pcipb/
The National Strategy to Secure Cyberspace, an implementing component of the National Strategy for Homeland Security, is part of the White House's overall effort to protect the

Nation. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control, or with which they interact.

BBBOnLine found at:
http://www.bbbonline.org
BBBOnLine is the arm of the Council of Better Business Bureaus that specifically deals with web sites. Working in concert with the 142 local BBBs in the United States and Canada, BBBOnLine encourages sound and ethical online business practices through its Privacy program, Reliability program, BBB Code of Online Business Practices, and an international initiative to promote safe e-commerce.

Organization for Economic Co-Operation and Development found at:
http://www.oecd.org/ict/guidelines
OECD governments have drawn up new Guidelines for the Security of Information Systems and Networks in the wake of the 9/11 attacks on the United States, in order to counter cyber terrorism, computer viruses, hacking and other threats.

Computer Crime and Intellectual Property Section, U.S. Department of Justice found at:
http://www.usdoj.gov/criminal/cybercrime/index.html
The Computer Crime and Intellectual Property Section (CCIPS) attorney staff focus exclusively on the issues raised by computer and intellectual property crime. Section attorneys advise federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups.

U.S. Department of Education Internet Safety Page found at:
http://www.ed.gov/about/offices/list/os/technology/safety.html
The Department of Education's Office of Educational Technology works to assist the education community with meeting the national goals for educational technology.

CyberSmart! found at:
http://www.cybersmart.org
CyberSmart! provides a comprehensive set of free lesson plans, student activities, and related materials for teachers and families to introduce the skills associated with 21st Century literacy, citizenship, and ethics.

CERT Coordination Center's Home Network Security Tips found at:
http://www.cert.org/tech_tips/home_networks.html
The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT's information ranges from protecting your system against potential problems; to reacting to current problems; to predicting future problems.

The National Infrastructure Protection Center (NIPC) found at:
http://www.nipc.gov/
The NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

National Institute of Standards and Technology Computer Security Resource Center's Small Business Corner found at:
http://csrc.nist.gov/SBC
The mission of NIST's Computer Security Division is to improve information systems security. This site focuses on resources for small businesses.

The Information Technology Association of America found at:
http://www.itaa.org/infosec
ITAA seeks to improve the information security of the nation's critical information infrastructure in both the private and public sectors. This site includes links to news articles, press releases and reports.

The Internet Security Alliance found at:
http://www.isalliance.org/
The Internet Security Alliance is a collaborative effort between Carnegie Mellon's CERT Coordination Center and the Electronic Industries Alliance to promote sound information security practices, policies, and technologies that enhance the security of the Internet and global information systems. The ISA recently released a guide to 10 of the highest priority and most frequently recommended security practices for business.

Consumerreports.org found at:
http://www.consumerreports.org/static/0206com0.html
Consumer Reports' Cyberspace Invaders site includes practical advice for consumers and a link to CR's online subscriber security survey. It also includes consumer security product ratings.

Center for Internet Security found at:
http://www.cisecurity.org
CIS provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances.

The World Bank found at:
http://www.worldbank.org
To educate policy makers, businesses, consumers of financial services, and others involved in E-finance and E-commerce, the World Bank offers an E-security Site focusing on the complex trade-offs and actions needed to manage the risks of fraud and of compromising the security of digital assets.

The Asia Oceania Electronic Marketplace Association found at:
http://www.aoema.org
The Asia Oceania Electronic Marketplace Association (AOEMA) was formed to promote the use of electronic commerce in the Asian region. Working closely with Asia-Pacific Economic

Cooperation, AOEMA has done a number of projects on the barriers to electronic commerce, including this booklet to help you protect yourself when using the Internet: http://www.aoema.org/safetynet.htm.

The Business Roundtable found at:
http://www.brtable.org
The Business Roundtable's Digital Economy Task Force has produced a resource to help CEOs and their senior executives develop a robust, effective program to protect their business as they incorporate sophisticated information systems into their operations. Access the resource at http://www.brtable.org/document.cfm/814.

The Business Software Alliance found at:
http://www.bsa.org
The Business Software Alliance (BSA), with programs in 65 countries worldwide, is dedicated to promoting a safe and legal digital world. BSA also educates consumers on software management and copyright protection, cyber security, trade, e-commerce and other Internet-related issues. Visit their security page:
http://www.bsa.org/usa/policy/security/issue/index.phtml.

Public Company Accounting Oversight Board – is responsible for improving the quality and transparency in financial reporting and independent audits, advancing corporate responsibility, and furthering the public interest.

Appendix B: Documents and Research Papers:

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Washington, D.C.; The White House, February 2003.

The National Strategy to Secure Cyberspace. Washington, D.C.; The White House, February 2003: www.**securecyberspace**.gov.

National Security Council (NSC) Working Group Findings Regarding Cyber Security Concerns, presented to the White House; May 2002.

Presidential Decision Directive (PDD)–63, May 22, 1998.

Homeland Security Presidential Directive (HSPD) – 7: Critical Infrastructure Identification, Prioritization, and Protection; December 17, 2003.

HSPD-8 National Preparedness; December 17, 2003.

National Association of Corporate Directors, KPMG's Audit Committee Institute, Institute of Internal Auditors and Critical Infrastructure Assurance Office. "Board Leadership Series: Information Security Oversight Essential Board Practices," December 2001.

The Institute of Internal Auditors' Critical Infrastructure Assurance Project. "Information Security Management and Assurance: A Call to Action for Corporate Governance," April 2000.

General Accountability Office, "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," May 2004.

Federal Communications Commission – "Fourth report on Broadband Availability;" FCC No. 04-208, September 9, 2004.

America Online/ National Cyber Security Alliance Safety Study; October 2004.