Testimony before the Senate Committee on Commerce, Science, and Transportation

Hearing on

"Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Defense"

19 March 2009

Statement of

Eugene H. Spafford

Professor and Executive Director
Purdue University Center For Education and Research in Information Assurance and Security (CERIAS)

Chair of The U.S. Public Policy Committee
Of The Association For Computing Machinery (USACM)

Introduction

Thank you Chairman Rockefeller and Ranking Member Hutchison for the opportunity to testify at this hearing.

By way of self-introduction, I am a professor at Purdue University. I also have courtesy appointments in the departments of Electrical and Computer Engineering, Philosophy, and Communication at Purdue, and I am an adjunct professor at the University Texas at San Antonio. At Purdue, I am also the Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). CERIAS is a campus-wide multidisciplinary institute, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we were recently ranked as the #1 such program in the country. CERIAS also has a close working relationship with dozens of other universities, major commercial firms and government laboratories.

Along with my role as an academic faculty member, I also serve on several boards of technical advisors, and I have served as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA. I was also a member of the most recent incarnation of the President's Information Technology Advisory Committee (PITAC) from 2003 to 2005. I have been working in information security for over 25 years.

I am also the chair of USACM, the U.S. public policy committee of the ACM. With over 90,000 members, ACM is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. USACM acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

USACM is a standing committee of the ACM. It tracks US public policy initiatives that may affect the membership of ACM and the public at large, and provides expert input to policy-makers. This advice is in the form of non-partisan scientific data, educational materials, and technical analyses that enable policy-makers to reach better decisions. Members of USACM come from a wide-variety of backgrounds including industry, academia, government, and end users.

My testimony is as an expert in the field. My testimony does not reflect official positions of either Purdue University or the ACM, although I believe that my comments are consistent with values and positions held by those organizations.

General Comments

Our country is currently under unrelenting attack. It has been under attack for years, and too few people have heeded the warnings posed by those of us near the front lines. Criminals and agents of foreign powers have been probing our computing systems, defrauding our citizens, stealing cutting-edge research and design materials, corrupting critical systems, and snooping on government information. Our systems have been compromised at banks, utilities, hospitals, law enforcement agencies, every branch of the armed forces, and even the offices of the Congress and White House. Although exact numbers are impossible to obtain, some estimates currently run in the tens to hundreds of billions of dollars per year lost in fraud, IP theft, data loss, and reconstitution costs. Attacks and losses in much of the government and defense sector are classified, but losses there are also substantial.

Over the last few decades, there have been numerous reports and warnings of the problems issued. When I was a member of the PITAC in 2003-2005, we found over a score carefully-researched and well-written reports from research organizations that highlighted the dangers and losses, and pointed out that the problem was only going to get worse unless drastic action is taken. Our own report from the PITAC, *Cyber Security: A Crisis of Prioritization*, published in 2005, echoed these concerns but was given scant attention. Other reports, such as *Toward a Safer and More Secure Cyberspace* by the National Academies have similarly been paid little attention by leaders in government and industry. Meanwhile, with each passing week, the threats grow in sophistication and number, and the losses accumulate.

I do not mean to sound alarmist, but the lack of attention being paid to these problems is threatening our future. Every element of our industry and government depends on computing. Every field of science and education in our country depends, in some way, on computing. Every one of our critical infrastructures depends on computing. Every government agency, including the armed forces and law enforcement, depend on computing. As our IT infrastructure becomes less trustworthy, the potential for failures in the institutions that depend on them increases.

There are a number of reasons as to why our current systems are so endangered. Most of the reasons have been detailed in the various reports I mentioned above and their lists of references, and I suggest those as background. I will outline some of the most significant factors here, in no particular order:

- Society has placed too much reliance on marketplace forces to develop solutions. This strategy has failed, in large part, because the traditional incentive structures have not been present: there is no liability for poor quality, and there is no overt penalty for continuing to use faulty products. In particular, there is a continuing pressure to maintain legacy systems and compatibility rather than replace components with deficient security. The result is a lack of reward in the marketplace for vendors with new, more trustworthy, but more expensive products.
- Our computer managers have become accustomed to deploying systems with inherent weaknesses, buying add-on security solutions, and then entering a cycle of penetrate-and-patch. As new flaws are discovered, we deploy patches or else add on yet new security applications.

There is little effort devoted to really designing in security and robustness. This also has contributed to unprotected supply chains, where software and hardware developed and sold by untrusted entities is then placed in trusted operational environments: the (incorrect) expectation is that the add-on security will address any problems that may be present.

- There is a misperception that security is a set of problems that can be "solved" in a static sense. That is not correct, because the systems are continuing to change, and we are always facing new adversaries who are learning from their experiences. Security is dynamic and changing, and we will continue to face new challenges. Thus, protection is something that we will need to continue to evolve and pursue.
- Too few of our systems are designed around known, basic security principles. Instead, the components we do have are optimized for cost and speed rather than resilience and security and those components are often needlessly complex. Better security is often obtained by deploying systems that do less than current systems – extra features not necessary for the task at hand too often provide additional avenues of attack, error, and failure. However, too few people understand cyber security, so the very concept of designing, building, or obtaining less capable systems, even if they are more protected, is viewed as unthinkable.
- We have invested far too little on the resources that would enable law enforcement to successfully investigate computer crimes and perform timely forensic activities. Neither have we pursued enough political avenues necessary to secure international cooperation in investigation and prosecution of criminals operating outside our borders. As a result, we have no effective deterrent to computer crime.
- The problems with deployed systems are so numerous that we would need more money than is reasonably available simply to patch existing systems to a reasonable level. Unfortunately, this leads to a lack of funding for long term research into more secure systems to replace what we currently have. The result is that we are stuck in a cycle of trying to patch existing systems and not making significant progress towards deploying more secure systems.
- Over-classification hurts many efforts in research and public awareness. Classification and restrictions on data and incidents means that it is not possible to gain an accurate view of scope or nature of some problems. It also means that some research efforts are inherently naive in focus because the researchers do not understand the true level of sophistication of adversaries they are seeking to counter.
- Too little has been invested in research in this field, and especially too little in long-term, risky research that might result in major breakthroughs. We must understand that real research does not always succeed as we hope, and if we are to make major advances it requires taking risks. Risky research led to computing and the Internet, among other things, so it is clear that some risky investments can succeed in a major way.
- We have too many people who think that security is a network property, rather than understanding that security must be built into the endpoints. The problem is not primarily one of "Internet security" but rather of "computer and device" security.
- There is a common misconception that the primary goal of intruders is to exfiltrate information or crash our systems. In reality, clever adversaries may simply seek to modify critical applications or data so that our systems do not appear to be corrupted but fail when relied upon for critical functions – or worse, operate against our interests. We seldom build and deploy sys-

tems with sufficient self-checking functions and redundant features to operate correctly even in the presence of such subversion.

- Government agencies are too disorganized and conflicted to fully address the problems. Authorities are fragmented, laws exist that prevent cooperation and information sharing, and political "turf" battles all combine to prevent a strong, coordinated plan from moving forward. It is debatable whether there should be a single overarching authority, and where it should be if so. However, the current disconnects among operational groups including DHS, law enforcement, the armed forces and the intelligence community is a key part of the problem that must be addressed.
- We have too few people in government, industry and the general public who understand what good security is about. This has a negative effect on how computing is taught, designed, marketed, and operated. I discuss this in more depth later in this testimony.

I would be remiss not to note that most systems handling personal information have also been poorly designed to protect privacy. Good security is necessary for privacy protection. Contrary to conventional wisdom, it is not necessary to sacrifice privacy considerations to enhance security. However, it takes additional effort and expense to design to both protect privacy **and** improve security, and not everyone is willing to make the effort despite the rewards.

This battle is global. Our colleagues in other countries are also under siege from criminals, from anarchists, from ideologues, and from agents of hostile countries. Any effective strategy we craft for better cyber security will need to take into account that computing is in use globally, and there are no obvious national borders in cyberspace.

Additionally, it is important to stress that much of the problem is not purely technical in nature. There are issues of sociology, psychology, economics and politics involved (at the least). We already have technical solutions to some of the problems we face, but the parties involved are unable to understand or agree to fielding those solutions. We must address all these other issues along with the technical issues if we are to be successful in securing cyberspace.

Rethinking Computing [1]

Fifty years ago, IBM introduced the first commercial all-transistor computer (the 7000 series). A working IBM 7090 system with a full 32K of memory (the capacity of the machine) cost about $3,000,000 to purchase – over $21,000,000 in current dollars. Software, peripherals, and maintenance all cost more. Rental of a system (maintenance included) could be well over $500,000 per month. The costs of having such a system sit idle between jobs (and during I/O) led the community to develop operating systems that supported sharing of hardware to maximize utilization. It also led to the development of user accounts for cost accounting and development of security

[1] Adapted from *Rethinking computing insanity, practice and research*, CERIAS Weblog, December 15, 2008, <http://www.cerias.purdue.edu/site/blog/post/rethinking_computing_insanity_practice_and_research/>. In turn, this post was derived from my essay in the October 2008 issue of Information Security magazine.

features to ensure that the sharing didn't go too far. As the hardware evolved and became more capable, the software also evolved and took on new features.

Costs and capabilities of computing hardware have changed by a factor of tens of millions in five decades. It is now possible to buy a greeting card at the corner store with a small computer that can record a message and play it back to music: that card has more memory and computing power than the multimillion dollar machine of 1958. Yet, despite these incredible transformations, the operating systems, databases, languages, and more that we use are still basically the designs we came up with in the 1960s to make the best use of limited equipment. We're still suffering from problems known for decades, and systems are still being built with intrinsic weaknesses.

We failed to make appreciable progress with the software because, in part, we've been busy trying to advance on every front. It is simpler to replace the underlying hardware with something faster, thus getting a visible performance gain. This helps mask the ongoing lack of quality and progression to really new ideas. As well, the speed with which the field of computing (development and application) moves is incredible, and few have the time or inclination to step back and re-examine first principles. This includes old habits such as the sense of importance in making code "small" even to the point of leaving out internal consistency checks and error handling. (Y2K was not a one-time fluke – it was instance of an institutionalized bad habit.)

Another such habit is that of trying to build every system to have the capability to perform every task. There is a general lack of awareness that security needs are different for different applications and environments; instead, people seek uniformity of OS, hardware architecture, programming languages and beyond, all with maximal flexibility and capacity. Ostensibly, this uniformity is to reduce purchase, training, and maintenance costs, but fails to take into account risks and operational needs. Such attitudes are clearly nonsensical when applied to almost any other area of technology, so it is perplexing they are still rampant in IT.

For instance, imagine the government buying a single model of commercial speedboat and assuming it will be adequate for bass fishing, auto ferries, arctic icebreakers, Coast Guard rescues, oil tankers, and deep water naval interdiction – so long as we add on a few aftermarket items and enable a few options. Fundamentally, we understand that this is untenable and that we need to architect a vessel from the keel upwards to tailor it for specific needs, and to harden it against specific dangers. Why cannot we see the same is true for computing? Why do we not understand that the commercial platform used at home to store Aunt Bea's pie recipes is **not** equally suitable for weapons control, health care records management, real-time utility management, storage of financial transactions, and more? Trying to support everything in one system results in huge, unwieldy software on incredibly complex hardware chips, all requiring dozens of external packages to attempt to shore up the inherent problems introduced by the complexity. Meanwhile, we require more complex hardware to support all the software, and this drives complexity, cost and power issues.

The situation is unlikely to improve until we, as a society, start valuing good security and quality over the lifetime of our IT products. We need to design systems to enforce behavior within each specific configuration, not continually tinker with general systems to stop each new threat. Firewalls, intrusion detection, antivirus, data loss prevention, and even virtual machine “must-have” products are used because the underlying systems aren’t trustworthy–as we keep discovering with increasing pain. A better approach would be to determine exactly what we want supported in each environment, build systems to those more minimal specifications only, and then ensure they are not used for anything beyond those limitations. By having a defined, crafted set of applications we want to run, it will be easier to deny execution to anything we don’t want; To use some current terminology, that’s “whitelisting” as opposed to “blacklisting.” This approach to design is also craftsmanship–using the right tools for each task at hand, as opposed to treating all problems the same because all we have is a single tool, no matter how good that tool may be. After all, you may have the finest quality multitool money can buy, with dozens of blades and screwdrivers and pliers. You would never dream of building a house (or a government agency) using that multitool. Sure, it does many things passably, but it is far from ideal for expertly doing most complex tasks.

Managers will make the argument that using a single, standard component means it can be produced, acquired and operated more cheaply than if there are many different versions. That is often correct insofar as direct costs are concerned. However, it fails to include secondary costs such as reducing the costs of total failure and exposure, and reducing the cost of “bridge” and “add-on” components to make items suitable. There is less need to upgrade and patch smaller and more directed systems far less often than large, all-inclusive systems because they have less to go wrong and don’t change as often. There is also a defensive benefit to the resulting diversity: attackers need to work harder to penetrate a given system, because they don’t know what is running. Taken to an extreme, having a single solution also reduces or eliminates real innovation as there is no incentive for radical new approaches; with a single platform, the only viable approach is to make small, incremental changes built to the common format. This introduces a hidden burden on progress that is well understood in historical terms – radical new improvements seldom result from staying with the masses in the mainstream.

Therein lies the challenge, for researchers and policy-makers. The current cyber security landscape is a major battlefield. We are under constant attack from criminals, vandals, and professional agents of governments. There is such an urgent, large-scale need to simply bring current systems up to some minimum level of security that it could soak up way more resources than we have to throw at the problems. The result is that there is a huge sense of urgency to find ways to “fix” the current infrastructure. Not only is this where the bulk of the resources is going, but this flow of resources and attention also fixes the focus of our research establishment on these issues, When this happens, there is great pressure to direct research towards the current environment, and towards projects with tangible results. Program managers are encouraged to go this way because they want to show they are good stewards of the public trust by helping solve major problems. CIOs and CTOs are less willing to try outlandish ideas, and cringe at even the notion of replacing their current infrastructure, broken as it may be. So, researchers go where the money is – incremental, “safe” research.

We have crippled our research community as a result. There are too few resources devoted to far-ranging ideas that may not have immediate results. Even if the program managers encourage vision, review panels are quick to quash it. The recent history of DARPA is one that has shifted towards immediate results from industry and away from vision, at least in computing. NSF, DOE, NIST and other agencies have also shortened their horizons, despite claims to the contrary. Recommendations for action (including the recent CSIS Commission report to the President) continue this by posing the problem as how to secure the current infrastructure rather than asking how we can build and maintain a trustable infrastructure to replace what is currently there.

Some of us see how knowledge of the past combined with future research can help us have more secure systems. The challenge continues to be convincing enough people that "cheap" is not the same as "best," and that we can afford to do better. Let's see some real innovation in building and deploying new systems, languages, and even networks. After all, we no longer need to fit in 32K of memory on a $21 million computer. Let's stop optimizing the wrong things, and start focusing on discovering and building the right solutions to problems rather than continuing to try to answer the same tired (and wrong) questions. We need a major sustained effort in research into new operating systems and architectures, new software engineering methods, new programming languages and systems, and more, some with a (nearly) clean-slate starting point. Failures should be encouraged, because they indicate people are trying risky ideas. Then we need a sustained effort to transition good ideas into practice.

I'll conclude with s quote that many people attribute to Albert Einstein, but I have seen multiple citations to its use by John Dryden in the 1600s in his play *The Spanish Friar*:

> "Insanity: doing the same thing over and over again expecting different results."

What we have been doing in cyber security has been insane. It is past time to do something different.

Education

One of the most effective tools we have in the battle in cyber security is knowledge. If we can marshal some of our existing knowledge and convey it to the appropriate parties, we can make meaningful progress. New knowledge is also necessary, and there too there are urgent needs for support.

History

In February 1997, I testified before the House Science Committee. At that time, I observed that nationally, the U.S. was producing approximately three new Ph.Ds. in cyber-security[2] per year. I also noted that there were only four organized centers of cyber security education and research in the country, that none of them were very large, and that all were judged to be somewhat at risk. Indeed, shortly after that testimony, one of the centers dissolved as institutional support faded and faculty went elsewhere.

[2] This and related numbers in my report exclude individuals working primarily in cryptology. Although cryptography is necessary for good security, there is a difference between those who study the mathematics of codes and ciphers, and those who study systems and network security; the two general areas are related much in the way mathematicians and mechanical engineers are.

Although the number of university programs and active faculty in this area have increased in the last dozen years, the number involved and the support provided for their efforts still falls far short of the need. As an estimate, there have been less than 400 new Ph.Ds. produced in cyber security in the U.S. over the last decade with some nontrivial percentage leaving the U.S. to work in their countries of origin. (Approximately 25% of those graduates have come from CERIAS at Purdue.) Of those that remained, less than half have gone back into academia to be involved in research and education of new students.

In my testimony[3] in 1997 and in subsequent testimony in 2000, I provided suggestions for how to increase the supply of both students and faculty in the field to meet the anticipated demand. Three of my suggestions were later developed by others into Federal programs: the Centers of Academic Excellence (CAE), the Scholarship for Service program, and the Cyber Trust program.

Today, we have about a dozen major research centers around the country at universities, and perhaps another two dozen secondary research groups. Many, but not all, of these institutions are certified as CAEs, as are about 60 other institutions providing only specialized cyber security education. The CAE program has effectively become a certification effort for smaller schools offering educational programs in security-related fields instead of any true recognition of excellence; there are some highly regarded programs that do not belong to the CAE program for this reason (Purdue and MIT among them). One problem with the way the CAE program has evolved is that it does not provide any resources that designated schools may use to improve their offerings or facilities.

The Scholarship for Service program, offered through NSF, has been successful, but in a limited manner. This program provides tuition, expenses and a stipend to students completing a degree in cyber security at an approved university. In return, those students must take a position with the Federal government for at least two years or pay back the support received. Over the last seven years, over 1000 students have been supported under this program at 30 different campuses. The majority of students in these programs have, indeed, gone on to Federal service, and many have remained there. That is an encouraging result. However, the numbers work out to an average of about four students per campus per year entering Federal service, and anecdotal evidence indicates that demand is currently five times current production and growing faster than students are being produced. This program address needs in other segments of U.S. society.

NSF has been the principal supporter of open university research in cyber security and privacy through its Cyber Trust program (now called Trustworthy Computing). That effort has produced a number of good results and supported many students to completion of degrees, but has been able to support only a small fraction (perhaps less than 15%) of the proposals submitted for consideration. Equally unfortunate, there has been almost no support available from NSF or elsewhere in government for the development and sustainment of novel programs that are not specifically designated as research; as an example, CERIAS as an important center of education, research and outreach has never received direct Federal funding to support core activities, staff,

[3] Available online <http://spaf.cerias.purdue.edu/usgov/index.html>

and educational development. If it were not for periodic gifts from generous and civic-minded industrial partners, the center would have disappeared years ago – and may yet, given the state the economy. Other defined centers are similarly precariously funded.

Future

We need significant, sustained efforts in education at every level to hope to meet the challenges posed by cyber security and privacy challenges. In the following, I will outline some of the general issues and needs, with some suggestions where Federal funding might be helpful. A study by an appropriate organization would be necessary to determine more precisely what program parameters and funding levels would be useful. Given the complexity of the issues involved, I can only outline some general approaches here.

Let me note that many of these activities require both a ramp-up and sustainment phase. This is especially true for postgraduate programs. We do not currently have the infrastructure to switch into "high gear" right away, nor do we have the students available. However, once students are engaged, it is disruptive and discouraging to them and to faculty if resources and support are not provided in a steady, consistent fashion.

I will start by reiterating my support for the existing Scholarship for Service program. It needs to include additional funding for more students, and to allow recipient institutions to pursue curricular development and enhancement, but is otherwise functioning well.

K-12

Our children are the future. We should ensure that as they are being taught how to use the technology of tomorrow that they also are getting a sound background in what to do to be safe when using computers and networks. We teach children to cover their mouths when they sneeze, to wash their hands, and to look both ways when they cross the street – we should also ensure that they know something about avoiding phishing, computer viruses, and sharing their passwords. Older students should be made familiar with some of the more complex threats and issues governing computing especially privacy and legal implications.

Avenues for teaching this material certainly include the schools. However, too many of our nation's schools do not currently offer any computing curriculum at all. In many schools, all that is taught on computers is typing, or how to use the WWW to research a paper. Many states have curricula that treat computing as a vocational skill rather than as a basic science skill. Without having a deeper knowledge of the fundamentals of computing it is more difficult to understand the issues associated with privacy and security in information technology. Thus, teaching of computing fundamentals at the K-12 level needs to be more widespread than is currently occurring, and the addition of cyber security and privacy material nationally should be considered as part of a more fundamental improvement to K-12 education. Recently the leaders of the computing community released recommendations on how the Federal Government's Networking and Information Technology Research and Development (NITRD) Program could be strengthened to address shortfalls in computer science education at the K-12 level.[4]

[4] http://www.acm.org/public-policy/NITRD_Comment_final.pdf

Consideration should be given to encouraging various adjunct educational opportunities. Children's TV is one obvious venue for conveying useful information, as is WWW-based delivery.

Computing has a significant diversity problem. Cyber security and privacy studies appear, anecdotally, to be very attractive to students from underrepresented groups, including females. Presenting meaningful exposure to these topics at the K-12 level might help encourage more eager, able young people to pursue careers in those or related STEM fields.

Undergraduate Degrees

Of the thousands of degree-granting institutions throughout the U.S., perhaps only a few hundred have courses in computer security basics. These courses are usually offered as an elective rather than as a part of the core curriculum. As such, basic skill such as how to write secure, resilient programs and how to protect information privacy are not included in standard courses but relegated to the elective course. This needs to change or we will continue to graduate students who do not understand the basics of the area but who will nonetheless be producing and operating consumer computing artifacts.

More seriously, we have a significant shortfall of students entering computing as a major area. Last year was the first year in six where the enrollment of undergraduates in CS did not decline. The significance of this concern is not only important from a national competitiveness standpoint, but it implies that we will have a significant shortfall of trained U.S. citizens in the coming years to operate in positions of national responsibility. We are already off-shoring many critical functions, and without an increase in the U.S. production of computing majors, this will pose a significant national security threat.

Graduate Degrees

There is disagreement within the field about the level of education needed for some positions in the workforce. Clearly, there is a range of positions, some of which may only require an undergraduate degree, but many that require at least a Master's degree. Some educators (myself included) believe that a strong undergraduate degree in computing or software engineering, or in some other field related to cyber security (e.g., criminal justice), should be obtained followed by a graduate degree to ensure appropriate depth of knowledge.

There continues to be a need for Ph.D. graduates in cyber security. Individuals at this level are needed for advanced concept development in academia, industry and government. Generally, a Ph.D. is also required for faculty positions and some senior technical supervisory positions. Given the strong demand in this field and the number of institutions with need of faculty with experience in security or privacy topics, there will undoubtedly be a continuing and increasing demand for graduates at this level.

One of the issues facing researchers in academia is the lack of access to current commercial equipment. Most funding available to researchers today does not cover obtaining new equipment. Universities also do not have sufficient resources to equip laboratories with a variety of current products and then keep them maintained and current. As a result, unless faculty are adept at striking deals with vendors (and few vendors are so inclined) they are unable to work with current commercial security products. As a result, their research may not integrate well with fielded equipment, and may even be duplicative of existing solutions. The situation is in some senses similar to that of the 1980s when major research institutions were able to seek grants to get connections to research networking, but has evolved to a point where almost every college and university has network access. We now need a program to fund the instantiation of experimental laboratories for cyber security with a cross-section of commercial products, with an eventual goal of having these be commonplace for teaching as well as research.

Some faculty and their students are willing and able to work on classified problems so long as that work is near enough to their home institution to make travel reasonable. The best solution is to have a facility on campus capable of supporting classified research. This is not common on today's campuses.[5] It is not inexpensive to build or retrofit a facility for classified processing, and it is costly to staff and maintain it. Research grants almost never cover these costs. A Federal program to identify institutions where such facilities would be useful, and then build and support them might be helpful.

To produce graduate students requires resources for stipends, laboratory equipment, and general research support, as well as support for the faculty advisors. Given university overhead costs, it will often cost more than $250,000 over a period of years for a graduate student to complete a Ph.D. That support must be consistent, however, because interruptions in funding may result in students leaving the university to enter the workforce. Additionally, there needs to be support for their advisors, usually as summer salary, travel, and other expenses. Here again, consistency (and availability) are important. If faculty are constantly worried about where the money will come from for the coming year, some will choose to leave the field of study or academia itself.

Other disciplines

Computing is not the only area where advanced research can and should occur. As noted earlier, the cyber security "ecology" includes issues in economics, law, ethics, psychology, sociology, policy, and more. To ensure that we have an appropriate mix of trained individuals, we should explore including training and support for advanced education and research in these areas related to cyber security and privacy. Encouraging scholars in these areas to work more closely with computing researchers would provide greater synergy.

On possibility that should be explored is to expand the current Scholarship for Service program in a manner that includes students taking advanced degrees with a mix of cyber studies and these other areas; as an example, the program might fund students who have completed an undergrad in cyber security to obtain a J.D., or a student with a degree in public policy obtaining an M.S. in cyber privacy. Upon graduation those individuals would be highly qualified to enter government service as policy experts, prosecutors, investigators, and other roles where there is currently an urgent and growing need for multidisciplinary expertise.

[5] As an example, I need to travel over 70 miles from Purdue to be able to find a cleared facility.

Training

There are many people working in the IT field today who have security and privacy as one of their job functions. Given the pace of new tool development, best practices, new threats, and other changes, it is necessary that these individuals receive periodic training to stay current with their positions. Many 3rd-party organizations are currently providing such training (although the expense per student is significant), but as demand grows it seems unlikely that these efforts will scale appropriately. It is also the case that not all individuals who currently need such training either know they need it, or can afford it.

There should be an effort made, perhaps through DHS and/or the Department of Education, to provide ongoing training opportunities to the workforce in a cost-effective and timely manner. This might be by way of some mechanism that is delivered over the Internet and/or through community colleges. "Train the trainer" opportunities should be considered as well.

Note that this is not the same as continuing education as it assumes that the students involved already know how to perform their jobs. Rather, this is training in new tools and techniques to enable individuals to stay current in their positions.

Adult Education

The majority of citizens today using personal computers do not know anything about computer security, yet they are common targets for fraud and abuse. Phishing, Spam, and botnets are all generally targeted at home computers. Most people do not know that they need additional knowledge about security, and those that do are often unsure where to go to obtain that knowledge.

This is an area where many different techniques could be employed. Having educational modules and resources available online for citizens to review at their leisure would seem to be an obvious approach. Providing incentives and materials for ISPs, community groups, public libraries, and perhaps state and local governments to offer courses and information would be another possibility. Public television is yet another avenue for education of the general population about how to defend their computing resources.

Coupled with this effort at citizen education might be some program to provide access and ratings of products that could be obtained and deployed effectively. Unfortunately, there are many ineffectual products on the market, and some that are actually malicious in the guise of being helpful. Providing resources for citizens to get product details and up-to-date information on what they should be doing could make a large difference in our national cyber security posture.

Professional Education

We have many people in professional roles who use computers in their work, but who were not exposed to computing education during their formal studies. These positions include law enforcement personnel, judges, doctors, lawyers, managers, C-level executives, bankers, and more. In these various professions the individuals need education and training in cyber security and privacy basics as they relate to their jobs. They also need to be made aware that lack of security has real consequences, if not for their organizations, then for the country, and that it should be taken seriously.

Many professional organizations already provide organized training along these lines; for example, the National White Collar Crime Center (NW3C) offers courses for law enforcement personnel. Mechanisms need to be developed to help scale these offerings and motivate more professionals to take them. Where no such courses are available they need to be developed in conjunction with experienced and competent advisors who understand both the material involved and the issues specific to the professions.

Concluding Remarks

The cyber security problem is real. Informed warnings have been large ignored for years, and the problems have only gotten worse. There is no "silver bullet" that will solve all our problems, nor are solutions going to appear quickly.

Any program to address our problems will need to focus on deficiencies in our regulatory system, in the economic incentives, and in user psychology issues as well as the technical issues. We need a sustained, significant research program to address questions of structure, deployment, and response. We need a significant boost to law enforcement to act as an effective deterrent. Most of all, we need a comprehensive and wide-reaching program of education and training to bring more of the population in line to address the problem than the small number of experts currently involved.

Thus, there needs to be a significant investment made in both students and research in cyber security and privacy. The PITAC report made a conservative recommendation of tripling available research funding per year in 2005, although the committee privately discussed that 4-5 times the base could be productively spent. We noted that much of the money designated as R&D funding is really spent on the "D" portion and not on research. In the years since that report, it is unlikely that the amount has more than doubled, and that is due, in part, to standard inflationary issues and across-the-board increases rather than any targeted spending.

A conservative estimate for FY 2010 would similarly be to at least triple the current allocation for basic research and for university fellowships, with some nontrivial fractions of that amount dedicated to each of privacy research, cyber forensics tools and methods for law enforcement, to cyber security infrastructure, and to multidisciplinary research. Equal or increasing amounts should be allocated in following years. An additional annual allocation should be made for community and professional education. This is almost certainly less than 1% of the amount lost each year in cyber crime and fraud in the U.S. alone, and would be an investment in our country's future well-being. Again, it is important to separate out the "R" from the "R&D" and ensure that increases are made to the actual long-term research rather than to short term development.

There must be a diverse ecology of research funding opportunities supported, with no single agency providing the vast majority of these funds. Opportunities should exist for a variety of styles of research to be supported, such as research that is more closely aligned with specific problems, research that is better coordinated amongst larger numbers of investigators, research that involves significant numbers of supporting staff beyond the PI's, and so on. The NITRD Coordination Office is well-suited to assist with coordination of this effort to help avoid duplication of effort.

There are many good topics for research expenditures of this order of magnitude and beyond. As already mentioned, there are numerous problems with the existing infrastructure that we do not know how to solve including attribution of attacks, fast forensics, stopping botnets, preventing spam, and providing supply chain assurance. More speculative tasks include protecting future architectures including highly portable computing, developing security and privacy metrics, creating self-defending data, semi-autonomous system protection, building high-security embedded computing for real-time controls, and beyond. The PITAC report listed 10 priority areas, and the National Academies report lists more. The community has never had a shortage of good topics for research: it has always been a lack of resources and personnel that has kept us from pursuing them.

Above all, we must keep in mind two important facts: First, protection in any realm, including cyber, is a process and not a goal. It is an effort we must staff and support in a sustainable, ongoing manner. And second, as with infections or growth of criminal enterprises, a failure to appropriately capitalize the response now will simply mean, as it has meant for over two decades, that in the future the cost will be greater and the solutions will take longer to make a difference.

References

(1) *Cyber Security: A Crisis of Prioritization;* Report from the President's Information Technology Advisory Committee; National Coordination Office, NITRD; 2005.

(2) *Toward a Safer and More Secure Cyberspace;* Seymour E. Goodman and Herbert S. Lin, Editors; National Academy Press; 2007.

(3) *Unsecured Economies: Protecting Vital Information;* McAfee Corporation; 2008.

(4) Security Cyberspace for the 44th Presidency; Center for Strategic & International Studies; 2008.

Acknowledgements

I wish to acknowledge comments and assistance provided to me in preparing this testimony from Becky Bace, Steve Cooper, Dan Geer, Harry Hochheiser, Lance Hoffman, Carl Landwehr, Ed Lazowska, Victor Piotrowski, Bobby Schnable, Carlos Solari and Cameron Wilson. Despite listing their names here, none of those individuals necessarily agrees with, nor endorses any of my comments or opinions.