Statement of Eugene H. Spafford
Professor of Computer Science and
Director of Purdue University's Center For Education and Research in Information Assurance and Security (CERIAS)

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

Member of the Board of Directors
of the Computing Research Association (CRA)

Thank you Chairman Boehlert for the opportunity to testify at this timely and important hearing. I want to commend you, the Science Committee members, and your staff for turning the attention of Congress to the vital issue of securing our nation's information infrastructure. My testimony focuses on the important role of university research in information security, and in particular on some of the challenges research faculty face.

By way of introduction, I am a professor of Computer Sciences at Purdue University, a professor of Philosophy, and the Director of the Center for Education and Research in Information Assurance and Security. CERIAS is a campus-wide multi-disciplinary Center, with a mission to explore important issues related to protecting information and information resources. We conduct research, educate students at every level, and have an active community outreach program. CERIAS is the largest such center in the United States, and we have a series of affiliate university programs working with us in Illinois, Iowa, North Carolina, the District of Columbia, Ohio, and New York State. In addition to my role as an academic faculty member, I also serve on several commercial boards of advisors, including those of Tripwire, Guardent, and Open Channel Software; and I act as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA.

My statement today represents the USACM, the Association for Computing Machinery's Committee on U.S. Public Policy. ACM is a non-profit educational and scientific computing society of about 75,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. USACM, of which I serve as the co-chair, acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. USACM seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

To underscore the significance of today's hearing, my statement has also been approved by the Computing Research Association - an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies. The CRA is particularly interested in issues that affect the conduct of computing research in the USA.

The USACM and CRA believe it is important to present a strong and unified message to Congress that investing in computer security education and research is vital to securing the information infrastructure of our Nation. I know you are aware of the continuing, substantial growth in malicious software, system attacks, and cyber crime and I will not speak to those numbers. I will note that the figures available to me show growth rates of more than doubling each year in the number of incidents, and current estimates of losses in the tens of billions of dollars per year.

We cannot hope to protect our information infrastructure without a sustained commitment to the conduct of research -- both basic and applied -- and the development of new experts. The incredible growth of our society's deployment of computing has too often been conducted with concerns for speed or lowest cost rather than with concern for issues of safety, security, and reliability. Security cannot be easily or adequately added on after-the-fact and this greatly complicates our overall mission. The software and hardware being deployed today has been designed by individuals with little or no security training, using unsafe methods, and then poorly tested. This is being added to the fault-ridden infrastructure already in place and operated by personnel with insufficient awareness of the risks. Therefore, none of us should be surprised if we continue to see a rise in break-ins, defacements, and viruses in the years to come.

There are a great many problems that need to be addressed to help secure our infrastructure. Some of these problems have known solutions that are infrequently applied — perhaps because of cost or availability. Other problems will require long-term basic research and development of new technologies. Some of these solutions are potentially within easy reach of current scientists performing short-term research, while others will require training at least a new generation of research scientists with sound foundations in information assurance.

I use the term "information assurance" here because those of us working in the field have learned that the issues are really larger than simply computer security. Information assurance covers issues of building safe and reliable information systems that are able to weather untoward events no matter what the cause — whether natural disaster or caused by a malicious individual. Whether critical data in a financial institution or defense agency is affected by a hardware failure, a power outage, a computer virus or a hacker doesn't matter in at least one sense: unless the system is resistant to the damage and built for assured operation, the data is gone. We seek to protect those data and systems from a wide range of threats.

I would also like to clarify a point that is not always obvious: information security is not cryptography. Cryptography is simply one component branch of information security, in the same way that carpentry and plumbing are components in building a house. Information assurance also involves issues of physical security, malicious software, privacy, authentication technologies, software engineering, database security, network security, computer forensics, intrusion detection, and a number of other fields.

Another point that I should make is in response to a myth that is often repeated, namely that industry will find incentives to solve our security problems. To the contrary, it is largely because of industry practices that we currently face such security problems! Industry is concerned with getting products to market as quickly as possible, at the lowest cost. The result is often software with extraneous, poorly designed and poorly tested features. To spend extra time or money on better security is to put the companies at a disadvantage in the marketplace. Instead, many software companies have disclaimed all liability in their licenses, and sought to insulate themselves from adverse reactions and scrutiny of their software via laws such as the UCITA (at the state level), and the DMCA (at the Federal level). In the current market that does not offer consumers significant choices, and where there is no liability for faulty products, there is little likelihood that industry players will invest in fundamental research to improve products.

In the remainder of my remarks, I will briefly discuss issues in five aspects of current university operations as being of the highest concern to those of us conducting research and advanced education in information security. Those areas are: support for research, development of infrastructure, access to real-world data, personnel shortages, and legal impediments.

Support

For research to be conducted, investigators need financial support. The support is needed to hire graduate student assistants, purchase hardware and software, travel to conferences, subscribe to necessary journals, and other expenses. There are two general sources for funding of the sort needed by information assurance researchers in academia: from industrial sources, and from the government.

Experience by my peers has shown that many companies are concerned with information security and are willing to provide some funding to research in this area. However, this funding is generally quite limited, both in quantity and in the number of researchers supported. Furthermore, this funding is almost always tied to short-term deliverables and with restrictions on publication of results. A common practice within industry is to terminate university-based projects after delivery of prototypes — evaluation and validation of design is not always supported, and may actually be damaging to marketing plans. The results of this kind of support may be of short-term value for a few students and the companies involved, but it does little to advance to state of the art. Funding from corporate America that has fewer "strings attached" is more difficult to come by, and is particularly susceptible to fluctuations in the overall economy, as has happened recently. As such, few researchers depend on corporate support for their work.

Funding from government is the major source of support for most academic faculty. Traditional sources of this funding are the National Science Foundation, NIST, DARPA, the military labs, the Department of Energy, national laboratories, and the National Security Agency. Each of these agencies funds some research, often under specific and narrowly defined initiatives. However, my colleagues have indicated that they have found that few (if any) of these sources have provided long-term, on-going funding for information assurance research. Several of my colleagues have reported that they have begun to gain understanding of a fundamental problem after several years of research, only to find that the program under which they did their work was discontinued and no further funding was available. Others report an inability to find any funding to try new and novel approaches, especially if those approaches require multiple years of funding for an involved, systems-based investigation.

Similar to industry support, much of the Federal funding that is available is focused on near-term, deployable results. In some cases, this research produces no new publishable results, and is thus of little academic benefit to the faculty or students involved. Of more concern, in recent years cost-cutting measures have driven funding agencies (particularly Department of Defense agencies) to focus more on short-term research than on basic research; instead of finding ways to design new systems resistant to attack, we thus find most of the research being directed to how to apply newer patches to the same old buggy code. This does not serve to fix the long-term problems, nor does it serve to help build the capacity of educational institutions to do further research.

Most of the funding reported by my colleagues seems to be from within a larger program at the indicated agencies. I have heard from a number of frustrated faculty colleagues that their applications for information security research were competing for limited dollars against proposals for research in delivery of multimedia, improved computer science education, and new WWW applications, Only a few information security-specific programs have been available in recent years, and these have generally been underfunded.

For example, NIST announced allocation of $5 million in research awards under their 2001 Critical Infrastructure Grants program. They received 133 submissions and were only able to fund nine, and the continuation of the program in fiscal year 2002 has been zeroed out in the Senate. This means some projects begun under this year's program won't be funded to completion. This is typical of many of the programs established to fund security. Instead of cutting this program, serious thought should be given to expanding it. The new NSF program in Trusted Computing that has recently been announced also shows promise as an important mechanism to fund research in this area.

A survey of my colleagues at 23 major universities (see the Appendix) reveals that with the exception of two universities with large project grants, the information security faculty at these institutions are averaging $105,000 per year per faculty member. This is enough to support some modest equipment, travel and a few graduate students. It is not enough to fund long-term projects to advance the state of the art.

Let me also note that it is extremely frustrating for researchers to see competitive, merit-based programs reduced or eliminated at the same time directed funding is being provided to institutions without any clear history of excellence in the area or capacity to use that funding. Such actions can actually serve to be destructive in the community rather than constructive.

Infrastructure

To perform relevant research and education requires that we have an up-to-date infrastructure. This includes modern hardware and software, adequate space to house that equipment, and personnel to configure and maintain it. However, because of the nature of the field and the speed of its evolution, few institutions have the resources necessary to continuously support and evolve the infrastructure needed for current infosec research, especially when they are already stretched to provide resources to surging needs in general computer science.

Most of the programs in information security in the USA have strong ties to computer science and computer engineering departments. The surge in undergraduate enrollments in many of these programs mean that those departments are critically short of space for offices, laboratories, and academic needs. Many of these universities are public institutions with limited funds, and thus there is little hope for new space in the coming years. Information security, as a relatively new (and underfunded) specialty has little priority for what little space is available. Those of us in the community regularly exchange stories about how we have commandeered storage closets and regularly violate fire codes to house our equipment and students.

Industry has not been forthcoming about providing significant contributions of current products to more than a few select programs without tying such support to onerous intellectual property agreements. Often, donations are made without support included, and without needed options, thus creating an additional burden on cash-strapped programs (few grants allow inclusion of support costs). And the Federal government has no on-going programs to support the range of needs at recognized centers of excellence. This significant lack of infrastructure limits the nature and scope of the research we can undertake, and the number of students we can support. In some cases, there is a real concern that some of the research centers pieced together over the last few years may wither from lack of support to update themselves.

Real-world Data

The nature of much of the research being undertaken in information security is such that it requires considerable real-world data for analysis and validation. Unfortunately, we are often unable to see that data. Companies and government agencies are unwilling or unable to provide access because they consider the data sensitive or proprietary. (Note: I have heard from personnel in companies and government agencies that they often won't even share with each other!) It is not possible to construct valid models or solutions unless we can properly analyze the actual problems.

Consider, for instance, the problem of correlating data to identify attacks in wide-scale networks. To properly test theories, identify data markers, and validate designs, researchers need millions of audit records representing "normal" and "abnormal" traffic patterns; artificially-generated records cannot be used because we have not yet been able to construct valid models. Then, after the data has been analyzed, we need to instrument and test a real network. There are serious concerns about doing this data collection and testing on a real network because of the potential for adverse effects. Yet, no experimental testbed of this size and complexity exists for researchers to use. There are many other examples that can be cited, in different subfields of information security.

Personnel

Currently, there is a large unmet need for computer scientists and computer engineers in the USA. Information security specialists are an even scarcer commodity. The situation is especially acute when it comes to qualified faculty: there are only a few dozen faculty in the US who have significant background in security research, and they are graduating only a few PhDs per year to add to the ranks. The 23 institutions reported in the Appendix graduated a total of 20 PhDs in security in the last three years — an average of less than seven per year. These are some of the largest and best-known programs in the country in information security! Of those graduates, only a fraction have been interested in faculty positions. This results in intense competition for the few new faculty available, new programs cannot get started with domain-experienced faculty, and few existing programs are able to grow in this area.

Based on figures I obtained from the 23 universities, it appears that the active programs in the area average 3 or 4 CS faculty working in security at each institution. Many of them report that their time is often spent teaching basic, non-security CS courses to support their departments, so they are not able to devote their full attention to security research or teaching. It is also the case that there are not enough good students applying for the best graduate programs, for a variety of reasons. Without sufficient numbers of students or faculty, our ability to conduct research is severely limited.

The National Science Foundation's Scholarship for Service program, and NIST's Computer Science Fellowship program are both examples of programs to help build personnel. However, they only address a very small portion of the need, and neither addresses the critical shortage of PhDs in the field.

Legal Impediments

As more content has been developed for use with computers and networks, there has been a greater concern for protecting intellectual property. Content owners have stridently lobbied for greater and greater protections for their on-line property. Unfortunately, the evolution of the law has led to unintended consequences for those of us working in security. In particular, I know of several instances where research into novel forms of information security has been curtailed because patent holders have threatened researchers. University faculty members do not have the resources to fight such threats.

More recently, provisions of the Digital Millennium Copyright Act (DMCA) have led to faculty being threatened with lawsuits for publishing their security research, and some faculty (myself included) have had to curtail or stop our research in security forensics because of the potential for us to be arrested or sued. Legislation that is scheduled to be introduced into the Senate, the Security Systems Standards and Certification Act (SSSCA), may further restrict what research is conducted in information security. Legislation against technology instead of against infringing behavior can only hurt our progress in securing the infrastructure.

I will be happy to expand on any of these points, now or in the future.

Thank you again for the opportunity to testify.

Appendix — Information Sources

Academic colleagues at the following institutions contributed comments and data for this testimony. This testimony is more complete for their contribution, but is not in any way suggested as representing their individual views.

Florida State University
George Mason University (VA)
George Washington University (DC)
Georgetown University (DC)
Georgia Institute of Technology
Iowa State University
Mississippi State University
Naval Postgraduate School (CA)
North Carolina State University
Purdue University (IN)
Syracuse University (NY)
University of California, Davis
University of Idaho
University of Maryland, Baltimore County
University of Maryland, College Park
University of Nebraska
University of New Mexico
University of North Carolina-Charlotte
University of Virginia
University of West Virginia
University of Wisconsin-Madison
US Military Academy (West Point, NY)
Yale University (CT)