One View of A Critical National Need: Support for Information Security Education and Research

Eugene H. Spafford
Director, *COAST* Project and Laboratory
Purdue University
W. Lafayette, IN 47907–1398

Abstract

We are facing a national crisis in the near term that threatens our national security, our individual safety, and our economic dominance. The rapid growth of information technology is a driving factor in this threat: we are relying on new and often fragile technology in critical applications. Furthermore, those applications present attractive targets to criminals, vandals, and foreign adversaries.

Our students and soon-to-be students will be designing our information technologies of the future. We are endangering them and ourselves because the majority of them will receive no training in information security. This is largely because of a severe shortage of resources for computer security education and research. Current programs in place in industry and government do not address these needs, and some may actually serve to increase the problem.

This paper serves to introduce the crisis in providing good computer security education. It presents some of the history and context of this problem. It then provides some suggestions for near-term actions that should help to ensure a safer future for us all.

Introduction

It is clear that computer security is an area of increasing, major concern and that all of society is facing an increasing number of severe challenges related to security. Incidents related to disclosure of information, wide-scale computer breakins, and the exponential growth in the number of computer viruses being written and discovered all indicate an increasing threat to effective use of computing resources.[1] There have already been many documented cases of economic espionage, vandalism, theft, and other major economic crimes, some of which involve losses in the tens of millions of dollars *per incident*.[Pow96]

Many computer crimes go undetected. Others go unreported because the victims fear that any publicity about their losses (and by implication, their vulnerabilities) will result in a loss of confidence in their businesses. Additionally, there has been a huge number of cases involving smaller losses, most of which may not have been reported to the authorities for a simple reason: nearly everyone is aware that law enforcement is

[1] See, for instance, [Pow95, Pow96], and the on-going series of advisories from response teams such as the CERT Coordination Center, Department of Energy CIAC, NASA NASIRC, and DISA ASSIST.

hopelessly undertrained, underequipped, and understaffed to cope with even a minute fraction of the current flood of computer crime—and this imbalance is steadily improving for the vandals and crooks.

The threat from violations of computer security are numerous and diverse. They include loss from fraud and theft, economic and international espionage, sabotage, terroristic activities, computer viruses, vandalism, and support of other forms of crime. Furthermore, not all of the criminal activities are directed at government, commerce and other organizations: violations of personal privacy, harassment, "stalking," libel, and other activities threaten individuals as well.

A few years ago, the report *Computers at Risk*[SSSC91], forcefully outlined several critical security problems facing computer users. Few of the recommendations in that study were addressed, and the problems have become even more pressing in the intervening years. Our increasing reliance on computers for critical applications poses increasing temptation for unauthorized criminal and terroristic activity. Our increased connectivity provided by new network technologies simply amplifies the existing threats that we do not yet completely understand. For example, sixteen years ago, the experimental IP protocol suite was introduced as the number of ARPANET hosts exceeded 210; today, we have a worldwide network of several million machines using the same protocol.

The increasingly widespread use of computer technologies involving distributed databases and parallel and distributed processing adds new variables that have not, as yet, been adequately examined. Initiatives that link together computing systems from around the world and that provide access to more users will only add to the potential for security problems. In his State of the Union Address in January 1997, President Clinton voiced a goal of connecting every school and library into the Internet. Are we prepared for the problems that may arise in addition to the perceived benefits of having such widespread access available by the general public?

As was noted in an Office of Technology Assessment report[OTA94, Forward]:

> Information networks are changing the way we do business, educate our children, deliver government services, and dispense health care. Information technologies are intruding in our lives in both positive and negative ways.... As businesses and governments become more dependent on networked computer information, the more vulnerable we are to having private and confidential information fall into the hands of the unintended or unauthorized person....[Safeguards are required] Otherwise, concerns for the security and privacy of networked information may limit the usefulness and acceptance of the global information infrastructure.

The problems are especially pressing in the arena of national defense. Consider this statement in Duane Andrews' cover letter in the Defense Science Board's November 1996 task force report on Information Warfare – Defense[Boa96]:

> We conclude that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States which would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions. We have observed an increasing dependency on the Defense Information Infrastructure and increased doctrinal assumptions regarding the continued availability of that infrastructure. This dependency and these assumptions are ingredients in a recipe for a national security disaster.

It is interesting to note that this conclusion is independent of whether or not there is concern for protection against directed "information warfare." Widespread criminal enterprises, selected actions by anarchists, or random acts of vandalism can also have ruinous effects on our safety as a nation. Furthermore, as more and more commercial entities move to "internet commerce," the potential for serious disruption of our national economy also looms large.

Consider: in 1980, there were under 200 hosts on the ARPANET.[Sal95] A few countries were beginning to experiment with national networks. The first commercial workstations were not yet on the market, and the PC industry was in its infancy. The first, primitive Usenet newsgroups were flowing among a few dozen machines using 30 cps[2] modem technology. And the World-Wide Web was pure science fiction and a dozen years away.

Now, a mere 17 years later — one-half of a human generation or one-fifth of human lifetime — we have a global network that reaches to over 120 countries on all seven continents. We have tens of millions of people using the Internet daily. Governments are using the Internet to run their daily affairs. Commercial overload of service providers makes front-page news in all the major newspapers. Late night comics and editorial cartoons commonly refer to the WWW and network address. The President's State of the Union address is broadcast live around the world over the Internet. Some people estimate that billions of dollars are already invested and changing hands in commerce facilitated through on-line communications.

Where will we be in another 17 years? Although it is difficult for any of us to even imagine the changes in store, there is at least one clear aspect of that future: it will be designed tomorrow, in large part, by today's students. Some of them will enter the workforce and design the technology that will change our lives. Others will initiate the changes with their research projects soon to be underway. And still others will be wrought by those who are soon to be seeking re-education in high-tech fields so as to be productive employees of the 21st century.

Academic Security Education in the U.S.

This incredible pace of technology is changing our world so rapidly, there is clearly little chance to roll back the clock and reimplement decisions that may have negative security implications. To ensure safe computing, the security (and other desirable properties) must be designed in from the start. To do that, we need to be sure all of our students understand the many concerns of security, privacy, integrity, and reliability.

Unfortunately, this has not happened in recent years. For instance, consider the production of the software on which we currently depend. Commercial software vendors are *still* writing and releasing software needing patches for "bugs" that were well-known as security problems over 20 years ago![3] Even when highly-publicized problems occur, such as the buffer overflow problem exploited by the 1988 Morris "Internet Worm"[a, b], or the year 2000 date problem, those same software faults continue to be incorporated into existing operating systems.

Systems continue to be built using techniques known to be unsafe. Why aren't these problems avoided? Why is it that our students do not learn better security techniques? It is almost certainly because so few of them have access to appropriate education in such topics.

[2] Characters per second

[3] C.f. [A+76], [Lin75] and [Neu95].

Information security/computer and network security, as an area of specialization, is difficult to accurately define. Even professionals working in the this area have difficulty agreeing on an exact definition that appropriately encompasses the field. Part of the reason that security is difficult to describe is because it draws heavily upon so many areas of computing. In at least one sense, it seems closely related to software engineering — computer security is devoted to ensuring that software and hardware meet their specifications and requirements when used in a potentially hostile environment. Computer security thus includes issues in computer system specification, verification, testing, validation, safety, and reliability. However, security encompasses much more than these issues, including topics in (at the least) operating systems design, architectural design, information security, risk analysis and prediction, database organization, encryption and coding, formal models of computation, fault tolerance, network and protocol design, supportive interface design, government regulation and policy, managerial decisions, security awareness, and education.

The difficulty in defining computer security is also reflected in the scattered and underdeveloped educational and research programs in the area. Many other fields of computing research have well-defined bodies of educational literature, major research centers funded by government and industry, and a substantial student interest. Meanwhile, the field of computer security has been represented in academic life in the past dozen years by short chapters in textbooks on operating systems, data communications, and databases, and by a few individuals working in isolation in academia. The field currently has only a few widely-circulated archival journals in computer security topics: e.g., *Computers & Security*, *Journal of Cryptography*, and the *Journal of Computer Security*. And the public perception of computer security is shaped[4] by sensationalism such as computer virus scares, stories of 14-year old children breaking into sensitive military systems, and movies such as "The Net" and "Hackers."

Few universities or colleges offer in-depth education in computer security. As of mid-1996, there were only three declared, dedicated computer security research centers in degree-granting departments at universities in the United States (these are discussed in the next section); in November of 1996, a fourth center came into public existence. When computer security courses are taught, relatively few textbooks on computer security are in use, and several of the most commonly used ones are principally devoted to cryptography (e.g., [Den83]) or are outdated.

Research in academia is being done by a limited number of faculty at scattered locations working with a few students. What research is being done, in academia or commercially, has traditionally been oriented towards limited military requirements because until recently that is where the major demand has been (and where the funding has been available). The recent trend has been somewhat more open, but is still focused on a few narrow areas involving cryptographic support for electronic commerce and network firewalls. Although these technologies are significant, they are not addressing more important security needs. By way of illustration, I have been using the following analogy in my lectures and seminars on this topic over the past few years:

> Focusing our research on cryptographic protocols for secure electronic commerce is akin to investing all our money to build heavily armored cars. However, those armored cars will spend their lifetimes transferring checks written in crayon by people on park benches to merchants doing business in cardboard boxes under highway overpasses. Meanwhile, there are no traffic regulations, anyone on a skateboard can change the traffic lights with a screwdriver, and there are no police.

[4] Warped?

This lack of visibility, training, and coordinated research efforts has led to a significant shortage of practitioners trained in *practical* computing security, and to a critical shortage of academic faculty prepared to offer advanced instruction in this area. This contributes to a lack of consideration of security issues when new computer systems are being designed, thus placing those new systems at risk. As technology propels us into a future where global networks of communicating, multi-vendor computer systems are commonplace, the lack of universally-accepted social norms and laws will lead to difficulties that only well-designed computer security tools and techniques may prevent. To design those tools and train that workforce, we need an experienced, well-educated core of faculty.[5]

Education and research in computer security-related issues has usually been conducted under a number of different rubrics reflecting its cross-disciplinary nature. Work in areas such as computer architecture, operating systems, data communications, database systems, and software engineering has addressed questions of computer security. Despite advances in all these areas, most direct security-related research in the last few decades has been largely directed towards only a few selected topics. For instance, most of the systems-oriented research done to date has been in support of formal trust models for multi-level secure machines employed in military settings, including compartmented-mode workstations. The results of this research is usually of little use in "real-world" computing environments. This is because the traditional focus of such research has primarily been focused on issues of confidentiality [Nat85, Nat88] (keeping information secret), rather than on related issues such as availability and integrity.[6] Thus, there has been little support for research in the area of designing security tools and techniques for everyday use on commercial and educational computing platforms. Furthermore, as more computer users seek to use COTS (commercial, off-the-shelf) components, we will need better protection methods built in to these common systems.

In particular, considerable research in computer security methods and protocols over the last few decades has largely been focused on theoretical models of secure systems, multi-level systems, covert channels, statistical intrusion detection systems, and communications security issues (e.g., cryptography). Insufficient research has been focused on the development of tools for improving general security, policy formation, audit techniques, availability models, network security, computer forensics, countering malicious software (e.g., computer viruses and worms), policy formation, reliability, authentication and integrity methods. In fact, research in many of these important areas has been discouraged by the military for fear that people might collaterally discover ways of penetrating government systems. Another reason work in these areas has been limited may be because such efforts require an interdisciplinary approach and few researchers and research groups have both the breadth and depth of expertise necessary to conduct such investigation. To conduct good research in this area with application potential requires a broad base of resources and focus.

Education and research tend to track sources of demand. Thus, over the past few decades, research funding was made available by the military to researchers to conduct research issues related to military concerns. This tended to direct narrowly the research done in computing security. Journals and conferences came into being to provide outlets for this research, thus leading to a climate that did not readily accomodate research in other areas. The demand for students also shaped this picture, as the majority of job offers for graduates in security would come from either the government itself, from military contractors, or from vendors supplying the military. The overall demand for such graduates was not large. The Internet "explosion" has taken many

[5]This is not to imply in any way that development of new network-based etiquette and laws will obviate the need for information security professionals!

[6]During the Cold War era, standard military computer security doctrine could be interpreted as allowing classified computers to be blown up, the users shot, and the surrounding building burnt to the ground so long as the data contained therein was not disclosed to enemy agents: policies such as these are not currently acceptable in most banks, universities, or retail establishments.

in the community by surprise, to put it mildly.

One result, education in computer and network security in the U.S. is currently provided in a narrow, haphazard and inconsistent fashion. Some standard undergraduate and graduate texts in major course areas (e.g., operating systems) may have a brief chapter on security. These chapters often contain vague information about general security properties that are not particularly helpful in actual use. The instructors have not had direct experience or education in security, so they are unable to augment the material in the texts in any meaningful ways. The result, in the usual case, is that the material is presented in a cursory and compressed manner. As the material is in a separate chapter rather than integrated into the rest of the text, students are further given the implicit impression that security is unimportant, lacking in detail, and a separable concern.

Luckily, this is not true at every college and university. There are a number of faculty with some deeper background and concern with security. These faculty members do attempt to present information security concepts at greater depth in their courses. Even so, few students are given the opportunity to concentrate in security as a specialty, or to see how it cuts across several areas of study. There are only a few score faculty at institutions in the U.S. who conduct some research or specialized education in computer or network security. There are fewer still who have any experience with front-line security response experience.[7]

At the high-end of this specialization, there are four recognized academic centers in areas related to computer and network security in the U.S. Each of the four has several senior faculty whose research specialization is in one or more fields of information security. Each of the four centers has outside funding, recognition by its home university as a center of education and research, and recognition in the community. These four centers are (in order of their founding):

- The Center for Secure Information Systems at George Mason University. This center has several faculty involved in research and education, with a primary emphasis on issues of information system security, database system security, and authentication methodologies.[8]
- The Computer Security Lab at the University of California, Davis. This group includes seven faculty and four post-doc staff, with a primary emphasis on verification methodologies, and security for large-scale systems and networks.
- The **COAST** Laboratory at Purdue University. This group consists of almost a dozen faculty (half with current funding for research projects), and several staff. The **COAST** group has a primary emphasis on issues of host security, intrusion and misuse detection, computer forensics, and audit technologies.[9] With over 35 students involved in research projects, this is the largest and most widely known of the four centers.
- The Center for Cryptography, Computer, and Network Security at the University of Wisconsin, Milwaukee. This center was formally announced in November of 1996, although the (three) faculty

[7] For instance, I am the only full-time professor in the world to be associated with a FIRST-accredited response team in a day-to-day, active role; there is no incentive within traditional academia to play such a role, as it is unlikely to lead to publications or grants. Ludicrously, this situation is akin to encouraging faculty at medical schools to teach without ever having seen a patient or performed an autopsy. (FIRST is the international Forum of Incident Response and Security Teams — the network of CERT teams.)

[8] It is important to note that all four groups provide educational material across the broad spectrum of computer and network security. The indications of particular expertise given here is to note an emphasis, and not describe limitations.

[9] See also the Appendix of this paper.

members involved have been working in security for several years. The primary focus of this group is on application and extension of cryptography and cryptographic methods.

As a set, these represent the most advanced groups involved in *both* security research and education in the U.S. today. One of the labs (**COAST**) is widely believed to be the largest such academic lab in the world; it is also located at the highest-ranked department of the four, according to statistics published by the National Research Council[10].

Consider the following information about these four centers combined:

- Over the last five years, approximately 5500 PhDs in Computer Sciences and Engineering were awarded by universities in the U.S. and Canada.[11] Only 16 of those (average of three per year) were awarded for security-related research at these major centers.
  - Only eight of those 16 graduates were U.S. nationals.[12]
  - Only three of the 16 went into academic careers.
- The average production of Ph.D.-level students from these combined centers may rise to as many as five per year over the next three years; however, the ratios of citizens and of graduates entering academia is expected to remain constant.
- The four centers combined produced fewer than 50 students with research-oriented Masters degree training over the last five years. Only 50% of those students were U.S. nationals. There is no significant increase in M.S. production beyond this level expected over the next few years.
- In the history of all these centers, only three commercial sponsors have provided funding for research and education in security over a majority of the years the centers have been in existence.
- In the history of all these centers, only three government agencies have provided multi-year support of any kind other than through competitive research bidding (e.g., DARPA BAA or NSF program solicitations).[13] This is not because of any lack of quality or need at these centers, but rather because there is *no* Federal program in place that would provide such funding, even when desperately needed.

Undoubtedly, graduates with good security training and interests are coming out of other colleges and universities, too. This is not consistent, however — it depends on students with the right interests and skills matching up with faculty members who happen to have recently found funding for work in a related area. This is not a dependable manner of producing a large cadre of trained professionals.

Even if these four centers account for only a fraction of the production of trained graduates in security-related areas, the numbers are still extremely distressing. Of particular note are the small numbers of Ph.D. graduates going into academia. It is clear that we are falling short in building an educational infrastructure to support the increased need for training in security.

[10] In their study *Research-Doctorate Programs in the United States: Continuity and Change.*

[11] Estimated from the Taulbee Survey conducted by the Computing Research Association; see <http://cra.org>.

[12] Some of the non-nationals stayed in the U.S. to work, and have since become U.S. permanent residents or citizens.

[13] N.B., To my knowledge, all funding from government agencies has been stringently reviewed for scientific content and purpose, no matter what funding mechanism was involved.

Although it is not possible to accurately interpret all the causes and implications of these numbers, some indications of problems are obtainable by interviewing faculty and recent graduates in the field. Here are a few of the concerns that have been expressed repeatedly in such meetings:

Opportunity. Currently, because of the extremely small number of people with advanced degrees and comprehensive training in information security, industry is willing to pay substantial premiums to new hires. For example, excluding benefits and hiring bonuses, 1996 and 1997 graduates from the **COAST** Laboratory have been offered starting industrial salaries of mid-$50,000 for B.S. degrees, $70,000 for new M.S. candidates, and to almost $100,000 for new PhD. graduates. Compare this to an average starting salary of circa $67,900 for a twelve-month appointment as an assistant professor.[14] Some senior faculty in security have repeatedly received unsolicited offers ranging well above $200,000 per year.

Advancement. There is a perception among some graduates that academic careers in experimental computer security are more difficult than in other areas of study. This is akin to the concerns of graduate students in experimental computer science in general.[15] This perception is reinforced by an observed difficulty in obtaining appropriate funding, and a perceived bias in publication and tenure rates for those involved in anything but abstract, theoretical studies.

Resources. Some forms of security research and education, especially those involving large networks or heterogeneous computing, require substantial resources and on-going maintenance. There are few institutions with existing resources to support such research, and those that do are often unable to sustain them beyond the lifetime of a single research project. There are currently no general programs of support for such collections. Furthermore, almost all current government programs sponsoring research in this field are highly focused and disallow any budgeting for support personnel, equipment upgrades, and other needed infrastructure improvements.

One result of this lack of infrastructure support results in academic faculty spending significant amounts of time on clerical work, acquisitions, and project management, thus taking them away from teaching, advising, and research. This serves both as an example to discourage senior students from seeking academic careers, and as a factor encouraging existing faculty to consider leaving academia for careers with less time spent in clerical duties.

Futures. The combination of circumstances, including lack of consumer awareness, government policies (e.g., restrictive cryptography export controls), lack of peer support, and lack of industry support imbues many graduates with a sense of futility concerning an academic career in security. Instead, they are much more interested in joining a commercial enterprise where the results of their efforts may make more of an immediate difference. This also tends to encourage existing faculty to leave academia.

[14] Based on the Taulbee Taulbee survey[Fle97] average of $55,653 for a nine-month salary for all assistant professors at 131 responding U.S. departments, and a 22% rate for summer support.

[15] C.f. [oacfecs94].

A Call to Action

Undoubtedly, the situation is more complex than can be presented in this paper. However, some trends are clear: information security is an increasingly vital concern, there are insufficient educational and research resources to fill the need, there is considerable demand from industry for appropriately trained personnel, and current methods of support for the combination of education and research in computer and network security is woefully inadequate.

We are facing a national crisis in the near term that threatens our national security, our individual safety, and our economic dominance. If we are unable to make a concerted and coordinated improvement in the situation within the next few years, we may find ourselves facing a "security awareness deficit" that we will not be able to overcome. That deficit will make us vulnerable to attacks from without and vandalism from within. It will also lead to increased pressure on our public servants to come up with immediate "solutions" that may be worse than the problems they solve, and that threaten some of the very principles from which our republic draws its strength. We must act quickly to prevent this from happening.

The following recommendations for action, if heeded, would undoubtedly make a significant improvement in this area of need:

1. We need to encourage more students to study in information security topic areas. To this end, we should explore programs that offer scholarships or forgiveable loans to students majoring in information security in graduate studies. One or more programs could also be designed to help support personnel already in the computing profession to retrain *appropriately* in information security careers. An increase of only one hundred a year more such personnel would constitute a huge increase, and would make a substantial improvement in our current personnel deficit.

2. We need to encourage more graduate students in computer and network security to consider careers in academia. One way to accomplish this might be to establish some "young security investigator/educator" awards that would be designated prior to graduation. These could be used only if the candidate accepts a tenure-track position at an accredited institution upon graduation and remains on the faculty for some minimum number of years. The awards would serve the additional purpose of jump-starting each young investigator's research.

3. We need to provide substantial, long-term support to some or all of the existing centers of expertise in computer and information security. These are a critical national resource, not only for academia, but for the commercial sector, the Department of Defense, and for other public institutions. These centers should be provided with multiyear infrastructure support for personnel and resources, and encouraged to develop (more) outreach programs to other schools and to the public. To lose one of these existing centers would be a tragedy, and to lose one of the larger ones would be a disaster; however, the continuing existence of several of these centers may be considered fragile because of uncertain and erratic external funding combined with the lure to existing faculty of industrial positions.

   Note that this is not necessarily a recommendation for (or against) providing significant *research* funds for faculty in these centers. There are already many competitive programs available via NSF, DARPA, DOE, and other agencies to provide major project support. Qualified faculty can compete for these merit-based awards alongside their peers. However, infrastructure support is needed to ensure that a long-term base for education and collaboration is kept viable. Some on-going seed funding for

research through these centers would be appropriate, however, to encourage continual exploration of frontiers not yet recognized by the traditional funding sources.

4. We need to build up other strong programs in research and education in security technology (but not at the expense of endangering the stability of the existing centers of expertise). As new faculty become available, as experience is gained with existing centers, and as society's needs continue to grow, we need to develop programs working in concert with each other to expand the output of trained students, as well as to work on some of the difficult research problems that are, as yet, unsolved.

5. We need to involve U.S. industry more in the research and education of students in information security. Industry will be (and is already being) severely impacted by the shortage of trained professionals and by the availablity of scalable, affordable, and *practical* security technology. They should step forward with funding, personnel, and their expertise to work in concert with academia to produce solutions.

Closing Comments

The future need not be bleak if decisive action is taken. A small level of funding[16] over the next decade would serve to dramatically increase our national readiness and capabilities in information security.

The urgency of the problem is well-stated in the summary of the report [17] of the Joint Security Commission (I have emphasized some text from the original):

> Nowhere is this more apparent than in the area of information systems and networks. The Commission considers the security of information systems and networks to be the *major security challenge of this decade and possibly the next century* and believes that there is *insufficient awareness of the grave risks we face in this area*. The nation's increased dependence upon the reliable performance of the massive information systems and networks that control the basic functions of our infrastructure carries with it an increased security risk. Never has information been more accessible or more vulnerable. This vulnerability applies not only to government information but also to the information held by private citizens and institutions. We have neither come to grips with the enormity of the problem *nor devoted the resources necessary to understand fully, much less rise to, the challenge. ... Protecting the confidentiality, integrity, and availability of the nation's information systems and information assets—both public and private—must be among our highest national priorities.*[Joi94, p. 2]

It is time that we joined together to treat this national priority with the seriousness it deserves.

[16] The *combined* suggestions in the previous section could probably be funded for $20-$25 million per year.

[17] This commission was composed of personnel of the U.S. Department of Defense, Central Intelligence Agency, and Department of Energy. The charter of the Commission was to evaluate the current state of security in their agencies and the U.S. Government, and to suggest needs and directions.

Acknowledgements

I would like to thank the following people for their thoughtful comments and input to this paper: Mikhail Atallah, Rebecca Bace, William Cook, Yvo Desmedt, Dan Geer, Mark Graff, Sushil Jajodia, Karl Levitt, Steve Lodin, Katherine Price, Ravi Sandhu, Christoph Schuba, and Chris Wee. The conclusions discussed in this paper do not necessarily represent the views of any organization or person except those of the author.

Appendix

For illustrative purposes, this is an annotated version of the mission statement and set of goals for the **COAST** Laboratory at Purdue. This should help explain why a center-based approach is being taken, and the benefits of such an approach. Unfortunately, researchers at **COAST** have been unable to identify any Federal programs that will provide support for most of these goals, except to fund very narrowly-focused research projects over a two or three year period. This is not sufficient to sustain a program of the (needed) scope of the one described below.

The mission of the **COAST** (**C**omputer **O**perations **A**udit and **S**ecurity **T**echnology) Project and Laboratory is to conduct research and education on general and practical tools and techniques for improving computer and network security. The specific focus of this research is on typical computing environments — systems without multi-level requirements, and without formal levels of trust. In particular, our short-term research is directed to developing approaches of increasing the security of existing systems without severely impacting their usability. Our goal is to explore how to increase confidence in existing systems in a cost-effective and user-friendly manner. Our long-term research is directed to how to integrate better security mechanisms into common computing platforms. Using this research as a teaching mechamism, we are committed to providing a comprehensive and thorough education in security to our students at every level.

Operationally, **COAST** will bring together expertise of many faculty from throughout the university environment, provide shared resources in computer security research, and provide a unified approach to the research and education efforts in this vital area. It will provide a focal point both for internal and external agencies seeking reliable information about computer and network security, computer crime investigation, and appropriate computer use.

The specific, long-term goals of **COAST** is to have it continue to be:

- A world-recognized center of research excellence. We intend to be known for our research into methods of practical computer security technology, including computer incident response, system management and network security technologies. We expect most of our research to be based on the real needs of the community, as conveyed to us through interactions with our sponsors and the general user population. **COAST** is already known world-wide, and we intend to build our existing reputation.

- A renowned source of educational and training materials in computer and network security. We intend to produce materials for use in computer security training, both for in-service training in government and industry, and for academic use. This includes traditional materials such as texts and lab materials, but may also include leading-edge technology as embodied in hypermedia and distance-learning methodologies.

- An on-going source of quality graduates with cutting-edge training in computer and network security. We expect our undergraduate and graduate students to receive a broad-based and comprehensive education that will give them a solid foundation for work in computer security, computer systems, and communication networks.

- A resource center for research. We intend to build a comprehensive collection of documents, references, tools, hardware, software, testbeds, and other resources necessary for comprehensive research

and experimentation in various areas of computer security. We expect to make the **COAST** Research Laboratory a significant, widely-available resource for visiting scholars, sponsor personnel, and **COAST** researchers.

- A resource center for independent evaluation of products. We intend to be able to provide unbiased, comprehensive testing and evaluation of security tools for computers and networks. By providing detailed test results to sponsors, vendors, and the general user population, we believe we will help improve the overall state of information system security and improve the general state of the art.
- A resource center for information dissemination to the non-technical community. There is a significant need for sources of information for the press and public that is unbiased by commercial interest or government policies. We expect to continue to be known and consulted as one such source. (**COAST** personnel have been quoted on issues of computer security and computer crime over 150 times in the last five years, including quotations in the *New York Times*, *Newsweek*, the *Wall St. Journal*, *NPR Radio*, *ABC Radio*, *Scientific American*, *Science* and more.)
- A source of useful tools for system management and security. Although not a primary focus of **COAST**, we expect that we will produce new tools and protocols as useful byproducts of our research activity that will be of wide-spread applicability to the community at large. The **COAST** on-line archive is already acknowledged as the single largest and most comprehensive security repository on the Internet.

References

[A+76] R.P. Abbott et al. Security Analysis and Enhancements of Computer Operating Systems. Technical Report NBSIR 76-1041, Institute for Computer Science and Technology, National Bureau of Standards, 1976.

[Boa96] Defense Science Board. Report of the task force on information warfare (defense). Government report, November 1996.

[Den83] Dorothy E. R. Denning. *Cryptography and Data Security*. Addison-Wesley, Reading, MA, 1983.

[Fle97] M. Fleck. Preliminary faculty salaries from survey. *Computing Research News*, 9(1):6–7, January 1997.

[a] Eugene H. Spafford. An analysis of the internet worm. In C. Ghezzi and J. A. McDermid, editors, *Proceedings of the 2nd European Software Engineering Conference*, number 387 in Lecture Notes in Computer Science, pages 446–468. Springer-Verlag, September 1989. Also available as http://www.cs.purdue.edu/homes/spaf/tech-reps/933.ps.

[b] Eugene H. Spafford. The Internet Worm: Crisis and aftermath. *Communications of the ACM*, 32(6):678–687, June 1989. An expanded version is available as http://www.cs.purdue.edu/homes/spaf/tech-reps/823.ps.

[Joi94] Joint Security Commission. Report of the joint commission. Technical report, U.S. Government, 1994.

[Lin75] Richard Linde. Operating system penetration. In *National Computer Conference*, pages 361–368, 1975.

[Nat85] National Computer Security Center. Trusted computer system evaluation criteria. Technical Report DoD 5200.28-STD, U.S. Department of Defense, 1985.

[Nat88] National Computer Security Center. Computer security subsystem interpretation of trusted computer system evaluation criteria. Technical Report NCSC-TG-009, U.S. Department of Defense, 1988.

[Neu95] Peter G. Neumann. *Computer-Related Risks*. Addison-Wesley, 1995.

[oacfecs94] Committee on academic careers for experimental computer scientists. *Academic Careers for Experimental Computer Scientists and Engineers*. National Academy Press, 1994.

[OTA94] Information security and privacy in network environments. U.S. Office of Technology Assessment report, September 1994.

[Pow95] Richard Power. Current and future danger. Technical report, Computer Security Institute, San Francisco, CA, 1995.

[Pow96] Richard Power. Current and future danger. Technical report, Computer Security Institute, San Francisco, CA, 1996. Second Edition.

[Sal95] Peter H. Salus. *Casting the Net: From ARPANET to INTERNET and Beyond*. Addison-Wesley, Reading, MA, 1995.

[SSSC91] National Research Council System Security Study Committee. *Computers at Risk: Safe Computing in the Information Age*. National Academy Press, 1991.