Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

A Breadth-First Approach to Computer Security

Kara L. Nance and Brian Hay, *University of Alaska Fairbanks*

Abstract – Information assurance provides us with the foundational means to protect our digital assets. As we build programs to meet the needs of our ever-growing computer user base, we seem to be fighting an uphill battle. This research effort describes some of the findings from an NSF-funded project to investigate the state-of-the-art in computer security laboratory environments and how they are being used in an effort to develop a plan for improving the capabilities and facilities available in the State of Alaska. The major ancillary finding is that research and educational environments do not exist in isolation. The best way to reach the diverse populations that need more computer security information is through a breadth-first approach that combines research, education, and outreach as an overarching umbrella to reach our many new constituencies. As computer systems become increasingly ubiquitous, we need to ensure that computer security research, education, and outreach are just as omnipresent in order to ensure that the next generation of computer users is better-prepared to protect their own digital assets and are an integral part of the future of information assurance.

Index terms – Computer Security, Information Assurance, Education

I. Introduction

In 1998, the National Security Agency (NSA) announced a revolutionary new program to address the lack of information assurance and computer security professionals available to support the U.S. critical infrastructure. The Center of Academic Expertise in Information Assurance (CAE) program has evolved and is now a partnership that includes the Department of Homeland Security (DHS) and the NSA in support of the President's National Strategy to Secure Cyberspace [1]. The U.S. Government recognizes that "securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.[2] Over time the criteria for becoming a CAE have evolved, but what has remained constant is the focus on a multidisciplinary approach to this issue as well as making it ubiquitous. These broad requirements have served as a driver for institutions to start down this path by developing and documenting institutional capacity in ten identified areas related to information assurance.

The National Science Foundation provided a unique opportunity for our research group to spend the 2005-2007 academic years visiting designated CAE and other institutions to see how they were meeting the needs of their computer security and information assurance constituencies in innovative ways. The valuable information gained during this exercise and subsequent visits to other institutions has helped our understanding of the situation and convinced us of the importance of educating the next generation of computer builders and users so that a proactive approach is taken to addressing computer security issues rather than a reactive approach.

Over and over, we found that the most successful programs integrate computer security principles and practice across the traditional tripartite mission of their faculty. They are successful at research, education, and outreach and at interweaving information assurance concepts between these missions and across disciplinary boundaries. They educate computer users from all disciplines and at all levels of computer user from the first exposure to computing as a child to the professor leading a theoretical research program. The traditional boundaries between disciplines, educational levels, and user competencies are pushed in an effort to provide a breadth-first approach to computer security.

II. Background

The original scope of the project was limited to an investigation of the state of the art in computer security laboratory facilities around the nation, and to subsequently develop lab resources that incorporated the existing strengths that were discovered, while also addressing identified weaknesses. Over the course of 18 months we were fortunate to be granted access to many exceptional university and research security labs across the country. An initial deficiency observed was the lack of remote access to hands-on computer security resources in a manner that appropriately isolated the lab from production networks, in order to ensure that planned or accidental malicious activity within the lab could not impact external system. Another identified issue was the duplication of effort between institutions, where the problem of providing a suitable computer security lab environment was being solved and re-solved independently by faculty members at various institutions.

A proposed solution to both of these issues is to apply enterprise level virtualization software, such as VMware Infrastructure [3], to create lab environments that allows remote access to the virtual machines interfaces (e.g., the operating system console, or graphical user interface), while only giving the virtual machines access to isolated physical and virtual networks. In addition, in a model borrowed from the national supercomputing community, a small number of these remote access virtual labs could be deployed around the country, thus ensuring that an institution that wanted to use such a resource would not be encumbered by the funding requirements and steep learning curve associated with installing and managing such resources, and could immediately focus on the use of the facility to meet their primary goals of research and education. A fully functional example of this infrastructure has been in place at the University of Alaska Fairbanks for the past 18 months, and has proved to be incredible valuable to local and remote faculty, students, and staff. The Remote Virtual Information Assurance Network (RVIAN) at the United States Military Academy provides similar functionality using VMware Server.

The project had an unexpected second benefit, in that discussion of the lab infrastructure typically evolved into the usage scenarios for the lab, and through this project, in conjunction with discussions at computer security conferences, the authors gained some insight into the methods used for information assurance (IA) research and education. This paper shares some of those findings. What follows is a distilled version of the knowledge accumulated from the observation of many exceptional institutions combined with needs expressed by many institutions. In each of the following tri-partite responsibility categories additional examples could have been provided, but the intent of the authors is to provide educators with a broad sweep of methods through which IA concepts can be made increasingly ubiquitous, and omissions should be attributed to space requirements, rather than a commentary on the quality of omitted programs.

III. Research

In 2008, a new category of CAE was introduced that demonstrates the Department of Homeland Security and National Security Agency recognition of the increased importance of research in information assurance. In June of 2008, the first cadre of CAE-Research institutions will be designated. In order to be eligible for the CAE-R designation, applicants must meet the Carnegie Foundation classifications of Research University/Very High, Research University/High, Doctoral Research University, or be a military academy before beginning the process [4], as well as the documenting and meeting the required criteria for CAE-R status. While this designation does not provide automatic funding, there are many national agencies that are providing funding programs that focus on computer security. It is expected that the CAE-R institutions will provide leadership to keep the U.S. at the forefront of computer security research.

Research in computer security and information assurance lies on a continuum from pure theoretical research to applied research. Most research programs in computer security fall somewhere between the two extremes with foundational theoretical work leading to applied work that is again redefined and reapplied as technological advances occur. Research across the continuum is necessary and important in order to continue to secure our increasingly more sophisticated technologies.

A. Theoretical Research

It seems clear that the current approaches to computer security, such an the exploit and patch cycle, signature based detection and prevention systems, and arguably most importantly the reliance on the end user to make good security decisions without arming them with the requisite knowledge, are not working, nor are they likely to begin working in the future. As such, the long term solution lies initially in theoretical research, through which models for creating the systems of the future can be developed, tested, and improved. Theoretical research provides advances in the field that form the stepping stones for applied research. It provides a root system from which many unique research branches can be developed.

B. Applied Research

Applied research provides the bridge between today's systems and the results from the theoretical research arenas, and can be pursued from either end of that spectrum. As an example, there are certainly many excellent cryptographic algorithms and protocols which in theory address computer security problems, including the all too common exposure of personal data when backup media is misplaced or stolen in transit, as well as the spam problem in email systems. However, the fact that such solutions do not enjoy widespread use speaks more, we believe, to the usability of products based on the cryptographic protocols, rather than the effectiveness of the protocols themselves.

A common exercise in several computer science and computer security classes at institutions we interacted with was to for the students to create an asymmetric key pair, which would be used for secure class communication primarily to demonstrate the associated concepts. Students were requested to supply the instructor with a public key, which the instructor would sign and post in class "key server". The following failures were observed in many of these classes, which we must recall are composed of primarily upper division, technically competent students:

- Students who sent both their public and private keys to the instructor.
- Students who sent one of the default keys from their PGP or GPG key ring to the instructor.
- Students who sent their passphrases to the instructor when encountering challenges.
- Students who encrypted messages to other students with their own public keys, rather than the public key of the recipient.

If this is the result from the most technologically savvy students on campus, then it can be expected that the results from a group more representative of the general computer-using population would be far worse, and as a result all of the benefits of public key cryptography would almost certainly be lost.

C. Cross-disciplinary Research

It is tempting to blame the user, and make the case that computer users should take more responsibility for their educations and actions. However, we feel that it is the computer industry that has failed users, and one focus of applied research lies in integrating security features into the computing environment in such a way that they work well (and seamlessly) for the diverse populations who are likely to use them. Obviously this is not a trivial task, but it is unreasonable to expect that computer users should have the in-depth knowledge necessary to make good choice in this regard. Using the analogy of an automobile, most drivers can operate almost any car quite safely based on a fairly basic user interface without an indepth understanding of the particular engine, transmission, brake system, etc.

Clearly this is not just a computer security issue, as many researchers in other fields write, market, and distribute their own programs with minimal (or no) formal training in computer science or computer security. This causes additional challenges that can be mitigated by including computer security personnel on cross-disciplinary research teams to investigate the unique security aspects associated with each field as they research, build, and deploy technologies.

An example of a case where cryptography is applied quite successfully in current systems is that of SSL/TLS [5, 6], which allows confidentially to be preserved a network connection, such as that between a web browser and a web server. The choice of a range of strong cryptographic algorithms are automatically negotiated then employed to protect transmitted data with little more direction from the user than the use of the *https* prefix in the URL. While the requirement that the user occasionally verify the identity of the server with which they are communicating (in the case of a certificate problem) may remain problematic, there are other aspects of the communication path that can be simplified. The fact that a cryptographically-protected communication path can be created so easily is an excellent example of where the industry, and education, must facilitate and further simplify the process. The use of SSL/TLS can be very favorably contrasted with the difficulty with which a similarly confidential email message could be sent and received using many common email clients…another area in which the process can be is becoming increasingly simplified for the casual user.

Applied research can also provide proof of concept to support theoretical research. One of the areas where this is meeting a current security need is through the academic institutions that partner with government agencies for technology transfer. One such example is TechLink which is housed at Montana State University [7]. Among other functions, TechLink has the capability to take Department of Defense (DoD) software products and provide a testbed environment to ensure that the software meets computer security requirements. The software packages can then be either transferred back to DoD or have the rights licensed to an industry partner for marketing. The U.S. Department of Commerce Office of Technology Policy identified this program as "one of nine exemplary models of federal technology transfer in the United States." [8] DoD is actively seeking additional academic partners to aid in the transition of technology with an emphasis on computer security and associated applications and with the establishment of cooperative research and development agreements between federal labs and organizations.

Both applied and theoretical research results become more valuable when they are disseminated widely. Traditionally, research finding are shared through technical publications, but they can serve as more active catalysts for further advances when results are shared in academic settings and also through outreach.

IV. Education and Training

There is much debate over the formal distinction between education and training and the associated needs for various user groups. Regardless of the definitions, there are definite needs for a wide range of programs to meet the many identified educational objectives. There are identified needs for graduate and undergraduate certificates and degrees in information assurance. There is a need for cross-disciplinary and multidisciplinary approaches to security. We need training programs, and K-12 opportunities that strengthen the computer user base in this country. Education and training are necessarily tightly coupled with research and outreach for many of the most successful computer security programs.

A. Graduate and Undergraduate Education

Perhaps the most obvious contribution of the CAE program to the computer security and information assurance arena is the growth of certificates and degrees at the graduate and undergraduate levels. The many programs that have evolved are unique, each designed with intent of meeting the needs of their diverse student populations. As expected, many of the new graduate programs are tightly coupled with research programs, although some graduate programs are more closely tied to meeting the needs of working professionals and provide the means for cohort groups to obtain professional certification in information assurance while retaining their fulltime jobs. The graduate programs may well be the most evolved of formal education options for aspiring computer security professionals.

B. Undergraduate Education

The introduction of information assurance concepts in the undergraduate curriculum is vital to ensuring that the current state of system insecurity does not perpetuate. Students in undergraduate computer science programs are the software developers and architects of the future, and at a minimum they must be given a clear understanding of security concepts. Some examples of areas for inclusion in the undergraduate curriculum include:

- *General security concepts*. These concepts can often be presented in a broader security perspective. A common security experience in the United States is that of airport security, and it is easy to present the problem of having an insecure path between a security check (the TSA checkpoint in which bags and belongings are searched) and a resource (the aircraft), if a branch of *Bob's Guns and Ammunition Supply Store* is allowed to open inside the security perimeter. In such a case the TSA checkpoint is ineffective, because the path between the checkpoint and aircraft is not free from prohibited items. To prevent weapons from being taken on board the aircraft, the security check in this case would need to be situated at the jetway door, after which the path to the aircraft was secure. A computer security analogy may be the deployment of intrusion detection systems at the boundaries of a campus network, while allowing connections to the internal wireless network from anyone present on campus.
- *Insight into the perspective of an attacker*. Many system compromises result from the failure of system architects, developers, or administrators to adequately understand the capabilities of attackers, and the level of effort they are willing to put forth into discovering and exploiting vulnerable systems. For example, an attacker motivated by the intellectual challenge of compromising systems may be willing to spend hours, days, or even months examining a system before finding an exploitable vulnerability. Such effort, when viewed from the perspective of a software company may seem to be economically unreasonable, and as such highly unlikely to occur, but attackers have different goals and motivations, and from their perspective other factors, such as elevated stature in their peer group, or even financial gain from criminal enterprise, may make the effort worthwhile. In addition, there is a tendency to consider systems or software from the perspective of normal users who want to use it successfully, rather than attackers whose goals is to make the software fail. Attackers are, as a consequence, willing to run the software under conditions that would be unthinkable for typical users, and are therefore generally unthinkable for, and un-thought of by, those charged with creating and managing such systems. For example, it is easy to assume that memory will always be available for allocation to an application on modern systems, which have typically have large amounts of physical RAM and swap space. However, if an attacker deliberately forces the system into a memory starved state, an application which assumes that memory will always be available may fail quite spectacularly, and in the worst case in manner which the attacker can control.
- *Practical examples of problems with computer security in current systems*. This serves two purposes: a demonstration of common problems to avoid in their future careers, and a motivator for research problems. These examples can be easily integrated into the current curriculum. During a discussion of scheduling in an operating systems class, for example, it is easy to integrate a discussion of kernel level rootkits, and their ability to hide processes from the system user (even the superuser). With the ease of access to kernel source code for Linux, BSD, and even Windows operating systems, students can be presented with real examples of schedulers, the mechanisms by which the operating system tracks processes, and basic

examples of how such data structures can be manipulated to hide a process, while still ensuring that it receives processor time. A homework assignment or group discussion can then involve how such rootkits might be detected by a careful system administrator, how the system may be redesigned to prevent such attacks, and what consequences this might have for the efficiency of the system. Similar types of examples can be produced on topics such as authentication and authorization, files systems, device drivers, kernel modules, interrupt handling, system calls, databases, network infrastructure, and so on.

Information assurance topics have proven to be of great interest to students, and as such can be used throughout the computer science curriculum to generate and maintain interest in the subject. In addition, the ability to provide hands-on examples has the benefit of allowing students to hear the theoretical foundations of a concept, see the concept in action, and actually apply the concept. This method of instruction can help to solidify the concepts for students.

C. Cross-Disciplinary Education

The current state of computer insecurity will likely not be solved by technical means alone, and a cross-disciplinary approach to education is important. Information assurance research topics and research partners need not be limited to the traditional disciplines. Partnerships and outreach within the academic community can be very rewarding. A project involving the creation of models for cascading failure in power systems, for example, may also have applications to computer networks, or the original model may be extended to determine how multiple interacting and interdependent complex systems, such computer networks, telecom systems, and power grids, are impacted by a failure in a component or components of one of the systems. Psychologists may be interested in studying how online social networking tools allow trusted relationships to be developed between parties that have not met in person. Business school faculty may want to pursue projects which model risk and return for security tools in a commercial environment. The combination of various disciplines with computer science is an important one as many disciplines develop technologies without a clear understanding of computer security and how it impacts the products they are producing. A recent computer security team report of hacking a defibrillator-pacemaker that included the delivery of potentially fatal jolts of electricity as well as the means to obtain personal patient data from the device demonstrates a need for computer security partnerships with those who develop medical implant devices. [9]

In addition to cross-disciplinary education, which we view as identifying specific needs associated with bridging specific disciplines, there are needs for overreaching computer concepts for the everyday user. Multidisciplinary education includes the foundational concepts that all computer users should have in order to utilize technologies safely and security.

D. Multidisciplinary Education

Since computer usage is not restricted to computer security experts, it is important that we commit to a multidisciplinary approach to safe computer usage. In corporate environments, even technical corporations, the budget is often controlled by non-technical managers and executives. Likewise, local, state, and national governments are generally not always staffed by technically savvy people. The result is that those in control of the budgets and laws capable of affecting change on the IT landscape often do so with very little knowledge of the real needs and problems of the system. Providing an opportunity in academia for the business and government leaders of the future to gain some understanding of IT security concepts can address this imbalance, even if it only serves to provide a basic, but eye-opening, introduction to the field. Modules can be made available to departments across the curriculum, including business and political science. An incredible example of how important such an education can be was provided in a conversation following a discussion of website credibility with Senate staffers and lobbyists. One of the attendees admitted to having cancelled a meeting between a Senator and a European visitor based on evidence that the visitor had mafia ties. It was only during our talk that the attendee learned that the content in Wikipedia, which was the sole source of the evidence, could be edited by any user, and was not subjected to systematic fact checking.

Personnel at the Advanced Systems Security Education, Research and Training (ASSERT) Center regularly present a module entitled "Website Credibility" to students in freshman-level core courses across the curriculum at the University of Alaska Fairbanks. The presentation covers many aspects to help students evaluate the web resources that they are likely to use in research projects throughout their academic careers. It includes a discussion of Wikipedia which students tend to find quite interesting as a discussion item. Another popular module that targets this audience is "Password Security" which provides them with valuable information about choosing and remembering passwords as well as a discussion of the methods that passwords are stored and used on the web.

E. Workshop Programs

Beyond the traditional boundaries of a university there is a need for formal training in computer security. This training can take the form of specialized workshops, specialized certifications, online resources, self-directed learning and e-learning activities, etc. This type of education is extremely diverse and the various needs of the communities are identified and met.

One excellent example of outreach is the Southeast Regional Forensics Training Center at Mississippi State University, which is funded in part by the U.S. Department of Justice, the National Science Foundation, and the U.S. Department of Homeland Security. [10] This program provides digital forensics training opportunities to law enforcement agencies around the nation, typically at no charge to participants beyond the cost of travel to and from the training site. Courses are offered at various levels, ranging from introductory sessions designed to provide law enforcement personnel with a basic understanding of how to identify and handle digital evidence, to advanced digital forensics topics.

An outreach capability widely available to CAE institutions is to identify, maintain, and publicize computer security resources relevant to university and community computer users. Topics may include defensive steps that users can take to protect their digital assets, and a process, including contact information, in the event of a suspected or confirmed system compromise. Specialized versions of this information can also be created, such as versions aimed at teachers that are publicized within the local school district. While the resources listed on such a site can be written in house, there are also many excellent sources of information already available on the web, such as those provided by The Center for Education and Research in Information Assurance and Security (CERIAS) [11] and the National Information Assurance Training and Education Center (NIATEC) [12]. As such the CAEs can act as a trusted directory of useful information by providing annotated links to web content that has been verified by the CAE experts.

An exceptional example of combining research, education and outreach in a single facility can be found at the Security Analysis and Information Assurance Laboratory (SAIAL) at the University of Texas at Dallas (UTD). The facility provides UTD with the ability to conduct cyber security research and greatly enhances their ability to collaborate with other universities and corporations doing leading-edge research in this critically important area. The rooms at the facility have been individually tested to meet MIL-STD-285 TEMPEST standards and can be used by corporate partners and researchers for research and testing. [13]. UTD provides an excellent model for partnerships with industry and is one of the few CAE institutions that specifically identifies partnerships with other universities, government agencies, and corporate entities as one of their goals to achieve their mission, and actively demonstrates their ongoing commitment to this goal.

F. K-12 Education

Children are exposed to computers earlier and earlier in their academic careers. Unfortunately, there is little consistency in what and how they are taught regarding computers in these informative years. Educating the K-12 educators so that the first exposure to computers begins with an emphasis on safety and security would make the online world more secure and could provide a strong foundation in computer security on which to build. Most children are taught to lock doors, fasten seat belts, and not talk to strangers. Imagine if a concept as simple as password safety was part of this foundational safety knowledge that they acquire during their informative years. This could play a significant role in securing our digital assets as the users are frequently the weakest link in a system.

V. Service and Outreach

For many students the first exposure to computers is in the home rather than the academic setting. Academia can extend beyond traditional educational boundaries to reach out to communities to provide resources to help bridge the gap in this area.

A. Institutional Service

For many academic institutions, service is further divided into university and public service. How can this ubiquitous computer security concept be extended to these missions? Most institutions that have been received the CAE designation have specialized skills that can benefit the institution as a whole. For some institutions, this may be a physical computer security lab in which specialized software for data recovery and digital forensics investigations can be undertaken. In these cases, institutions can serve and educate their peers by providing access to these specialized resources. If this approach is cost-prohibitive, there is always knowledge to be shared. Many contemporary professors are not trained in the use of the technologies they use each day. For many, the personal computer is an evolutionary step that post-dates their initial academic appointment. As a result, many of these innovative colleagues are largely self-taught computer users. They tend to learn reactively by picking up new skills as they are needed. Unfortunately, this approach does not encourage secure computer usage, with minimal information accumulated related to safe computer usage. We can provide a valuable service to this population by conducting interesting faculty development workshops that focus on information assurance topics that are most likely to affect these populations. Some examples might include backups, web site credibility, password safes, FERPA, and other issues that are relevant to identified user groups. As this is a population that is not likely to gain this knowledge through another forum, meeting the university service need, could help contribute to the overall security of the institution's digital assets.

B. Public Service

One exemplary model of K-12 outreach is offered through CERIAS at Purdue University. The mission of the CERIAS K-12 Outreach Program is to "to increase the security of K-12 information systems, integrate information security as a discipline into the K-12 curriculum, and to raise parent and community awareness of information security issues through K- 12 schools" [14, 15]. Public service is the single area in which we can make the biggest difference. Very few teachers are formally trained in computer usage, yet these teachers are responsible for training the next generation of computer users. How can we help these teachers to train the next generation in safe computer usage? There are several NSF initiatives that specifically address this issue and that the computer security community can participate in, in order to increase computer security awareness.

The National Science Foundation (NSF) GK-12 program [16] provides funds to place graduate students in science, technology, engineering, and mathematics (STEM) disciplines in K-12 classrooms as scientists in residence. The ASSERT Center at the University of Alaska Fairbanks has placed a Computer Science Graduate student in the public schools with a focus on educating the teachers and the students on computer security. The benefits of this program to the community are significant and the compensation provided to the graduate students is substantial.

A second NSF program is Broadening Participation in Computing [17]. While this program focuses on populations that are traditionally underrepresented in computing, it does provide an opportunity to perform public service in a diverse range of environments to educate individuals about safe computer usage while exciting them about the many opportunities available in technology fields.

There are many other programs that provide funding that could be used by computer security researchers and educators to increase the level of awareness of the issues associated with computer security. The previous two examples are just two that are currently being used by the ASSERT Center for computer security outreach.

VI. Conclusion

Don't put boundaries around your information assurance program. Make it a ubiquitous component of your IA career. Investigate theoretical IA topics, but don't underestimate the value of applied research in addressing the issues we face today. Share your research results with your colleagues, graduate, and undergraduate students as a regular part of your teaching. Teach your students theoretical concepts, but also practical information that they can take to their homes, offices and communities. Expand the boundaries of teaching beyond the traditional university walls to meet the unique education and training needs of your external academic, industry, and government constituencies. Don't limit your teaching to the university classroom. Break down walls. Take it to the streets, so that the next generation of computer users is better-prepared to protect their own digital assets and are an integral part of the future of information assurance.

VII. Acknowledgements

This research effort was funded by the National Science Foundation through the GK-12, CISE Capacity Building, CRI, and Broadening Participation in Computing Programs and with support from the many institutions that opened their doors and provided access to their facilities during the 2005-2007 academic years.

VIII. References

[1] National Security Agency Press Release. "National Security Agency and the U.S. Department of Homeland Security Form New Partnership to Increase National Focus on Cyber Security Education" April 22, 2004. Retrieved December 10, 2007 from http://www.nsa.gov/releases/relea00077.cfm

[2] Bush, George W., Forward to The National Strategy to Secure Cyberspace. Retrieved December 4, 2007 from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[3] Transform IT Infrsatructure with Enterprise-Class Virtualization. Retrieved February 15, 2008 from http://www.vmware.com/products/vi/

[4] National Security Agency. Centers of Academic Excellence. http://www.nsa.gov/ia/academia/caeiae.cfm?MenuID=10.1.1.2#reviewAndSP. Retrieved February 15, 2008 from http://www.nsa.gov/ia/academia/caeiae.cfm?MenuID=10.1.1.2#reviewAndSP

[5] Transport Layer Security Working Group. The SSL Protocol Version 3.0. Retrieved February 15, 2008 from http://wp.netscape.com/eng/ssl3/draft302.txt.

[6] TLS CITE Network Working Group. The TLS Protocol Version 1.0. Retrieved February 15, 2008 from http://www.ietf.org/rfc/rfc2246.txt

[7] TechLink: Moving Technology from Minds to Markets. Retrieved February 15, 2008 from http://www.techlinkcenter.org/techlink/images/About_TechLink_Backgrounder_2_06_07.pdf

[8] United States Department of Commerce Office of Technology Policy, November 2003.

[9] Feder, P. and J. Barnaby. "Computer Security Team to Report Hacking Into Defibrillator-Pacemaker." New York Times (03/12/08)

[10] Center for Computer Security Research. Retrieved February 15, 2008 from http://www.security.cse.msstate.edu/ftc/index.php

[11] CERIAS The Center for Education and Research in Information Assurance and Security. Retrieved February 15, 2008 from http://www.cerias.purdue.edu/

[12] NIATEC National Information Assurance Training and Education Center. Retrieved February 15, 2008 from http://niatec.info/(S(24uhjizfo31xqtn34khdck45))/index.aspx

[13] CyberSecurity and Emergency Preparedness Institute. University of Texas at Dallas. Retrieved February 10, 2008 from http://csrc.utdallas.edu/

[14] The Center for Education and Research in Information Assurance and Security – Purdue University. "K-12 Outreach Program: An Overview." Retrieved January 10, 2008 from http://www.cerias.purdue.edu/assets/pdf/k-12/k12overview.pdf

[15] The Center for Education and Research in Information Assurance and Security – Purdue University. "CERIAS K-12 Outreach Program." Retrieved January 10, 2008 from http://www.cerias.purdue.edu/assets/pdf/k-12/k12_program_packet.pdf.

[16] National Science Foundation. NSF Graduate Teching Fellows in K-12 Education (GK-12). Retrieved January 15, 2008 from http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5472

[17] National Science Foundation. Broadening Participation in Computing (BPC). Retrieved January 15, 2008 from http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13510