Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

One Professor's Odyssey into the Realm of Information Assurance

Richard G. Epstein, Member, IEEE

Abstract: This paper discusses how the author integrated issues in Information Assurance into parts of the undergraduate curriculum at his university. The emphasis is on his course on computer ethics and the social implications of computing. .

Index terms – Integrating information assurance topics into the undergraduate curriculum; visions for the future.

I. Introduction

This paper will discuss how the author's thinking has evolved over the past ten years or so with respect to the topic of Information Assurance. The paper's title refers to this evolution as an odyssey, and an odyssey it certainly has been. The purpose of recounting this odyssey is to suggest ways in which Computer Science and Information Technology instructors might integrate topics in Information Assurance into existing courses in their undergraduate curricula. The idea is to show how one's perception of a particular subject area in Computer Science or Information Technology (e.g., computer ethics and the social implications of computer technology) can be re-examined and expanded to include more significant and in-depth coverage of topics in Information Assurance.

The author has created a new Introduction to Computer Security course which integrates important topics in computer ethics and the social implications of computing with important topics in Information Assurance. Our department has a topics course (CSC495) which allows instructors to introduce new subject matter into the curriculum. The author had been teaching a topics course on computer ethics and the social implications of computing for about ten years. This topics course evolved into the new Introduction to Computer Security course (CSC301) which will be offered with that new course number and title for the first time this spring (2006).

The original topics course in computer ethics and the social implications of computer technology evolved into a course stressing Computer Security during the past five years. Year by year, step by step, the author wrestled with the best ways to modify the ethics and social implications of technology course so that Computer Security became the major focus. This paper will discuss how the course evolved and will give a detailed description of where the course now stands. However, one realization that the author came to as he developed this new course is that it must continue to evolve year by year as the field of Computer Security evolves. The author feels that necessarily the course must contain a component that addresses the future of Computer Security, including "hot topics" that are just emerging and topics that are likely to be hot topics in the future. Perhaps one reason that our security problems are so severe at the present time is that Computer Scientists and Information Technologists during the past few decades did not pay enough attention to the security implications of new technologies that they were creating and deploying.

II. THE ODYSSEY BEGINS

The author's introduction to Computer Security and Computer Ethics occurred when he was an ACM member of the IEEE CS/ACM Computing Curricula '91 Task Force. The author was truly honored to work with so many inspiring individuals on that Task Force, but the most important impact of that Task Force on his own thinking about Computer Science and the curriculum was the fact that several members of the Task Force, most notably Eugene Spafford from the ACM and several IEEE members of the Task Force (including Bruce Barnes and Gerald Engel) emphasized the importance of introducing ethics into the undergraduate curriculum.

We began our work shortly after Robert Morris launched his Internet Worm (in 1987). Eugene Spafford had just published his influential paper on that worm in the Communications of the ACM [1]. The aftershock of the Internet Worm definitely had an impact upon the way that the Task Force thought about what undergraduate students should know about professional responsibilities, ethics and security. This author was truly inspired by what he learned as a member of the Task Force, especially with respect to the role professional responsibilities, computer

RICHARD G. EPSTEIN, DEPARTMENT OF COMPUTER SCIENCE, WEST CHESTER UNIVERSITY OF PENNSYLVANIA, WEST CHESTER, PA 19383

ISBN 1-933510-98-6/$15.00

ethics and security should play in Computer Science education. This led him to introduce professional and ethical issues into his software engineering courses. It also led to him to write the Case of the Killer Robot [2], which tried to show how important ethical and professional considerations were during the software development process.

It would be difficult to exaggerate how much enjoyment the author got out of the Killer Robot project. It allowed him to integrate his work in Computer Science with his love for writing and his interest in human character development (i.e., how we humans evolve as moral beings). However, when the book version of the Killer Robot was written in 1995-6, (the original scenario was written around 1990) security issues were not a major focus. Only one chapter (out of twenty-nine) of the Killer Robot book was devoted to security issues (hacking, in particular) and the ethical issues underlying those security issues (e.g., privacy and confidentiality). Major influences on the author's thinking about security at that point in time were Eugene Spafford and Clifford Stoll.

As mentioned in the introduction, the author taught an occasional "topics" course relating to the social implications of computing during the late 1990s. Computer ethics was a major component of these topics courses, which were taught about once each year. In retrospect, the author tended not to discuss security heavily in his software engineering courses, but left the coverage of security issues discussions to his topics courses in the social implications of computing. The social implications of computing courses he taught in the late 1990s covered topics in Computer Security such as hacking, computer crime, and malicious code. There was some discussion of preventive measures (e.g., anti-virus software), but not much. In addition, these courses covered important topics in computer ethics, with a focus on including privacy, intellectual property, and honesty (e.g., the impact of persuasive technologies). The ethics topics often touched upon issues in security, but security was not the major focus in these courses.

These topics courses on the social implications of computing always had a major component devoted to the future of computer technology. During the period 1997-8 the author wrote over eighty short stories about the future of computer technology. The ACM SIGCAS publication, Computers and Society, used to feature one of these stories on the back page of every issue back in the old days when it was still a printed publication. In retrospect, quite a few of these stories (although not necessarily those that were published in Computers and Society) dealt with security issues, although the author did not see security as his main focus. The main focus was on what could go wrong with the technologies we were developing. How could those technologies be misused? Identity theft and violations of privacy and hacking were aspects of what could go wrong with the future of computer technology and that is why quite a few of the stories (again, in retrospect) do touch upon issues in Computer Security. The author's main focus was on the ways in which computer technologies might evolve and impact human culture in the future.

III. THE BIG TRANSITION

The big transition (for the author) occurred during the spring of 2001 when the author decided to cooperate with the University administration in its push to get our university to develop courses in Computer Security (or, Information Assurance, as we came to know it). Since I was already teaching some materials in Computer Security in my social implications of computing topics courses, I thought it would be interesting to explore the field of Computer Security in more depth.

However, almost from day one of the author's new investigation into this field of Computer Security, he suffered from one major inferiority complex, which can be summarized with the following sentence: "I am not a hacker!!!" The author is not a hacker and is not really interested in becoming a hacker. The author realized that a hacker mentality is certainly a plus for teaching certain kinds of courses in Computer Security. The author faced the challenge of creating an interesting course in Computer Security without possessing the hacker mentality. The author's interests remained more in the domains of the social implications of the technology as well as the important ethical issues that Computer Science and Information Technology students are expected to understand. Many of these ethical issues lie at the very heart of our discussion of what constitutes a violation of security and what kinds of behavior should be considered criminal in nature.

So, the challenge was to create a new course which was consistent with the author's primary scholarly interests, a course that would contribute to our University developing a program in Information Assurance, and a course that would be fun and challenging for students. Many faculty members within Computer Science and Information Technology face this challenge: How can we integrate security topics into our curriculum by taking advantage of existing faculty interests, expertise and enthusiasm? How can we make sure that Computer Science and Information Technology students have access to courses that will introduce them to the situation that the world currently faces with regard to the security of our information infrastructure?

Starting with the spring of 2002, the author developed his new Introduction to Computer Security course in an

iterative fashion (although it was still a topics course back then). Every spring he tried to reorganize the course and introduce new materials as he gained a clearer and clearer idea of what he wanted to achieve in the course. Obviously, the author drew upon many books and scholarly resources in order to develop the course. As the course evolved, the author de-emphasized formal ethics to some degree, and paid more and more attention to the evolving security problems in cyberspace and the technologies that Computer Scientists and Information Technologists are developing to address the growing security concerns in cyberspace.

The author realized, over the course of the past several years, that this course, by its very nature, must be flexible and contain components that will address "hot topics" in Computer Security and the security implications of new and developing technologies.

So, the basic emphasis of the new course that the author has developed is on looking at the basic security issues in cyberspace and then studying how Computer Scientists and Information Technologists attempt to develop new technologies to address these developing issues and to improve the security of our information infrastructure. In the following sections, we will look at the topics covered in the course in more detail. We will emphasize how the ethics and security topics are interwoven and also how the author tries to encourage student creativity and initiative and enthusiasm in the course.

IV. INTERWEAVING ETHICS AND SECURITY

The new Introduction to Computer Security course (CSC301) tries to accomplish two fundamental goals: to introduce students to important topics in computer ethics and to introduce students to important security issues for the information infrastructure. In some sense, the course interweaves the ethics and security topics. This means that the course will introduce a host of security concerns by first addressing the ethical concerns underlying those security concerns. The bulk of the course focuses on security, but many security topics are introduced by first discussing the underlying ethical issues that are relevant to discussing why a certain security issue is an issue at all.

For example, the course includes a lecture that gives an overview of privacy as an ethical issue. The students are given several fundamental ethical frameworks (e.g., as introduced in Tavani [3]) for discussing privacy. This discussion of privacy is immediately followed by a discussion of some technologies that Computer Scientists and Information Technologists have developed to protect privacy issues in cyberspace.

Our discussion of privacy-protection technologies centers around several articles from IEEE Computer Society and ACM publications. These include an article that gives an overview of privacy issues in cyberspace (Rezgui et al. [4]), another article that discusses the Platform for Privacy Preferences (Cranor [5]), and another article that discusses a somewhat out-dated technology for anonymous Web browsing (Reiter et al. [6]). The article by Michael Reiter and his co-authors is about anonymous Web browsing using Crowds. Although Crowds has not been successful in terms of its public acceptance, the article is clearly written and provides a segue into the more successful Open Source product, TOR, which accomplishes many of the same ends. Our discussion of Crowds and TOR allows us to consider the possibility of technologies that will allow anonymous Web browsing and to consider both the security shortfalls and strengths of such technologies. For example, many credit card thieves have used anonymous Web browsing to try to shop on-line with stolen credit cards. On the other hand, anonymous Web browsing can be a useful tool for dissidents in oppressive regimes who otherwise would not be able to post their dissenting opinions on the Web.

Another example of how ethics and security issues are interwoven in the course comes from our study of intellectual property. We start with a consideration of the ethical and legal frameworks for intellectual property protection. We then consider in some detail the controversies within the Computer Security community regarding the DMCA (Grosso [7]) and patent law. We then look at technologies that have been developed to protect intellectual property, as summarized in the article by Naumovich et al. [8]. These technologies include digital watermarks and code obfuscation.

V. TOPICS COVERED

The previous section of this paper gave two brief examples of how ethical issues are interwoven with the security issues. However, the interweaving of these issues runs much deeper than these examples might suggest. This is because just about every security issue has an underlying ethical dimension. The purpose of this section is to give a more complete introduction to the topics covered in the current version of the course.

The course starts with a basic introduction to the topic of Computer Security. The author uses current information (like results of the CSI/FBI Security Survey) which show how serious the situation is. Students are given lists of information assets (including a list of personal information assets and another list of information assets for a pretend company) and are asked to consider the importance of those assets and the types of attackers that

might be interested in either defeating the confidentiality, integrity, or accessibility of those assets.

The emphasis is on communicating as clearly as possible just how fundamental the topic of Computer Security (or, Information Assurance) is to the fields of Computer Science and Information Technology. This leads naturally into a discussion of who should be liable for insecure systems (as discussed by Mead [9]). The purpose of this discussion is to make these future Computer Scientists and Information Technologists aware that there can be severe legal and financial implications when insecure systems are produced.

The course then moves on to the discussion of privacy, as discussed in the previous section. The students are introduced to privacy as an ethical concern and then the class examines some technologies that have been created to protect privacy in cyberspace. This portion of the course also includes a discussion of acceptable Internet use policies (Siau [10]) since the author believes it is important to communicate the students the fact that employers have the right to monitor Internet use at work. We discuss some existing technologies for monitoring employee Internet use.

There are other important privacy issues in cyberspace that the course will cover in some detail. However, before we get into these additional privacy issues (e.g., spyware and SPAM), the course gives the students a basic introduction to what the author calls "Nasty Stuff". The nasty stuff lectures give a historical introduction to computer crime and malicious code. The emphasis is on the historical evolution of attack trends and where we seem to be heading. We look at incidents such as the Internet Worm, the Melissa Virus, the Code Red Worm, and the Blaster Worm. We look at the attack trends and the growing threat of worm epidemics in high speed networks (Chen et al. [11]).

This introduction to "nasty stuff" allows us to return to the topic of privacy in cyberspace. Once again we interweave the ethical issue (privacy) with the security concerns by considering the specific privacy threats posed by various technologies, including SPAM and spyware. For example, we look both at the nature of SPAM and proposed technological solutions (e.g., as described in the paper by Pfleeger et al. [12]). We examine the severe security concerns relating to spyware and also to newer threats to privacy such as phishing (e.g., as described in Geer [13]).

The course then moves on to the intellectual property component, as described at the end of the previous section.

The next portion of the course has evolved dramatically within the past year. This section of the course is entitled "The Weakest Link". This title was inspired by an article by Ivan Arce which describes the desktop as the new weakest link [14]. Arce's article shows how the weakest link has evolved from the days of the mainframe. The author tells his class (in going over the article by Ivan Arce): "The first the weakest link was the mainframe. Now, let's examine how the weakest link has evolved since then."

The author's vision of the weakest link is a bit broader than Ivan Arce's, in that it includes the human user as a significant component of the weakest link. (It's not that Arce ignores this at all. It's just that the author places more emphasis on looking at the human user as a weak link in Computer Security.) To bolster this perception (of the human user as the weakest link) we study an article relating to cognitive hacking (Cybenko et al. [15]).

Our discussion of cognitive hacking is followed by a discussion about Web Spam (as described by Gyongyi et al. [16]). In this fascinating article by Gyongyi and his co-authors, the reader learns about the interesting technologies that are being used to influence the result of search engines, such as Google. Zoltan Gyongyi and his co-authors characterize Web Spam as the emerging technology that is being used to perform this kind of manipulation of search engine results. In some sense, Web Spam is a kind of cognitive hacking.

Finally, in the Weakest Link component of the course, we consider what many are now calling the greatest threat of all – devices like flash drives and iPods. These devices pose a threat on many levels to an organization's security, as wonderfully espoused by Michael Thelander in his recent paper, "The Great Wall Syndrome" [17]. The security industry seems to be waking up to this relatively new kind of threat in a major way. When the author discussed this topic recently on two separate occasions with two industry experts in Computer Security, they both had the same kind of response, which was somewhat tongue in cheek (or was it?). They said it is time to return to the days of the mainframe. That seems like a good way to end our discussion of how the weakest link has evolved over the past sixty years. It started as the mainframe and now the security experts would like us to go back to the days of the mainframe!

The next component of the course relates to information warfare. We discuss Denning's theory of information warfare [18] and also materials from various Web resources and books regarding the threat of cyberterrorism. We then look at proposals for how organizations might defend themselves against information warfare types of attacks (as described in Jajodia et al. [19]).

The course then moves on to a discussion of protection mechanisms. This component of the course begins with the author's "gentle introduction to cryptography". We then consider the vulnerability life-cycle as described by Arbaugh et al. [20]. This influential paper alerted us all to the reality that most attacks occur after a vulnerability has been publicized by the publishing of a patch by the software vendor. We then move on to discuss technologies for protecting computer systems, including intrusion detection systems, intrusion prevention systems, and firewalls. The author has experts from industry give guest lectures on their experience with intrusion detection systems, such as SNORT.

The final topic covered in this component of the course is computer immunology. The author often introduces this as his favorite topic. Although the article we use was published back in 1997 (Forrest et al. [21]), computer immunology is a fascinating topic that continues to generate a lot of interest in the security community (as a recent multi-million dollar grant to the University of Virginia would seem to indicate). Can we use the ideas of the biological immune system to create more secure computer systems? The author comes to class all enthused about this idea. In some sense he is trying to be provocative, and it is always great to see how students can come up with good counter-arguments to the effect that there are essential differences between computer systems and biological systems. Perhaps the best counter-argument to the computer immunology idea occurred last year (Spring 2005) when the author came down with a really nasty cold just two hours after he finished his computer immunology presentation!

The remaining components of the course will be devoted to hot topics and / or the future of security in the world of ubiquitous computing. For example, during 2004 (an election year) the hot topic that the author chose was security in electronic voting. This year (Spring 2006) the author has decided to focus on biometrics and authentication in this portion of the course. We will be discussing face recognition technology (Bowyer [22]) and other forms of biometric recognition, emphasizing the role that biometrics can play in authentication systems. An interesting topic to consider for future semesters would be the ethical and security concerns surrounding the use of RFIDs.

This brings us to the end of the instructor's materials for the Introduction to Computer Security course. The last two weeks of the course are devoted to student presentations. We will discuss these and the more general question of promoting student creativity and enthusiasm in the next section of this paper.

VI. EMPHASIS ON STUDENT CREATIVITY

The author was greatly inspired by the writings of Richard Florida [23] which emphasize the role that creativity plays in promoting American prosperity. The author tries, as much as possible, to encourage student creativity in his courses, including the Introduction to Computer Security course. In this section we will discuss some of the devices the author uses to promote creativity and enthusiasm among his students.

First, let us mention the responsibility of students to read and submit discussion points relating to the assigned readings from publications of the IEEE Computer Society and the ACM. Of special significance in recent years has been the Computer Society's new publication, IEEE Security and Privacy. IEEE IT Professional, IEEE Software, IEEE Computer and Communications of the ACM are also important resources for this course. The midterm exam and the final exam are essay-oriented take-home exams that require, in part, in-depth reviews of specific articles that we have discussed.

In addition to the exam materials, students also have various options for replacing at least some of the exam materials with special individual projects that they might choose to pursue. These individual project options include the possibility of reporting on investigations into the use of defensive tools for computer security (like P3P, SNORT, PGP, TOR, etc.). Individual research papers are also encouraged. Students are also given the option of creating creative projects. One such creative project is to write a cyberwill which expresses the student's perception of what is ethical and what is not ethical in the use of cyberspace.

The instructor has also created various class exercises (what he calls "classercises") in order to encourage classroom participation and creativity. One classercise is called "The Case of Brian Birdwhistle". In this classercise, the students are asked to pretend that they are members of a jury that must decide the fate of Brian Birdwhistle, who is accused of causing the death of a diabetes patient. It seems that the Internet worm that Brian Birdwhistle launched as a DDoS attack on his former employer had unexpected side-effects and these included damaging a database that was used by a device that enabled a diabetes patient to control her insulin injections remotely. The patient died because of an insulin overdose that was due to the damage done to the medical database by Birdwhistle's worm. At issue is whether Brian Birdwhistle should be convicted of manslaughter in this case. In previous semesters, Brian hasn't fared too well during these jury proceedings. (The database administrators haven't fared too well either.)

Another classercise involves conducting a meeting at the Department of Homeland Security. Using Dorothy Denning's theory of information warfare (cited earlier), the students are asked to discuss important information assets that the United States needs to defend in case of an attack by cyberterrorists. Who are the likely attackers? What would be their objectives? What kind of defensive postures must be in place to protect these important resources?

An important component in the grading for this course is the team presentation project. Each student works on a team consisting of three or four students. Each team gives an in-class presentation during the last two weeks of the semester. The author believes that many of these team presentations in recent semesters (when the security course was taught as a topics course) have been remarkable and some have even been inspiring.

The formal assignment handed out to the students for this team presentation project encourages creativity. Some teams stick to the usual PowerPoint presentation format. However, this is not intended as a criticism. Most of these formal presentations have been stimulating and informative, perhaps even provocative. However, some teams use their creativity to create in-class theatrical improvisations and even DVDs with dramatic presentations and these generally have been of a truly high quality.

The DVDs are generally dramatic presentations that relate to something going on in the realm of Computer Security. However, one team last spring created a DVD that involved interviewing a person whose job is to keep the campus computing systems secure.

The author would like to specifically mention (and praise) a DVD one team created last spring (2005) that was a dramatic presentation involving a cyberterrorist attack on Wall Street. The intent of the cyberterrorists was to do significant damage to our nation's economic infrastructure. Four students played various roles in this DVD, which was filmed at various locations on campus. The students obviously did some set-up work to make things look somewhat authentic (although, of course, we are not talking Hollywood quite yet). Two of the students played the attackers and two of the students played federal agents who tracked them down using a honeypot. The presentation was truly wonderful and contained many interesting technical details, including the architecture of the system being attacked and information about the honeypot the federal agents used to catch the cyberterrorists.

The creativity aspect seems especially effective in this context of a fairly introductory level course that is intended for students in our Computer Science major and in our Information Technology minor (which hopefully will be formally approved by the Commonwealth of Pennsylvania by the time of the CISSE conference). One goal of the course is to "turn on" the students to this realm of Information Assurance and to get them to see how vast this field is, how provocative it is, and how interesting it will be to work in a field that is this stimulating.

VII. EMPHASIS ON THE FUTURE

This is the first semester that the author has consciously decided to include concerns about the future as an essential and regular component in this course. Although he wanted to include the consideration of RFID devices in the course, it just didn't fit in. (However, he will encourage at least one student team to consider this topic for their in-class presentation.) This semester (Spring 2006) the author used biometrics as the topic which focuses on future technologies. The emphasis will be on the promise that biometrics holds for improving the security of systems as well as some of the privacy concerns that surround some biometric technologies.

There would seem to be many, many topics relating to the future of computer technology that have a security dimension. In addition to RFIDs, there is the issue of ubiquitous computing and the use of automated appliances and vehicles (e.g., automated automobiles). Also of concern are the security issues surrounding nanotechnology and quantum computing (and its potential impact upon cryptography).

Artificial intelligence also raises security issues for the future. How can we trust the intelligent agents we create on the Web? What are some of the security issues surrounding the newly approved standards for the semantic Web?

Artificial Intelligence and the use of intelligent agents raise huge issues of trust. Can we trust an intelligent agent? How much power can we give to such an agent? What might an attacker do to modify the behavior of such an agent? There are profound security issues surrounding the deployment of AI technology that we need to carefully consider.

VIII. CONCLUSIONS

The purpose of this paper was to show how the author's interests and teaching materials have evolved over the years as he has incorporated Information Assurance into his undergraduate courses on ethics and the social implications of computing. The author used several strategies to accomplish this end. These include the interweaving of topics in computer ethics with topics in Information Assurance. This interweaving included the

introduction of papers regarding research projects conducted by Computer Scientists and Information Technologists. These research projects can help students see the kinds of solutions that Computer Scientists and Information Technologies come up with to address the security issues.

Another important dimension of this course was its emphasis on the social implications of security vulnerabilities and the future evolution of the technology. Finally, the author emphasized student creativity, in order to get students "turned on" to the subject matter and also to exercise their neurons so that they might learn how to play a more creative role in their evolving careers.

The author has also integrated security into his software engineering course, a course which introduces students to a variety of software processes (like PSP, CMM, eXtreme Programming, Open Source) and asks them to create their own software process for a pretend company. The students work on teams to do this. An important concern in their team projects is to consider how security issues will be incorporated into their process.

The author's own experience suggests that many faculty members can introduce security concerns into existing courses and it would seem almost irresponsible for them not to do so in the broadest possible way. Furthermore, security issues can be introduced into courses in ways that are truly stimulating for the students. Creating courses of this nature may help attract new students into the field.

IX. REFERENCES

[1] Eugene H. Spafford, "Crisis and Aftermath," Communications of the ACM, June 1989, pp. 678-687.
[2] Richard G. Epstein, The Case of the Killer Robot, John Wiley and Sons, 1997, 242 pp.
[3] Herman T. Tavani, Ethics and Technology, John Wiley and Sons, 2003, 400 pp.
[4] Abdelmounaam Rezgui, Athman Bouguetta, and Mohamed Y. Eltiweissy, "Privacy on the Web: Facts, Challenges, and Solutions," IEEE Security and Privacy, November/December 2003, pp. 40-48.
[5] Lorrie Faith Cranor, "P3P: Making Privacy Policies More Useful," IEEE Security and Privacy, November / December 2003, pp. 50-55.
[6] Michael K. Reiter and Aviel D. Rubin, "Anonymous Web Transactions with Crowds," Communications of the ACM, February 1999, pp. 32-38.
[7] Andrew Grosso, "Why the Digital Millennium Copyright Act is a Failure of Reason," Communications of the ACM, February 2002, pp. 19-23.
[8] Gleb Naumovich and Nasir Memon, "Preventing Piracy, Reverse Engineering, and Tampering," IEEE Computer, July 2003, pp. 64-71.
[9] Nancy R. Mead, "Who is Liable for Insecure Systems," IEEE Computer, July 2004, pp. 27-34.
[10] Keng Siau, Fiona Fui-Hoon Nah, and Limei Teng, "Acceptable Internet Use Policy," Communications of the ACM, January 2002, pp. 75-79.
[11] Thomas M. Chen and Robert Jean-Marc, "Worm Epidemics in High-Speed Networks," IEEE Computer, June 2004, pp. 48-53.
[12] Shari Lawrence Pfleeger and Gabrielle Bloom, "Canning Spam: Proposed Solutions to Unwanted Email," IEEE Security and Privacy, March/April 2005, pp. 40-47.
[13] David Geer, "Security Technologies Go Phishing," IEEE Computer, June 2005, pp. 18-21.
[14] Ivan Arce, "The Weakest Link Revisited," IEEE Security and Privacy, September/October 2004, pp. 72-76.
[15] George Cybenko, Annarita Giani, and Paul Thompson, "Cognitive Hacking: A Battle for the Mind," IEEE Computer, August 2002, pp. 50-56.
[16] Zoltan Gyongyi and Hector Garcia-Molina, "Spam: It's Not Just for Inboxes Anymore," IEEE Computer, October 2005, pp. 28-34.
[17] Michael Thelander, "The Great Wall Syndrome," IEEE IT Professional, September/October 2005, pp. 25-30.
[18] Dorothy E. Denning, Information Warfare and Security, Addison-Wesley, Reading, MA, 1999, 522 pp.
[19] Sushil Jajodia, Paul Ammann and Catherine D. McCollum, "Surviving Information Warfare Attacks," IEEE Computer, April 1999, pp. 57-63.
[20] William A. Arbaugh, William L. Fithen, and John McHugh, "Windows of Vulnerability: A Case Study Analysis," IEEE Computer, December 2000, pp. 52-59.
[21] Stephanie Forrest, Steven Hofmeyr, and Anil Somayaji, "Computer Immunology," Communications of the ACM, October 1997, pp. 88-96.
[22] Kevin W. Bowyer, "Face Recognition Technology: Security versus Privacy," IEEE Technology and Society Magazine, Spring 2004, pp. 9-20.
[23] Richard Florida, The Rise of the Creative Class, Basic Books, New York, 2002, 434 pp.