Security, Safety and Privacy – Pervasive Themes for Engineering Education[•]

S. Meldal[*†], K. Gates[†], R. Smith[*], X. Su[*†]
[†]NSF STC Team for Research in Ubiquitous Secure Technology, UC Berkeley, USA
[*]Computer Engineering Department, SJSU, San Jose, USA

Index Terms: security, safety, general education, core knowledge.

Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. The last decade has seen a rapid increase in computer security attacks at all levels, as more individuals connect to common networks and as motivations and means to conduct sophisticated attacks increase. A parallel and accelerating trend has been the rapidly growing integration role of computing and communication in critical infrastructure systems, with complex interdependencies rooted in information technologies [1][12]. The ubiquitous nature of IT technology deployment also has deep consequences for personal privacy and ultimately on individual freedom [6]. These overlapping and interacting trends force us to recognize that trustworthiness of our computer systems is not an IT issue alone; it has a direct and immediate impact on the nation's critical infrastructure and on the core values of our society.

The interplay (and possible conflicts) of these factors compel us to conclude that an understanding of the policy and security issues of IT deployment is part and parcel of being an educated member of society. Furthermore, an understanding of these issues is a necessary requirement for *every* professional engineer, and in particular for engineers in the IT domains: *Trustworthiness is a key concept to be taught in general education, and in particular in* engineering *education.*

Engineering education currently lacks a holistic view of the interplay of security in systems design. Security appears in engineering curricula (if at all) as add-ons, and discussions of public policy issues are insignificant.

Creating a new generation of professionals who understand the technology and policy aspects of trustworthiness in our critical infrastructure systems is part of the US national agenda and a central objective for TRUST, the *NSF Science and Technology Center for Research in Ubiquitous Secure Technology* [1].

Based on work done at and with NSF STC TRUST we are adopting a multi-pronged approach to integrating trustworthiness into the general and the engineering education experiences.

- In the general education curriculum (which *all* students have to complete) we have created a course where security and privacy issues serve as a vehicle for the *social issues* education requirement.
- In the engineering core classes we are introducing security as a key design component.
- Internships in security organizations are offered to students across the US as part of engineering degrees.
- The role of national certification and accreditation standards (such as the NSA CAEIAE certification, ABET EAC and CAC accreditation) are evaluated for curricular adoption and adaption.
- National and regional workshops that establish security development communities are organized, and they assist universities in understanding and achieving such standards.

Our ultimate goal is to change the current situation and to engage the educational community to work towards a broader understanding of systems, security and policy options among future technologists and policy shapers.

In this paper we will present three aspects of this strategy: The introduction of security and privacy to the general student population through a *general education* course, secondly the more technical introduction to security in the context of a network security course, and thirdly, the confirmation of these academic modes through the placement of students into internships in security organizations in Silicon Valley.

[•] This work was supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies.

[1] E-mail: smeldal@nsftrust.org, kgates@eecs.berkeley.edu, xsu@nsftrust.org

I. How the World Changes

It has become a truism that "*the internet has changed the world.*" The easy access to a universe of information and the transformation of how corporations, organizations and government entities present themselves to the public and to each other has been profoundly affected by the collapse of (communication) distance and the diminishing cost of communicating and storing truly vast amounts of data.

The growth has been explosive – most directly illustrated by two snapshots of the Internet, in 1980 (Fig. 1) (ARPANet, the precursor of the Internet) and in 2005 (Fig. 2).

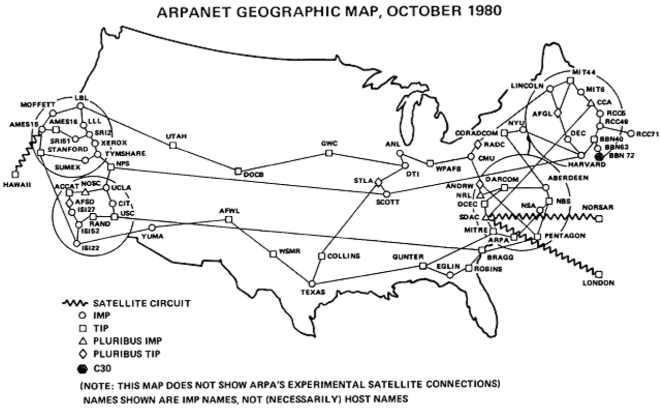

Fig. 1 The ARPANet in 1980

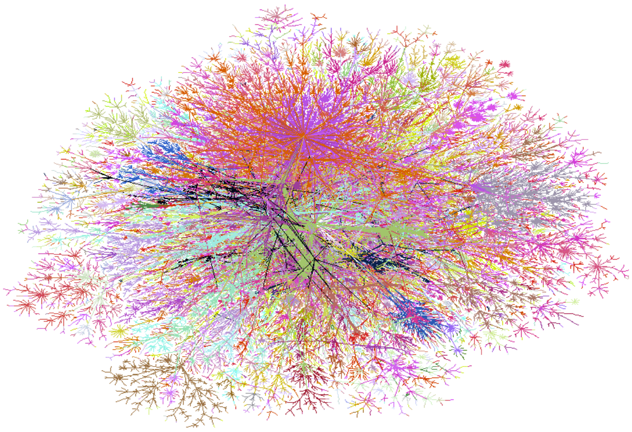

Fig. 2 The Internet in 2005 [7]

With the radically increased connectivity, and with the equally radical increase in computing power (and thus the size of computationally feasible systems), the challenges of software (systems) development have changed from the objective of achieving efficient *calculation* to that of building software from extant components where making tradeoffs involving *reliability*, *cost*, *time* and *safety* – s*tructural complexity management* becomes the critical issue. Such tradeoffs are quintessentially *engineering* decisions. Consequently, software professionals must have a *practical knowledge of engineering principles*.

The complexity of the networks of computer systems has its dual in the ubiquity of computer systems as part of our societal infrastructure. We have moved from a world where (some) mainframes were networked to one where our households, telecommunications, financial, medical and even physical infrastructures are critically dependent upon the trustworthiness of our computing platforms (be they cell phones, laptops or server farms).

In parallel with the increasing connectedness of computer systems as such we have also experienced an explosion in the use of *embedded* computer systems in stand-alone, self-contained products. Obvious examples of life critical systems with embedded systems as key components are medical devices and avionics, and now in automobiles and other, more mundane systems.

Sastry has observed that

> *"…we are poised for a revolutionary transformation in embedded systems as embedded computers become networked. The transformation is analogous to the enormous*

> *increment in the utility of personal computers with the advent of The Web. Just as personal computers changed from word processors to global communications devices and information portals, embedded computers will change from self-contained control systems to cyber-physical systems, sensing, monitoring, controlling, and optimizing our intrinsically distributed human environment, and interacting with humans in ways that we can only begin to imagine today."* [9]

As educators, and as members of our societies, we are faced with the rather daunting prospects of

- The trustworthiness of our computing (and network platforms) is critically important to our physical well-being.
- The interconnectedness of our information repositories makes (lack of secure) information protection a paramount challenge to our civil society.
- The ubiquitous nature of data-gathering devices coupled with the interconnectedness of data repositories makes privacy a core challenge to civil liberties.
- The increasing connectivity of embedded devices in (life) critical systems makes a lack of trustworthiness a matter of personal health and safety.
- Decisions of policy and technology require a sophisticated understanding of *both* engineering *and* how a civil society arrives at framework decisions.

Three components of the NSF STC TRUST education effort are to (1) generate curricula suitable for a general education within a liberal, comprehensive university, (2) generate curricula that specifically educate future technology innovators and designers, and (3) bring students in the computing disciplines into a structured engagement with relevant industry partners during their studies.

II. Educating the general population The Digital Impact on Society

In the United States most undergraduate degree programs have a significant *general education* component that aim to create broadly competent members of society with an understanding of core academic and societal values beyond the requirements of any one discipline. At San José State University the general education coals are defined as:

> "*A university brings together many separate areas of learning, yet it is more than just a collection of specialized disciplines. The SJSU General Education Program incorporates the development of skills, the acquisition of knowledge, and the integration of knowledge through the study of facts, issues, and ideas. Regardless of major, all who earn undergraduate degrees should share common educational experiences, as they become university scholars. In combination with major, minor, and elective courses, the General Education curriculum should help students attain those attributes found in an educated person.*" [9]

Specifically, all graduates are expected to be able to demonstrate:

- a broad understanding of the sciences, social sciences, humanities, and the arts;
- an ability to communicate ideas effectively both in speaking and in writing;
- the capacity for critical and creative thinking;
- an understanding of ethical choices inherent in human development;
- an ability to assess information (information literacy);
- an ability to address complex issues and problems using disciplined analytic skills and creative techniques;
- multi-cultural and global perspectives gained through intellectual and social exchange with people of diverse backgrounds and experiences;
- the characteristics of "intentional learners" who can adapt to new environments, integrate knowledge from different sources, and continue learning throughout their lifetimes; and
- the capacity to participate as a socially responsible member of civic, professional, cultural, and other communities.

The interplay of security, privacy and digital technology serves as a fertile field for exploring general education topics.

Computer Engineering 25 at San Jose State University is designed to partially satisfy the general education requirements for undergraduate students – specifically the area of social sciences – human behavior. The goal of this course is to make the general student population aware of the impact IT Technology has on fundamental social issues such as security, identify, safety and privacy.

IT Technology and especially the Internet allow a single individual without any special resources to have worldwide impact within a matter of hours. At no point in history has the swiftness and magnitude of an individual's potential impact been greater. In general society reacts to issues once the impact has been felt. There was no general awareness to computer viruses until after virus attacks caused widespread network problems. Today there is a large market for anti-virus software.

Another change brought about by IT Technology and the Internet is the global nature of issues. The laws regulating the use of IT Technology in areas of security, identify, safety and privacy can differ widely from one country to another. Currently there is no generally accepted mechanism to create uniform global regulations.

An objective of Computer Engineering 25 is to create a population that is more aware and proactive in demanding solutions to these issues. Specifically the class will address the issue of how one nation can regulate topics such as gambling and pornography when the services are provided globally. There is no single global view or definition of these subjects. The question becomes how can local restrictions be placed on products and services provided globally.

National, state and local boundaries have historically been the basis for imposing local regulations. With the advent of the Internet those boundaries do not exist.

There is no global view of what data is private and needs to be secure. For example in the United States medical records are considered private. If an unauthorized person accesses another's medical records there are consequences. When medical records were kept on paper keeping the records secure is relatively simple. Put those same records in an on-line data base, host that data base in a location that is off-shore, now does the information remain private? If the same notion of privacy does not exist, unauthorized access to those medical records may not be protected. Often users of the Internet assume that security and privacy protections are uniform throughout the Internet.

Until the advent of the Internet the news and media in one region was largely independent from other regions. Publishers often only had direct access to a limited region. Therefore material was generally tailored to one specific region and was slow to reach other regions. With the advent of global publishing material that may be inoffensive in one region but highly offensive in another region could reach that region almost instantly.

A related issue is identity. When publishing required a newspaper, radio or television station, identifying a publisher was not difficult and legal protection could be given to the identity of sources of information. This is the question that Internet Publishing presents: Is the publisher of a website, blog or myspace page the same as the publisher of a newspaper? If they are, then the publisher of a website should receive the same protection as the publisher of a newspaper. If they are different what determines the difference?

Generally laws in the United States distinguish between public and private citizens for the purposes of libel and slander. Prior to the advent of the Internet this determination could be made based on their position in society and their use of the media. For example elected officials and movie stars are public citizens. In addition individuals who are in the public eye are also considered public citizens. Does publishing on the Internet create a public person? Has a widely read Internet blogger become a public person? None of these questions has a simple answer nor was thought given to these issues by the first blogger or the creators of social networking sites.

Much of what we do in our daily lives is public information. Without the use of IT Technology this information is just independent bits of data. Given a database of these independent bits of information and a search engine patterns can emerge. These patterns often reveal behaviors that most individuals would consider private. Yet the pattern is derived only from public information.

Computer Engineering 25 will use student exercises to develop an awareness of these issues in students. Students will be asked to search websites and then determine the physical location where the site is hosted. Then they will be asked to determine the regulations and customs that exist where those sites are hosted. Another example exercise will be to focus on the conversion of public data to private data. Students will be asked to keep a journal of all the stores that they visited during the week, including the time when they enter and when they leave. Individually this is all pubic data. Students will when be asked about their comfort level with sharing that information with the class.

Through exercises, lecture and student research Computer Engineering 25 will elevate the level of awareness of the impact that IT Technology has on our social issues.

At the end of the course the students will be able to

- Function as informed citizens in a high-tech world of cyberspace.
- Describe those areas of culture and human behavior that are directly impacted by technology.
- Describe the risks inherent in the digital world and demonstrate a basic knowledge of the role technology plays in both mitigating and exacerbating these risks.
- To put the fundamental shifts the digital technology made in society into historical perspective.
- Describe how government policy decisions affect technology, particularly with respect to security and privacy.
- Describe the impact of the digital world on identity, gender, societal, ethnic, and cultural values.

III. Moving from the General to the Particular

The ethical and technical challenges introduced in the general education course is revisited by the instructor in the technical courses where security and safety issues are presented and the students need to gain an operational understanding of the issues. For instance, in teaching network security – what role does the creation of attacks and malware play in the students' learning? How do we provide the students with the necessary experience as well as the academic appreciation of what forms attacks can take, as well as the proper precaution and risk management strategies available to guard against such attacks?

A. Good Side? Bad Side? or Both?

In training engineering students to understand security technologies, we believe that the students should understand all aspects in security engineering, from vulnerability, risks, and attacks to effective defense mechanisms. Current curricula development has put a much stronger focus on the "good side" of this spectrum, for example, security standards, tools, and technologies to defend against attackers can be found in almost every security course taught, but it is not a common practice to teach how to perform attacks. In 2005, G. Ledin started to teach how to write malware in his class [8] and spurred an international controversy regarding whether students should be presented with mechanisms and strategies for *creating* tools for computer and network attacks.

To give students a good grasp of both sides of security, we have structured our network security class in an unusual way: teaching how "bad guys" think in the first half of the course, and then teaching what "good guys" use to defend against the attacks in the second half. After learning various attacking phases and tactics, students become very motivated to learn how to build good security solutions. From a pedagogical aspect, this works very well too. The topics on attacks and vulnerabilities are easier to grasp, as they require technical background more than mathematical sophistication. This gives students a gentle but steady start on their learning curve. With the knowledge and motivation gained in the first half, students are better prepared to take on more involved topics, such as cryptography algorithms and security standards.

Based on Ed Skoudis' popular book [8], we model networking attacks into five phases: reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

In the reconnaissance phase, students learn to use various public domain tools, such as web search, whois database, and name server queries, to gather as much information as possible about the target domain. Depending on networking configurations, they may be able to get IP address assignments, name servers, web servers, and mail exchange servers associated with the domain.

In the scanning phase, attackers need to find out target domain's network topology, network setup, and configuration. The objectives are to discover whether there is a demilitarized zone (DMZ), how a firewall is configured, if present, and open ports and services running on each host, and above all, list of vulnerabilities on each host. Students learn to use ping and traceroute for finding network paths and topology, use nmap to scan opening ports and services, and nessus to discover vulnerabilities on the targets.

In the gaining access phase, "bad guys" can launch attacks using different tactics and venues; they may exploit vulnerabilities in operating systems or applications, such as buffer overflow or SQL injection, to gain unauthorized access into the target, or they may perform active eavesdropping on the network to gather authentication information. An excellent instructional example is to show how a web man-in-the-middle attack can be set up to read confidential information out of "secure" web transactions. Through such an example, students not only learn how Secure Socket Layer (SSL) works but also understand how important it is to do careful inspection about certificate warnings: ignoring them will make the web transaction continue but meanwhile give out sensitive information to attackers.

The next objective for the attackers is to set up compromised machines in a way that they can be accessed in the future, when needed, for example, in a distributed denial-of-service attack. They usually install Trojan horse programs, or backdoors, or spyware to allow further access. Students learn the common types of Trojan horse programs, such as kernel-level and user-mode rootkits.

After the attackers have set up a communication path between compromised hosts, they need to camouflage their packets as much as possible to avoid being filtered by firewalls or caught by intrusion detection systems. Tunneling and encapsulation are two common mechanisms used for this purpose. By experimenting with covert channel tools -- reverse HTTP, lokid, covert TCP, students have also reinforced their understanding of HTTP, ICMP, and TCP protocols and gained hands-on knowledge on protocol tunneling.

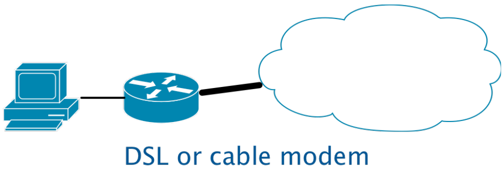

Fig. 3 A single computer connected to the Internet.

B. Experiences and Challenges in Experimental Setups

In learning network attacks, students need experimental environments to practice available tools and programs involved in each phase. We have leveraged 3 types of setups. The first setup simply consists of a single computer connected to the Internet, readily available from students' ISP access to the Internet. In such a setup, the student can practice either stand-alone tools or client-side utilities. For example, they can run the majority of reconnaissance tools, including dig, nmap, traceroute, ping, nessus and whois, given that the target for scanning and probing is available somewhere on the Internet. They can also experiment with stand-alone programs, such as password cracking software -- John the ripper -- to understand why weak passwords are dangerous.

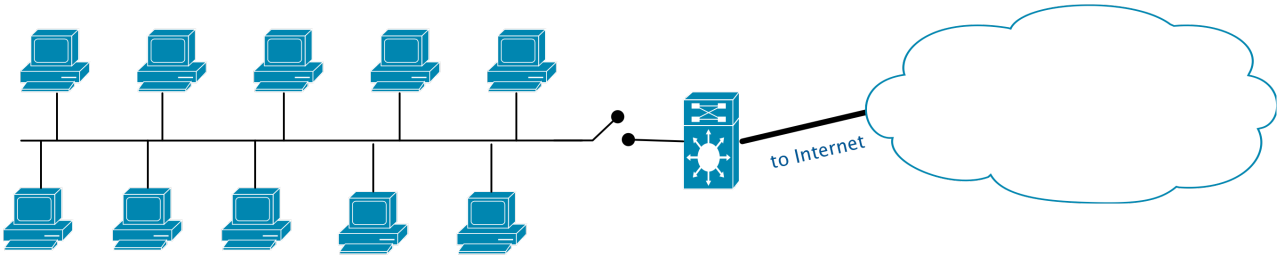

Fig. 4 A local network with or without connection to the Internet.

For experiments that involve both customized clients and servers, we run out of luck with students' home network. For this purpose, we have set up a local network with an on/off switch to the school network, as shown in Fig. 2. In most cases, we would like to turn off the Internet switch to contain the traffic of students' attacks and defenses within the local network, as such traffic may interfere with normal network operations or raise false alarms from school's security software. Using this local test bed, we can set up a man-in-the-middle HTTPS attack by running a victim machine, a HTTPS proxy, an attacking computer that redirects the HTTPS traffic from the victim to the HTTPS proxy, and a malicious HTTPS server. We can also set up covert channels using lokid, reverse HTTP, and covert_TCP programs for students to embed traffic in network headers or other protocols that are safe from packet filtering.

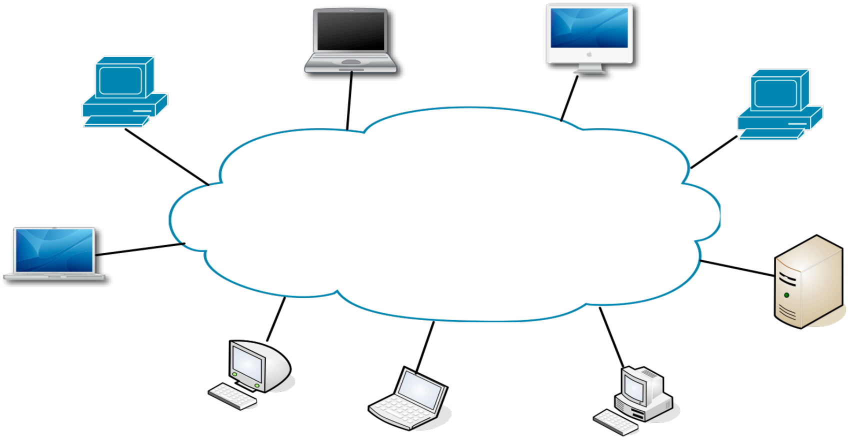

Fig. 5 A planetary test bed.

Some attacks can only be generated in a planetary test bed consisting of hosts from different parts of the Internet, such as in Fig. 3. For example, to teach worm propagation through peer-to-peer networks, we need to have full control of the peers in the network; to experiment with attacks towards an inter-domain routing protocol, Border Gateway Protocol (BGP), we need to set up routing domains and install BGP routing software on selective hosts across the Internet.

PlanetLab [8] is such a global research network consisting of 434 members from educational institutions, research organizations, and industrial partners. Since its inception in 2003, PlanetLab has been widely accepted as a de-facto standard in evaluating new network services and distributed systems. Currently, the PlanetLab test bed consists of 851 nodes contributed by its members across the world.

PlanetLab users access distributed nodes through association with a slice, which is essentially a set of virtual servers on each assigned node within the slice. Even though PlanetLab is not specially designed and configured for experiments involving network attacks and defenses, its adoption of virtualization technologies helps to isolate anomalous events, such as extensive usage of computer resource and network bandwidth, and to trace down to individual slices and its associated users.

However, as a test bed to support security experiments, PlanetLab leaves a lot to be desired. Being a shared open-service platform, its resource usage has been constantly monitored, making it hard to run resource-intensive experiments. As virtual servers are not shared on different PlanetLab nodes inside the same slice, setting up a security experiment involving a large number of nodes calls for expertise in system administration and, sometimes, tedious efforts in duplicating configuration process to all the nodes. Above all, its web-based user management process is not automated, requiring significant manual efforts in creating users, creating slices, associating users to slices, renewing and deleting slices, and cleaning up users.

IV. CONFIRMING THEORY THROUGH ENGINEERING PRACTICE

The benefits of exposing students to a learning environment where a professional experience is integrated with scholarship is well known [11][3]. A key to a successful internship is to

- Bring cooperative education into the realm of *experiential* learning.
- Integrate work term experience into classroom instructions.
- Encourage cooperative education coordinators to administer reflective work term assignments to help students transform their work experience into learning experience. [3]

Taking these as guidelines, the Summer Experience, Colloquium and Research in Information Technology (SECuR-IT) is a ten-week residential program with paid internship co-located at Stanford University and San Jose State University. SECuR-IT is a graduate student (MS and PhD) academic immersion with internship experience—with a learning cohort . Seminars and presentations in security related topics are held weekly at Stanford University. Graduate student internship opportunities are at Silicon Valley technology firms in the areas of security architecture, security awareness and security management, host and OS security, application security, network security, secure software engineering, risk management, policy and legal compliance.

The SECuR-IT 2008 applicant pool included a diverse group of some 100 graduate students representing 40 US universities and the Federal University of Santa Catarina, Brazil. Of particular note is the fact that forty-six percent of the applicants are women.

In addition to working with an industry mentor over the ten-week program, SECuR-IT scholars participate in the programmatic components:

- Seminars conducted by faculty and industry experts that expose students to a wide range of information technology and computer security research instruction. (Faculty participation from Stanford University, University of California, Berkeley, San Jose Sate University, and Vanderbilt University);
- Informal social gatherings that provide a relaxed setting for students and faculty to exchange ideas and share experiences;
- Learning community via residential on campus housing at San Jose State University;
- Ten week, paid 40-hour per week internship.

With participants from across the US, the 2007 SECuR -IT program was successful in establishing cross-institutional communities of students, creating a learning platform that made the professional work experience a confirmation of the scholarly material (and reflective assignments) shared with the students during the more academic instruction component of SECuR -IT.

Based on the 2007 success the program will be deployed more broadly in 2008, with an additional two sites being added to the one in Silicon Valley – one in Tennessee and one in New York.

V. Conclusion

With the ever-increasing embedding of interconnected computing platforms at the core of our lives and of society, the successful trust systems issues education of the population in general and of the engineering professionals in particular becomes a matter of critical societal concern.

Educational institutions benefit from taking an holistic approach to teaching security- and trust-related topics. The very ubiquity of the challenge can be made a vehicle for education, allowing for a pervasive injection of the concepts (and underlying technological and political challenges) of the interplay of security, trust, privacy and technology throughout the core as well as the discipline-specific curriculum components.

References

[1] Dressler, S., Keeling, A.E. "Student benefits of cooperative education." In R.K. Coll &. Eames (Eds.), *International handbook for cooperative education: An international perspective of the theory, research and practice of work-integrated learning,* 2004, pp. 217-236. Boston: World Association for Cooperative Education.

[2] Fiuczynski, M. E., "PlanetLab: Overview, history, and future directions." *SIGOPS Oper. Syst. Rev*. vol. 40, no. 1, pp. 6-10, Jan. 2006.

[3] Haddara, M., Skanes, H., "A reflection on cooperative education: from experience to experiential learning," *Asia-Pacific Journal of Cooperative Education*, 2007, vol. 8, no. 1, pp. 67-76

[4] Illman, D.. "Profiles in Team Science". Technical report, National Science Foundation, University of Washington, December, 2007.

[5] Landau, S., Stytz, M. R., Landwehr, C. E., and Schneider, F. B. "Overview of Cyber Security: A Crisis of Prioritization". *IEEE Security and Privacy* 3 (3):9-11, May. 2005.

[6] Ledin, G. Jr, "Not teaching viruses and worms is halmful," *Communications of the ACM,* vol. 48, no. 1, pp. 144-144, Jan. 2005.

[7] Lumeta Corporation, http://www.lumeta.com/research/

[8] Meingast, M., King, J., Mulligan, D. "Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond". *Journal of Communications*, Vol. 2, no. 7, pp. 36-48, Dec. 2007.

[9] San Jose State University catalog.

[10] Sastry, S.S., Annual Progress Report, Joint EU-US-Tekes Workshop, "Long Term Challenges in High Confidence Evolutionary Embedded Systems", Grant No CNS-06369330". Technical report, Team for Research in Ubiquitous Secure Technology (TRUST), July, 2007.

[11] Skoudis, E., Liston, T., "Counter hack reloaded, a step-to-step guide to computer attacks and effective defenses," 2nd edition, Prentice Hall PTR, Jan. 2006.

[12] UK House of Lords. "Personal Internet Security". Technical report, UK House of Lords, December, 2007.