07

Carnegie Mellon · Cornell University · MILLS COLLEGE · San José State UNIVERSITY

SMITH COLLEGE · STANFORD UNIVERSITY · Berkeley UNIVERSITY OF CALIFORNIA · VANDERBILT UNIVERSITY

TRUST 2006-2007 Annual Report

http://www.truststc.org

TABLE OF CONTENTS

1 GENERAL INFORMATION

1.1 Summary

Date submitted	April 2, 2007
Reporting period	June 1, 2006 – May 31, 2007
Name of the Center	Team for Research in Ubiquitous Secure Technology
Name of the Center Director	Shankar Sastry
Lead University	University of California, Berkeley
Contact information, if changed since last reporting period	
Address	337 Cory Hall
Phone Number	510-643-5883
Fax Number	510-642-2718
Email Address of Center Director	Sastry@eecs.berkeley.edu
Center URL	http://www.truststc.org

Below are the names of participating Center institutions, their roles, and (for each institution) the name of the contact person and their contact information at that institution.

Institution Name	Carnegie Mellon University, Mike Reiter
Address	2123 Collaborative Innovation Center Pittsburgh, PA 15213
Phone Number	412-268-1318
Fax Number	412-268-6779
Email Address of Center Director	reiter@cmu.edu
Role of Institution at Center	CMU is a lead research, education, and outreach partner.

Institution Name	Cornell University, Stephen Wicker
Address	386 Rhodes Hall Ithaca, NY 14850
Phone Number	607-255-8817
Fax Number	607-255-9072
Email Address of Center Director	wicker@ece.cornell.edu
Role of Institution at Center	Cornell University is a lead research, education, and outreach partner.

Institution Name	Mills College, Almudena Konrad
Address	CPM 204 Oakland, CA 94613
Phone Number	510-430-2201

Fax Number	510-430-3314
Email Address of Center Director	akonrad@mills.edu
Role of Institution at Center	Mills is a research partner in the area of privacy and an outreach partner to encourage greater female participation in engineering.

Institution Name	International Computer Science Institute Berkeley Foundation for Opportunities in Information Technology, Orpheus Crutchfield
Address	1947 Center Street, Ste. 600 Berkeley, CA 94704
Phone Number	510-685-0681
Fax Number	
Email Address of Center Director	orpheus@bfoit.org
Role of Institution at Center	BFOIT is an education and outreach partner to encourage greater youth participation in engineering.

Institution Name	San Jose State University, Sigurd Meldal
Address	ENGR 284 San Jose, CA 95192
Phone Number	408-924-4151
Fax Number	408-924-4153
Email Address of Center Director	smeldal@email.sjsu.edu
Role of Institution at Center	SJSU is a lead education partner to spread curriculum and encourage greater minority participation in engineering.

Institution Name	Smith College, Judith Cardell
Address	Clark Science Center, EGR 105b, Northampton, MA 01063
Phone Number	413-585-4222
Fax Number	413-585-3827
Email Address of Center Director	jcardell@smith.edu
Role of Institution at Center	Smith is a research partner in the area of sensor networks and outreach partner to encourage greater female participation in engineering.

Institution Name	Stanford University, John Mitchell
Address	Gates Building 4B-476 Stanford, CA 94305-9045
Phone Number	650-723-8634
Fax Number	650-725-7411
Email Address of Center Director	mitchell@cs.stanford.edu
Role of Institution at Center	Stanford is a lead research, education, and outreach partner.

Institution Name	Vanderbilt University, Janos Sztipanovits
Address	2015 Terrace Place VU Station B 356306

	Nashville, TN 37235-6306
Phone Number	615-343-7572
Fax Number	615-343-6702
Email Address of Center Director	janos.sztipanovits@vanderbilt.edu
Role of Institution at Center	Vanderbilt is a lead research, education, and outreach partner.

1.2 New Center Faculty

Please see Appendix A for biographical information on each new faculty member added to the Center during this reporting period.

1.3 Report Point of Contact

Below is the name and contact information for the primary person to contact with any questions regarding this report.

Name of the Individual	Larry Rohrbough
Center role	Executive Director
Address	391 Cory Hall, Berkeley, CA 94720-1774
Phone Number	510-643-3032
Fax Number	510-643-2356
Email Address	larryr@eecs.berkeley.edu

1.4 Context Statement

The Team for Research in Ubiquitous Security Technology (TRUST) was created in response to a growing sense of urgency in dealing with all aspects of cybersecurity as it affects society. First, the role and penetration of computing systems and networks in our societal infrastructure continues to grow, and their importance to societal safety and the security has never been greater. Beyond mere connection to the internet and access to global resources, information systems are now used for controlling critical infrastructures for electricity, healthcare, finance, and medical networks. Second, and somewhat contradictorily, many such control systems remain untrustworthy. Waves of viruses and worms sweep the Internet and exhibit increasing virulence and rate of speed that is also directly proportional to their growing ease of deployment. Privacy remains poorly understood and poorly supported; security is generally inadequate, and some speak of a “market failure” in the domain. Broader issues of software usability, reliability and correctness remain challenging. Industry stakeholders are unable to recruit new employees adequately trained in these technologies. Society is placing computers into critical roles, although they do not meet the requirements of trust.

TRUST is composed of several universities—Berkeley, Carnegie Mellon, Cornell, San Jose State, Stanford and Vanderbilt—which have joined forces to organize a multifaceted response. TRUST represents the strongest and most diverse engagement of the issue of trusted systems ever assembled. TRUST is the first to recognize the breadth of the problem and to combine fundamental science with a broader multidisciplinary focus on economic, social and legal considerations and a substantial educational mission. TRUST will enable dialog with stakeholders whose needs simply cannot be approached in a narrower and purely technical manner, or by any single research group. TRUST seeks to be an intermediary between the

policy makers and society at large on the one hand, and the researchers, academics, and industrial providers of services and technology on the other.

TRUST seeks to achieve its mission through research as well as a global policy for engaging in education of society as a whole. This annual report of TRUST details the experience of the center along many dimensions—research, industrial outreach and knowledge transfer, education, and diversity outreach.

In research, TRUST has achieved success along several fronts—in model-based integration of trusted components and co-design of networked embedded systems, in the creation of new software tools for monitoring and controlling large sensor infrastructures, creation of integrative testbeds for critical infrastructures, in understanding privacy and other legal issues surrounding identity theft, and designing tools for anti-phishing technology, etc. All these are reported in detail in the research thrusts area of this report.

In education, TRUST is leveraging an existing learning technology infrastructure to quickly enable TRUST courseware and material to be assembled, deposited in a repository, and adapted for wide web-based content dissemination. In addition to developing special courses for undergraduate and graduate curricula, and regular seminars in all campuses as well as webcasts, TRUST has hosted a series of workshops on sensor networks, privacy, identity theft, electronic medical records. The major thrust in the second year was the TRUST Academy Online (TAO) and the Education Community Development efforts. Again, all these are reported below in the section on education.

In knowledge transfer, TRUST has begun an aggressive program of technology transition with industry (from bug reports of open source software to tools such as Spoofguard and various consulting activities) and active engagement with governmental agencies such as the Department of Homeland Security (DHS), the Air Force Office of Scientific Research (AFOSR), the Department of Defense (DoD), and the Department of Energy (DoE) which are all concerned with issues of security. Also, TRUST has a large and growing set of industrial partners such as Intel, Microsoft, Sun, and United Technologies with whom we are beginning to engage in collaborations of mutual interest. For example, one such partner, Telecom-Italia, will harvest the incipient technology that comes out of TRUST in the healthcare sector to better understand and build upon its own base.

TRUST has an ambitious goal of reaching a diversity goal of 30% of women in its faculty and students, and 10% of researchers from underrepresented communities, and has been proactive in this regard. Several activities for enhancing diversity are reported in the corresponding section.

Overall, we are happy to report that the center is making excellent progress towards its goals, its participants are actively engaged, and the outlook is positive.

2 RESEARCH

2.1 Goals and Objectives

The TRUST vision is to provide a unique opportunity for a wide range of cybersecurity issues to be addressed from many points of view—technological, scientific, social, policy, and legal. Of paramount importance to TRUST is the creation of a science that will simultaneously address the imperatives of all these points of view and allow scientists and technology developers, policy

makers, and social scientists to make informed and rigorous decisions with the full understanding of tradeoffs involved. We think that this new science, though exciting and far-reaching, will come about from an evolution of more traditional areas that impinge on this "science of TRUST" as theory and praxis of these areas co-evolve. In particular, the primary areas of new science creation include cryptographic protocols and supporting systems, high confidence software science, security functionality, policy and management guidance, and complex interconnected networked systems. Furthermore, TRUST will have strong, well proven ties with Information Technology (IT) vendors and infrastructure providers which will serve to both ground TRUST research in real-world problems and enable avenues for knowledge and technology transfer. TRUST will have a significant impact at a national scale as its research results will lead to new concepts and doctrine for (1) public policy issues around privacy, access control, and security; (2) technology for protecting and preventing information security breaches; and (3) increased protection of the nation's critical infrastructures, most notably in the areas of telecommunication, healthcare, electric power, financial services, and military networks.

2.2 Performance and Management Indicators

TRUST projects are both continuously and periodically monitored for meeting the center's overall research objectives and the project's individual research objectives. Periodic monitoring consists of bi-annual meetings of all TRUST personnel where progress in each research thrust area is formally reviewed. Continuous monitoring consists of evaluation by both the project leaders in research thrust areas as well as by the TRUST Executive Board. The evaluation metrics are outlined in the table below.

Objective	Metric	Frequency
Scientific Impact	Publications, Presentations, Recognition	Annual
Technological Impact	Transitions, Industry Interest	Annual
Timeliness	Milestone Completion	Semi-Annual
Social Impact	Policy Papers, Legal Policy	Annual

2.3 Current and Anticipated Problems

No significant problems were encountered during the reporting period. No significant problems are anticipated in the next reporting period.

2.4 Research Thrust Areas

TRUST projects are organized into several research areas. During the first two years of the center, TRUST research projects were focused on anywhere from 5 to 11 challenge areas. Evolution of the research areas has occurred due in part to consolidation of similar research interests and a collective agreement among TRUST management and campus principal investigators to focus TRUST researcher efforts in certain areas.

Each research thrust was selected to encourage projects that are integrative in nature and provide opportunities for TRUST researchers to work on topics that cross disciplines and allow collaboration across campuses.

For this reporting period, there were five research thrust areas, listed below:

1. Electronic Medical Records
2. Identity Theft and Phishing
3. Network Defenses
4. Secure Sensor Networks
5. Trustworthy Systems

Research activities in each thrust area are described in more detain in the following sections.

2.4.1 Electronic Medical Records

Project Leaders: *Janos Sztipanovits (Vanderbilt University), Ruzena Bajcsy (UC Berkeley), Michael Eklund (UC Berkeley)*

Computer technology, patient sensors, and networking are revolutionizing several aspects of healthcare and medical information processing. Small wireless sensors will free many patients from managed care facilities, while providing timely medical assistance when needed. At the other end of the spectrum, virtually all patients will soon gain greater control over their records and treatment options through web portals. The TRUST Electronic Medical Records (EMR) research thrust addresses the complex security and privacy issues emerging from the rapidly increasing use of electronic media for the archival and access of patient records. This change is driven and strongly influenced by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). EMR has become an area where technology, public policy and individual interests intersect and conflict, making the development of information systems for EMR archiving and access a very challenging problem. There is clear evidence that without a detailed understanding of the relevant issues on all sides, an acceptable solution cannot and will not emerge. The projects leverage a cooperative relationship established with the Informatics Institute and the Biomedical Informatics Department of the Vanderbilt University Medical Center. The MyHealth at Vanderbilt System – a functioning web-based patient portal – is a unique resource that serves as the basis for experimentation and interaction through real-life deployment scenarios. The EMR projects also utilize the on-going Information Technology for Assisted Living at Home project at the University of California, Berkeley to develop the tools necessary to produce high confidence and secure embedded software systems necessary to investigate the nature of automated and semi-automated sensor data inclusion into EMRs. This project develops smart sensing technologies that enable alert monitoring and gathering long-term out-patient biometric data. Decisions on how and when to include this data in an EMR and how to apply the methods to existing and new in-patient sensor systems are of primary importance. EMR researchers collaborate extensively with TRUST Secure Sensor Networks researchers, with a particular emphasis on the latter's Real-Time Patient Monitoring Project.

We have five areas that represent challenges for the TRUST research agenda and have direct relevance and applicability in EMR. They are:

- Dynamic Access Control
- Data Privacy
- Architecture Modeling and Vulnerability Analysis
- Study Group on Unintended Consequences
- Real-Time Patient Monitoring.

The accomplishments of each project are discussed in more detail below.

Dynamic Access Control – The Stanford University team has begun adapting prior work on privacy policy languages to the MyHealth at Vanderbilt Patient Portal. The assumption of policy enforcement is determining the semantic type of information contained in communicated messages because the portal is used to exchange free-text messages written by patients and medical professionals. Hence, the language was extended with a notion of "nominal" information types, or "tags" for messages, that is, possibly incorrect assertions by agents about the actual semantic type of information in the message. Second, we have extended the language to express utility goals, functional requirements on the system.

The Patient Portal can be viewed as a workflow, a division of responsibly among various agents and a mechanical workflow engine. Privacy and utility requirements expressed in LPU are then used by MyHealth in two ways. First, algorithms analyze the design of the workflow assuming the agents fulfill their responsibilities, in particular, that they accurately tag messages. Under this assumption, the workflow engine can use the message tags to accurately enforce the privacy requirements. As both privacy and utility can be expressed in the logic, we can evaluate, as suggested by many privacy advocates, whether MyHealth's design discloses the minimum information necessary to achieves its utility goals. Second, we provide auditing algorithms for finding individuals who fail to correctly tag messages. These algorithms analyze the apparent exchange of information asserted by the tags for inconsistencies, and such suspicious actions indicate the presence of incorrect tags in "nearby" messages. The culpable individuals are found with the assistance of a human auditor, whose work is reduced by the algorithm.

The effort to developing an architecture for an in home medical monitoring sensor network which publishes data to, and interacts with, EMR systems has continued. This medical sensor network project is a joint work of Cornell University, Vanderbilt University, and the University of California, Berkeley. An architecture has been developed that allows us to identify avenues through which physicians and patients will interact with the system and the EMR, as well as indicate if additional features or privacy preserving techniques must be implemented by the EMR. This includes identifying users contextually, by factors such as whether they are submitting or retrieving information. At the implementation level, the system architecture suggests limits on the capability of certain devices to perform cryptographic or other privacy preserving actions.

Data Privacy – The Stanford University and Cornell University team has worked on privacy-preserving database querying and privacy-preserving data publishing. Privacy-preserving database querying deals with the problem of information leakage of private data through database queries. Research challenges include definitions of data privacy that make enforcement efficient while permitting the answers to large classes of queries. Privacy-preserving data publishing deals with the problem of publishing private data such that an adversary cannot discover much new information about any individual in the population from the published data. Research challenges include the right notion of data privacy especially given that an attacker might have demographic or other information about patients and that an attacker might use external databases. For both of these topics the team has developed techniques and algorithms for addressing them, concentrating on methods that have broad applicability and then tailoring them to the medical field. The Carnegie Mellon University team has been working on developing efficient cryptographic techniques for distributed privacy-preserving information sharing, and is applying this in distributed privacy-preserving set operations for EMRs.

The real time notification aspect of the patient monitoring systems suggests new challenges in protecting data privacy. Notifications generated by the mobile phone carried by the patient may be sent to a variety of destinations by various methods, such as a computer at a physician's office, or to family members through a similar device, or to their own mobile phone through voice or SMS. The computer at the physician's office may in turn indicate to the patient's phone that it must directly contact a phone carried by a physician. Preservation of data privacy requires a synchronization of policy across these devices and an understanding of how data may spread from various devices

Architecture Modeling and Vulnerability Analysis – The Vanderbilt University team has introduced a formalized design approach to EMR based on standards-based design methodologies that have been successfully applied in other domains: Service-Oriented Architecture (SOA), Platform-Based Design (PBD), and Model Integrated Computing (MIC). We believe that the combination of SOA, PBD, and MIC techniques can enable the design of complex CIS to ensure reliability, performance, privacy, and security beyond what can be achieved by current ad hoc practices. A primary reason we selected SOA as the target platform is the dynamic environment it provides for policy-driven access control, privacy, and security implementation. We have developed a new layer of abstraction that is formally captured as a suite of domain specific modeling languages. The unique requirements and operational characteristics of health care delivery provide the underlying basis for these languages. The abstraction layer is supported by a suite of modeling, model transformation, model analysis, and configuration tools that we build using components of the metaprogrammable MIC tool suite. By introducing the most effective domain abstractions, we make models that are concise, understandable, and reusable. By cooperating with the Vanderbilt University Medical Center, we were able to apply our methods to a real-life example: the MyHealth@Vanderbilt (MHAV) patient portal. The MHAV example was crucial in demonstrating the effectiveness of our design approach.

The Vanderbilt University team has developed a precise architecture model for a set of services of the Patient Portal and the back end EMR system and has investigated using these models for vulnerability analysis. Several vulnerabilities were identified. The MyHealth at Vanderbilt University team, in turn, has fixed these issues. TRUST researchers have also initiated discussions with the designers/developers on future architectural changes to the Patient Portal in order to increase its security.

Study Group on Unintended Consequences – TRUST and MyHealth researchers and developers have formed a study group on understanding scenarios in Patient Portal use cases that can have potentially negative consequences. A diverse set of people have been participating in these ongoing meetings including the project manager of the Patient Portal, the Chief Security Officer of Vanderbilt University, the lead developers of the Patient Portal and the Vanderbilt University internal EMR system as well as representatives from the legal office, the medical library, patient billing, etc. This study group has identified a list of important issues that are being addressed with detailed follow-on investigation. One important topic being investigated currently is the question of delegates and surrogates, that is, giving people other than the patient access to his or her medical record. Another future extension of the Patient Portal is expanding it beyond the Vanderbilt University Medical Center by providing it as a service for local community physicians and labs. The group has also recommended farming out payment handling to a third party so that the portal does not have to deal with such sensitive issues as processing credit card information.

The group has also studied past privacy issues that have come up with EMR. In the process of the precise architectural modeling of the Patient Portal, TRUST researchers have identified a number of potential security/privacy violations and recommended short term as well as long term solutions to address them. These have been incorporated in the deployed system. The group has also studied current legal regulation of medical privacy (which is one of the most highly regulated areas of privacy law), consequences of making large amounts of medical data available to the public (even if initially made available only to the rightful recipients) and the potential consequences of unwanted access to personal sensor information that is being communicated to EMRs wirelessly and by telecom means, and of the possibility of tampering with personal sensor data when it is collected without supervision, relative merits of competing models for generating security standards (including the HIPAA data security regulations).

Real-Time Patient Monitoring – The collaborative team of the University of California, Berkeley, Cornell University, and Vanderbilt University has been working on the system architecture design, sensor network deployment and software prototyping, and end-to-end data privacy preserving mechanisms of the patient monitoring project. The system architecture consists of three major components: medical sensing (which provides patient monitoring) medical data collection and fusion), backhaul communication (which provides remote communication between patient home and care provider (patient portal)), and patient portal interface (which provides medical data archive and uniform monitoring data access).

The unique characteristics of the medical sensing environment and its strong requirements in terms of reliability, Quality of Service (QoS), security, and privacy poses several challenges to the system architectural design. To address these challenges, the team has developed a home health monitoring architecture which can be used for a variety of medical conditions. This system monitors patients in real-time using a tiered heterogeneous wireless network as it collects information from multiple sensors and analyzes that data. The first layer of the system is the wearable sensors. These sensors are primarily physiological. These devices will transmit their data via short range PAN link in a single hop fashion allowing optimization for minimum energy expenditure and maximum battery life. The next layer of the system is an intermediate network of powered dual wireless interface nodes. These devices serve both to forward data from the worn sensors to the fusion center, and as a high bandwidth sensor network for cameras for patient monitoring and interaction. These nodes shall form a mesh network fusing medium range WLAN links with the fusion center. The fusion center interacts with the backhaul network and forms the third layer of the system. The fusion center is responsible for completing on site processing of sensor data, generating notifications to care providers with varying levels of urgency, and forwarding data using available wide-area networking technologies, such as cellular network and Internet access network.

2.4.2 Identity Theft and Phishing

Project Leaders: *John Mitchell (Stanford University), Doug Tygar (UC Berkeley)*

This research area is concerned with online identity theft and related threats that pose risks for millions of Americans using the World Wide Web on a daily basis. Online identity crimes involve multiple victims, result in large dollar losses, compromise privacy, are often used by organized criminal groups, and may be associated with other crimes such as illegal drugs, mail fraud, and terrorism. This research area was originally conceived around technology for preventing phishing, which uses fraudulent e-mail to deceive consumers into visiting fake replicas of familiar Web sites and disclosing sensitive information. While TRUST researcher developed and deployed various ways of mitigating phishing prior to 2006, the problem still remains and the opportunity exists for greater TRUST impact through improved methods, outreach, and

technology transfer. In addition, perpetrators are developing and deploying increasingly sophisticated and powerful methods, leveraging spyware, botnets, and related malware. These advancing threats pose new technical problems, and raise questions about legal status of organizations that produce and deploy software that facilities identity compromise.

This collaborative TRUST research area, involving faculty and students from computer science and law at the University of California, Berkeley, Carnegie Mellon University, and Stanford University, has studied the social and legal context of identity theft, developed improved technology to combat phishing, spyware, botnets, and related threats, pursued technology transfer opportunities, and studied the policy and legal implications of intrusive activities and possible defensive measures.

The main topics addressed during this reporting period were:

- Web Authentication and Phishing Defenses
- Alternate Methods for Stealing Information
- User Studies and Policy Issues
- Semantic-Based and Host-Based Malware Detection
- Education and Outreach.

The sections below provide more details on the key accomplishments and outcomes in each Identity Theft and Phishing topic.

Web Authentication and Phishing Defenses

- SafeHistory/SafeCache: SafeHistory and SafeCache are browser extensions that prevent a class of context-aware phishing attacks that present an adaptive phishing page to the user based on user's browsing history. SafeHistory is a Mozilla Firefox browser extension that protects your privacy by silently defending against visited-link-based tracking techniques. It allows offsite visited links to be marked only if the browser's history database contains a record of the link being followed from the current site. SafeCache is a browser extension that protects your privacy by silently defending against cache-based tracking techniques. It allows embedded content to be cached, but segments the cache according to the domain of the originating page.

- Password Hash: PwdHash is a previously developed browser extension that transparently converts a user's password into a domain-specific password. The user can activate this hashing by choosing passwords that start with a special prefix (@@) or by pressing a special password key (F2). PwdHash automatically replaces the contents of these password fields with a one-way hash of the pair (password, domain-name). As a result, the site only sees a domain-specific hash of the password, as opposed to the password itself. A break-in at a low security site exposes password hashes rather than an actual password. We emphasize that the hash function we use is public and can be computed on any machine which enables users to login to their web accounts from any machine in the world. Hashing is done using a Pseudo Random Function (PRF). During this reporting period, we collaborated with RSA Security on integration with the RSA SecurID hardware token. SecurID generates a one-time password that is still vulnerable to "attacker-in-the-middle" password stealing attacks. With the server-side software developed as a result of this collaboration, RSA SecurID one-time passwords are protected from phishing attacks.

- Dynamic Security Skins: We continued to develop our dynamic security skins technology that uses a visual hash algorithm to present a browser skin that prevents users from mis-entering responses to phishing queries.

- Authentication via Mobile Devices: Phishing attacks succeed by exploiting a user's inability to distinguish legitimate sites from spoofed sites. Most prior research focuses on assisting the user in making this distinction; however, users must make the right security decision every time. Unfortunately, humans are relatively ill-suited for performing the security checks necessary for secure site identification, and a single mistake may result in a total compromise of the user's online account. Fundamentally, the site should authenticate the user based on information that the user cannot readily reveal to a malicious parties. Placing less reliance on the user during the authentication process will enhance security and eliminate many forms of fraud. We have developed several design principles needed to counter phishing attacks: 1) sidestep the arms race, 2) provide mutual authentication, 3) reduce reliance on users, 4) avoid dependence on the browser's interface, and 5) forgo network monitoring. Anti-phishing solutions that fail to follow these principles will likely be overcome or circumvented by phishers. Second, to fulfill our design principles, we propose a foolproof anti-phishing system that does not rely on users to always make the correct security decision. Our mutual authentication protocol uses a trusted device (e.g., a cell phone) both to manage a second authenticator for the user and to authenticate the server. Since a user cannot readily disclose the additional authenticator to a third party, attackers must obtain the user's password and compromise the trusted device to gain account access. By making the trusted device an active participant in the authentication process, our protocol protects the user against Man-in-the-Middle attacks. Our approach also defends against keyloggers and other mechanisms designed to monitor user input. The user can easily employ our scheme across multiple platforms without relying on the information in the browser's display. Finally, we demonstrated the practicality of our system with a prototype implementation. We used a cell phone as the trusted device, and we showed that the system introduces minimal overhead. In addition, the server-side changes are minor, as well as backwards compatible.

- Cookie Management: Browser cookies are important aspects of protecting against identity theft. As part of our research, we developed a new browser structure, "Doppelganger", that allows browsers to retain cookies only when web sites actually require them for use; using parallel "retained" and non-retained cookies to support alternatives. Doppelganger has been publicly released. We also invented a new "locked IP address" cookie structure that we argue has considerable benefits over existing cookies in resisting attack.

- Spyblock: Spyblock is a system that protects web passwords from malicious spyware and keyloggers. The system consists of two components: a browser extension that runs in an untrusted environment with the browser and other applications, and an authentication agent that runs in an environment that is protected from spyware. Using a virtual machine monitor, the trusted and untrusted components can both run on the same physical machine. The user only interacts with the trusted component during authentication; all other web browsing activity can be conducted using the untrusted application environment. The SpyBlock system protects user passwords from Keyloggers and Transaction Generators on the user's machine. All user passwords are kept hidden from the VM and any spyware running inside the VM. Instead, users enter

passwords into the SpyBlock agent running on the host OS. The agent embeds (hashed) passwords in outgoing HTTP login requests. As a result the VM never sees user passwords. The agent enables users to confirm transactions so that a malicious transaction generator cannot fake user requests. Deploying the system on a large scale can now be done free of charge thanks to freely available virtual machine monitors.

Alternate Methods for Stealing Information

- Web Timing Attacks: We identified a new class of web attacks, called cross-site timing. The method exposes private user information by measuring response times from a web site. For example, cross-site timing enables a phisher to test if a user is actively logged into a banking site. The phisher can also learn the number of items in the user's shopping cart. Such leaks help phishers mount context aware phishing attacks. We are currently designing generic mitigation tools that will help web sites defeat this attack.

- Keyboard Acoustic Emanations: When users type on keyboards, they generate sounds. These sounds can easily be recovered by recording devices such as microphones attached to a computer, telephone handsets, sensors in a room, and external microphones (e.g., parabolic or laser microphones). We have developed algorithms for determining keystrokes from audio recordings of users typing on a keyboard. These algorithms do not require a traditional learning phase – they infer the characters being typed merely from the assumption that users are typing English (they automatically figure out the assignment of keystrokes to characters typed.) We plan to investigate these issues more deeply and develop (1) effective measures to limit leakage of information from keyboard acoustic emanations, (2) theoretical structures for information leakage from a variety of emanation types, and (3) demonstration of emanation limitation measures together with anti-spam tools. Automated detection of keyboard strokes from acoustic emanations is part of a larger effort exploring machine learning algorithms and their role in protecting against identity theft. During this reporting period, we have expanded considerably on the acoustic emanations work by exploring those same techniques to facilitate malware identification. We have also shown theoretical limits in the effectiveness of machine learning techniques and the necessity to use broader strategies.

- Radio Frequency Identification: In this area, we performed research that examined the vulnerability of RFID technology, and in particular the potential dangers associated with RFID chips in passports.

User Studies and Policy Issues

- Anti-Phishing Technologies: We conducted a major study examining techniques used by phishers and their degree of relative effectiveness, which was published in the CHI conference and received wide note. A follow-on study examined the effectiveness of different anti-phishing technologies, and received considerable comment including an article in the New York Times.

- User Studies: During the summer, one TRUST student (Collin Jackson) did an extensive user study of the effectiveness of picture-in-picture phishing attacks. Picture-in- picture attacks forge all security indications at the site (such as the SSL lock icon) by wrapping the entire web page in a frame. Modern browsers attempt to block such

attacks using chrome. The user study showed that the chrome is not very effective and new methods are needed to defeat picture-in-picture attacks. This study led to a joint paper written by two Stanford students and two Microsoft researchers.

- End User License Agreements: We examined the legal and user impact of "click-through" end user license agreements (EULAs). Our study confirmed the widespread impression that EULAs are not effective in informing users even when the agreements are read in full by the user. We examined alternative approaches including short notices before or after installation.

Semantic-Based and Host-Based Malware Detection

- Semantic-Based Malware Detection: Traditional approaches to malware attempt to find a “signature” (or code-fragment) to detect threats. These approaches are necessarily limited because they require a network of individuals to find instances of malware and then report signatures to some central facility. Instead of relying on the traditional signature-based detection approach, we designed semantic-based detection techniques to detect malware based on their behavior. Three particular systems developed and evaluated this reporting period are Minesweeper, Panorama, and BotSwat (all described in more detail below).

- Minesweeper: Malware often contains hidden behavior which is only activated when properly triggered. Well known examples include: the MyDoom worm which DDoS's on particular dates, keyloggers which only log keystrokes for particular sites, and DDoS zombies which are only activated when given the proper command. We call such behavior *trigger-based behavior*. Currently, trigger-based behavior analysis is often performed in a tedious, manual fashion. Providing even a small amount of assistance would greatly assist and speed-up the analysis. We proposed that automatic analysis of trigger-based behavior in malware is possible. In particular, we designed an approach for automatic trigger-based behavior detection and analysis using dynamic binary instrumentation and mixed concrete and symbolic execution. Our approach showed that in many cases we can: (1) detect the existence of trigger-based behavior, (2) find the conditions that trigger such hidden behavior, and (3) find inputs that satisfy those conditions, allowing us to observe the triggered malicious behavior in a controlled environment. We have implemented Minesweeper, a system utilizing this approach. In our experiments, Minesweeper has successfully identified trigger-based behavior in real-world malware. Although there are many challenges presented by automatic trigger-based behavior detection, Minesweeper shows us that such automatic analysis is possible and encourages future work in this area.

- Panaroma: Once installed, malicious software such as keyloggers, packet sniffers, backdoors, spyware, and rootkits can spy on users' behavior and compromise their privacy. Even software from reputable vendors, such as Google Desktop and Sony DRM media player, may perform undesirable actions. Unfortunately, existing techniques for detecting malware and analyzing unknown samples are insufficient and have important shortcomings. Signature-based detection, for example, cannot detect new malware and watch-point-based behavioral detection can be evaded by a stealthier malware design. Previously proposed information flow analysis mechanisms are too coarse-grained to capture malware behavior and fail to address kernel-level attacks. We proposed Panaroma, a system that applies *whole-system fine-grained taint analysis* to

discern information access and processing behavior of malware. Our approach captured the intrinsic behavior of a wide spectrum of malware, and cannot be easily evaded. We used 42 malware samples and 50 benign samples for evaluation. Our experimental results showed that Panaroma yields no false negatives and very few false positives. Furthermore, by using Google Desktop as a case study, we showed that our system can accurately capture its information access and processing behavior, and we can confirm that it does send back sensitive information to remote servers. We believe that a system such as Panaroma will offer indispensable assistance to code analysts and malware researchers by enabling them to quickly comprehend the behavior and inner workings of an unknown sample.

- BotSwat: We are developing a host-based botnet slave detection system using system call fingerprinting in Windows. The idea is to correlate contents of incoming network packets with arguments to subsequent system calls. Since known bots react in a predictable manner to network commands we can identify when a machine has been assimilated into a botnet. This basic idea was designed for sdbot, and performed well on other bots such as spybot 1.3, agobot, and others, suggesting that this may be generally applicable to other bots that were not used in the experiment. Initial testing suggested that to reduce false alarms, a user input module should be added, so that user control can be distinguished from remote control. With this modification, few false alarms were generated when benign programs were traced.

Education and Outreach

Education and outreach are central goals of this research area. Identity theft is a real problem, and we continued to work with law enforcement groups such as the U.S. Secret Service, the Federal Bureau of Investigation, Infragard, the Department of Homeland Security Identity Theft Technology Council, the anti-phishing working group (www.antiphishing.org), and industry to get our anti-phishing information, our vulnerability testing information, and our legal and policy analyses as widely disseminated as possible. Our ultimate goal is to effect real change that will touch everyone who uses the Web. Several transition partners have been identified and engaged to varying degrees, including PassMark Security, RSA Security, and divisions of Microsoft. In order to increase public awareness of this problem and its potential solutions, we also continue to talk with the press.

We have also worked to influence the teaching of security, by developing a study unit on online identity theft that can be incorporated into security classes. Our fast-track teaching module, produced during this reporting period, includes lecture material on web browser and server security, and a hands-on programming project that develops understanding of the power of malicious javascript in the browser environment. This fast-track module, which can be added as a single lecture to a class on computer security, is backed up with additional lecture material, homework, exam questions, and projects that we use in our own classes and that is freely available to anyone interested.

2.4.3 Network Defenses

Project Leaders: *Anthony Joseph (UC Berkeley), Ken Birman (Cornell University)*

Computer networks are, arguably, the key technical development of our era. They have enabled us to construct powerful systems of tremendous scope and complexity. But with this scope and complexity they also bring exposures to failures, concurrency-related bugs, poor management, and outright misuse. Modern networks have become exceedingly hard to defend

against mishap, whether accidental or deliberate, and this observation has made research into network defense, broadly construed, an obvious and central area for investigation by members of the TRUST team.

TRUST researchers are pursuing a gamut of innovative topics in the area of computer networks, which we classify roughly into the area of “network defenses” techniques. During the 2006-2007 reporting period, Network Defenses activities unified 10 closely related internal TRUST projects. Most of these activities involved multiple institutions and all had an “organic” need for dialog, sharing of ideas, and other forms of participation by multiple organizations and multifaceted research teams capable of looking at a spectrum of issues that range from social and pragmatic to highly technical. The remaining activities fall into categories in which TRUST researchers are proposing work complementary to the primary, more collaborative, activities. In aggregate, the work includes efforts from essentially every facet of the TRUST Center.

During 2006-2007, substantial progress was made in all areas. The DETER testbed has grown to encompass more TRUST partners, with Cornell University and the University of California, Berkeley also extending the basic concept to explore questions associated with long-haul, high latency links. The shared testbed is an exceptionally powerful resource, not just for the original purpose of studying virus outbreaks but also for exploring new concepts that might be developed further in the context of the National Science Foundation Global Environment for Network Innovations (GENI) initiative.

The University of California, Berkeley work with DETER has grown to include threats from Distributed Denial of Service (DDoS), stepping-stone, zombie/botnet, and virus/worm propagation threats that can be identified and contained by dynamically instantiating and analyzing an approximate global view of network activity on the basis of which individual nodes can react by applying an appropriate policy in a consistent manner. This is the view of the network design explored in the security attribution project area. Alternatively, the network can be re-designed with functionality that enables more secure operation. Three of the project areas (network design for secure information, efficient distributed network attack detection, and using machine learning techniques for network defense) address this domain. These areas could work in conjunction with the broader NSF GENI effort to provide useful design guidance and implementation components.

At the edge of the network (i.e., client nodes, servers, etc.), end system behavior can be analyzed to detect intrusion attempts or attempts by worms/viruses to propagate. Two of the project areas address this domain (using machine learning techniques for network defense, and network support for attribution using causal information).

Finally, at the application level, there is an opportunity to better understand the network challenges when meeting the requirements of applications with strong real-time requirements and in the presence of on-going network attacks.

Cornell University research has been focused on evaluating new concepts for backing up entire data centers over long-haul WAN links that combine high speeds with high latencies, and where hiding the latency is key to success. One major accomplishment during 2006-2007 involved the discovery of a new class of network protocols that extend FEC to work when clusters of computers are connected in this manner. Cornell University researchers are now working to demonstrate a new kind of file system in which all data can be mirrored in real-time at a remote data center with only minor impact on local file system performance.

An interesting new option for the research team involves the discovery of power-savings opportunities afforded by these kinds of architectures. What we've noticed is that when file systems are mirrored in the manner just outlined, it may not be necessary to store the entire file system on both ends of the high speed link. For example, one side might maintain a complete file system, while the other side only maintains active files, and hence can "manage" with just a few spinning disks. In situations where one datacenter is situated in a cool climate with nearby power sources, and the other datacenter is in a hot region where power is at a premium, such an approach could slash costs – and also have an environmentally beneficial side-effect! We could not have identified this opportunity had it not been for the collaborative structure made possible by TRUST and the shared DETER testbed.

The Carnegie Mellon University team also reports some major successes. This team designed and developed an end-to-end automatic worm defense system which can automatically detect new exploit attacks and generate effective anti-bodies to protect vulnerable hosts and networks from further attacks. The anti-bodies created in this manner include input-based filters (network or host-based signatures) and dynamic patches, and have the salient features that they can be effective even against polymorphic attacks. Evaluations demonstrate that our worm defense system can protect over 98% of vulnerable hosts from being compromised in the Slammer worm attack, the fastest attack up to date, in a realist deployment scenario.

The Stanford University team, headed by John Mitchell, has developed a new method for secrecy analysis of authentication protocols. The group has formalized this in Protocol Composition Logic and developed a proof of secrecy properties for Kerberos, including verification of a recently repaired version that uses public keys in its initial steps. Mitchell and Dan Boneh have also developed improved connections between logic-based security analysis (so-called symbolic model) and crypto-style analysis (so-called computational model) for network protocols. This approach has enabled important steps in improved computational analysis of practical, deployed network protocols.

At the University of California, Berkeley, Venkat Anantharam had a success story that draws on cryptographic techniques. In environments requiring secret key generation, it is often important to provide external randomness to the agents. For example, sensor networks are often deployed in places where it is possible to beam randomness (e.g., from a satellite). Information theoretic security is the most stringent form of security. While once commonly considered infeasible in view of Shannon's one time pad result, the recognition that externally provided randomness can be used to create information theoretically secure keys has led to a rethinking of this pessimistic viewpoint and to significant work over the last decade in to develop protocols to extract high rate secret keys in such situations.

The University of California, Berkeley group studied the fundamental problem in information-theoretic cryptography in which a group of agents together with an eavesdropper have access to possibly correlated random sources. In particular, they focused on the secret key rate of the parties (secret from eavesdropper). Initial results strictly improve the best known bounds on the secrecy capacity. The results further unify and improve several earlier results in this area which had been studied separately. Looking forward to the next reporting period, the group is hoping to explore several new ideas for maximizing the achievable secret key rate.

Although all of our groups do much of their work independently, the whole TRUST team is united by a shared vision, and many of the accomplishments just cited benefited from the extensive interactions, the opportunities to compare ideas and share results, and the sense of common cause created by the TRUST Center. The DETER testbed has emerged as a powerful

resource for many projects. More and more, our teaching materials use shared examples and approaches, and we're starting to see common curricular approaches in the network defenses area – ideas that are being transitioned through talks we give, consulting activities, materials placed on the TRUST educational web sites, textbooks, etc.

If the accomplishments of these first years are indicative of the longer term potential, over a ten year period, TRUST will more that achieve its goals. We'll have a tremendous range of foundational research results to point to, published in prestigious conferences and journals. We'll have established an enduring network of contacts and collaborations spanning the country, and involved a diverse community of researchers in our work, including a disproportionate percentage from underrepresented groups (we note that almost all of the work cited above included female, African-American, and underrepresented minority researchers) We'll have created an approach to hands-on education that uses testbeds to give students the kind of physical experience no classroom can ever replicate, and shared curricular materials and content that will establish a leadership role for the TRUST research team relative to national standards for education in this vital area. In a nutshell, the experience of the Network Defenses team makes it clear that TRUST is succeeding.

2.4.4 Secure Sensor Networks

Thrust Leaders: *Steve Wicker (Cornell University), Deirdre Mulligan (UC Berkeley)*

The TRUST Secure Sensor Networks initiative focuses on the development and use of secure embedded sensor networks in a variety of large-scale applications. Applications to be emphasized include the protection and monitoring of critical infrastructure, rapid response systems for homeland defense, and the remote monitoring of individuals for clinical purposes, whether living at home or in group facilities. Recent developments in the field of sensor and networking technology have made such networks possible; this initiative will consider the further development of the requisite deployment, network configuration, data dissemination and query generation and response, and security technologies. This initiative also considers the privacy and security issues arising from the use of sensor networks, and the ways in which embedded sensor networks affect the expectations, experiences and activities of individuals in public and private spaces. An emphasis is currently being placed on developing privacy metrics, and limiting the acuity of sensing technologies to the minimum required to meet mission objectives. As well as considering the questions raised about the relationship between citizens and government by the possibility of constant monitoring enabled by widespread deployment of visual and other sensors in public spaces. A significant educational and outreach component has been developed with the joint objective of increased diversity in the ongoing development of these technologies and an increase in public awareness of the surrounding technical, legal, economic, and social issues.

The TRUST sensor networking team has four primary objectives.

- Develop technologies that facilitate the use of large-scale embedded sensor networks in applications that are critical to the nation's economy, security, and health.
- Demonstrate these technologies through the use of realistic testbeds, enhancing technical development while enabling ties to our corporate sponsors.
- Examine the legal, economic and societal issues that emerge from the use of these technologies in public and private places, and develop policies that guide their design, development, deployment, use, and regulation to protect the privacy, security, and economic and societal interests of the public.

- Develop security technologies that limit and characterize the potential threat from passive and active network intruders.
- Develop mechanisms for increasing diversity among the practitioners of sensor networking technology and social sciences, while building teaching tools that increase awareness of the capabilities of this technology.

In the past year we have established a two-dimensional managerial approach that pushes the simultaneous development of technology and policy. We have established a series of technical thrusts, while identifying and pursuing privacy and policy issues that are common across the range of thrusts. Within the technical thrusts, there are two main categories: networking technology and security. In the former area, we are developing networked sensing systems for public surveillance, structural integrity, medical sensing, power systems. We are also developing software tools that enhance data dissemination and querying within these networks. The security thrusts include the development of an attack taxonomy and tools for security co-design (details will follow later in this section). Cross-cutting privacy and policy issues include the analysis of privacy and security issues in specific sensor network application areas including healthcare, energy and camera networks in public places, the development of technologies and policies for addressing privacy and related issues. Specific activities within these efforts are discussed in more detail below.

The following are the primary technical thrusts within the TRUST secure sensor networking effort.

Medical Sensing Systems – Sensing devices such as body temperature monitors, blood pressure measurement devices, glucometers, accelerometers, acoustic sensors and video cameras are playing an increasingly prominent role in health care. Such devices have become increasingly integrated and networked within the confines of modern medical centers – the electrocardiograph in emergency rooms immediately dispatch their measurements, through wireless networks, to staff cardiologists who may begin to evaluate a patient within seconds of the test, regardless of the patient's placement within the building. Physicians may also download CAT scans and other tests onto laptops as they move from patient to patient in a typical care facility.

We are extending the scope and reach of these technologies so that they can support remote monitoring of patients. The goal is to facilitate the movement of patients into medium-care facilities or their own homes while still allowing frequent monitoring of their condition by a physician, as well as rapid detection medical events that require rapid care.

While it is clear that remote and in-home patient care have the potential to reduce medical care expenses and improve the quality of life individuals lives, addressing the privacy and security issues are key to adoption and use in this highly regulated and highly sensitive and private application space. Passed by Congress and signed into law in 1996, the Health Insurance Portability and Accountability Act (HIPPA) defined three major Rules in its Administrative Simplification provisions (Table II, Subtitle F, Part C): (1) Electronic Transactions and Code Sets (TCS), (2) Privacy, and (3) Security. HIPAA requires that virtually all the 1.2 million U.S. healthcare providers establish and maintain a formal, comprehensive information security management program, which covers all health information maintained or transmitted electronically. While much has been written about the implications of Privacy and Security Rule, little has been developed in the way of detailed policies for biomedical information security technologies. The application of the privacy and security rules in the context of in-home sensing technologies has not been explored.

We are exploring the development of the technology and its security at the same time and in the same context. On the technology side, we are exploring the suitability of various technologies and architectures for the system, and have identified two appropriate scenarios. First, a tiered network is under consideration that uses several classes of network technology. A single-hop PAN linking sensors and intermediate nodes placed throughout the home serves as the first-level network. A linking network is provided by a WLAN that links intermediate nodes and a fusion center in the home. The fusion center serves as generator for real time notification, as well as the focus for queries/orders by a physician. A WAN links the fusion center and Patient Portal – the central records facility at the Vanderbilt medical facility (see discussion under the Electronic Medical Records research area in this report).

A second approach to the network is being considered, this one focusing on the multi-channel, variable QoS capabilities of the 3rd and 4th generation cellular. In the proposed system, a single-hop PAN links sensors and a 3rd generation mobile platform. The mobile phone serves as personal fusion center and communication device.

A mote-based testbed has been deployed on the Cornell University campus to test over-the-air programming capabilities and a cellular interface. The testbed includes TinySec for MicaZ, a revised MAC layer for power saving for the MicaZ, and power-aware routing through the network.

Privacy concerns are being addressed at several levels. In one subtask focusing on "End-to-End Content Protection for Video Sensor Systems," the primary concern lies in content protection; specifically, protecting large-scale massive information/video flows from passive eavesdropping. Our solution is based on three key elements: content decomposition within the data stream, binary-tree-based hierarchical key generation, and a label-guided watermarking and distribution strategy. *Contextual privacy protection is provided through* Traffic Pattern Privacy Protection. The key issue here is disclosure of confidential information through network traffic analysis. Our solution takes the form of routing control. In particular, we have developed an information entropy-based traffic privacy model, penalty-based shortest path routing (PBSP). Finally, we have developed a novel source location protection scheme for wireless sensor networks. This scheme also contributes to the protection of contextual privacy, in that it focuses on source location privacy that is vulnerable to direction estimation. Our basic approach relies on a utility-based privacy model and a game-theoretic formulation that results in an optimal privacy aware routing protocol design.

Power Sensing Systems – The use of sensors to monitor power consumption is being considered as a prominent element in next-generation Supervisory Control and Data Acquisition (NG-SCADA) systems for the power grid. NG-SCADA may provide a novel, powerful means for stabilizing, monitoring, streamlining and protecting our nation's power distribution system. It may also present unexpected security and privacy problems that may significantly cloud, or completely obscure the potential benefits. We are exploring the confluence of sensor networking, power distribution, economics, privacy, and security issues that will emerge from a major increase in power consumption monitoring. We consider a scenario in which the granularity of monitoring is sufficiently fine to be an effective basis for demand-response systems targeted at the home and also to be a source of serious privacy concerns.

We are evaluating the efficacy and problems associated with residential-level power consumption sensing in a microgrid. A microgrid is a semiautonomous power sub-system, located within a single distribution system, and designed to operate as a unified, controllable

entity from the perspective of the high voltage system. Traditional distribution systems are radial systems with no active devices, and are thus limited to one-way power flow from the substation to load buses. A microgrid fills the role of a distribution system, yet contains active devices (distributed generation and storage), allows for bidirectional power flow, and can be controlled as a single entity that can disconnect from the grid for the health of itself and/or the high voltage grid. The technology to operate and control microgrids as autonomous units within the power system, thus allowing for individual distributed resources to participate in markets, does not yet exist.

We are developing a scalable architecture that will support wireless transport of residential data to fusion points. We are considering the use of such information in a demand-response system – a system in which users receive pricing information that they can use as a basis for consumption/timing decisions, while giving the microgrid operators information that can be used to estimate future demand. We have identified the type of sensing information that is required for such a system, and use information-theoretic tools to determine the extent that such information provides information regarding activities within the home. We are now considering the resulting privacy issues, developing means for limiting the extent to which sensitive information leaves the home, while proposing design strategies and policies for the use and maintenance of this information by the power industry and regulatory agencies to protect privacy and security. Finally, we are also considering the various means by which such a system can be attacked, whether by insiders (the homeowners themselves) or external hostile agents. We are using a taxonomy of attacks developed at Berkeley (see below), and are developing a series of means by which such attacks can be mitigated or avoided entirely.

Policy Development – The following are the primary legal and policy issues explored in the sensor network thrust.

- *Camera Networks*: The emphasis thus far in this area has been an exploration of the privacy issues and broader questions about policing and democracy posed by the potential capacity of the state to engage in persistent monitoring of public places. Data about the configurations and use of deployed systems and related policies has been sought for analysis. The ability of current privacy law to respond to the qualitative and quantitative changes in the use of camera networks by the government has been examined and found insufficient. The use of theories considering the relationship between policing and democracy are currently being explored as vehicles to more successfully frame the conversation about the policies that should guide the development, deployment, and use of permanent public video surveillance systems. We have developed impact assessment tools, guidelines, and model legislation to create opportunities for public input into system decisions and substantive policies designed to protect the privacy, associational, expressive, and equality interests of society in camera networks. We are exploring the ability of technology to affirmatively protect privacy or other values in camera networks including technical options for de-identification, abstraction, and triggering that reduce the collection of data in ways that respond to articulated privacy concerns. We are also considering potential attacks on these networks and creating technical counter-measures and design options to diminish the attack surface. This area has included outreach with relevant state and federal agencies as well as localities considering camera networks.
- *Power Grid*: This area is building off work initially conducted under a grant from the California Energy Commission examining the potential privacy and security issues raised by the move to a demand response energy infrastructure in which two way communication between utilities and residences is the norm, data about energy consumption is collected in fifteen to thirty minute increments, and appliances, other

energy consuming devices within the home, and sensors are in communication with programmable, computable thermostats within the home. The security and privacy challenges presented by the in-home sensor networks, the increasingly detailed data flowing out of the home, the introduction of additional players into home energy management, and the ability to remotely control devices within the home are formidable. Our current work focuses on influencing standards, regulations and rules around demand response energy systems to ensure that the heightened ability of detailed energy data to reveal personal in-home activities is addressed. As discussed above understanding the extent to which the increased frequency of energy readings and the information from in-home appliances, devices and sensors alter the privacy concerns around utility records and sensor readings is essential to identifying appropriate policy and technology options. Legal and technical analysis, work with regulators and industry, as well as theoretical exploration of the relationship between in-home sensor networks and existing privacy and computer security statutes and laws are among the contributions in this area.

Specific deliverables from the various Secure Sensor Networks research projects are described below.

Medical Sensing Systems – The emphasis thus far in this thrust area has been on medical sensor devices, sensor platforms, and transport mechanisms. In particular, students and faculty at Berkeley have developed several types of medical sensors including an accelerometer and a highly portable. Vanderbilt has focused on the development of video sensors and Mica2 motes, while Cornell students and faculty have concentrated on transport mechanisms that marry platform QoS requirements to appropriate wireless technologies.

An integrated experiment in which body movement sensors trigger the operation of video sensor has been the basis for our initial privacy-aware sensing efforts. A policy-driven video delivery mechanism has been developed based on this initiative.

Industry and medical center collaboration has already been established, with the most important development being an agreement with Vanderbilt Home Care Services, Inc. to test our technology in a realistic medical environment.

Another important result to emerge from these efforts was a 2007 CyberTrust proposal that included Berkeley, Cornell, and Vanderbilt.

Camera Motes – Research at Berkeley and CMU in collaboration with the Industrial Technology Research Institute (ITRI) in Taiwan resulted in the design of Wireless Camera Motes. The motes include a hardware platform, software programming environment, and a library of computer vision algorithms.

Specific security issues considered include detection mechanisms based on high rate of packet loss and the managing of access permissions specific to video images.

Camera Networks Policy – The work in this area has focused on four areas. First, we are assessing currently deployed camera network systems in use in the public sector domestically, examining the technology and configuration, the policies governing them (where they exist), the motivation for installation, examining the availability of footage through open records laws, and where available the footage itself to understand what they are being used to observe. Second, we have developed a video surveillance system privacy impact assessment tool, based upon

the generic privacy impact assessment tool created by the Department of Homeland Security's privacy office, for use by states and localities considering the use of such systems. We have engaged DHS as well as its external Privacy and Integrity Advisory Board in this work. We are currently exploring opportunities to require the use of the assessment tool by localities receiving federal funds for their creation through grants and contracting requirements. This work is coupled with technical efforts to reduce the privacy concerns around the installation of camera networks, through techniques that obscure the identity of the observed. Third, we have been exploring, through surveys and interviews, public perception of privacy issues raised by government use of camera networks. Finally, we are exploring the use of theories about democracy and policing as a mechanism for framing and highlighting the questions related to cheap, ubiquitous sensor networks (including camera networks) that should be subject to policy development.

This work has led to a project that will commence this summer in which an expanded team of Berkeley researchers will be analyzing the deterrent, investigatory and prosecutorial effects of the existing camera system in San Francisco. This is coupled with a use of our privacy impact assessment team, and surveys of the observed population to understand their knowledge of the camera system and their feelings about proposed advances in the system.

Software Tools – Our software tools effort, based at Cornell, has focused on the building of systems that provide the end user with well-known abstractions for deploying sensor networks and embedded systems. These include two primary products. First, a secure, opportunistic file system for mobile ad-hoc networks (MobOS) has been developed that effectively and securely shares data in the absence of traditional all-to-all wired network infrastructure. Second, a publish/Subscribe system to query sensor nodes from a mobile node (SENSTRAC) has been developed. This system allows users to subscribe to sensor or interest, and sensors to publish sensor readings. The identification of sensors to query changes as the user moves through the area.

Secure Sensing – A taxonomy of wireless sensor network attacks was developed at Berkeley. The taxonomy details threats in terms of the OSI layer and the technology and knowledge available to the attacker. This tool has proven important in our later work on security design, as it allows threat analysts to identify and focus on threats that are specific to a given context.

In related work at Vanderbilt, faculty and students have developed security co-design tools that couple security with the initial design stages of sensor networks. The basis idea is that embedded (a.k.a. cyber-physical) systems must be designed with security considerations in mind. At its core, interactions are established between embedded system properties (response-time, bandwidth, data lifetime) and computer security issues. Co-design then takes the form of interweaving security and para-functional aspects in the design process. Ongoing work is focused on security property verification of design-models and metamodel composition for integrating security modeling into embedded system design languages.

Exemplary Workshops – Several workshops were held to bring together faculty and students from the TRUST partner institutions. The workshops were particularly effective in motivating PhD student exchanges and in developing joint proposals. The workshops are described below.

- A workshop on "Secure Sensor Networks" was held on May 9 - 10, 2006 on the Carnegie Mellon University campus. The event was sponsored by TRUST, the National Science Foundation, and the Army Research Office. Organizers included Adrian Perrig (TRUST/CMU), Karl Levitt (NSF), Radha Poovendran (University of Washington), and

Cliff Wang (ARO). Topics included Data Privacy in Ad hoc Networks, WSN Architecture, WSN Attacks and Security, and WSN Data Routing/Aggregation

- A workshop for TRUST student researchers was held in October 2006, in which leading privacy experts, as well as TRUST faculty, provided feedback and advice on the privacy issues in the students work and identified promising technical research opportunities related to privacy policy.
- A symposium entitled "New Perspectives on Visual Privacy in the 21st century" was held November 3-4, 2006 on the Berkeley campus. The workshop was sponsored by TRUST, the Samuelson Law, Technology, and Public Policy Clinic, the Boalt School of Law, and the Center for Information Technology Research in the Interest of Society (CITRIS). Participants include TRUST faculty; faculty in law, engineering, literature, history, sociology, and geography; and the ACLU.
- A Patient Monitoring Workshop was held at the Vanderbilt Medical Center and ISIS, September 12, 2006, Nashville, TN. Participants included faculty and students from the Vanderbilt Medical School, Cornell, Stanford, and Vanderbilt-ISIS.
- A Privacy and Confidentiality Workshop was held at the Vanderbilt Center for Better Health, September 13-14, 2006, Nashville. Participants included students at faculty from Cornell, Stanford, and Vanderbilt-ISIS.
- A Patient Monitoring Workshop was held on the Berkeley campus December 15, 2006. Participants included faculty and students from Berkeley, Cornell, Vanderbilt, and the University of Illinois at Urbana-Champaign. Topics discussed include the development of a uniform and/or interoperable sensor platform, and integrated experiment scenario, and medical industry collaboration for system deployment and experiment.
- In addition, bi-weekly Modeling Working Group meetings were held on the Vanderbilt campus. Participants include ISIS, Vanderbilt Medical School, and the Vanderbilt Medical Center.

PhD Student Exchanges – Several PhD students have been exchanged between Cornell Vanderbilt, and Berkeley. This effort has resulted in substantial multi-institutional collaboration that is beginning to bear fruit in the form of collaborative publications and proposals. Several conference papers and a journal article have already been accepted (see list of publications elsewhere in this report).

Group Proposals for Additional Funding – Collaborative activity in the Secure Sensor Networks area has led to several proposals in an effort to leverage TRUST funding. In the past year, this includes the following.

- Networking Technology and Systems - Networking of Sensor Systems (Nets-NOSS)
    - Cornell, Berkeley, Smith
- CyberTRUST
    - Illinois, Berkeley, Cornell, Vanderbilt
- Analysis of effectiveness and effects of San Francisco Cameras
    - Expanded Berkeley team
    - Public Sector Policy Development

Publications – Several multi-disciplinary, multi-institutional publications were written in the past year by faculty and students in the TRUST secure sensor networking thrust. They are listed in the publications section of this report.

The general focus in Secure Sensor Networks in the next reporting period will be on increasing the breadth and complexity of ongoing projects through increased cross-layer integration,

bringing together technology, software tools, testbeds, and policy development. There will also be an increased focus on multi-institutional interaction, primarily through PhD student exchanges and additional workshops.

We propose to expand the Cornell sensor networking testbed to serve as a developmental facility for the "on-line" health care facility testbed in Nashville.

We also propose to increase the integration of policy development with that of technology, with a particular focus on power monitoring. The residential power monitoring project will be combined with an opportunity to review data taken by the California Energy Commission. We also propose the development of a novel concept - Respectful, Adaptive Sensing Networks. The basis idea will be to combine an understanding of legal thresholds (provided by TRUST faculty at the Berkeley Law School) with and understanding of current and future sensing capabilities (provided by TRUST faculty at Cornell).

The Security Co-Design project will be enhanced and used as a means to join ongoing efforts. In particular, two ongoing sensor networking design efforts – a Water Supply On-Line Testing Project (Cornell, La Water Authority) and the above Residential Power Monitoring Project (Smith, Cornell, Berkeley) will be used to demonstrate the effectiveness of the co-design tool and enhance project-specific security research. We intend to use the results as the basis for an application toolbox to enhance the education and knowledge transfer roles of the co-design project. In an initial step, Cornell PhD students have been dispatched to Vanderbilt for training with the co-design tool.

2.4.5 Trustworthy Systems

Thrust Leaders: *Alex Aiken (Stanford University, Mike Reiter (Carnegie Mellon University), David Wagner (UC Berkeley)*

The Trustworthy Systems area of the TRUST center encompasses research addressing the full range of issues in trustworthy computing via securing software, securing hardware, and ensuring survivability of critical systems. During this reporting period, Trustworthy System research projects were focused in the following areas:

- Robust Software
- Security Policies
- Platform Integrity
- Intrusion-Tolerant Systems

The activities of each project are discussed in more detail below.

Robust Software – Software robustness is a central problem in the construction of trustworthy systems. These projects address ways to eliminate software vulnerabilities and to better enforce least privilege in software programs. Projects were focused in two areas:

- *Eliminating Software Vulnerabilities*: It is well-known that software errors are the source of numerous vulnerabilities. This area of research seeks to eliminate the errors and/or vulnerabilities through automated means. One project focused on formally verifying a number of properties of a large, real-world software system, the Linux kernel, which together would imply that the system cannot under any circumstances commit a class of undefined behaviors that would result in either a security hole or system crash. These properties include such things as verifying the absence of buffer overruns, null pointer dereferences, use of un-initialized variables, misuse of user/kernel pointers (this one is

specific to Linux), and the absence of certain integer overflows, among others. In contrast to safe C compiler projects (e.g., George Necula's CCured) where the goal is to ensure that any undefined behavior is detected, the goal here was to prove that such errors do not arise in the first place. The same basic techniques could be used, for example, to show that uncaught exceptions do not arise in programs written in safe languages such as Java. A second project in this area focused on applying static and dynamic program analysis tools for error detection to find bugs in important C++ code bases using the Mozilla code base as an example. This project used techniques such as dimensional type systems, tainting analysis, and symbolic execution to identify a range of vulnerability types. Applying these techniques to Mozilla is a compelling demonstration of the ability of these techniques to scale, along with improving the security of a widely used software program. A third project in this area researched methods of automating and performing vulnerability and exploiting analysis and defense in commercial off-the-shelf software, where source-code may not be available. In particular, this effort designed and developed novel techniques by employing program slicing, model checking, and other program analysis techniques to automatically identify whether a potentially vulnerable point can be reachable by un-trusted inputs, and then to automatically generate input-based filters to filter out malicious attacks and hardening mechanisms to protect vulnerable software from malicious incoming attacks. By enabling reachability analysis of un-trusted inputs, this effort can determine whether there exists an un-trusted input capable of exploiting a potential vulnerability in the software, and by automatically identifying the conditions under which a vulnerability can be exploited, this effort can automatically generate input-based filters that can filter out attack packets even for polymorphic worms. A fourth project developed more advanced static and dynamic techniques for finding security vulnerabilities in Java web applications. The project used existing model checking techniques such as Java Pathfinder to design, develop, and evaluate new algorithms and apply them to a large number of open-source Java web applications. The software will be made freely available so others can use the results as well as build upon our work.

- *Enforcing Least Privilege*: A system satisfies the principle of least privilege if it possesses only the permissions it requires to perform its tasks. Unfortunately, today's systems do a poor job of supporting and implementing least privilege. For instance, when you run a mail client program, it inherits the power to read and write all files in your user account; this is far more than the mail client legitimately needs, and it means that an email worm can destroy all your files. One project developed a language, called Joe-E that will be familiar and accessible to programmers but that helps improve least privilege. To make Joe-E accessible, Joe-E is chosen to be a subset of Java. Joe-E builds on prior work on object capabilities (i.e., where a reference to an object represents a capability to affect that object) and the system is built so that this is the only way that code can get any kind of privilege. The goal of Joe-E is to bring object capabilities to a mainstream language, eliminating the need for programmers to learn a new language and thereby reducing barriers to adoption. In addition, Joe-E is intended to enable programmers to reason about the flow of privilege in the program, thereby enabling composition of modules into a larger system without putting security at risk. That is, a key goal is to support modular reasoning, so that a programmer who examines one module in isolation (along with the interface to all other modules that it calls) can reason about the set of privileges available to that module and about the trust relationships it has with other modules.

Security Policies – To a first approximation, a trustworthy system is one that enforces desired security policies, and so security policy research is central to the trustworthy systems agenda.

These projects distill and enforce security policies in a variety of settings. One project uses information flow to derive the access-control policy implemented by a program. Currently, most applications make use of access-control checks spread through out the code. The goal in this project is to develop a tool that aggregates such checks together into an access-control policy that could ease the transition to using a centralized policy. Users could examine the extracted policy and analysis engines could answer queries about it. Such tools could check if the extracted policy matches a specified policy. Even in the absence of a formal specification, change-impact analysis could be possible: given application code before and after edits, one could compare the extracted policies to ensure that no new security holes were introduced. Another project constructs a servlet framework for building web applications that respect explicit information security policies. This technology will close the loop of information flow between the server and the browser by automatically annotating inputs and outputs in the web pages displayed to the user and by using static checking of information flow to ensure that information flows between inputs and outputs do not violate the explicitly expressed information security policies. The user can inspect browser user interface appliances to learn what policies are being enforced on the data. So, for example, a user asked to enter private information such as a social security number can determine how it will be used and the trustworthiness of displayed information can also be assessed. A third project seeks to define, validate, and optimize a unified framework for QoS (including access-control) policy management that enables the predictability and resource control required by information management systems, while preserving the modularity, scalability, and robustness that's the hallmark of Service-Oriented Architecture (SOA) platform technologies. This includes approaches for converting user intent - in conjunction with a static/dynamic runtime environment - into QoS policies and building technologies that (1) enable the decentralized creation of access control policies for distributed resources and (2) exercise that authority efficiently when resources need to be accessed. Finally, a fourth project seeks to ensure that an authenticated user has access to only those services for which he/she has authorization. Web based resources available via Web Services are typically dynamic and distributed in nature and hence require adaptive authorization models that can keep pace with the dynamically changing security requirements of the target enterprise. The goal of this project is to develop an approach aimed at a more generalized and reusable solution which provides the flexibility to handle authorization rule updates in real time.

Platform Integrity – Platform integrity refers to techniques to validate a computing platform or to limit users' dependencies to those properties that can be validated. This includes validating the software platform (or its properties) running on a host (also often referred to as "trusted computing"), or validating that a component encountered in an unfamiliar environment can reasonably be trusted for a limited purpose. One project in this space seeks to build system infrastructure for trustworthy computing spanning basic research in operating systems, cryptography, and distributed systems. This project is centered on the construction of a new operating system called Nexus that will provide new abstractions and mechanisms for trusted computing. The Nexus will provide strong isolation, reduce application TCB, and support the principle of least privilege. It will also provide higher-layer programming abstractions that virtualize the primitives offered by the secure coprocessor. A second component of this project is to integrate privacy-preserving attestation into Nexus. This type of attestation provides the same assurances as traditional hash-based attestation with signatures but without revealing the identities of the hosts and without enabling a third party to link together independent activities performed by a given node. A third component of this effort involves using Nexus to wrap a process inside another, track all inputs to and outputs from the encapsulated process and ensure via active attestation through a reference monitor that the process is behaving correctly (i.e., that outputs are legitimate given the set of inputs). Finally, this project seeks to develop an application-oriented security policy language and enforcement structure to capture higher-level

security policies and ensure that they are correctly mapped to the available primitives. Included in this are uses of attestation in connection with data collection and provenance (e.g., so that data can be reliably "timestamped" upon its collection and its credibility can be evaluated based on what influenced it). A second project in this area focuses on increasing the security of mobile computing environments, focusing on two specific challenges: (1) simple and secure trust establishment in local environments, and (2) execution of un-trusted components in isolated execution environments. The first of these refers to developing techniques to help users identify what components (e.g., base stations, printers) in an unfamiliar environment should be trusted. The second involves mechanisms to limit the effects of using components (and, e.g., the drivers they require) when their trustworthiness cannot be established, using virtualization and isolation technologies. A third project in this area seeks to develop a System-on-a-Programmable-Chip (SoPC) implementation of a trustworthy hardware platform that provides software protection against malicious attacks. With the programmable nature of FPGAs, several techniques can be evaluated in isolation or in combination for tunable levels of security (e.g., watermarking, cryptographic algorithms). The programmability also allows implementation of stronger encryption techniques in future systems. In addition, processor cores from different vendors (e.g., Nios II from Altera, MicroBlaze from Xilinx) are being investigated to evaluate the performance impact of various levels of security. Other tradeoffs being studied are the choice between hard microprocessor cores and soft microprocessor cores and the use of multiple processor cores. This project benefits from collaboration with other TRUST members to provide contextual applications that quantify the security benefits of FPGAs. A fourth project constructs a more robust, secure and flexible operating system by "deconstructing" a modern operating system using micro-kernel principles. Instead of using the traditional approach to micro-kernel construction of designing a small, elegant micro-kernel and constructing an operating system out of multiple protected subsystems, the project starts with a trusted virtual machine monitor capable of running a modern operating system and then rips major subsystems out of the operating system to run in specialized virtual machines on the same platform. The project extracts the OS components responsible for external communication including the file system, networking stacks, and user interface. These changes will result in an architecture similar to a 1980s micro-kernel, but one that is compatible with today's software environments.

Intrusion-Tolerant Systems – "Intrusion tolerance" refers to utilizing cryptography and/or distribution in the implementation of a service so that the service will retain desired properties despite the hostile corruption of components implementing the service. This area is itself very broad, including work in, for example, secure multiparty computation and Byzantine fault-tolerant protocols. These techniques have been used to construct experimental services implementing secure key distribution and certification, secure DNS, secure file systems, and even secure electronic voting systems. Projects were focused in two areas, each described in more detail below.

- *Deployment of Distributed Intrusion-Tolerant Services*: While coordination protocols in the context of intrusion tolerance continue to receive ample attention, other challenges of deploying such protocols have received less attention. One area of work focuses on where to locate the servers implementing a distributed intrusion-tolerant service in a wide-area system. Intrinsic to most coordination protocols is accessing (perhaps subsets of) the servers in the course of issuing requests to the service, and so where these servers are placed can impact the performance or survivability of the service. For example, widely dispersing servers might increase operation latencies as observed by clients, and clustering servers within close proximity to one another might induce significant congestion on links of the network as clients attempt to access them. TRUST collaborations have been helpful for the empirical aspects of this work since TRUST

itself constitutes a wide-area confederation across which intrusion-tolerant services could be deployed. In addition, numerous TRUST faculty have a history of contributions in intrusion-tolerance and scalable protocols. As such, this effort could potentially springboard collaborations across TRUST institutions and support the deployment and use of intrusion-tolerant services among the TRUST institutions.

- *Secure File Systems*: Recent advances in cryptography have opened new doors for securing file systems against attempts to corrupt or steal data by someone who is not authorized with write or read access, respectively. In particular, new broadcast encryption schemes would enable a writer to encrypt a file under each allowed reader's public key, while storing in the file server a ciphertext whose size is independent of the number of readers. Other schemes we have developed provide for the very efficient revocation of a reader's rights, and particularly efficient integrity-checking of file contents. Research in this area includes experimenting with these tools in file system implementations, in an effort to evaluate their impact on performance and security. We believe that this effort can bring these techniques closer to practice and enhance the possibilities to transition them to industry. We also expect this effort to reveal additional gaps in file system security and the performance thereof, which will open new directions for research.

2.5 Research Metrics/Indicators

A key component of the Center research lifecycle is the monitoring and evaluation of individual projects. TRUST projects are both continuously monitored and periodically reviewed to ensure that they support the Center's overall research goals and make progress against the project's research objectives. The evaluation metrics are described below.

- **Scientific Impact** – How significantly does the project contribute to the knowledge base and general understanding of advances in the research area? This impact is typically measured by the number of published papers, presentations in open research conferences, and awards or other recognition for contributions to the research field.
- **Technological Impact** – How well does the project advance the state-of-the-art or state-of-the-practice in the research area? This impact typically is measured by ways in which research results are transitioned to industry, government, or the end-user community and examples where research results have been leveraged by industry in the creation of commercial or open source technologies.
- **Timeliness** – How effectively does the project meet its planned milestones? This is an evaluation of the actual project progress and advancement against planned activities, milestones, and deliverables.
- **Social Impact** – How well does the project contribute in ways that benefit society as a whole? This impact may be measured in terms of how the project research has influenced the development or refinement of public policies, federal, state, and local legislation, and legal decisions.

The TRUST Executive Committee continuously monitors Center research projects. If it seems unlikely that a particular project will meet its planned goals or objective or is not delivering the desired impact in one or more evaluation areas, that project will be ramped down in a period not to exceed six months from the determination of its lack of viability.

2.6 Next Reporting Period Research Plans

The goal of the TRUST center thrusts is to align individual projects into a coordinated research agenda. For the next reporting period (Year 3), TRUST center thrusts build on prior year

achievements and introduce new topics to encourage innovative, novel project ideas from the TRUST research community. The sections below provide a description of the planned TRUST center thrusts. For each center thrust, the name(s) and institution(s) of the lead TRUST faculty member(s) is included.

2.6.1 Education

Thrust Leader: *Kristen Gates (UC Berkeley)*

TRUST education and outreach focuses on the integrating trustworthy technologies, systems, and policy into learning opportunities for a broad range of community participants. TRUST education projects drive curriculum reform and training to teach the next generation of computer scientists, engineers, and social scientist. TRUST education activities are focused at undergraduate, graduate, and community partners. Education is a core value for all TRUST initiatives. As such, the center is continuously looking for innovative ways to (1) enhance curricula, (2) develop teaching and training material that will enable organizations to design, build, and operate trustworthy information systems for critical infrastructure, (3) strengthen partnerships with educational institutions serving under-represented populations, and (4) increase the participation of underrepresented students in undergraduate and graduate research in the field of cybersecurity and trusted systems.

2.6.2 Electronic Medical Records

Thrust Leader: *Janos Sztipanovits (Vanderbilt University)*

Computer technology, patient sensors, and networking are revolutionizing several aspects of healthcare and medical information processing. Small wireless sensors will free many patients from managed care facilities, while providing timely medical assistance when needed. At the other end of the spectrum, virtually all patients will soon gain greater control over their records and treatment options through web portals. The TRUST Electronic Medical Records (EMR) thrust addresses the complex security and privacy issues emerging from the rapidly increasing use of electronic media for the archival and access of patient records. This change is driven and strongly influenced by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. EMR has become an area where technology, public policy and individual interests intersect and conflict, making the development of information systems for EMR archiving and access a very challenging problem. There is clear evidence that without a detailed understanding of the relevant issues on all sides, an acceptable solution cannot and will not emerge.

2.6.3 End User Security

Thrust Leaders: *John Mitchell (Stanford University); Doug Tygar (UC Berkeley)*

This area will look at security problems from the perspective on an end-user, focusing on concerns such as: web browser vulnerabilities, privacy, malware, and forensics. Everyday home computer and Internet users are subject to a broad range of risks and malicious attacks, some based on deception and others exploiting design and implementation flaws in end-user software. Current best practices, such as running a signature-based virus scanner, a firewall, and perhaps anti-phishing tools, are after-the-fact responses to deeper problems. We therefore aim to improve web authentication, improve user awareness of privacy risks, study fundamental underpinnings of next-generation browser security, develop the science of malware detection and mitigation, and improve our ability to understand the status of systems that have been attacked through improved forensic techniques. In all of these areas, the project will aim to identify core scientific questions, develop and evaluate systematic solutions, and consider user interfaces and human factors as well as computer system solutions.

2.6.4 Network Defenses

Thrust Leaders: *Vern Paxson (UC Berkeley), Adrian Perrig (Carnegie Mellon University)*

Computer networks are, arguably, the key technical development of our era. They have enabled us to construct powerful systems of tremendous scope and complexity. But with this scope and complexity they also bring exposures to failures, concurrency-related bugs, poor management, and outright misuse. Modern networks have become exceedingly hard to defend against mishap, whether accidental or deliberate, and this observation has made research into network defense an obvious and central area for investigation by the TRUST center team. TRUST researchers are pursuing a gamut of innovative topics in the area of computer networks, which we classify roughly into the area of "network defense" techniques. The objective of this thrust is to develop new technologies for defending applications against network-level intrusions and attacks and to leverage testbeds with which we can study the behavior of compromised and malfunctioning legacy applications, viruses, worms, and spyware. This thrust will also address the pressing need to develop much more sophisticated ways of leveraging hardware for network security analysis. Since Moore's Law no longer allows us to analyze network traffic using uniprocessors, it is crucial to parallelize such analysis and address the problem in terms of (1) using clusters of commodity PCs, (2) multicore/multi-threaded architectures, (3) lightweight FPGA front-ends, and (4) heavyweight use of FPGAs or ASICs for massive parallelism. In addition to network analysis, this area could include host-based hardware such as "taint checking".

2.6.5 Policy

Thrust Leader: *Deirdre Mulligan (UC Berkeley)*

TRUST's research agenda includes a robust, interdisciplinary policy component. This research is aimed at contributing to the creation of secure, private and trustworthy systems by structuring incentives for research, investment, policies and procedures directed towards privacy and security enhancing technology.

Trustworthy systems are achieved through a mix of component parts, some technical, some procedural, some informed by economics and others by legal obligations. To create secure, private and trustworthy technology and systems requires an understanding of the relationship between the component parts and an active consideration of how one domain interacts with the other. Technology deployment decisions made without an understanding of how the decisions relate to policy, and policy decisions made without an understanding of the existing assumptions of the security architecture often yield problematic results. In the absence of a holistic approach to considering how to embed values in technical systems a range of failure modes appear. Policy makers may not appreciate the dependence of the policy model on a particular feature of a given technological system. Similarly, technologists may not understand the way in which the policy framework disparately supports a value based on seemingly innocuous technological design choices. We seek interdisciplinary research proposals that will help policymakers and technologists create optimal decisions and investments in trustworthy systems. This might include research on how technology investments are made, empirical work on current influences on decision making, the policies and procedures that accompany the technology, and the types of research that informs these decisions and influences the architecture. It might include research on how to leverage technologies to implement policies, and how to structure policies to incentivize research and deployment of trustworthy systems.

In sum, the policy thrust will seek to understand organizational and individual roles in making security and privacy decisions for trustworthy systems, look at the barriers to implementing security and privacy policies, and identify potential policy avenues for achieving better privacy, security and compliance.

2.6.6 Secure Sensor Networks

Thrust Leaders: *Steve Wicker (Cornell University), Deirdre Mulligan (UC Berkeley)*

The TRUST Secure Sensor Networks thrust is focused on the development and use of secure embedded sensor networks in a variety of large-scale applications that are critical to the nation's economy, energy, security, and health. Recent developments in the field of sensor and networking technology have made such networks possible and this initiative drives the further development of the requisite deployment, network configuration, data recovery, and security technologies, while continuing to develop the theoretical foundations for this field. Equally important, the TRUST Secure Networked Embedded Systems initiative also considers the privacy issues arising from the use of sensor networks, and the ways in which embedded sensor networks affect the experience and use of public spaces.

2.6.7 Trustworthy Systems

Thrust Leaders: *Alex Aiken (Stanford University, Mike Reiter (Carnegie Mellon University), David Wagner (UC Berkeley)*

Software robustness is a central problem in the construction of trustworthy systems. Research in this thrust seeks ways to eliminate software vulnerabilities, and to better enforce least privilege in software programs. TRUST projects in this area have focused on (1) eliminating software vulnerabilities, (2) enforcing least privilege, (3) enforcing security policies, (4) ensuring platform integrity, (5) building intrusion-tolerant systems, (6) deploying distributed intrusion-tolerant services, (7) and developing secure file systems. It is envisioned that the Trustworthy Systems thrust will encompass research addressing the full range of issues in trustworthy computing via securing software, securing hardware, and ensuring survivability of critical systems.

3 EDUCATION

3.1 Goals and Objectives

One of the drivers of this Center is the view that concerns regarding security must be consciously engineered into new and legacy critical infrastructure systems, and that to do so requires a rethinking of every component level of the system. To ensure that these concerns are shared and addressed by the next generation of computer scientists, engineers and social scientists, TRUST researchers will incorporate their findings and methods wherever possible into the standard. Thus, this project will result in a broad curriculum reform of existing computer science and engineering courses. We will develop a whole set of courses from the lower division to the advanced graduate level as the research on trust matures.

The center has distinct education constituencies – both undergraduate and graduate programs – for which there are distinct mechanisms for knowledge dissemination. For undergraduates, the center has adopted a two-pronged approach. On the one hand, the center will have activities concerned with diffusing ideas of trustworthiness throughout the entire undergraduate curriculum. On the other hand, the center needs is working towards defining a modern "standard" computer security course at the undergraduate level. For graduate students, the center finds that a series of summer schools on specific disciplines is where a significant impact can be made, in addition, of course, to developing topic specific customized courses. The summer schools are to be 1-week courses, where research leaders provide intensive short courses in areas of current research interest.

Beyond the above partition, the realization that **TRUST solutions = policy options + technology options** requires TRUST to bring together two communities of researchers: *technology* researchers and *policy* researchers. Technology done independent of policy risks irrelevance; policy done independent of the technology risks obsolescence or suppresses options.

From the marriage of policy and technology arises some horizontal partitions in addition to the ones by education level, and the TRUST center will engage the educational community to work towards:

- A broader understanding of TRUST *technology* options as such among (future) *technologists*
- A broader understanding of TRUST *technology* options as such among (future) *policy shapers*
- A broader understanding of TRUST *policy* options as such among (future) *policy shapers*
- A broader understanding of TRUST *policy options* as such among (future) *technologists*.

The center strategy for achieving this broad influence is through a combination of *push* and *pull* tactics: to *generate learning material* (such as learning modules, course syllabi, textbooks, broader curricula), provide *effective dissemination structures* (such as on-line repositories, internet delivery mechanisms, summer schools, center-wide seminar series), and establishing *broad educator communities* (such as summer schools, education conference participation) that engage with the center in adopting and adapting the results of the center to their instructional context.

Specifically, the TRUST Objectives in Research are to establish the following:

a) Learning Technology Infrastructure
b) Undergraduate Programs: generate best-practices material for computer science courses, security modules for other engineering programs and the social sciences, create a signature new undergraduate trusted system course, capstone experience for undergraduates
c) Graduate programs: specialized material for both engineering and policy
d) TRUST Summer Schools for Students, for Industry, for Instructors and for Researchers
e) A recurring and significant presence at key education conferences
f) A series of TRUST domain workshops.

During this past year the center-wide activities in the education area have focused on c, d, e and f with a ramping up of the efforts related to a and b: on establishing the infrastructure for the learning modules repository, and on establishing a set of pilot course modules within this repository, bringing together material from the various TRUST partner institutions in an integrative learning material generation exercise. Summer programs to be offered during 2007 include: SECuR-IT at Stanford, WISE at UC Berkeley, SUPERB-IT at Berkeley, SIPHER at Vanderbilt, and Discovering Sensor Networks at Cornell.

3.2 Performance and Management Indicators

During the second-half of 2007, a compressive review and evaluation of TRUST online learning modules will begin. This review will include subject mater experts, familiar with TRUST

research topics. Currently, a small-scale review is in progress with feedback forthcoming. Comments generated from this pilot evaluation will help formulate evaluation tools and criteria.

3.3 Current and Anticipated Problems

No significant problems were encountered during the reporting period. No significant problems are anticipated in the next reporting period.

3.4 Internal Education Activities

The items below describe in more detail specific education activities of the TRUST Center during this reporting period.

Activity Name	TRUST Academy Online (TAO) Learning Technologies: CAPE and eLMS
Led by	Larry Howard (Vanderbilt)
Intended Audience	Students, Faculty and Industry Professionals
Approx Number of Attendees (if appl.)	Unlimited. Portal and content is open access via the Internet

TRUST is leveraging an existing learning technology infrastructure for the development and online dissemination of its educational materials that was created by the NSF VaNTH Engineering Research Center for Bioengineering Educational Technologies (http://www.vanth.org). This infrastructure has three principal components:

- A web-based dissemination portal/content management system
- A repository-based authoring technology for adaptive web-based courseware (CAPE)
- An online learning platform (eLMS)

The dissemination portal is based on an open source content management system (Plone, http://www.plone.org) that has been adapted for educational materials.

The CAPE and eLMS technologies primarily address online learning in blended learning environments. CAPE can additionally be used for curriculum modeling, where the elements can be classroom-based, online, or blended. Online courseware authored with CAPE is delivered to learners using the eLMS learning platform. This standards-based platform can be used directly, or it can be used as a service from campus learning platforms such as Blackboard, WebCT, or Moodle.

CAPE is used to design online learning experiences involving static, interactive, and dynamic content elements created with conventional web authoring tools and within CAPE itself. The designs specify when, or under what circumstances, content elements are presented to a learner during the course of a learning experience. Interactive elements can elicit information from a learner, and the outcomes are available immediately to adaptations incorporated into designs. A data modeling facility enables capturing facts, including data defined abstractly by expression, for use in realizing adaptation schemes. Simple sequencing constructs can be extended with computational components for more advanced reasoning.

CAPE supports both elaborative (top-down) and integrative (bottom-up) approaches to design. Rapid prototyping of adaptation schemes can be performed prior to content development. Existing content and design elements can be readily incorporated into new designs. The environment supports design-time adaptation by providing abstraction facilities that can be used to capture invariants among families of designs and elements as

instructional design patterns. While CAPE—as a general-purpose design tool—is pedagogically neutral, these design abstractions can be used to scaffold particular learning strategies that can then be shared with other authors through an integrated web-based design repository.

CAPE is built on open source technologies from ISIS—particularly, the Generic Modeling Environment (GME) and Meta-GME—and uses the open source Python dynamic programming language for realizing its extension components and for computational aspects of CAPE designs.

eLMS Learning Platform

eLMS is an adaptive learning platform that supports interoperation using web services, both in conjunction with enacting courseware designs and in managing domain-specific objects, such as classes, users, and courseware.

The platform automatically captures detailed instrumentation of these design enactments, and additional instrumentation—to support grading using custom rubrics, for example—can be incorporated into courseware designs with CAPE. The resulting delivery records can be queried by instructors and authors using an integrated data mining facility. These capabilities enable an intimate understanding of what learners actually do with on-line learning experiences, which is essential to making incremental improvements over time.

While eLMS can be employed directly to manage the use of CAPE-authored designs by classes of learners, it can also be transparently embedded into other learning platforms, such as WebCT, as well as non-commercial platforms, such as Moodle and (eventually) Sakai.

eLMS is built on open source technologies, including the Zope web application server and Apache, and is deployed on the secure open source OpenBSD operating system.

Activity Name	TRUST Academy Online (TAO)
Led by	Larry Howard (Vanderbilt)
Intended Audience	Undergraduate students in Computer Science
Approx Number of Attendees (if appl.)	Not applicable: Pilot Study

Undergraduate Programs: Generate best-practice materials for computing science courses, security modules for other engineering programs and the social sciences, create a significant new undergraduate trusted systems course, capstone experience for undergraduates.

In preparation for the use of these learning technologies and the dissemination portal, during the period under review we have undertaken a set of pilot projects to better understand how to effectively employ the infrastructure and to determine what adaptations might be needed to the technologies themselves.

The objective was also to collect material and establish a set of learning modules for each of three domains – *Network Security*, *Computer Security*, and *Chemical Network Plant Security* – and to use the VaNTH repository and the CAPE system to organize the material into a form suitable for re-use and easy adaptability into new course architectures.

The material was collected from across the TRUST partners, organized by personnel at Vanderbilt, San Jose State and Stanford, and collected into the VaNTH system.

For the Network Security collection Yuan Xue (Vanderbilt) and Xiao Su (San Jose State) drew upon material from Vanderbilt (CS291 Network Security), San Jose State (CmpE 209 Network Security) and Stanford (CS259 Security Protocols).

For these courses, we were interested in similarities and differences in terms of sequencing and course content (concepts taught). We were also interested in granularity and the extent to which elements of these courses could be offered to other instructors in units called modules, or in sequences of modules called *mosaics*. To conduct these investigations, the courses (in whole or part) were modeled using the CAPE environment. The representations capture how the course was organized into units and how these units were sequenced. Learning objectives for the units were expressed and a common curricular taxonomy developed by Yuan Xue was used to indicate the mapping of subjects to units. Finally, companion resources (typically, lecture notes) were associated with the units. These design representations were shared among the authors using the CAPE Repository.

For the Computer Security set Weider Yu (San Jose State) and Simon Shim (San Jose State) brought together materials from UC Berkeley (CS161 Computer Security, CS276 Cryptography) and Stanford (CS155 Computer and Network Security) for a similar exercise.

In addition to understanding the design of these courses and their relationships, we were also interested in the ability to generate information for the dissemination portal from these formal representations. We used CAPE to create a content generation wizard that assembled information about the course units using their structure, metadata, and taxonomic descriptions.

An additional pilot investigation was conducted of creating online courseware. An interesting dimension of this investigation concerned adapting concepts from information system security for teaching security in another domain: chemical plant security. This pilot is a collaboration between Ken Debelak of Chemical Engineering, Yuan Xue and Janos Sztipanovits of EECS, and Larry Howard of ISIS at Vanderbilt. The concept for the project is to use role-based access control as a design and analysis approach to teach security concepts in a chemical process engineering capstone design course.

These pilot efforts have informed our thinking about adapting VaNTH's dissemination platform for the new TRUST Academy Online (TAO). In particular, TRUST presents issues of varying granularity that were less important to VaNTH. The pilots have also influenced changes to the CAPE authoring environment to support direct publishing to the dissemination portal.

The partners in the center are developing rich new material for courses offered locally and that will be prepared for broader systematic dissemination. The course material ranges from first year experience courses such as the first year experience course at Stanford (CS55N Ten Ideas in Computer Security and Cryptography), through more directly systems- or technically oriented courses such as *System Security* (Cornell), *Fault-tolerant Distributed Computer Systems* (Cornell), *Secure Software Systems* (Carnegie Mellon), *Secure Technologies* (San Jose State) to more policy oriented courses such as *ID-Theft* (Stanford) and *Public Policy for Engineers* (UC Berkeley).

Activity Name	Fast-Track Modules
Led by	Kristen Gates (UC Berkeley)
Intended Audience	TRUST portal users: students, faculty and Industry Professionals
Approx Number of Attendees (if appl.)	N/A

The TRUST Academy Online (TAO) is an online repository for TRUST Learning Modules. Accessible by the public, the TAO contains leading-edge learning materials available at no cost. By using these modules, educators have access to leading-edge research and teaching materials specific to trusted systems technology and policy issues.

Learning modules were created for each of the TRUST research trust. The modules were given the project title "Fast-Track" to emphasis to TRUST faculty that these modules were to show-case topics associated with the centers research thrust: Electronic Medical Records, ID Theft, Sensor Networks, Network Defense and Trusted Systems. The format for the Fast-Track modules was a self-standing short-course content (one to four hours) that reflected current research conducted by the centers' faculty. The purpose of the module was to create learning materials that would be placed on the TAO portal and used by teaching faculty as course content, lecture material, support materials for a computer science course.

Our initial goal was to have **five** Fast-Track modules online at the start of 2007; the actual number completed was **seven**. The modules represent a variety of learning materials and include: PowerPoint slide decks, lecture notes, case studies, assignments, related web site links and video clips. This first round of modules is under a preliminary review by several subject matter experts. Once feedback from this initial review has been received, assessment and evaluations tools with user tracking will be put into place. The TAO portal currently has an inventory of 17 items; including the seven Fast-Track modules, learning objects, and materials generated by TRUST faculty, workshops and symposiums.

Activity Name	Women's Institute in Summer Enrichment (WISE)
Led by	Kristen Gates (UC Berkeley), Ruzena Bajcsy (UC Berkeley)
Intended Audience	Graduate students, post-doctoral fellows, and professors from all disciplines that are interested in Ubiquitous Secure Technology and the social, political, and economical ramifications that are associated with this technology. Focused recruitment effort toward underrepresented minority groups and women.
Approx Number of Attendees (if appl.)	30 participants with 11 speakers

WISE is a 1-week residential summer program on the University of California, Berkeley campus that brings together graduate students, post-doctoral fellows, and professors from all disciplines that are interested in Ubiquitous Secure Technology and the social, political, and economical ramifications that are associated with this technology. This year's program is scheduled for June 10-15, 2007.

Summer 2007, the program topic is sensor networks with a healthcare and policy emphasis and the topics may include but are not limited to:

- Sensor Networks within healthcare
- Radio Frequency Identification
- Electronic Medical Records

- Privacy enhancing software
- Networks and policy Rights
- Responsibilities associated with data, data owners and data users

WISE 2007 Seminar Speakers are:

- Terry Benzel, USC – Information Science Institute
- Ruzena Bajcsy, UC Berkeley – TRUST
- Deborah Estrin, UCLA – Center for Network Sensing
- Stephanie Forrest, University of New Mexico
- Jennifer Hou, University of Illinois
- Maryanne McCormick, UC Berkeley – TRUST
- Deirdre Mulligan, UC Berkeley – TRUST
- Priya Narasimhan, Carnegie Mellon University
- Diana Smetters, Palo Alto Research Center (PARC)
- Dawn Song, Carnegie Mellon University – TRUST
- Yuan Xue, Vanderbilt University – TRUST

Tuition for WISE 2007 is $2,500; however, NSF-TRUST fellowships are available to US professors, post-doctoral fellows, and Ph.D. candidates studying at US universities. There is a maximum of 20 fellowships with travel stipend.

WISE participation is open to US professors and post-doctoral fellows, and Ph.D. candidates studying at US universities. Participation is limited to 30 people and will be selected from a nationwide pool of applicants, who have demonstrated, outstanding academic talent. The WISE target audience is underrepresented minority groups and women in information technology.

Learning and presentation materials will be cataloged on the TAO portal for future reference.

New to the WISE 2007 format will be the addition of a panel discussion at the Richard Tapia Celebration of Diversity in Computing in October 2007. This panel will include graduate students, post docs and junior faculty from both 2006 and 2007 WISE programs. Participants in this panel discussion will be asked to reflect on WISE program activities and their current progress at meeting their professional and career development goals in the sciences.

Program Evaluation: Each WISE fellow will complete a program evaluation. WISE participants will also be tacked over a one-year period to evaluate the programs impact on educational, professional development, job placement and retention.

This is the second-year WISE has been hosted at the UC Berkeley campus; WISE 2008 will be hosted by Cornell University. An evaluation of first-year WISE participants was conducted with a follow-up survey scheduled for years one, three and five. Recommendations from the 2006 survey were put into place for the 2007 program. The WISE 2007 cohort will be surveyed at the end of the program and at years one, three and five. Tracking of WISE cohorts will determine if participants leveraged workshop information into their professional and career development goals. For example, they will be asked if they initiated a course or research activity, incorporated research ideas from the workshop, initiated collaboration with WISE speakers, and or maintained contact with the network of participants.

Activity Name	Summer Program for Smith Undergraduates: Discovering Sensor Networking
Led by	Stephen Wicker (Cornell), Judith Cardell (Smith)
Intended Audience	Undergraduate students from Smith College
Approx Number of Attendees (if appl.)	20 Students and 10 presenters

Smith undergraduate engineering students will have the opportunity to participate in a three-day summer program to be hosted by Cornell University and the TRUST Center July 9-13, 2007. Dormitory space in a secure and comfortable setting will be provided on the Cornell campus. Local arrangements will be subsidized by the TRUST Center. This program will consist of three basic elements:

- Learning Module: Prominent researchers from universities in the northeast will give tutorials on telecommunications, networking, and the growing role of sensor technology in industry and national defense. Several of the speakers will be women faculty, giving Smith students an opportunity to meet and talk with successful women in engineering academia.

- Discovery Module: Students will engage in hands-on experiments with sensors and wireless sensor platforms. With the aid of Cornell graduate students, they will develop a system for remotely monitoring power consumption in a home environment. The discovery module is tied to an active research topic, giving students an opportunity to participate in a real research project.

- Graduate Experience Module: Participants will have the opportunity to tour research laboratories on the Cornell campus, and to meet and talk with graduate students. Tours will also be provided of the Cornell campus, and a graduate admissions office of the Cornell College of Engineering will host an information session.

Program Evaluation: The students will evaluate the program at the end of the program, using a questionnaire. The results of this survey are distributed to participating faculty and graduate students and used as feedback for program development. Discovering Sensor Networking participants will be tacked overtime to identify those students considering graduate school and those that have been accepted into graduate school programs.

Activity Name	Summer Internship Program in Hybrid and Embedded Systems Research (SIPHER)
Led by	Gabor Karsai (Vanderbilt)
Intended Audience	Undergraduate students, underrepresented minority groups and women
Approx Number of Attendees (if appl.)	10

SIPHER is Summer Internship Program for Hybrid and Embedded System Research, funded under the NSF large ITR project titled Foundations of Hybrid and Embedded Systems (Berkeley is the lead). The research aims at laying the scientific and technological foundations of embedded system design. Embedded computing systems are present in all traits of modern society: in cars and airplanes, in cell phones, in household devices, in medical devices, just to name a few. This is a multi-year research project that builds the

science: the principles and the math, and the technology: the tools that the next generation of engineers will use to build these systems in the future, better than ever before.

SIPHER students work in teams and are mentored by senior graduate students, who are in turn supervised by TRUST faculty member Gabor Karsai. Program faculty participate in the student selection, midterm, and program end reviews of the student projects. TRUST students worked on security analysis of software and hardware systems topics. In 2006, TRUST provided faculty support and additional funding for security research topics and two TRUST students.

The objective of this program is to enable undergraduates from underrepresented groups (women of any race, and also Native-Americans, African-Americans, and Hispanics) to participate in a research program, receive training in the science and technology developed by researchers, and work on specific research problems. The program will be coordinated with UC Berkeley, and joint teleconferences are expected.

The SIPHER program runs for 10 weeks each summer, with this year's program scheduled for May 29 – August 3, 207. There are seven positions available, with a $6,000 stipend for the period. This year, the participants will be partly funded by the Tennessee Louis Stokes Alliance for Minority Participation (TLSAMP) project (supported by NSF).

Program Evaluation: The students are evaluated at midterm and at the end. They also report on their progress at the regular weekly meetings. They receive feedback on their work at the weekly meetings and after the midterm from the faculty advisors.

The students evaluate the program at the end of the program, using a questionnaire. The results of this survey are distributed to participating faculty and graduate students and used as feedback for program development.

SIPHER participants are tacked overtime to identify those students considering graduate school and those that have been accepted into graduate school programs.

Activity Name	Summer Undergraduate Program in Engineering Research at Berkeley-Information Technology (SUPERB-IT)
Led by	Shankar Sastry (UC Berkeley)
Intended Audience	Undergraduate students, underrepresented minority groups and women
Approx Number of Attendees (if appl.)	6

The Summer Undergraduate Program in Engineering Research at Berkeley - Information Technology (SUPERB-IT) in the Electrical Engineering and Computer Sciences (EECS) Department offers a group of talented undergraduate engineering students the opportunity to gain research experience. The program's objective is to provide research opportunities in engineering to students who have been historically underrepresented in the field for reasons of social, cultural, educational, or economic barriers by affirming students' motivation for graduate study and strengthening their qualifications. The program provides students with the opportunity to gain research experience by participating in research projects with engineering faculty and graduate students. Upon completion of this program students will be better prepared and motivated to attend graduate school.

Students work with graduate student mentors throughout the summer performing research and supporting activities in the area of information technology and TRUST related topics. Past TRUST research topics have included:

- Design of a Distributed Tracking System for Camera Networks
- Camera Networks and Computer Vision
- Time Synchronization Security in Sensor Networks
- Implementation of an Electronic Medical Record System
- Analysis of Wireless Connectivity in Sensor Network Deployments.

The SUPER-IT program is a nine week program, with this year's program scheduled for June 10 – August 3, 2007. In 2006, SUPERB-IT had six students participating in TRUST related research topics. For 2007, six students have been accepted. Each student is given a $3,750 stipend for the period, travel allowance, and provided on-campus housing. In addition to the undergraduate research experience, SUPERB-IT students participate in educational activities including lab tours and industry field trips. Graduate school advising and subsidized GRE prep course is also included.

Program Evaluation: The students are evaluated at midterm and at the end. They also report on their progress at the regular weekly meetings. They receive feedback on their work at the weekly meetings and after the midterm from the faculty advisors.

The students evaluate the program at the end of the program, using a questionnaire. The results of this survey are distributed to participating faculty and graduate students and used as feedback for program development.

SUPERB-IT participants are tacked overtime to identify those students considering graduate school and those that have been accepted into graduate school programs.

Activity Name	Summer Experience, Colloquium and Research in Information Technology (SECuR-IT)
Led by	Kristen Gates (UC Berkeley), Sigurd Meldal (San Jose State)
Intended Audience	Graduate level (MS & Ph.D.) students in computer science
Approx Number of Attendees (if appl.)	20

SECuR-IT is a ten-week residential program with paid internship co-located at Stanford and San Jose State. This year's program is scheduled form June 3 – August 10, 2007.

SECuR-IT is a Graduate Student Academic Immersion with Internship Program. In addition to working with an industry mentor over the ten-week program, scholars participate in the following 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, UC Berkeley, and San Jose Sate
- Informal social gatherings that provide a relaxed setting for students and faculty to exchange ideas and share experiences
- Residential housing at San Jose State
- Ten week, paid 40-hour per week internship.

Graduate student internship opportunities available in: Security Architecture, Security Awareness and Security Management, Host and OS Security, Application Security, Network Security, Secure Software Engineering, Risk Management, and Policy and Legal Compliance. A partial list of participating TRUST industry partners supporting this program is: Intel Corporation, Sun Microsystems, Symantec Corporation, Visa International, Yahoo, and Xilinx.

This is a 40-hour per week obligation to internship, research, and learning activities. Students who participate in SECUR-IT should view this program as a full-time summer experience and are required to participate in San Jose State residential cohort, attend courses, and be employed as an intern by a participating SECuR-IT industry partner. Internships are paid employment and student housing at San Jose State has been set-aside for this program, but housing cost is the responsibility of the student participant.

Learning materials generated by this program will be placed on the TAO portal.

Program Evaluation: Each student will complete a pre and post program evaluation. SECuR-IT participants will also be tacked over a one-year period to evaluate the programs impact on educational, professional development, and job placement. Industry partners and mentors will also be evaluated as to the programs' structure, effectiveness, and means for improvement. The number of new hires resulting from this program will also be tracked.

3.5 Professional Development Activities

TRUST students are active in a number of professional development activities within the domains of computer science, information technology, law and social policy as well as additional activities such as internships, entrepreneurial business course, career preparation workshops and professional societies.

TRUST students have participated in the following business development courses and internship programs:

- The Entrepreneurial Business of Software, UC Berkeley
- Presenting Data and Information One-Day course taught by Edward Tufte
- Professional Speaking and Negotiation, Carnegie Mellon University
- Internship at Google as a member of the application security team.

TRUST students have membership in:

- IEEE: Institute of Electrical and Electronics Engineers
- WICSE: Women in Computer Science and Electrical Engineering
- HKN: Eta Kappa Nu National Electrical Engineering honor society
- California State Bar.

TRUST students have participated in number workshops, conferences and symposiums:

- Information Processing in Sensor Networks (IPSN 2006), Nashville, TN
- ACM Conference on Embedded Networked Sensor Systems, Boulder, CO
- Grace Hopper Celebration of Women in Computing 2006, San Diego, CA
- RTAS 2006: IEEE Real-Time and Embedded Technology and Applications Symposium, San Jose, CA
- Collaboration on model driven design and security codesign, Technical University in Munich

- Privacy and Confidentiality Workshop, The eHealth Initiative and the Vanderbilt Center for Better Health, Nashville, TN
- The Workshop on the Economics of Securing the Information Infrastructure, Washington, DC
- Conference on Innovative Data Systems Research, Asilomar, CA
- IEEE Symposium on Reliable Distributed Systems (SRDS 2006), Leeds, UK
- Privacy Implications of Trustworthy Information Systems Workshop, Berkeley Center for Law and Technology, University of California; Berkeley, CA
- EEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS), Tucson, AZ
- DIMACS Workshop on Information Security Economics, Newark, NJ
- Usable Security (USEC'07), Trinidad/Tobago
- Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA
- Technology, Management, and Policy Graduate Consortium, Lisbon, Portugal
- Asia-Pacific Economic Cooperation Telecommunications & Information Working Group meeting (APECTEL 33), Calgary, Canada
- IEEE International Workshop on Software Patterns: Addressing Challenges (SPAC 2007), Beijing, China
- IEEE Symposium on Security and Privacy, Oakland, CA
- IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Niagara-Falls, Buffalo-NY
- TAMI/Portia Workshop on Privacy and Accountability, Cambridge MA
- IEEE Symposium on Logic in Computer Science (LICS 2006), Seattle, WA
- ACM Computer and Communications Security, Alexandria, VA

The TRUST Center provides a unique opportunity for a wide range of cybersecurity issues to be addressed from many points of view—technological, scientific, social, policy, and legal. The diversity academic and professional interests by TRUST students is a major contribution to the Center's success. TRUST students have a wide range of academic and professional interests reflected by the attended conferences, supported workshop, personal development courses, and social and professional memberships. Professional development activities support student development of cross-domain and multi-domain knowledge, professional development, student success, and retention–all of which benefit TRUST and the student learning experience and impact provided by the Center.

3.6 External Education Activities

The items below describe in more detail specific external education activities of the TRUST Center during this reporting period.

Activity Name	Trustworthy Interfaces for Passwords and Personal Information (TIPPI)
Led by	Dan Boneh (Stanford)
Intended Audience	Academics and Industry Professionals
Approx Number of Attendees (if appl.)	85

The purpose of the workshop is to facilitate an effective solution to these problems by bringing together the designers of the cryptographic protocols with the implementers of the user interfaces. TIPPI is in its third year with this year's workshop scheduled for June 22, 2007 at Stanford University. TIPPI brings together academic researchers and industry

personnel in a forum for sharing ideas. The TRUST Center benefits from the workshop outputs in the forms of research papers and presentations and modules for the TRUST Portal.

Ideally, a user should have confidence that when she provides a password or other personal information, she can trust the interface she interacts with to protect her data from misuse - even if an attacker happens to be the one that asked her to provide it. The hope is that this workshop will motivate a trend where trustworthy interfaces for passwords and personal information - TIPPI - are the typical ones in our industry.

In the first two years of this workshop, researchers have shared many different ideas about how to improve the situation with user interfaces for authentication, and industry efforts are starting to move along toward implementing some of them. We look forward to further reports both from the research community and developers on new ideas as well as progress in the field.

Activity Name	Unblinking: New Perspectives on Visual Privacy in the 21st Century
Led by	Deirdre Mulligan (UC Berkeley), Pam Samuelson (UC Berkeley)
Intended Audience	Academics, Industry Professionals and Students
Approx Number of Attendees (if appl.)	45

Privacy is a complex and often abstract topic. This two-day, cross-disciplinary symposium was held at UC Berkeley November 3-4, 2006. It addressed "visual privacy," a subset of the much broader topic of data privacy, and brought together experts from a range of perspectives: art, law, engineering, public policy, psychology, architecture, urban planning, sociology, human rights, and others and included both academic and industry participants.

This symposium explored issues in a single track format. To ground the discussions, each submitted paper was paired with at least one specific image selected from the symposium web site or of the authors choosing. Presenting authors initiated each presentation in the context of this image, and the images will appear with each article in a published volume. Presenters were encouraged to draw images from a wide range of contexts: Rodney King news photographs, Hitchcock's Rear Window, video, webcams, paintings, Bentham's diagrams, Cinema Verite reality television, home security, etc.

The TRUST Center benefited from the workshop outputs in the forms of research papers and presentations, modules for the TRUST Portal, and the program’s web-based Wiki.

Activity Name	Berkeley Foundation for Opportunities in Information Technology (BFOIT)
Led by	Orpheus Crutchfield, Executive Director
Intended Audience	Middle school and high school students
Approx Number of Attendees (if appl.)	24

BFOIT is a non-profit organization that supports historically underrepresented ethnic minorities and women in their desire to become leaders in the fields of computer science, engineering and information technology. The intent is to provide youth with knowledge, resources, practical programming skills and guidance in their pursuit of higher education and

production of technology. Classes include general offerings and labs in IT to both middle-school and high school students.

TRUST supports the BFOIT Summer Institute for Future Computer Scientists program to be held at UC Berkeley August 6 – 17, 2007. One direct impact of this support is during the summer 2007, a former BFOIT alumni was accepted into the SUPERB-IT summer program at UC Berkeley.

Activity Name	Silicon Valley Industry Computer Security Curriculum Group
Led by	John Mitchell (Stanford)
Intended Audience	Chief Security Officers (CSOs) of computer security technology companies
Approx Number of Attendees (if appl.)	12

The industry-backed *Computer Security Curriculum* is a document created by the Industry/Academic work group. The group meets on a monthly basis with representatives from Silicon Valley industries, Stanford University, UC Berkeley, San Jose State University, and the TRUST Center.

The *Computer Security Curriculum* document outlines a plan for an industry-backed computer security curriculum and collects the contributions received so far from academic and industrial contributors. A salient feature of the developing recommendations is that while the focus began with computer security, additional topics such as risk management, legal issues, and regulatory compliance are considered essential knowledge areas for computer security professionals. Our goal with this document is not to formulate an entire curriculum constituting a degree program, but to collect input from industrial contributors and present those curricular recommendations in the form of teaching units that can be adopted and added to existing programs.

Activity Name	Computer Security Distinguished Speakers Series
Led by	Kristen Gates (Berkeley), Robert Rodriguez (Stanford)
Intended Audience	Chief Security Officers (CSOs) of computer security technology companies
Approx Number of Attendees (if appl.)	75 + unlimited viewing via Web access

The Computer Security Distinguished Speakers Series is a monthly event alternating between Stanford University and UC Berkeley. Presentations will have a live audience with Web streaming over the Internet and will be archived on the TRUST portal for additional viewing.

The Computer Security Distinguished Speakers Series will showcase leading industry and academic figures in computer security. These distinguished speakers are chief security officers (CSO) and chief information security officers (CISO) of technology companies, financial services companies, and health care organizations as well as leading academics and scholars in this field.

The inaugural Computer Security Distinguished Speakers Series event will take place in Fall 2007 at the Hover institute on the Stanford University campus. The distinguished speaker will be Mary Ann Davidson of Oracle. The series will alternate between Stanford and UC

Berkeley and later will travel to the Cornell, Vanderbilt, Carnegie Mellon, and Smith campuses.

Activity Name	Information Assurance Capacity Symposium
Led by	Sigurd Meldal (San Jose State University)
Intended Audience	Participants of the 2006 and 2005 IACBP at CMU
Approx Number of Attendees (if appl.)	19

Information Assurance Capacity Symposium is outreach to Hispanic Serving Institution (HSI) and Historically Black College and University (HBCU) faculty members, to work with them to introduce and strengthen the Information Assurance components of their curriculum. Participants first attend a one-month summer school at Carnegie Mellon followed by a symposium at San Jose State the next summer. This year's summer symposium is scheduled for June 14-15, 2007 and all participants in the 2006 and 2005 summer schools are invited.

The symposium will (1) showcase the participants' achievements after the summer school, (2) further update their expertise, and (3) bring them into closer touch with industry.

3.7 Activities to Integrate Research and Education

Education deliverables were tied to all TRUST research, education and outreach projects. Learning materials and modules were distilled from the TRUST research trust and archived on the TRUST Academy Online TAO portal. Workshops and symposiums such as TIPPI and UnBlinking were available via the TAO portal. During WISE 2006, several TRUST speakers included TRUST research topics and module content as presentation material. WISE 2007 will archive presentations to the TAO portal. The summer program, Discovering Sensor Networks, will use TRUST research topics with learning modules as the course theme. SUPERB-IT and SIPHER have students working on TRUST research topics. The SECuR-IT summer immersion program with internship contains a computer security focused curriculum and SECuR-IT seminars will feature TRUST faculty from UC Berkeley, Stanford, and San Jose State presenting topics directly related to TRUST center research and activities.

3.8 Education Metrics/Indicators

The items below describe how the Center is doing with respect to the education metrics and indicators and data that have been collected during this reporting period. Information is provided for both Learning Materials and Technology and Workshops and Symposiums.

Learning Materials and Technology

With respect to Learning Materials and Modules on the TAO Portal, the Center met and exceeded its February 2007 project goal of five modules. Currently, we have 17 Learning Modules on the TAO portal.

Workshop and Symposiums

Trustworthy Interfaces for Passwords and Personal Information (TIPPI) has an expected attendance of 85 academic and industry professionals. Topic will continue on the subject of trustworthy systems. 2006 workshop materials have been placed on the TAO portal.

The November 2006 UnBlinking symposium had an attendance of 45 participants. UnBlinking has created a community of scholars and practitioners that continue the dialog of privacy and

social issues via the program Wiki (a website that allows visitors to add, remove, and edit content). Symposium Learning Modules have been placed on the TAO portal.

The Information Assurance Capacity Building Program (IACBP) at Carnegie Mellon will again have participation by TRUST faculty and the Information Assurance Capacity Symposium (IACS) at San Jose State is outreach and follow-up to the 2005 and 2006 Information Assurance Capacity Building Program cohort. The summer 2007 IACS program will generate learning modules that will be placed into the TAO portal.

The Education Community Development (ECD) continues to grow. The ECD is community of educators that utilize and contribute to Trusted system topics. This includes TRUST-developed learning modules and courseware. For example, the San Jose State course *The Digital World and Society* created by TRUST faculty is currently under evaluation for possible adoption as a university-wide general education course. TRUST faculty and staff have participated at education oriented conferences through panels, associated workshops or a series of presentations, including: Frontiers in Education, Learning 2006, Computer Alliance for Hispanic Serving Institutions, Silicon Valley Crime Task Force Meeting, and the Department of Homeland Security SRI International Identity Theft Technology Council.

Summer Programs SUPERB-IT and SIPHER are undergraduate research experiences. The student research and projects support the centers research thrust and goals. Both SUPERB-IT and SIPHER have supported the Center's goal of increasing the number of underrepresented minority groups and women that are conducting research in Trusted systems research.

3.9 Next Reporting Period Education Plans

The education initiatives detailed in this document will continue into the next reporting period. No major changes in the direction are anticipated but the level of activity will increase.

The Trust Academy Online will continue to develop. Course modules and learning objects will be developed as educational deliverables of each TRUST research trust. As the review process continues, refinement will be made to the module design and the portal.

TRUST Summer Programs will continue at UC Berkeley, Vanderbilt, and Cornell. TIPPI is expected to have a fourth workshop in 2008 and initial plans are underway for a second UnBlinking Symposium.

TRUST visibility and influence in Education Community Development is continuing to grow as TRUST participation in educational conferences, workshops, panel discussions, and Silicon Valley Industry Group activities take hold.

The Information Assurance Capacity Symposium at San Jose Sate has NSF funding through 2008.

The Silicon Valley Industry Group will continue to meet in 2007 and is expected to grow in industry participation. The SECuR-IT summer program has created a great deal of interest among CSOs of Silicon Valley computer security companies and we expect to expand the SECuR-IT program from 20 graduate students in the summer of 2007 to 40 graduate students for the summer of 2008.

There are three education initiatives that are new or under development:

- **Computer Security Distinguished Speakers Series**: The Computer Security Distinguished Speakers Series will begin in the fall of 2007. This will be a monthly series traveling to TRUST partner campuses. This program will build the TRUST brand in security and provide industry outreach and professional development while bringing people to the TRUST portal. Modules and webcasts from the series will be placed on the TAO for future access.

- **TRUST/CSU Curriculum Design**: This is a two-phase program that will partner with computer science programs at five of the California State University (CSU) campuses: San Francisco State University, CSU East Bay, CSU Sonoma, CSU Sacramento, and CSU Monterey Bay. For Phase 1, faculty from each of the five campuses will be supported over the summer 2007 by TRUST funding to redesign a computer science course within their program offerings integrating TRUST security-related topics. Five CSU faculty will participate in this program. The five faculty will meet twice with TRUST faculty over the summer in a workshop format. The final product of the workshops will be a revised computer science course containing computer security topics appropriate to the course and CS program. For Phase 2, the project faculty will deliver their revised computer science course in the fall 2007 at their respective campuses. The revised and redesign computer courses will be placed on the TAO for access by other computer science faculty. Deliverables for this initiative are: revised/redesigned computer science courses, teaching the course in the fall 2007, teaching evaluations, and a two-page white paper to be presented at the Frontiers in Education 2008 conference.

- **EL Alliance**: The Empowering Leadership: Computing Scholars of Tomorrow Alliance (EL Alliance) goal is to increase retention of minority undergraduate students from freshmen year through the Ph.D. at tier one research universities. The program is in the initial planning stages (March 13-15, 2007 kickoff meeting) thus program details are not yet available. Program leadership is provided by Richard Tapia of Rice University, Roscoe Giles of Boston University, Ruzena Bajcsy of the University of California, Berkeley, and Cynthia Lanius of Drexel University.

4 KNOWLEDGE TRANSFER

4.1 Goals and Objectives

The Center's knowledge transfer goal is to establish TRUST as a true public private partnership—namely a trusted intermediary between industry, government, infrastructure stake holders, and academia.

TRUST knowledge transfer objectives are to: (1) develop strong liaison with the concerns of industry and with infrastructure stakeholders; (2) produce legislative and legal policy papers and amicus briefs; (3) leverage testbeds for demonstrating Center research project results; (4) enabling student internships and supporting entrepreneurial clubs; and (5) convening meetings, summits, and workshops to share the results and knowledge gained through Center research activities.

The structure of TRUST lends itself to a comprehensive approach to knowledge transfer. Since TRUST addresses well defined and long term societal needs, the results in computer security, privacy, and critical infrastructure protection can be easily communicated to decision makers, policy makers, and government agencies. With respect to industry, the selected integrative

testbeds represent focal points for interaction and dialog with major stakeholder industries (e.g., power, telecommunication, embedded systems). In fact, several integrative testbeds are being provided by the stakeholders, which offer significant leverage for the Center. To facilitate technology transfer from the research community to the industrial community a number of the investigators on this proposal, led by Sastry and Sztipanovits, have created the Embedded Systems Consortium for Hybrid and Embedded Research (ESCHER), a non-profit organization that provides a repository for the tools and algorithms developed by researchers and establishes case-studies for design. TRUST will utilize ESCHER as a repository for developed tools and reference solutions. Finally, TRUST researchers are leaders in their scientific communities. Their broad cooperation to achieve the TRUST objectives will serve as a catalyst to turn attention of the community toward the emerging science of secure systems.

TRUST comprises multiple institutions, technology vendors, and infrastructure users and providers. Broad participation from leading research universities, undergraduate colleges serving under-represented groups, computer vendors (e.g., IBM, HP, Intel, Microsoft, Cisco, Symantec), and infrastructure providers (BellSouth, Raytheon, Boeing, Qualcomm, General Motors) will result in wide spread dissemination, adaptation and continued evolution of ubiquitous secure technology. TRUST research will learn and evolve with our results using an iterative investigate-develop-educate-apply cycle. We will develop science, technology, and proof of concept prototypes that will be tested through models that emerge from a series of analytical and case studies, experimentation, and simulations. We plan to use periodic updates of living reports and community workshops throughout the life-cycle of TRUST.

The research output of the Center will be disseminated in four ways: (1) publications in the open literature and on the web, (2) Short courses held at major ACM and IEEE conferences as well as Infrastructure Protection Meetings, (3) Public Lectures and Meetings with the general public concerned about security and privacy issues on the internet and critical infrastructure protection, and (4) Curriculum development and courses taught at the partner institutions as well as the outreach institutions.

During the reporting period, we believe that TRUST has been solidly on track with respect to its knowledge transfer objectives. Success is measurable in many ways: technologies that are being commercialized, TRUST researchers who are working hand-in-hand with industry and standards groups to help improve trustworthiness of major infrastructure systems, activities aimed at educating the public and exploring non-technical ramifications of TRUST themes, and development of significant TRUST spin-offs (e.g., the AF-TRUST-GNC center for the U.S. Air Force), the exploratory work on a center for research on trustworthy electronic health records, and the TRUSTED Financial Systems center under discussion with the U.S. Department of Treasury.

4.2 Performance and Management Indicators

TRUST knowledge transfer activities are periodically monitored for meeting the Center's overall knowledge transfer objectives and the individual activity's knowledge transfer objectives. Periodic monitoring consists of meetings of the TRUST Executive Board where progress of each knowledge transfer activity (or sets of activities) is formally reviewed. The evaluation metrics are outlined in the table below.

Goals	Objectives	Evaluation Criteria	Frequency
Economic, Legal, Social Impact of TRUST	Policy paper, amicus briefs, legislation	Scholarly impact, Societal impact, Legislative impact, Judicial impact	Bi-Annual
Testbeds	Demonstrations to scale of TRUST technology on realistic platforms	Industrial interest, Industrial adoption, Stakeholder interest, Stakeholder adoption	Annual
Financial infrastructures	Identify generic/unique features of TRUST issues, propose solutions, privacy issues	Stakeholder interest, stakeholder support	Annual
Electric power demand side infrastructures	Identify vulnerabilities of SCADA systems, propose secure network embedded systems solutions	Stakeholder interest, Stakeholder support	Annual
Secure Global Information Grid Architectures	Examine and critique proposed architectures, propose security architectures and solutions	Stakeholder interest, Stakeholder support	Annual

4.3 Current and Anticipated Problems

No significant problems were encountered during the reporting period. No significant problems are anticipated in the next reporting period.

4.4 Knowledge Transfer Activities

The TRUST industrial collaboration and technology transfer initiatives support the goals and objectives of the Center's knowledge transfer component. Within TRUST, knowledge transfer is enabled by (1) using partner knowledge and experience to focus research on real-world problems; (2) verifying our science and technology at partner sites to ensure they work in practice; (3) including partners in every stage of the research, science and technology development process; and (4) aggressively licensing TRUST intellectual property to corporate partners for commercialization. (In particular, the Center has developed an interesting open source software IP model to facilitate interactions with industry.)

The items below describe in more detail specific knowledge transfer activities of TRUST researchers.

Domain Analysis		
Led by	Vanderbilt University (ISIS)	
Organizations Involved		
	Name	Address
1	Vanderbilt University Medical Center	Nashville, TN 37235
2	Vanderbilt University (ISIS)	Nashville, TN 37235

In order to define a precise architectural model for EMR systems in general, and the MyHealth at Vanderbilt Patient Portal in particular, TRUST researchers have been organizing a series of meetings with VUMC personnel including Patient Portal designers, developers, and other associated personnel. The objective of these meetings for the TRUST researchers was to understand this domain deeply, so that the modeling language being developed, as well as the actual models, constitute a high quality abstraction layer. Conversely, VUMC personnel gained insight into Model Integrated Technology with special emphasis on the benefits it can provide in developing EMR systems.

Vulnerability Analysis		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Vanderbilt University Medical Center	Nashville, TN 37235
2	Vanderbilt University (ISIS)	Nashville, TN 37235

TRUST and MyHealth researchers and developers have formed a study group on understanding scenarios in Patient Portal use cases that can have potentially negative consequences. A large group of people have been participating in these ongoing meetings including Dr. Jim Jirjis, the project manager of the Patient Portal, the Chief Security Officer of Vanderbilt, Gay Smith from the Vanderbilt privacy Office, lead developers of the Patient Portal and the Vanderbilt internal EMR system, as well as representatives from the legal office, the medical library, patient billing, etc. All participants gained deeper understanding of the wide variety of issues that are raised by publishing medical data on the web. Several issues were uncovered that would otherwise may have remained hidden.

Architectural Modeling and Policy Languages		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	Vanderbilt University (ISIS)	Nashville, TN 37235

Vanderbilt and Stanford has been having regular telecons where they explore the ways how the temporal logic based policy language developed at Stanford can be integrated into the Model Integrated Computing toolsuite of Vanderbilt. The modeling environment, model analysis and model transformation tools support the precise specification of workflows in the system, while the policy language captures the policies that influence the execution of those workflows as well as guarantee the privacy, confidentiality and integrity of the data involved. The ongoing regular meetings have been helping both groups to gain better understanding of each other's technology.

Privacy Issues in EMR		
Led by	Stanford University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	Vanderbilt University Medical Center	Nashville, TN 37235
3	Vanderbilt University (ISIS)	Nashville, TN 37235

Currently, the Stanford model of the MyHealth system is a simple workflow graph on the roles in the portal (patient, secretary, nurse, doctor, etc). Based on our analysis of this

simplified workflow, we have made several design suggestions to the MyHealth team at the Vanderbilt Medical Center. Specifically, we have suggested (1) MyHealth include tags for messages, (2) use these tags to enforce privacy requirements, and (3) use these tags to route messages more accurately. The Vanderbilt team at ISIS is currently creating a hi-fidelity model of the MyHealth system, including its workflow. We will use this model to further evaluate MyHealth.

Patient Portal Privacy Working Group Meeting		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	Vanderbilt University Medical Center	Nashville, TN 37235
3	Vanderbilt University (ISIS)	Nashville, TN 37235
4	Cornell University	

Privacy and Confidentiality Workshop		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	Vanderbilt University	Nashville, TN 37235
3	UC Berkeley	Berkeley, CA
4	Cornell University	Ithaca, NY

The two-day TRUST Privacy and Confidentiality Workshop was held at the Vanderbilt Center for Better Health on September 13-14, 2006. In addition to TRUST researchers from Vanderbilt, Stanford, Berkeley, and Cornell, participants included Jim Jirjis, the project manager of the Patient Portal, Dan Masys and Mar Johnson from the Vanderbilt Medical School. The previous day there was also a Patient Portal Privacy Working Group Meeting at Vanderbilt.

Article in Economist		
Led by	Stanford University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	The Economist	London SW1A 1HG, United Kingdom

The January 4, 2007 issues of the Economist magazine, a widely respected weekly with a worldwide audience, published an article on Data Privacy that described the research conducted by Prof. John Mitchell's groups at Stanford under TRUST.

Body Sensor Technology Transfer		
Led by	Cornell University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850
2	Qualcomm	San Diego, CA 92121

Prof. Wicker's group at Cornell has been in contact with Don Jones of Qualcomm to negotiate a collaboration between the medical sensor network group at Cornell and Qualcomm who is developing an ultra low power body area network technology.

Visitor Monitoring		
Led by	Cornell University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850
2	Johnson Museum	Ithaca, NY 14850

The Cornell team is applying results from TRUST to developing software and components on our existing testbed for visitor monitoring in the Johnson Art Museum on Cornell's campus. These include link encryption, power saving/management, and other components, which will be also applied to the medical monitoring network.

Sensor-Based Remote Health Care System Deployment		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Vanderbilt Home Care Services, Inc.	Nashville, TN 37232
2	Vanderbilt University	Nashville, TN 37235
3	Cornell University	Ithaca, NY 14850
4	University of California, Berkeley	Berkeley, CA 94720

Industry and medical center collaboration has been established in the area of medical sensing system, with the most important development being an agreement with Vanderbilt Home Care Services, Inc. to test TRUST technology in a realistic medical environment. Additionally, researchers from TRUST have worked with the care givers at Vanderbilt Home Care Services on understanding in-home patient care scenarios. TRUST researchers have accompanied the nurses to visit the patient homes and the assisted living facilities to get first-hand experience in terms of an appropriate target group who will benefit most from our patient monitoring system, the medical data that are critical for their health, and the sensor devices that are feasible for deployment. All participants gained deeper understanding of the wide variety of issues that are raised by remote patient monitoring.

Security Co-Design Toolbox		
Led by	Gabor Karsai, Vanderbilt	
Organizations Involved		
	Name	Address
1	Vanderbilt University	Nashville, TN 37235
2	Cornell University	Ithaca, NY 14850

We have developed security co-design tools that couple security with the initial design stages of sensor networks. The basis idea is that embedded (a.k.a. cyber-physical) systems must be designed with security considerations in mind. At its core, interactions are established between embedded system properties (response-time, bandwidth, data lifetime) and computer security issues. Co-design then takes the form of interweaving security and para-functional aspects in the design process. Ongoing work is focused on security property verification of design-models and metamodel composition for integrating security modeling into embedded system design languages. The final objective is a toolbox with

application-specific extensions that can be used to develop secure sensor networks in a wide variety of application domains.

Technology Transition to the Department of Defense		
Led by	Cornell University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850
2	University of California, Berkeley	Berkeley, CA 94720
3	Vanderbilt University	Nashville, TN 37235

TRUST researchers work closely with DoD, especially with the Air Force Research Laboratory (AFRL) and the Air Force Office of Scientific Research (AFOSR). TRUST members consult for OSD at many levels and have participated in development activities underway at major defense vendors such as Raytheon, which is adopting TRUST-developed real-time communication technologies as part of the DDG 1000 architecture. Cornell, Berkeley, and Vanderbilt researchers are assisting the Air Force CIO office in an ongoing study of the GIG and its implications for the military, and this activity is now expanding to include dialog with Andre Von Tilborg, DDR&E for the overall OSD. For the DDG 1000, TRUST researchers are actively working to transfer real-time replication mechanisms into the Apache Axis2 platform for web services with teams at WSO2 and Red Hat. Raytheon is eager to use these same tools and is working to create a consortium focused on the DDG 1000 architecture and the RTI-supplied event notification bus it uses. Moreover, these activities are leading to new web services standards proposals aimed at extending the WS-EVENTING standards to encompass more powerful real-time and consistency properties.

Government and Industry Financial Services Research and Development		
Led by	Cornell University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850

TRUST researchers are also working to explore the creation of a research institute for the U.S. Department of Treasury. The goal is to transfer TRUST insights into the financial sector to help create more secure and more robust solutions for large banks and other financial institutions. We're also working to help companies like Amazon develop new scalability solutions for their data centers, which turn out to host data center applications on behalf of lots of other companies. For example, the Astrolabe system, developed by TRUST researchers, is being used by Amazon and is already saving that company tens of millions of dollars while also reducing downtime and improving the flexibility of their systems management approach. One TRUST researcher spent much of the summer of 2006 working with one of the largest Wall Street firms which wanted to upgrade an in-house trading system that integrates transactions for about 45% of the industry, clears some trades internally, and forwards others to the major stock exchanges.

Research Dissemination via Conferences and Workshops		
Led by	Cornell University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850

2	University of California, Berkeley	Berkeley, CA 94720
3	Stanford University	Stanford, CA 94305
4	Carnegie Mellon University	Pittsburgh, PA 15213
5	Vanderbilt University	Nashville, TN 37235

Knowledge transition takes other forms as well. The TRUST research team is prominent in roles such as keynote and other invited talks, both at major research conferences, industry-oriented conferences, and at some of the largest platform vendors, such as IBM, Microsoft and Cisco and are infusing these talks with TRUST themes. Such activities are good opportunities for dialog with folks "on the ground". Additionally, multiple TRUST members often support the same government workshops. For example, several TRUST researchers participated in a series of NSF sponsored workshops associated with the national cybersecurity research and development strategy, embedded sensors, and other small real-time devices. NSF is now exploring the creation of a new research program in this area.

The second Trustworthy Interfaces for Passwords and Personal Information (TIPPI) workshop was held on June 19, 2006 at Stanford University with about 85 participants. In the first two years of this workshop, researchers have shared many different ideas about how to improve the situation with user interfaces for authentication, and industry efforts are starting to move along toward implementing some of them. We look forward to further reports both from the research community and developers on new ideas as well as progress in the field. The 3rd TIPPI Workshop is planned for June 22, 2007.

Industry Technology Transition and Product Adoption		
Led by	Cornell University and Stanford University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850
2	Stanford University	Stanford, CA 94305

TRUST team members are collaborating with Cisco to look at options for improving management of high performance routers of the kind used for the Internet backbone (and probably GENI). The hope is to increase flexibility, reduce risks of errors, and dramatically reduce downtown. The team is in dialog with several big consulting firms who work with Fortune 500 companies on their data centers and enterprise architectures to inject robustness-promoting technologies into such settings. Additionally, the TRUST team is producing a tremendous range of software products – real systems that can be downloaded, for free (often in source form) and used worldwide to build new and more robust application systems. Cornell alone has at least a dozen such systems available today. For example, Fireflies is currently being used by the University of Tromso, Norway in a product called "Firepatch" that can be used to disseminate security-sensitive software patches without the concern of reverse engineering approaches that hackers use to discover the security hole and attack unpatched hosts.

Researchers from Stanford University collaborated with RSA Security on integration with the RSA SecurID hardware token. SecurID generates a one-time password that is still vulnerable to “attacker-in-the-middle” password stealing attacks. With the server-side software developed as a result of this collaboration, RSA SecurID one-time passwords are protected from phishing attacks.

Industry Technology Collaboration and Consulting	
Led by	University of California, Berkeley and Stanford University

Organizations Involved		
	Name	Address
1	University of California, Berkeley	Berkeley, CA 94720
2	Stanford University	Stanford, CA 94305

David Wagner from the University of California, Berkeley has partnered closely with Hewlett Packard Labs researchers on the Joe-E project. HP Labs researchers are serving as the first users of Joe-E, and two internal HP projects have decided to adopt Joe-E. In particular, the Waterken server is implemented using 18K lines of Joe-E code and 3K lines of Java code. HP Labs researchers have helped us ensure that our techniques work in practice and to improve the Joe-E programming language. HP Labs researchers have been closely involved in the development of Joe-E; we have held day-long meetings approximately once each month. In addition, Wagner's research group at UC Berkeley and researchers at HP Labs jointly organized a security review of the Waterken server, to assess our experience with how well Joe-E was able to support the security goals of the Waterken project. Wagner also consults for Fortify Software, a startup producing software security tools, on their security products. Fortify Software is in the process of commercializing research into program analysis from several TRUST participants, including research by Aiken, Dawson, Song, Wagner, and others. Wagner has helped Fortify to transition his own research into their commercial products, as well as to transition research by other software security researchers from TRUST and elsewhere.

Dan Boneh and John Mitchell from Stanford University were advisors to Passmark, which was acquired by RSA. Rachna Dhamija from the University of California, Berkeley started a company based on the Berkeley Dynamic Skins technology.

Technology Industry Media Awards and Coverage		
Led by	Stanford University and the University of California, Berkeley	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	University of California, Berkeley	Berkeley, CA 94720

Stanford University received the *Computerworld* 2006 New Horizons Award for PwdHash. Additionally, we have been actively involved in media discussions of identity theft. Work by the Berkeley on keyboard acoustic emanations received comment in over three hundred publications worldwide. We have also been actively involved in producing, together with the AARP, special information for the elderly community on identity theft disseminated through AARP publications.

Open Source Software Dissemination		
Led by	Stanford University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	University of California, Berkeley	Berkeley, CA 94720

Pwdhash, SafeCache, SafeHistory, and SpyBlock are all available as freely downloadable open-source software. At least tens of thousands of downloads have occurred, and there has been continuing media attention through 2006-07. Additionally, we have made available open source software releases of our Doppelganger code (http://www.umeshshankar.com/doppelganger/).

Book Series		
Led by	University of California, Berkeley	
Organizations Involved		
	Name	Address
1	University of California, Berkeley	Berkeley, CA 94720

We have entered into a new book series with the scientific publisher Springer to more widely disseminate our research results.

4.5 Other Knowledge Transfer Outcomes

No additional knowledge transfer outcomes to report.

4.6 Knowledge Transfer Metrics/Indicators

Knowledge transfer provides the means by which research results are transitioned from Center faculty and students to society. TRUST knowledge transfer activities are both continuously monitored and periodically reviewed to ensure that they support the Center's overall knowledge transfer goals and make progress against the activity's knowledge transfer objectives. The evaluation metrics are described below.

- **Economic, Legal, and Social Impact of TRUST** – How does the activity improve the understanding of economic, legal, and social aspects of cybersecurity and critical infrastructure protection technologies? This impact is measured by the number of policy papers and amicus briefs produced as well as efforts to provide subject matter expertise that helps shape legislation and influences judicial decisions.
- **Testbeds** – How well does the activity leverage testbeds to promote industry and stakeholder interest and adoption? The role of the testbeds is to integrate and evaluate technologies in specific and realistic systems, keep the research on track to answer societal objectives, and demonstrate technologies to stakeholders in real systems.
- **Financial Infrastructures** – How does the activity address the unique security, privacy, and data protection challenges of the financial services industry? While a number of the problems encountered in financial infrastructures are generic to the development of trusted systems, there are several unique problems having to do with strong needs for privacy, selective revelation, and forensics.
- **Electric Power Demand Side Infrastructure** – How does the activity address the unique challenges being faced by electric power service providers, SCADA operators, and government organizations and research laboratories? The problems associated with securing electric power systems, and their associated network of SCADA components, is demanding and complex and requires solutions that solve specific issues in the security of SCADA networks.
- **Secure Global Information Grid Architectures** – How does the activity address challenges within the Department of Defense as it strives to interconnect enterprise networks, information exchange networks, and tactical networks via the Global Information Grid (GIG)? In particular, there are opportunities to provide impact in information assurance, specifically in the areas of multiple levels of security, real time information sharing architectures, and command and control architectures.

Knowledge transfer activities are periodically monitored by the TRUST Executive Board where progress of each activity (or sets of activities) is formally reviewed. Knowledge transfer

activities are expected to produce specific deliverables or results such as amicus briefs, position papers, industrial liaison consultations, solution repositories, summits, and case studies.

4.7 Next Reporting Period Knowledge Transfer Plans

For the next reporting period, the Center will increase dialog with major stakeholder industries and specific companies within those industries. In particular, the Center is hoping to leverage its growing relationships with industry via the following activities:

- **Summer Experience, Colloquium and Research in Information Technology (SECuR-IT)** – SECuR-IT is a 10-week residential program for graduate students with paid internship co-located at Stanford University and San Jose State University. This is a 40-hour per week obligation to internship, research, and learning activities. Students who participate in SECUR-IT participate in San Jose State University residential cohort, attend courses, and are employed as an intern by a participating SECuR-IT industry partner. TRUST has arranged for participants to access student housing at San Jose State University and is coordinating with industry partners to place students in pain internships Participating technology companies include TRUST industry partners Intel, Yahoo, Sun Microsystems, Symantec, Visa International, and Xilinx.

- **Silicon Valley Industry Computer Security Curriculum Group** – The Industry-Backed Computer Security Curriculum is a document created by the Industry/Academic work group. The group meets on a monthly basis with representatives from Silicon Valley industries, Stanford University, UC Berkeley, San Jose State University, and TRUST. The group's charge is to develop a plan for an industry-backed computer security curriculum and collect contributions from academic and industrial contributors. This curriculum is expected to not only address computer security but also additional topics such as risk management, legal issues, and regulatory compliance—all of which are considered to be essential knowledge areas for computer security professionals.

- **Computer Security Speakers Series** – The Computer Security Speakers Series is a monthly event that presents leading figures in computer security. Speakers are Chief Security Officers (CSOs) or Chief Information Security Officers (CISOs) of technology companies, financial services companies, and health care organizations as well as leading academics and scholars in this field. Presentations will have a live audience with Web streaming over the Internet and talks will be archived on the TRUST education portal. The inaugural Computer Security Speakers Series event will take place in Fall 2007 at the Hover institute on the Stanford University campus with Mary Ann Davidson of Oracle. The series will alternate between Stanford University and UC Berkeley and later will travel to TRUST partner campuses at Cornell, Vanderbilt, Carnegie Mellon, and Smith. This program will build the TRUST brand in security, provide industry outreach, support professional development, and attract people to the TRUST education portal.

Additionally, the Center plans on expanding the collaborative research being conducted in support of the Air Force Team for Research in Ubiquitous Secure Technology for GIG/NCES (AF-TRUST-GNC) and the International Collaboration for Advancing Security Technology (iCAST). For AF-TRUST-GNC, TRUST researchers are providing expertise and conducting research on Air Force trusted computing needs. For iCAST, TRUST researchers are not only collaborating with international researchers to develop information security technologies, they're also working on ways to increase information security public awareness and foster information

security partnership among government organizations, academic institutions, and private sector companies.

The hope is to see similar sets of TRUST researchers form mini-centers in the areas of SCADA computing, electronic health care records, and trusted computing for financial applications. These mini-centers will bring additional resources to TRUST enabling the Center to leverage the government investment being made in core TRUST research and provide concrete application areas on which TRUST researchers can focus their efforts.

5 EXTERNAL PARTNERSHIPS

5.1 Goals and Objectives

One of the goals of the Center is to serve as a trusted intermediary between academics, industry, and policy makers, while simultaneously addressing long term societal needs in its research and education activities, and pursuing knowledge transfer. To integrate these objectives together, TRUST has sought to partner with representatives from the Information Technology (IT) industry and national laboratories. These partnerships not only facilitate the transfer of TRUST research results to industry but they provide an opportunity for TRUST to receive guidance in the Center's overall strategic planning and implementation through senior industry personnel on the TRUST Scientific Advisory Board (SAB).

5.2 Performance and Management Indicators

Several performance indicators are used to track progress in meeting the overall metric of global impact of the Center. As with other areas, TRUST partnerships are periodically monitored for their effectiveness in supporting the Center's partnership goals objectives. The evaluation metrics are outlined in the table below.

Objective	Metric	Frequency
Increased External Partnerships	Number of TRUST partners	Annual
Increased Amount of External Funding	Level of funding from industrial partners	Annual
Growth in Base of Knowledge Transfer Collaborators	Number of Knowledge Transfer collaborators	Annual
Joint Research Impact	Number and magnitude of joint research activities with National Laboratories	Annual
Policy and Legislation Influence	Level of interaction with Policy/Legislative organization	Annual

5.3 Current and Anticipated Problems

No significant problems were encountered during the reporting period. No significant problems are anticipated in the next reporting period.

5.4 External Partnership Activities

Partnership Activity		Industrial Research Partnership	
Led by		Shankar Sastry	
Organizations Involved			
	Name of Organization	Shared Resources (if any)	Use of Resources (if applicable)
1	University of California, Berkeley (Lead Organization)		
2	Carnegie Mellon University		
3	Cornell University		
4	Mills College		
5	San Jose State University		
6	Smith College		
7	Stanford University		
8	Vanderbilt University		

TRUST researchers and staff at all partner institutions are working with a number of industrial companies. The Industrial Research Partnership initiative strives to strengthen ties between TRUST and industry. Through this initiative, a number of industrial partners participate in knowledge transfer, serve on the Center's Scientific Advisory Board, or collaborate actively with TRUST researchers. Current TRUST industrial partners are:

- British Telecom
- Cisco Systems
- ESCHER Research Institute
- Hewlett Packard
- IBM
- Intel
- Microsoft
- Pirelli
- Qualcomm
- Sun
- Symantec
- Telecom Italia
- United Technologies.

The primary means of supporting the Center through the Industrial Research Partnership is for a company to become an official corporate partner at one of the Center's sponsorship levels (Affiliate, Small or Minority-Owned Business, Partner, or Premium Partner) and provide the associated level of funding to the Center. Sponsorship benefits and types of collaboration with Center faculty vary by membership level.

Partnership Activity	International Collaboration for Advancing Security Technology (iCAST)
Led by	Shankar Sastry
Organizations Involved	

	Name of Organization	Shared Resources (if any)	Use of Resources (if applicable)
1	University of California, Berkeley		
2	Carnegie Mellon University		

iCAST is a team consisting of members from the Taiwan Information Security Center (TWISC), the Institute for Information Industry (III), the Industrial Technology Research Institute of Taiwan (ITRI), and the Chung Cheng Institute of Technology at the National Defense University (NDU). iCAST collaborates with international institutions in various fields related to information security. In particular, TRUST currently works closely with TWISC to expand information security research and development activities, to increase information security public awareness, and foster information security partnership among government organizations, academic institutions, and private sector companies. TWISC research is in the areas of cryptology, network security, multimedia security, software security, and information security management. For this proposal, we will partner with the TWISC Education & Training Division which is focused on creating material for educational programs on information security, offering training courses and promote information sharing and public awareness of information security, and hosting training workshops in information security for academic and industrial professionals.

Partnership Activity		Air Force Team for Research in Ubiquitous Secure Technology for GIG/NCES (AF-TRUST-GNC)	
Led by		Shankar Sastry	
Organizations Involved			
	Name of Organization	Shared Resources (if any)	Use of Resources (if applicable)
1	University of California, Berkeley		
2	Cornell University		
3	Vanderbilt University		

AF-TRUST-GNC is funded by the U.S. Air Force Office of Scientific Research (AFOSR) and is researching challenges associated with the Global Information Grid (GIG) and Network Centric Enterprise System (NCES). AF-TRUST-GNC focuses on top research priorities identified in a recent study of plans to unify three major Air Force enterprise subsystems and to link the Air Force network with networks operated by other Department of Defense (DoD) services. The objective of AF-TRUST-GNC is to advance the state-of-the-art on cyber-assurance to address key trust- and QoS-related properties simultaneously throughout the lifecycles of large-scale Air Force systems via a novel combination of analytical and experimental techniques. Researchers on AF-TRUST-GNC are exploring innovation in the following areas:

- Guaranteed scalable, real-time, and fault-tolerant quality of service (QoS) for network-centric AF operational and tactical systems
- Techniques for large-scale information assurance and security policy management
- New algorithms and tools for secure scalable, information discovery, information architecture, and mediation.

5.5 Other External Partnership Outcomes

None to report.

5.6 External Partnership Metrics/Indicators

During this reporting period, there was significant progress made in the area of external partnerships. TRUST faculty and staff worked closely with a number of companies through the Center's Industrial Research Partnership program to obtain support for TRUST research projects as well as education and outreach activities. For example, several technology companies in the Silicon Valley area are allocating internship slots to graduate students for the TRUST Summer Experience, Colloquium and Research in Information Technology (SECuR-IT) program coordinated by Stanford University, San Jose State University, and the University of California, Berkeley. Additionally, the Center has received external funding and increased the base of knowledge transfer collaborators through the iCAST and AF-TRUST-GNC research programs. These programs provide an opportunity to leverage fundamental cybersecurity and critical infrastructure protection research being conducted in the Center and apply it to other areas.

5.7 Next Reporting Period External Partnership Plans

During the next reporting period, we hope to increase the number of companies participating in the Center's Industrial Research Partnership program and, in particular, further pursue opportunities for external industry funding to augment the government investment made in the Center. We feel that this effort will not only further grow the number of knowledge transfer opportunities for Center research results but it will also provide TRUST faculty and students more opportunities to collaborate with industry executives and professionals and apply their research to real-world problems.

6 DIVERSITY

6.1 Goals and Objectives

No changes are anticipated. Below is the centers current activity.

The overall TRUST goal is to have no weak links left in the education of our society about the technical, compositional, privacy, economic and legal aspects of trusted information systems. To this end, we will begin locally but spread our outreach as far as we can along as many diverse axes as we can.

To meet this objective, the center has delivered the following programs:

- Grades 6-12 outreach: educating children about cyber security 6-12 through the Berkeley Foundation for Opportunities in Information Technology (BFOIT)

- Capacity Building Program for Faculty from Historically Black and Hispanic Serving Institutions: Information Assurance Capacity Building Program at San Jose Sate University

- Summer Research Experience for underrepresented minority groups and women: SIPHER at Vanderbilt, SUPERB-IT at UC Berkeley and SECuR-IT at Stanford and San Jose State University

- Women Research Programs: supporting underrepresented minority groups and women in Information Technology: Women's Institute in Summer Enrichment (WISE) at UC Berkeley and Trust Summer Program for Smith Undergraduates: Discovering Sensor Networking at Cornell.

- Community Outreach at all TRUST campus

6.2 Performance and Management Indicators

TRUST diversity activities are periodically monitored for meeting the Center's overall diversity objectives. Periodic monitoring consists of meetings of the TRUST Executive Board where progress of each diversity activity (or sets of activities) is formally reviewed. The diversity evaluation metrics are outlined in the table below.

Goals	Objectives	Evaluation Criteria	Frequency
6-12 Outreach	6-12 Student Education	Education Materials, Number of Students, Assessment of Effectiveness	Bi-Annual
Minority Faculty Research	Guided Summer Program	Number of faculty, Exit Surveys, Tracking surveys of alumni	Every 3 Years
Curriculum Development	NSA certified program in IA modules	Accreditation, Modules transferred to other campuses	Every 3 Years
Immersion Institute	Attract more women students to TRUST and related fields	Exit surveys, Tracking surveys of alumnae, Module development	Every 3 Years
SIPHER-TRUST	Research opportunities for minority grad students at non-partner institutions	Exit surveys, Tracking surveys of alumni, Repeat visits	Every 3 Years
SUPERB-TRUST	Research opportunities for minority undergrad students at non-partner institutions	Exit surveys, Tracking surveys of alumni, Graduate school applications	Every 3 Years
Community Outreach	Dialog with public about policy, privacy, and economics	Exit surveys	Every 2 Years

Recruitment of underrepresented minority groups and women is a high priority for TRUST. For example, announcements for the SECuR-IT program were distributed via email to the following organization and websites: The Computer Alliance of Hispanic Serving Intuitions (CAHSI), Historically Black Colleges and Universities (HBCU), Louis Stokes Alliance for Minority Participation (LSAMP), Alliances For Graduate Education and the Professoriate (AGEP), Committee for the Status of Women in Computing Research (CRA-W), California State

University Computer Science Department Chairs and EECS university department chairs, CraigsList.com listings in Atlanta, Chicago, Denver, Houston, Miami, Minneapolis, Phoenix, Portland, Raleigh, Sacramento, and the San Francisco Bay Area and Quality Education for Minorities Network (QEM).

Additional promotion and recruitment has been performed by conference and workshop attendance. During 2006-2007, the executive director of education and outreach attended or plans to attend conferences and workshops such as: CAHSI All-Hands Meeting, IEEE Frontiers in Education panel participant, Cyber Trust, CRA-W Grad Cohort in San Francisco, STC Broadening Participation Workshop, National Society for Black Engineers (NSBE) Grad Lab presentation, National Science Foundation's Research Centers Educators Network (April 2007), the Richard Tapia Celebration of Diversity in Computing and the Grace Hopper Celebration of Women in Computing Conference (October 2007).

6.3 Current and Anticipated Problems

No significant problems were encountered during the reporting period. No significant problems are anticipated in the next reporting period.

6.4 Diversity Activities

We have the concrete goal of having 30% being women and 10% being under-represented minorities among all the participants in TRUST—faculty, students, and Center staff. In addition, we will direct our outreach activities, starting locally at each campus and then as our curriculum and research gets more integrated we will also broaden the scope to TRUST-wide activities. The center will also make special attempts at outreach to Native American populations and disabled Americans.

The sections below describe some of the Center's activities which are contributing to the development of US human resources in science and engineering at the postdoctoral, graduate, undergraduate, and pre-college levels—especially those aimed at attracting, increasing, and retaining the participation of women and underrepresented groups.

6-12 Outreach

TRUST educational outreach at the pre-college level will be implemented by leveraging our partnership with an existing program, Berkeley Foundation for Opportunities in Information Technology (BFOIT). BFOIT conducts outreach to bring historically underrepresented minorities and girls in elementary and secondary schools into Information Technology. Academic-year activities, such as college preparation workshops, culminate in a two-week summer institute. BFOIT's workshops spark excitement in IT, develop programming skills, engage students in important and relevant issues (like cyber-security and the need for more minorities and women in computer science and engineering) and introduce students to successful mentors and professionals in the field.

Summer Research in Information Assurance for HBCU/HSI Faculty

As a National Security Agency-designated Center of Academic Excellence (CAE) in Information Assurance Education, Carnegie Mellon has developed and offers during the summer an intensive, month-long, in-residence summer program to help develop Information Assurance education and research capacity at colleges and universities designated as Minority Serving Institutions – specifically, Historically Black Colleges and Universities (HBCUs) and Hispanic Serving Institutions (HSIs). The first two offerings of this program have been a resounding success. Carnegie Mellon has forged strong ties with a number of minority serving institutions

and has significantly increased their ability to address Information Assurance in their computer science and information systems curricula. TRUST Center partner San Jose State will participate with Carnegie Mellon and will host the 2007 Information Assurance Capacity Symposium (IACS) summer schools and follow-up workshops under the IACBP.

Curriculum Development for Minority Serving Institutions

Stanford and Berkeley will work with San Jose State to develop their computer security curriculum. San Jose State focuses on profession oriented undergraduate and masters-level education.

San Jose State has defined and received approval for a new course titled, CMPE 025: *The Digital World and Society*. The course is currently under evaluation for possible adoption as a university-wide general education course.

> *CMPE 025: The Digital World and Society*
> The secure, effective, and ethical use of information technology. The effect of such technology on people and institutions. Technology-related challenges to society and policy. Frameworks for the analysis of information technology with respect to its cultural, historical, environmental, and spatial contexts.

Summer Internship for HBCU Faculty in TRUSTED Embedded Systems: SIPHER

It is our experience that research partnerships set up during the periods of intense collaborations over the summers continues through the academic year and result in further collaborations on other projects. California Community Colleges have a large population of under-represented minorities in the state of California. Vanderbilt has established the Summer Internship Program in Hybrid and Embedded Systems Research (SIPHER). We will augment it to include topics in information security. The program focuses on institutions with high enrollments from underrepresented groups, including community colleges (with high minority enrollments) in the Southern United States and in California.

Summer Undergraduate Research Opportunities: SUPERB-IT

The REU program at UC Berkeley, Summer Undergraduate Program in Engineering Research at Berkeley – Information Technology (SUPERB-IT) offers a group of talented undergraduate engineering students the opportunity to gain research experience. The program's objective is to increase diversity in the graduate school pipeline by affirming students' motivation for graduate study and strengthening their qualifications. SUPERB-IT participants spend eight weeks at UC Berkeley during the summer working on exciting ongoing research projects in information technology with EECS faculty mentors and graduate students. Students who participate in this research apprenticeship explore options for graduate study, gain exposure to a large research-oriented department, and are motivated to pursue graduate study. TRUST is dedicated to developing a research experience for undergraduates from institutions serving under-represented groups during an eight-week summer term.

Women Only Colleges and Universities

As part of our outreach program at the undergraduate level, Cornell and Smith have designed a one-week Summer Immersion Institute to be held at Cornell. The first offering will be in the summer of 2007. The Institute will emphasize the inclusion of women and underrepresented students and will be designed to engage 20 students each summer in challenging problems that they can continue to pursue at their home institutions, and to develop leadership skills. Participants will have the opportunity to tour research laboratories on the Cornell campus and to meet and talk with graduate students. Tours will also be provided of the Cornell campus and a

graduate admissions office of the Cornell College of Engineering will host an information session.

Women's Institute in Summer Enrichment
WISE is a one-week residential summer program on UC Berkeley that brings together graduate students, post-doctoral fellows, and professors from all disciplines that are interested in Ubiquitous Secure Technology and the social, political, and economical ramifications that are associated with this technology. The first offering was in the summer of 2006 and had 20 participants. The Institute will emphasize the inclusion of women and underrepresented students and will be designed to engage 20 participants each summer.

Community Outreach
TRUST will hold public forums for discussing issues relating to privacy and security, economic and legislative issues for secure and trusted systems and the role of the media in reporting on security. These town-hall style meetings will be held at each of the partner campuses with the participation of the community, local and state authorities, first responders and the media.

In the fall of 2007, the Computer Security Distinguished Speakers Series will be launched. The program will be a monthly event alternating between Stanford and UC Berkeley. Presentations will have a live audience with Web streaming over the Internet. The Computer Security Distinguished Speakers Series will also be archived on the TRUST portal for additional viewing. The Computer Security Distinguished Speakers Series will present leading figures in the realm of computer security that are chief security officers (CSO), chief information security officers (CISO) of technology companies, financial services companies, health care organizations, and leading academics and scholars in this field. The inaugural Computer Security Distinguished Speakers Series event will take place in the fall of 2007 at the Hover institute on the Stanford campus. The distinguished speaker will be Mary Ann Davidson of Oracle. The series will alternate between Stanford and UC Berkeley and later will travel to Cornell, Vanderbilt, Carnegie Mellon, and Smith.

6.5 Diversity Activity Impact

The goal of TRUST diversity activities is to concretely impact the number of women and personnel from under-represented groups and address issues of diversity in technical fields. Ultimately, we would like to see TRUST diversity activities positively change findings such as the following from the National Research Council of the National Academy of Sciences study *To Recruit and Advance: Women Students and Faculty in Science and Engineering*:

> "Although women have made great strides in becoming full members of the science and engineering (S&E) enterprise, they are still underrepresented among graduate students and postdoctorates and among faculty in science and engineering programs." (NRC, 2006:1)*

To that end, TRUST faculty and staff are engaged in a number of diversity activities:

The Women's Institute in Summer Enrichment: WISE supports the development and advancement of women academics and researchers in the field of Information Technology and Trusted Systems.

TRUST Summer Program for Smith Undergraduates: Discovering Sensor Networking: The objective of this program is to increase the number of women applying to graduate research programs in information technology and trusted systems.

SIPER and SUPERB-IT: Both programs have the objective of increasing the number of students in underrepresented minority populations and women applying to graduate research programs and hopefully conducting graduate level research at a TRUST institution.

Information Assurance Capacity Symposium (IACS): The IACS is a capacity building program supporting faculty development and retention in minority serving intuitions. This program also creates opportunity for future collaboration between IACS and TRUST faculty.

Community Outreach: Programs like the Computer Security Distinguished Speakers Series provide information and technology transfer to the community at large. The series, in addition to having on campus presentations, will be viewable as real time Internet Webinars, as well as archived presentations on the TRUST portal. The speaker's series will showcase professionals and academics in the security profession– the first scheduled speaker is Mary Ann Davidson, a leader in the security industry and a women. Her participation in the TRUST speaker series will attract women and underrepresented minority groups to the event and future TRUST center activities.

6.6 Diversity Metrics/Indicators

The tables below provide detail on the gender, race, and US citizenship breakdown of participants in the TRUST WISE, SIPHER, and SUPERB-IT programs in 2006.

WISE 2006

Constituency	**Gender**		**Race**				**US Citizen**		**Total**
	M	F	White	African American	Asian	Hispanic	Y	N	
Faculty	1	5	2	0	3	1	3	3	6
	17%	*83%*	*33%*	*0.0%*	*50%*	*17%*	*50%*	*50%*	*30%*
Graduate Students	0	12	4	2	6	0	5	7	12
	0%	*100%*	*33%*	*17%*	*50%*	*0%*	*42%*	*58%*	*60%*
Research Scientists	0	1	1	0	0	0	1	0	1
	0%	*100%*	*100%*	*0%*	*0%*	*0%*	*100%*	*0%*	*5%*
Post Doctorates	0	1	1	0	0	0	1	0	1
	0%	*100%*	*100%*	*0%*	*0%*	*0%*	*100%*	*0%*	*5%*
TOTALS	**1**	**19**	**8**	**2**	**9**	**1**	**10**	**10**	**20**
	5%	***95%***	***40%***	***10%***	***45%***	***5%***	***50%***	***50%***	***100%***

SIPHER 2006

Constituency	**Gender**		**Race**				**US Citizen**		**Total**
	M	F	White	African American	Asian	Hispanic	Y	N	
Undergraduate Students	2	0	2	0	0	0	2	0	2
	100%	*0%*	*100%*	*0%*	*0%*	*0%*	*100%*	*0%*	*100%*
TOTALS	**2**	**0**	**2**	**0**	**0**	**0**	**2**	**0**	**2**
	100%	***0%***	***100%***	***0%***	***0%***	***0%***	***100%***	***0%***	***100%***

SUPERB-IT 2006

Constituency	Gender		Race				US Citizen		Total
	M	F	White	African American	Asian	Hispanic	Y	N	
Undergraduate Students	2	4	0	2	2	2	6	0	6
	33%	*67%*	*0%*	*33%*	*33%*	*33%*	*100%*	*0%*	*100%*
TOTALS	**2**	**4**	**0**	**2**	**2**	**2**	**6**	**0**	**6**
	33%	***67%***	***0%***	***33%***	***33%***	***33%***	***100%***	***0%***	***100%***

6.7 Next Reporting Period Diversity Plans

The recruitment of women and underrepresented minorities is a collaborative and ongoing process. The TRUST recruitment strategy for enhancing diversity is based on recommendations developed by the National Research Council as part of the study *To Recruit and Advance: Women Students and Faculty in Science and Engineering* (NRC, 2006: 47)* and includes the following recommendations:

- Advise and mentor prospective and current women and underrepresented minority undergraduate, graduate students and postdocs.
- Conduct outreach to 6-12 institutions to help prepare women and underrepresented minority students for college.
- Networking with faculty at community colleges and other four-year institutions to broaden the search for prospective recruits.
- Invite women and underrepresented minority students to participate in research opportunities.
- Participate in bridge programs, lectures and seminars.
- Broaden admission criteria and cast a wider net in recruiting students.

Listed below are new and continuing efforts that we have made towards this goal:

- We our continuing commitments to support underrepresented undergraduate summer students at all our sites (SUPERB-IT, SIPHER, WISE, and Cornell)

- We will continue our commitment to BFOIT (nurturing underrepresented high schools students and their teachers in engineering with focus on TRUST agenda) both financially as well via active participation by Dr. Ruzena Bajcsy and Dr. Kristen Gates.

- We are actively participating in National conferences for underrepresented faculty and students. Dr. Kristen Gates, Executive Director of Education attended: CAHSI All-Hands Meeting, IEEE Frontiers in Education, Cyber Trust, CRA-W Grad Cohort in San Francisco, STC Broadening Participation Workshop, National Science Foundation's Research Centers Educators Network (April 2007), the Richard Tapia Celebration of Diversity in Computing and the Grace Hopper Celebration of Women in Computing Conference (October 2007).

- Dr. Ruzena Bajcsy together with Dr. Richard Tapia of Rice University, Dr. Roscoe Giles of Boston University, and Dr. Cynthia Lanius of Drexel University are building the Empower Leadership: Computing Scholars of Tomorrow Alliance (EL Alliance). This

program will work to increase retention of minority undergraduate students from freshmen year through the Ph.D. at tier one research universities.

- We organized a one-week long summer institute at UC Berkeley, called WISE which has registered 20 participants out of which 19 were women (graduate students and junior faculty). WISE 2007 program is scheduled for June 10-15 at UC Berkeley.

- We are starting to increase our visibility among underrepresented faculty and students. In the summer of 2006, Stanford hosted Dr. Mario Garcia from Texas A&M University – Corpus Christi. This visit was sponsored by NSF Quality Education for Minorities (QEM) Program. Based on the success last year, multiple QEM visiting scholar candidates are being considered for appointments at one or more TRUST institution for the summer of 2007.

- Smith College is an active participant in TRUST. Dr. Judy Cardell from Smith College participated in TRUST research in the area of Secure Sensor Networks and supported the summer 2007 TRUST Summer Program for Smith Undergraduates: Discovering Sensor Networking.

- Dr. Mike Reiter from Carnegie Mellon organized the Information Assurance Capacity Building Program (IACPB) with participation from Dr. Weider Yu from San Jose State in the summer of 2006.

- As a follow-up to the IACB program, the Information Assurance Capacity Symposium (IACS) will be hosted at San Jose State in the summer of 2007.

- Dr. Sigurd Meldal from San Jose State has a new Computer Science course CMPE 025 (The Digital World and Society) that includes security and trusted system topics. The course is currently under evaluation for possible adoption as a university-wide general education course.

- Dr. Ruzena Bajcsy together with Prof. Nahrsted from the University of Illinois at Urbana-Champaign Prof. Wymur from UC Berkeley, and Prof. Katherine Mezure from Mills College are building a cyber infrastructure for distributed dance performances in cyberspace and using it to test issues of privacy. On this project, all the Principal Investigators and most of the students are women.

- We are engaged in continuous efforts of fundraising that should increase and extend our outreach efforts. TRUST has applied for an Integrative Graduate Education and Research Traineeship (IGERT) grant from NSF. The proposal, titled *Training the Next Generation of Cybersecurity Technologists and Policymakers*, is lead by TRUST Principal Investigator Dr. Shankar Sastry. This project would support interdisciplinary teams of students studying both the technical and non-technical aspects (e.g., law, policy, usability, privacy, security, economics) of trustworthy networks and systems.

*National Research Council (NRC). 2006. To recruit and advance women students and faculty in US Science and engineering/Committee on the Guide to Recruiting and Advancing Women Scientists and Engineers in Academia, Committee on Women in Science and Engineering, Policy and Global Affairs, National Research Council of the National Academies.

7 MANAGEMENT

7.1 Organizational Strategy

TRUST is organized to support the Center's strategic goals and objectives and to provide an operational structure that enables collaboration and allows the Center's researchers to primarily focus on research. At the same time, the TRUST organization has the necessary management and leadership resources that allow such a large, diverse organization to effectively function.

The TRUST organization chart is shown in Appendix B. The Center is guided by the Director (and Principal Investigator) Prof. Shankar Sastry from the University of California, Berkeley. Additional Center leadership is provided by the Chief Scientist, Prof. Fred Schneider from Cornell University; the Executive Director, Larry Rohrbough, from the University of California, Berkeley; the Education Director, Dr. Kristen Gates from the University of California, Berkeley; and the Program Manager, Mary Margaret Sprinkle from the University of California, Berkeley.

The Executive Board manages and executes the overall administration of the Center. The Executive Committee consists of the Center Director, Chief Scientist, Executive Director, Education Director, Program Manager, and university Principal Investigators.

Since the last reporting period, Dr. Kristen Gates joined the Center as the Education Director and Larry Rohrbough joined the Center as the Executive Director.

7.2 Performance and Management Indicators

Effective operation and management of the Center depends on several key processes and agreements. One of which is the set of TRUST Center By-Laws. The By-Laws were drafted and accepted into practice in the first year of the Center and govern the operation and management of the Center.

The TRUST Center By-Laws are as follows:

1. The TRUST center will be administered by a board of directors with no more than nine directors and no fewer than five directors. The Board will have a Chairman.

2. The board will have as ex-officio members the co-PIs of the NSF STC TRUST proposal: that is, John Mitchell, Mike Reiter, Shankar Sastry, Janos Sztipanovits and Steve Wicker will be the Board members. Shankar Sastry will be the Chairman of the Board. The chairman of the board will be responsible for conducting the meetings, or delegating the conducting of the meeting to another board member.

3. Directors are elected to or removed from the board by 2/3 vote of the standing directors rounded up to the next integer (for example, if the board has 5, then 4 must vote in favor, if 4, then 3, and if 3, then 2).

4. A quorum for a directors meeting consists of 2/3 of the directors. Meetings will be scheduled at an average interval of once a month until modified by the directors.

5. Directors meetings can be scheduled by a 2/3 vote, and directors will be notified at least one week in advance.

6. A quorum for a directors meeting consists of 2/3 of the directors and decisions made at such a meeting are final. Participation by telephone at the meetings is fine.

7. Unless otherwise stated, any decision by the board is by majority vote (either a majority of the directors present at a meeting, or a majority of the standing directors if the decision is made without a meeting). Obtaining votes by email is acceptable.

8. Major TRUST activities including research, education and outreach directions will be reported to the board on a periodic basis, not to exceed three months, for concurrence.

9. A Secretary will be appointed by the board, and will be responsible for recording decisions made by the board and distributing a summary of the deliberations to any board members not present at a meeting.

10. A Treasurer will be appointed by the board, and will be responsible for reporting financial status to the board, including cash flow position and projections for all accounts that are part of the TRUST center.

11. The bylaws can be modified by a 2/3 vote of the standing board. Amendments will be logged in and kept current by the secretary of the Board.

7.3 Management Metrics/Indicators

During this reporting period, the Center leadership provided effective management and guidance. Center staff, Principal Investigators, and members of the Executive Board worked together to provide an operational structure that supported the research, education, and knowledge transfer goals of the Center as well as an infrastructure for running the day-to-day aspects of the Center.

As an example, members of the Executive Board worked extensively this past year to address two significant management and leadership changes—hiring a new Education Director and replacing the outgoing Executive Director.

In order to better support the growing education and outreach activities of the Center, the TRUST Executive Board identified the need to hire a well qualified, full-time Education Director. To achieve this, the Executive Board consulted with the External Advisory Board and Scientific Advisory Board, canvassed TRUST faculty, and discussed among themselves the needs of the Center. This analysis enabled the Executive Board to clearly define the scope of the position, describe the position's role and responsibilities, and define the desired and required candidate educational and professional qualifications. As a result, the Executive Board was able to conduct a thorough and extensive job search which generated a lot of interest in the position and resulted in the hiring of Dr. Kristen Gates as the Center's Director of Education.

Similarly, the TRUST Executive Committee was presented a potentially difficult situation when it was given notice by the Center's Executive Director of his desire to leave TRUST. The TRUST Executive Board similarly worked together to support a full job search process that involved defining the scope of the Executive Director position, describing the position's role and responsibilities, defining the desired and required candidate qualifications, and interviewing candidates with the full Executive Board. Through this professional and collaborative process, the TRUST Executive Board was able to quickly hire a new Executive Director and minimize the impact to the Center's operations and leadership.

7.4 Current and Anticipated Problems

No significant problems were encountered during the reporting period. No significant problems are anticipated in the next reporting period.

7.5 Management and Communications System

The TRUST management structure includes a number of systems and processes that foster communication within the Center. First, the TRUST website (www.truststc.org) is designed to be a comprehensive resource for obtaining TRUST-related material and communicating with TRUST researchers and staff. The TRUST website provides e-mail lists, collaborative workspaces, access to publications and presentations, news items, blogs, information on past and future TRUST events, and workshop/conference registration pages. Industrial, governmental and academic participants have individual accounts and membership in multiple workspaces via a secure login procedure. E-mail lists and newsgroups are linked to each other providing easy access to discussion threads. E-mail messages are archived and are searchable. Resources such as workgroups and publications have fine grained access control and the website provides workgroup web pages via participant supplied HTML and Wiki pages. There have been no problems with the website, despite that fact that its content has grown significantly as has the number of registered users and page views and its infrastructure has become the primary means by which information is communicated to TRUST researchers and the wider TRUST community.

In order to ensure regular dialogue and communication across partner institutions, the TRUST Executive Board holds standing monthly meetings to discuss the current status of projects, funding and resource allocation, and other management and operational issues. Ad hoc meetings are also arranged as necessary in addition to these regularly scheduled meetings and the frequency of the Executive Board meetings has changed from monthly to bi-monthly to weekly as necessary to allow the group ample opportunities to confer and make timely decisions.

7.6 Center Advisory Personnel

3. Provide a list of names and affiliations of the Center's internal and external advisors or advisory bodies in the reporting period. Attach summary minutes of advisory committee meetings as Appendix C.

TRUST receives outside advice, guidance, and counsel from two groups: the External Advisory Board (EAB) and the Scientific Advisory Board (SAB). Each group is described in more detail below.

External Advisory Board – The TRUST EAB is a distinguished group of experts in research, education, policy, and management whose guidance supplements the strategic planning by TRUST management and the TRUST Executive Board. The primary goal of the EAB is to offer an independent assessment of TRUST research, education, outreach, and diversity accomplishments, goals, and plans. EAB input plays a crucial role in the annual revision of the TRUST strategic plan.

The EAB's effectiveness is directly related to its ability to offer unbiased counsel; as such, self-governance is a guiding principle in the EAB's charter. EAB members are appointed for three year terms and the EAB is headed by a chairperson, who is also appointed for a term of three years.

NSF policies on conflict of interest govern the independence of the EAB and require that EAB members do not have financial interests or collaborations with faculty and staff being supported by TRUST funding. The EAB meets annually and performs the following functions:

- First, it reviews the TRUST strategic plan, project plans, and annual report on research, education, and outreach. Unfettered Q&A sessions during TRUST briefs facilitate collecting information on pivotal points.
- Second, the EAB conducts deliberations, which occur in closed session presided by the EAB chairperson.
- Third, the EAB produces a report and presents its findings to the TRUST Executive Board and the Vice Chancellor of Research at the TRUST lead institution, UC Berkeley.

EAB members and their affiliations are listed in the table below.

	Name	**Affiliation**
1	Alfred Aho	Columbia University
2	Annie Anton	North Carolina State University
3	Patricia Bellia	University of Notre Dame
4	Matthew Davis	University of California
5	Lee Burge	Tuskegee University
6	David Clark	Massachusetts Institute of Technology
7	George Cybenko	Dartmouth College
8	James Johnson	Howard University
9	Jay Lala	Raytheon
10	Carl Landwehr	University of Maryland
11	Teresa Lunt	Palo Alto Research Center
12	Dan Manson	California State Polytechnic University
13	Andrew Odlyzko	University of Minnesota
14	William Sanders	University of Illinois at Urbana-Champaign
15	Joseph Sifakis	CNRS, Verimag
16	Gene Spafford	Purdue University

Scientific Advisory Board – The TRUST SAB consists of senior executives and thought leaders from industry, academia, and government and commercial research laboratories. The primary goal of the SAB is to engage the TRUST Executive Board to communicate industry's perspective and research needs and help the Executive Board develop and execute a successful Center/Industry partnership model.

SAB members and their affiliations are listed in the table below.

	Name	**Affiliation**
1	Andrew Chien	Intel
2	Jean Colpin	United Technologies Research Center
3	Phil Edholm	Nortel Networks
4	Pieroguido Iezzi	Perelli
5	Wayne Johnson	HP Laboratories
6	William Mark	SRI International
7	John W. Noerenberg	Qualcomm
8	Giovanni Penna	Telecom Italia

9	Emil Sarpa	Sun Microsystems
10	Steve Trilling	Symantec

7.7 Center Strategic Plan Changes

Changes to the TRUST Strategic Plan will be indicated within that document.

8 CENTER-WIDE OUTPUTS AND ISSUES

8.1 Center Publications

The following sections provide lists of various TRUST Center publications produced during this reporting period. These publications are grouped by Peer Reviewed Publications, Books and Book Chapters, and Non-Peer Reviewed Publications.

8.1.1 Peer Reviewed Publication

- Reliable Multicast for Time-Critical Systems, Mahesh Balakrishnan and Ken Birman. Reliable Multicast for Time-Critical Systems. 1st Workshop on Applied Software Reliability, June, 2006.
- How the Hidden Hand Shapes the Market for Software Reliability, Ken Birman, Coimbatore Chandersekaran, Danny Dolev, and Robbert van Renesse. How the Hidden Hand Shapes the Market for Software Reliability. First IEEE Workshop on Applied Software Reliability, IEEE, June, 2006.
- Extensible Web Services Architecture for Notification in Large-Scale Systems, Krzysztof Ostrowski and Ken Birman. Extensible Web Services Architecture for Notification in Large-Scale Systems. International Conference on Web Services (ICWS 2006), IEEE, September, 2006.
- Preserving Traffic Privacy in Wireless Mesh Networks, Taojun WU, Yuan XUE, Yi CUI. Preserving Traffic Privacy in Wireless Mesh Networks. Proceedings of WOWMOM 2006, IEEE, June, 2006.
- Achieving Anonymity via Clustering, Gagan Aggarwal, Tomas Feder, Krishnaram Kenthapadi, Samir Khuller, Rina Panigrahy, Dilys Thomas, An Zhu. Achieving Anonymity via Clustering. 25th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, June, 2006.
- Bump in the ether: A framework for securing sensitive user input, J. M. McCune, A. Perrig and M. K. Reiter. Bump in the ether: A framework for securing sensitive user input. Proceedings of the 2006 USENIX Annual Technical Conference, 185-198, June, 2006.
- Towards Robustness in Query Auditing, Shubha U. Nabar, Bhaskara Marthi, Krishnaram Kenthapadi, Nina Mishra, Rajeev Motwani. Towards Robustness in Query Auditing. Proceedings of the 32nd International Conference on Very Large Data Bases (VLDB), September, 2006.
- Learning modules for security, privacy and information assurance in undergraduate engineering education, Daniel Manson, Sigurd Meldal, Carol Sledge, Stephen M. Maurer, John C. Mitchell, Erich Spengler, Janos Sztipanovits, and Javier Torner. Learning modules for security, privacy and information assurance in undergraduate

engineering education. 36th ASEE/IEEE Frontiers in Education Conference, ASEE/IEEE, October, 2006.

- Quorum placement in networks: Minimizing network congestion, D. Golovin, A. Gupta, B. M. Maggs, F. Oprea and M. K. Reiter. Quorum placement in networks: Minimizing network congestion. Proceedings of the 25th ACM Symposium on Principles of Distributed Computing, 16–25, June, 2006.

- Scalable Multicast Platforms for a New Generation of Robust Distributed Applications, Ken Birman, Mahesh Balakrishnan, Danny Dolev, Tudor Marian, Krzysztof Ostrowski, Amar Phanishayee.. Scalable Multicast Platforms for a New Generation of Robust Distributed Applications. Proceedings of The Second International Conference on Communication System software and Middleware (COMSWARE), IEEE/Create-Net/ICST, January, 2007.

- Defense Against Intrusion in a Live Streaming Multicast System, Maya Haridasan, Robbert van Renesse.. Defense Against Intrusion in a Live Streaming Multicast System. 6th International Conference on Peer-to-Peer Computing (P2P2006), IEEE, September, 2006.

- Reliable Multicast for Time-Critical Systems., Mahesh Balakrishnan and Ken Birman.. Reliable Multicast for Time-Critical Systems.. First Workshop on Applied Software Reliability (WASR 2006), IEEE, June, 2006.

- How the Hidden Hand Shapes the Market for Software Reliability., Ken Birman, Coimbatore Chandersekaran, Danny Dolev, and Robbert van Renesse.. How the Hidden Hand Shapes the Market for Software Reliability.. First Workshop on Applied Software Reliability (WASR 2006), IEEE, June, 2006.

- inTrack: High Precision Tracking of Mobile Sensor Nodes, B. Kusy, Gy. Balogh, A. Ledeczi, J. Sallai, M. Maroti. inTrack: High Precision Tracking of Mobile Sensor Nodes. 4th European Workshop on Wireless Sensor Networks (EWSN 2007), January, 2007.

- Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport, Marci Meingast, Jennifer King, Deirdre Mulligan. Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport. IEEE International Conference on RFID, March, 2007.

- Relay Secrecy in Wireless Networks with Eavesdroppers, P. Venkitasubramaniam, Ting He and Lang Tong. Relay Secrecy in Wireless Networks with Eavesdroppers. 44th Allerton Conference on Communication, Control and Computing, September, 2006.

- Networking with Secrecy Constraints, P. Venkitasubramaniam, Ting He and Lang Tong. Networking with Secrecy Constraints. IEEE MILCOM 2006, Washington D.C, October, 2006.

- Reliable Multicast for Time-Critical Systems, Mahesh Balakrishnan and Ken Birman.. Reliable Multicast for Time-Critical Systems. First IEEE Workshop on Applied Software Reliability (WASR 2006), IEEE, June, 2006.

- Defense Against Intrusion in a Live Streaming Multicast System, Maya Haridasan, Robbert van Renesse. Defense Against Intrusion in a Live Streaming Multicast System.

Proceedings of the 6th IEEE International Conference on Peer-to-Peer Computing (P2P2006), September, 2006.

- A Scalable Services Architecture, Tudor Marian, Ken Birman, and Robbert van Renesse. A Scalable Services Architecture. Proceedings of the IEEE Symposium on Reliable Distributed Systems (SRDS 2006), October, 2006.
- Scalable Multicast Platforms for a New Generation of Robust Distributed Applications, Ken Birman, Mahesh Balakrishnan, Danny Dolev, Tudor Marian, Krzysztof Ostrowski, Amar Phanishayee. Scalable Multicast Platforms for a New Generation of Robust Distributed Applications. Proceedings The Second IEEE/Create-Net/ICST International Conference on Communication System software and Middleware (COMSWARE)., January, 2007.
- Robust Detection of Stepping-Stone Attacks, Ting He and Lang Tong. Robust Detection of Stepping-Stone Attacks. Proceedings of 25th Army Science Conference, Cornell University, November, 2006.
- Packet Scheduling Against Stepping-Stone Attacks with Chaff, Ting He, Parvathinathan Venkitasubramaniam, and Lang Tong. Packet Scheduling Against Stepping-Stone Attacks with Chaff. Proceedings of IEEE MILCOM, Cornell University, October, 2006.
- Geolocalization on the Internet through Constraint Satisfaction, Bernard Wong, Ivan Stoyanov and Emin Gun Sirer. Geolocalization on the Internet through Constraint Satisfaction. Proceedings of Workshop on Real, Large Distributed Systems (WORLDS), Workshop on Real, Large Distributed Systems (WORLDS), November, 2006.
- Integrating Security Modeling into Embedded System Design, Matthew Eby, Jan Werner, Gabor Karsai, Akos Ledeczi. Integrating Security Modeling into Embedded System Design. International Conference and Workshop on the Engineering of Computer Based Systems, IEEE, March, 2007.
- Digital Rights Management for Video Sensor Network, Taojun Wu, Liang Dai, Yuan Xue, Yi Cui. Digital Rights Management for Video Sensor Network. Proceedings of ISM 2006, IEEE, December, 2006.
- Capacity of Cooperative Fusion in the Presence of Byzantine Sensors, Oliver Kosut and Lang Tong. Capacity of Cooperative Fusion in the Presence of Byzantine Sensors. Proceedings of the 44th Annual Allerton Conference on Communication, Control, and Computation, Cornell University, September, 2006.
- Embedded Intelligent Intrusion Detection: A Behavior-Based Approach, Adrian P. Lauf, Richard A. Peters, William H. Robinson. Embedded Intelligent Intrusion Detection: A Behavior-Based Approach. IEEE 4th international symposium on Embedded Computing, IEEE, N/A, May, 2007.
- Doppelganger: Better Browser Privacy Without the Bother, Umesh Shankar and Chris Karlof. Doppelganger: Better Browser Privacy Without the Bother. Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS 2006), 154-167, November, 2006.

- Minimal TCB code execution (Extended abstract), J. M. McCune, B. Parno, A. Perrig, M. K. Reiter and A. Seshadri. Minimal TCB code execution (Extended abstract). Proceedings of the 2007 IEEE Symposium on Security and Privacy, May, 2007.
- ARSL: A Language for Authorization Rule Specification in Software Security, Weider D. Yu, Ellora Nayak. ARSL: A Language for Authorization Rule Specification in Software Security. The 11th IEEE International Symposium on Computers and Communications, 54-62, June, 2006.
- ARSL: A Language for Authorization Rule Specification in Software Security, Weider D. Yu, Ellora Nayak. ARSL: A Language for Authorization Rule Specification in Software Security. The 11th IEEE International Symposium on Computers and Communications, 54-62, June, 2006.
- ARSL: A Language for Authorization Rule Specification in Software Security, Weider D. Yu, Ellora Nayak. ARSL: A Language for Authorization Rule Specification in Software Security. Proceedings of The 11th IEEE International Symposium on Computers and Communications, 54-62, June, 2006.
- A Privacy Assessment Approach for Service Oriented Architecture Applications, Weider D. Yu, Sharanya Doddapaneni, Savitha Murthy. A Privacy Assessment Approach for Service Oriented Architecture Applications. Proceedings of The Second IEEE International Symposium on Service-Oriented System Engineering, 67-75, October, 2006.
- MiniSec: A Secure Sensor Network Communication Architecture, Mark Luk, Ghita Mezzour, Adrian Perrig, and Virgil Gligor. MiniSec: A Secure Sensor Network Communication Architecture. Proceedings of IEEE International Conference on Information Processing in Sensor Networks (IPSN), April, 2007.
- Low-cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup, Cynthia Kuo, Jesse Walker, and Adrian Perrig. Low-cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup. Usable Security (USEC), February, 2007.
- Secure Sensor Network Routing: A Clean-Slate Approach, Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig. Secure Sensor Network Routing: A Clean-Slate Approach. Conference on Future Networking Technologies (CoNEXT), December, 2006.
- Private Eyes, Amy Goldwitz. Private Eyes. *California Magazine*, 118(5), September 2006.
- A Practical Approach to Peer-to-Peer Publish-Subscribe, Ryan Peterson, Venugopalan Ramasubramanian, and Emin Gun Sirer. A Practical Approach to Peer-to-Peer Publish-Subscribe. *;login*, 31(4):42-46, July 2006.
- Sources of Insecurity: What the SonyBMG DRM incident tells us about the relationship between law, interface design and security, D. Mulligan, A. Perzanowski. Berkeley Technology Law Journal. Forthcoming, 2007.
- User choices and regret: Understanding users' decision process about consensually acquired spyware, Nathaniel Good, Jens Grossklags, David Thaw, Aaron Perzanowski

and Joseph Konstan. I/S: A Journal of Law and Policy For The Information Society, Vol. , Issue (2006).

- Hunting for metamorphic engines, Mark Stamp and Wing Wong. Hunting for metamorphic engines. *Journal in Computer Virology*, 2(3):211-229, December 2006.
- Solvable Problems in Enterprise Digital Rights Management, Mark Stamp and E. John Sebes. Solvable Problems in Enterprise Digital Rights Management. *Information Management & Computer Security*, 15(1):33-45, January 2007.
- Tracking and coordination of multiple agents using sensor networks: system design, algorithms and experiments, Songhwai Oh, Luca Schenato, Phoebus Chen, and Shankar Sastry. Tracking and coordination of multiple agents using sensor networks: system design, algorithms and experiments. *Proceedings of the IEEE*, 95(1):234-254, January 2007.
- Performance Modeling and Analysis of the IEEE 802.11 Distributed Coordination Function In Presence of Hidden Stations, Fuyi Hung, Sameer Pai, Ivan Marsic. Performance Modeling and Analysis of the IEEE 802.11 Distributed Coordination Function In Presence of Hidden Stations. Proceedings of the Military Communications Conference, 7, October, 2006.
- A Fast and Efficient Source Authentication Solution for Broadcasting in Wireless Sensor Networks, Taojun Wu, Yi Cui, Brano Kusy, Akos Ledeczi, Janos Sallai, NathanTaojun Wu, Yi Cui, Brano Kusy, Akos Ledeczi, Janos Sallai, Nathan Skirvin, Jan Werner, Yuan Xue. A Fast and Efficient Source Authentication Solution for Broadcasting in Wireless Sensor Networks. Proceedings of New Technologies, Mobility and Security, 2007, ifip, IEEE, May, 2007.
- Taxonomy of Security Attacks in Sensor Networks and, Tanya Roosta, S. P. Shieh, Shankar Sastry. Taxonomy of Security Attacks in Sensor Networks and. The First IEEE International Conference on System Integration and Reliability Improvements, December, 2006.
- Security and Privacy Issues with Health Care Information Technology, Marci Meingast, Tanya Roosta, Shankar Sastry. Security and Privacy Issues with Health Care Information Technology. IEEE International Conference of the, August, 2006.
- Convergence Analysis of Reweighted Sum-Product Algorithms, Tanya Roosta, Martin J. Wainwright, Shankar Sastry. Convergence Analysis of Reweighted Sum-Product Algorithms. International Conference on Acoustic, Speech and Signal Processing, April, 2007.
- P3P Privacy Enhancing Agent, Mark Stamp and Hsu Hui Lee. P3P Privacy Enhancing Agent. 2006 ACM Workshop on Secure Web Services, ACM, 109, November, 2006.
- Role based access control and the JXTA peer-to-peer framework, Mark Stamp, Amit Mathur and Suneuy Kim. Role based access control and the JXTA peer-to-peer framework. Proceedings of 2006 International Conference on Security & Management, June, 2006.

- Distributed Networked Control System with Lossy Links: State Estimation and Stabilizing Communication Control, Songhwai Oh and Shankar Sastry. Distributed Networked Control System with Lossy Links: State Estimation and Stabilizing Communication Control. IEEE International Conference on Decision and Control (CDC), IEEE, December, 2006.
- Communication For Omniscience by a Neutral Observer and Information-Theoretic Key Agreement of Multiple Terminals, Amin Aminzadeh Gohari, Venkat Anatharam. Communication For Omniscience by a Neutral Observer and Information-Theoretic Key Agreement of Multiple Terminals. IEEE International Symposium on Information Theory, January, 2007.

8.1.2 Books and Book Chapters

- Reliable Distributed Systems Technologies, Web Services, and Applications, Ken Birman, Springer, 2006, 0-387-21509-3
- Applied Cryptanalysis: Breaking Ciphers in the Real World, Mark Stamp, Richard M. Low, Wiley-Interscience, 2007, 978-0470114865
- Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Christopher J. Clifton, Deirdre K. Mulligan, Raghu Ramakrishnan. *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Katherine Strandburg, Daniela Stan Raicu, 11, 191-208, Springer, 2006.
- Privacy Preservation in Wireless Mesh Network, Taojun Wu, Yuan Xue, Yi Cui. *Privacy Preservation in Wireless Mesh Network*. 7, CRC Press LLC, 2007.
- Time Synchronization Attacks in Sensor Networks, Tanya Roosta, Mike Manzo, Shankar Sastry. *Time Synchronization Attacks in Sensor Networks*. Poovendran, Wang, Roy, 30, Springer, 2007.
- Multilevel security models (in The Handbook of Information Security), Mark Stamp and Ali Hushyar. *Multilevel security models (in The Handbook of Information Security)*. Wiley, 2006.
- Information Security: Principles and Practice, Mark Stamp. *Information Security: Principles and Practice*. Wiley InterScience, 2006, 978-0-471-73848-0.

8.1.3 Non-peer Reviewed Publications

- The FTC and Consumer Privacy in the Coming Decade, Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good, Jay Grossklages. *The FTC and Consumer Privacy in the Coming Decade*. Technical report, University of Pennsylvania and University of California, Berkeley, November, 2006.
- Locked cookies: Web authentication security against phishing, pharming, and active attacks, Chris Karlof, Umesh Shankar, Doug Tygar, and David Wagner. *Locked cookies: Web authentication security against phishing, pharming, and active attacks*. Technical report, University of California at Berkeley, UCB/EECS-2007-25, February, 2007.

8.2 Conference Presentations

The following is a list of conference presentations made by TRUST Center personnel during this reporting period.

- Network Experimentation and the DETER Testbed for Network Security Experiments, Sonia Fahmy. *Network Experimentation and the DETER Testbed for Network Security Experiments*. Talk or presentation, July, 2006.
- Automatic Generation and Analysis of Attach Graphs, Jeanette M. Wing. *Automatic Generation and Analysis of Attach Graphs*. Talk or presentation, July, 2006.
- Security in Wireless Sensor Network, Yuan Xue. *Security in Wireless Sensor Network*. Talk or presentation, July, 2006.
- TRUST: Team for Research in Ubiquitous Secure Technologies Overview, Shankar Sastry, Ruzena Bajcsy, Sigurd Meldal, John Mitchell, Mike Reiter, Fred Schneider, Mary Margaret Sprinkle, Janos Sztipanovits, Stephen Wicker. *TRUST: Team for Research in Ubiquitous Secure Technologies Overview*. Talk or presentation, 24, August, 2006.
- TRUST Research: Direction and Strategy, Fred B. Schneider. *TRUST Research: Direction and Strategy*. Talk or presentation, 24, August, 2006.
- Year 1:Research Overview, John Mitchell, Mike Reiter, Janos Sztipanovits. *Year 1:Research Overview*. Talk or presentation, 24, August, 2006.
- TRUST Center Activities, Stephen B. Wicker. *TRUST Center Activities*. Talk or presentation, 24, August, 2006.
- Education Initiatives, Sigurd Meldal, Janos Sztipanovits. *Education Initiatives*. Talk or presentation, 24, August, 2006.
- Outreach Initiatives, Ruzena Bajcsy. *Outreach Initiatives*. Talk or presentation, 24, August, 2006.
- TRUST Distinguished External Advisory Board Outbrief, Jay Lala, Carl Landwehr. *TRUST Distinguished External Advisory Board Outbrief*. Talk or presentation, 24, August, 2006.
- What Price Insularity? Dialogs about Computer Security Failings, Fred Schneider. *What Price Insularity? Dialogs about Computer Security Failings*. Talk or presentation, 4, October, 2006.
- Feedback from NSF, Industrial Advisory Board, External Advisory Board, Shankar Sastry. *Feedback from NSF, Industrial Advisory Board, External Advisory Board*. Talk or presentation, 8, October, 2006.
- EMR Project, Janos Sztipanovits. *EMR Project*. Talk or presentation, 9, October, 2006.
- TRUST Sensor Networking and Embedded Systems, Steve Wicker, Deirdre Mulligan. *TRUST Sensor Networking and Embedded Systems*. Talk or presentation, 9, October, 2006.
- TRUST Legacy, Ken Birman. *TRUST Legacy*. Talk or presentation, 8, October, 2006.

- CMU Knowledge Transfer, Mike Reiter. *CMU Knowledge Transfer*. Talk or presentation, 8, October, 2006.
- Trustworthy Systems, Mike Reiter, Alex Aiken, David Wagner. *Trustworthy Systems*. Talk or presentation, 9, October, 2006.
- Workshop on Future Directions for NSF's Cyber Trust Program, Karl Levitt, David Du, Lee Gruenwald, Steve Mahaney, Ralph Wachter, Mike Reiter, Helen Conti. *Workshop on Future Directions for NSF's Cyber Trust Program*. Talk or presentation, 8, October, 2006.
- Online Identity Theft Web Authentication and Threats, Doug Tygar, John Mitchell. *Online Identity Theft Web Authentication and Threats*. Talk or presentation, 9, October, 2006.
- Detection of attacks on cognitive channels, Annarita Giani. *Detection of attacks on cognitive channels*. Talk or presentation, 12, October, 2006.
- Privacy and Utility in Patient Portals, Anupam Datta. *Privacy and Utility in Patient Portals*. Talk or presentation, 9, October, 2006.
- When a Good Reputation isn't Good Enough, Jonathan Traupman. *When a Good Reputation isn't Good Enough*. Talk or presentation, 19, October, 2006.
- Automated Intruder Tracking using Particle Filtering and a Network of Binary Motion Sensors, Jeremy Schiff. *Automated Intruder Tracking using Particle Filtering and a Network of Binary Motion Sensors*. Talk or presentation, 2, November, 2006.
- Shades-of-High Confidence, Tariq Samad. *Shades-of-High Confidence*. Talk or presentation, 8, November, 2006.
- Governance of Trusted Computing, Clark Thomborson. *Governance of Trusted Computing*. Talk or presentation, 25, October, 2006.
- Security of Sensor Networks, Tanya Roosta. *Security of Sensor Networks*. Talk or presentation, 9, November, 2006.
- Scalable Trusted Computing, Ken Birman. *Scalable Trusted Computing*. Talk or presentation, 24, October, 2006.
- Experiences with Countering Internet Attacks, Vern Paxson. *Experiences with Countering Internet Attacks*. Talk or presentation, 6, December, 2006.
- Using Model Based Intrusion Detection for SCADA Networks, Alfonso Valdes. *Using Model Based Intrusion Detection for SCADA Networks*. Talk or presentation, 18, January, 2007.
- Security is Broken, Rik Farrow. *Security is Broken*. Talk or presentation, 31, January, 2007.
- Legal Issues in Network Security Research, Aaron Burnstein. *Legal Issues in Network Security Research*. Talk or presentation, 30, November, 2006.
- Industrial Wireless Systems: Implications for Everyone, Peter Fuhr. *Industrial Wireless Systems: Implications for Everyone*. Talk or presentation, 8, February, 2007.

- Noticing Notice: A large-scale experiment on the timing of software license agreements. Nathaniel Good, Jens Grossklags and Joe Konstan. CHI Proceedings, Forthcoming 2007.
- Taking the "long view" on the Fourth Amendment: Stored Records and the Sanctity of the Home. Jack Lerner. Stanford Law and Technology Review Symposium, Forthcoming 2007.
- TRUST:Team for Research in Ubiquitous Secure Technologies Overview, S. Shankar Sastry. *TRUST:Team for Research in Ubiquitous Secure Technologies Overview*. Talk or presentation, 19, March, 2007.
- TRUST Center Activities, Stephen B. Wicker. *TRUST Center Activities*. Talk or presentation, 19, March, 2007.
- Sensor Networks and Embedded Systems, Stephen Wicker, Deirdre Mulligan, Judy Cardell. *Sensor Networks and Embedded Systems*. Talk or presentation, 19, March, 2007.
- Electronic Medical Record (EMR) Project, Janos Sztipanovits. *Electronic Medical Record (EMR) Project*. Talk or presentation, 19, March, 2007.
- Trustworthy Systems, Mike Reiter. *Trustworthy Systems*. Talk or presentation, 19, March, 2007.
- Online ID Theft, Phishing, and Malware, John Mitchell, Doug Tygar. *Online ID Theft, Phishing, and Malware*. Talk or presentation, 19, March, 2007; Presented at the TRUST March 2007 NSF Site Visit/All Hands Meeting, Berkeley, CA.
- Network Defense Research, Anthony D. Joseph, Vern Paxson, Robbert van Renesse. *Network Defense Research*. Talk or presentation, 19, March, 2007.
- TRUST Education and Outreach, Kristen Gates. *TRUST Education and Outreach*. Talk or presentation, 19, March, 2007.
- Disseminating Learning Materials:TRUST Academy Online (TAO), Larry Howard. *Disseminating Learning Materials:TRUST Academy Online (TAO)*. Talk or presentation, 19, March, 2007.
- SECuR-IT: A Summer School and Immersion Program, Sigurd Meldal. *SECuR-IT: A Summer School and Immersion Program*. Talk or presentation, 19, January, 2007.
- TRUST Summer Study Programs, Ruzena Bajcsy, Kristen Gates. *TRUST Summer Study Programs*. Talk or presentation, 19, March, 2007.
- Developing an Industry Supported Computer Security Curriculum, John Mitchell. *Developing an Industry Supported Computer Security Curriculum*. Talk or presentation, March, 2007.
- Knowledge Transfer - Policy, Deirdre K. Mulligan. *Knowledge Transfer - Policy*. Talk or presentation, 19, March, 2007.

- Sensor Networks: Technology Transfer, Stephen Wicker. *Sensor Networks: Technology Transfer*. Talk or presentation, 19, March, 2007.

- ID Theft Technology Transfer, Doug Tygar, John Mitchell. *ID Theft Technology Transfer*. Talk or presentation, 19, March, 2007.

- TRUST Knowledge Transfer EMR Project, Gabor Karsai. *TRUST Knowledge Transfer EMR Project*. Talk or presentation, 19, March, 2007.

- TRUST Education and Outreach Year 3 Projects, Kristen Gates. *TRUST Education and Outreach Year 3 Projects*. Talk or presentation, 19, March, 2007.

- Knowledge Transfer, Larry Rohrbough. *Knowledge Transfer*. Talk or presentation, 21, March, 2007.

- TRUST: Team for Research in Ubiquitous Secure Technologies: Home Work Assignment, S. Shankar Sastry. *TRUST: Team for Research in Ubiquitous Secure Technologies: Home Work Assignment*. Talk or presentation, 21, March, 2007.

- Sensor Networks and Embedded Systems: Breakout Session Report, Stephen Wicker. *Sensor Networks and Embedded Systems: Breakout Session Report*. Talk or presentation, 21, March, 2007.

- End user security outbrief, Chris Karlof. *End user security outbrief*. Talk or presentation, 21, March, 2007.

- Policy Outbrief, Deirdre K. Mulligan. *Policy Outbrief*. Talk or presentation, 21, March, 2007.

- Cross-cutting Opportunities in Network Defenses, Robbert van Renesse. *Cross-cutting Opportunities in Network Defenses*. Talk or presentation, 21, January, 2007.

- Integrative Projects Ideas, Mike Reiter. *Integrative Projects Ideas*. Talk or presentation, 21, March, 2007.

- Hunting for metamorphic engines, Mark Stamp and Wing Wong. *Hunting for metamorphic engines*. Talk or presentation, 6, August, 2006.
- Unconditionally Secret Key Agreement using Public Discussion, Amin Aminzadeh Gohari, Venkat Anatharam. *Unconditionally Secret Key Agreement using Public Discussion*. Talk or presentation, 15, February, 2007.

- Vulnerabilities in First Generation RFID-enabled credit cards, Kevin Fu. *Vulnerabilities in First Generation RFID-enabled credit cards*. Talk or presentation, 22, May, 2007.

8.3 Other Dissemination Activities

The following is a list of other dissemination activities associated with TRUST Center personnel during this reporting period that are not covered elsewhere in this report.

- March 21, 2006: TRUST Participant Chris Jay Hoofnagle testified at the hearing on "Identity Theft: Innovative Solutions for an Evolving Problem" for the U. S. Senate Committee on the Judiciary Subcommittee on Terrorism, Technology and Homeland Security.

- January 18-19, 2006: Deirdre Mulligan and Pam Samuelson will speak at the DIMACS Workshop on Information Security Economics at Rutgers University.

- November 6-8, 2006: Deirdre Mulligan spoke at the Federal Trade Commission Public Hearings on Protecting Consumers in the Next Tech-ade at George Washington University. (Report: The FTC and Consumer Privacy in the Coming Decade)

- November 3-4, 2006: Unblinking: New Perspectives on Visual Privacy in the 21st Century," a Cross-Disciplinary Symposium was held on the Berkeley campus.

- July 5-28, 2006: CMU's 2006 Capacity Building Workshop occurred.
"The IACBP is an intensive in-residence summer program designed to help build Information Assurance education and research capacity at minority-serving universities. The program is organized into several sessions, offering both theoretical Information Assurance education and hands-on experiences through a boot camp on network security offered by CISCO. Specific sessions are also dedicated to curriculum development."

- June 21-23, 2006: Joint US-EU-Tekes workshop: "Long Term Challenges in High Confidence Composable Embedded Systems" (Helsinki, Finland)

- June 19, 2006: 2nd TIPPI Workshop Trustworthy Interfaces for Passwords and Personal Information (Stanford)

- June 2006: Network Security Architecture for Demand Response/Sensor Networks, for the California Energy Commission, Public Interest Energy Research Group, P.S. Subrahamanyam, D. Wagner, E. Jones, U. Shankar and J. Lerner.

8.4 Awards and Honors

The following table describes awards and honors received by TRUST Center personnel during this reporting period.

	Recipient	Reason for Award	Award Name and Sponsor	Date	Award Type
1	John Mitchell and Dan Boneh	PwdHash (Password Hash)	Computerworld 2006 Horizon Award Winner	August 21, 2006	Scientific

8.5 Graduates

No undergraduate, graduate, or Ph.D. students graduated during this reporting period.

8.6 General Knowledge Transfer Outputs

Details of knowledge transfer outputs are provided in Section 4.

8.7 Participants

The following table lists all TRUST Center participants alphabetically by category and includes each person's demographic characteristics.

9 INDIRECT/OTHER IMPACTS

9.1 International Activities

As part of TRUST's goals of disseminating results, we are eager to establish relationships with international programs where mutually beneficial opportunities exist. Our first large effort in this area is with Taiwan. The TRUST Center has received significant attention from Taiwan, and funds for cooperating with TRUST have been approved the National Legislature (the Legislative Yuan) and a member of the Taiwanese Cabinet at the level of Minister of State has been assigned to oversee the program: The International Collaboration for Advancing Security Technology (iCAST).

Taiwan is a leading player in the world of electronics and IT. Taiwan has been expanding its scope from more narrowly focused areas in manufacturing and integrated circuit design to become an aggressive player in the world of IT services. Taiwan by most accounts has the second or third largest penetration of broadband services (as of July 2005, with 10.5 million broadband users and 14.6 Internet users out of a total population of 22.8 million.) Taiwan also faces unique challenges because of its relationship with mainland China, and both public and private institutions in Taiwan are under constant attack from mainland Chinese sources. Some of these are believed to be government sponsored.

Based on TRUST, Taiwan has set up an inter-university institute called the Taiwan Information Security Center (TWISC) and has adopted an international collaboration center for research in computer security, directed by Dr. D. T. Lee, a former NSF program officer. TWISC is overseen by the cabinet level Science and Technology Advisory Group (run by a Minister of State). Major members include the National Science Council (NSC, the “Taiwanese NSF”); the Institute for Information Industry (III, a public/private software industry coordinating group); the Industrial Technology Research Institute (ITRI); major infrastructure groups (e.g., telecommunication companies); and government representatives from public safety and law enforcement.

Funding has been provided to TRUST and partner institution Carnegie Mellon University at approximately US$2M per year. The Center is very excited about this collaboration because of the outstanding quality of our Taiwanese research counterparts, their impact in the IT area, and the chance to observe and address the emerging patterns of cyber attack within Asia (and particularly emerging from mainland China) firsthand.

Please see Section 5.4 for additional information on iCAST and TRUST.

9.2 Other Outputs, Impacts, and Influences

None to report.

10 BUDGET