TRUST
Team for Research in Ubiquitous Secure Technology

Annual Report
(2011 – 2012)

May 23, 2012

TRUST is funded by the National Science Foundation
(award number CCF-0424422)

Berkeley UNIVERSITY OF CALIFORNIA Carnegie Mellon Cornell University

San José State UNIVERSITY STANFORD UNIVERSITY VANDERBILT UNIVERSITY

TABLE OF CONTENTS

1 GENERAL INFORMATION

1.1 Summary

Date Submitted	April 30, 2012
Reporting Period	June 1, 2011 – May 31, 2012
Name of the Center	Team for Research in Ubiquitous Secure Technology
Name of the Center Director	S. Shankar Sastry
Lead University	University of California, Berkeley
Contact Information	
Address	320 McLaughlin Hall
Phone Number	510-642-5771
Fax Number	510-642-9178
Email Address of Center Director	sastry@coe.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, Adrian Perrig
Address	2110 Collaborative Innovation Center Pittsburgh, PA 15213
Phone Number	412-268-2242
Fax Number	412-268-6779
Email Address of Center Director	adrian@ece.cmu.edu
Role of Institution at Center	Carnegie Mellon 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	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 underrepresented minority 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	1025 16th Avenue South Suite 102 Nashville, TN 37212
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	337H Cory Hall Berkeley, CA 94720-1774
Phone Number	510-643-3032
Fax Number	510-642-2718
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 cyber security as it affects society. 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 form the backbone of our nation's financial services and electronic commerce, are used for controlling critical infrastructures such as power, water, and telecommunications, and enable the rapid evolution in healthcare toward enhanced services increasingly supported by the digital storage of and instant access to patient health and medical data.

That said, many such computing and 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. Issues affecting privacy are poorly understood and, when they are understood, are often not sufficiently addressed in system design and development. 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 that have joined forces to organize a multifaceted response to these issues. TRUST represents the strongest and most diverse engagement in the area of trusted systems ever assembled. TRUST recognized the breadth of the problems and has combined fundamental science with a broader multidisciplinary focus on economic, social, and legal considerations as well as a substantial education mission. TRUST is enabling dialog with stakeholders whose needs simply cannot be approached in a narrower and purely technical manner or by any single research group. As such, TRUST acts as an intermediary between policy makers and society at large on the one hand, and 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, education, diversity, and knowledge transfer.

In research, TRUST has achieved success along several fronts and is addressing fundamental scientific and technological problems and advancing the state-of-the-art in a number of areas: security and privacy issues associated with the rapidly increasing use of electronic media for the archival and access of patient medical records; web authentication, end-user privacy, next-generation browser security, malware detection, and improved system forensic techniques to combat online attacks; application defenses for network-level intrusions and attacks including compromised and malfunctioning legacy applications, viruses, worms, and spyware; incentives for research, investment, policies, and procedures for technology that enhance system security, privacy, and trustworthiness; secure embedded sensor networks for large-scale applications critical to the nation's economy, energy, security, and health; and techniques that ensure trustworthy computing by securing hardware, improving software robustness, and increasing the survivability of critical systems.

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 and webcasts, TRUST has organized a series of number of workshops and conferences and a major thrust recently has been the development of online courses and support for defining an improved security curriculum for the nation's higher education system that leverages the rapid technological developments in the security area.

In diversity, TRUST has an ambitious goal of reaching a diversity goal across the Center of 30% women and 10% from underrepresented minorities. The Center has been very proactive in this regard and expanded several programs for enhancing diversity and broadening the participation of women and underrepresented minorities.

In knowledge transfer, TRUST has continued a robust program of technology transition with industry (from reporting security vulnerabilities to software vendors to various consulting activities) and active engagement with governmental agencies such as the Department of Homeland Security (DHS), the Department of Defense (DoD), and the Department of Energy (DoE) which are all concerned with issues of cyber security and trustworthiness. Recently, this has been expanded to include key constituents in the financial sector, in particular through dialogue and exchange of ideas with BITS. TRUST also has an

active set of industrial partners with whom we are engaging in research and development collaborations of mutual interest.

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 cyber security 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 commercial 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 on 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 electric power, telecommunication, healthcare, 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 research results are presented and progress in each research thrust is formally reviewed. Continuous monitoring consists of evaluation by both the research thrust area leaders 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 is addressing technical, operational, privacy, and policy challenges via interdisciplinary projects that combine fundamental science and applied research to deliver breakthrough advances in trustworthy

systems in three "grand challenge" areas as well as a Science of Security. Each research area is structured 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. An overview of the research areas is below.

- **Financial Infrastructures.** TRUST researchers aim to develop central science and engineering principles to ensure the long-term security, reliability, and ubiquitous usage of the nation's financial infrastructure. This comprises financial service enterprises, online retail businesses, and customers linked together in a trustworthy environment that supports commercial transactions. TRUST is addressing needs and challenges of a trusted financial infrastructure and its key components:
  - *Service Providers.* Financial service providers and online retailers interact with customers through e-mail, operate web servers, carry out back-office operations subject to rigorous security and performance requirements, have complex partnering agreements, and rely on their brand image and reputation for competitive advantage.
  - *Customers.* Individuals interact with financial service providers through e-mail and the web. These individuals are usually not technology experts yet they need to be assured of reliable interaction.
  - *Interconnection.* Financial infrastructure customers rely on open networking standards, browser architecture, and web application development practices. Providers may also communicate through private networks, leverage federated identity management solutions, and outsource functions to other providers through complex networking practices.
  - *Policy.* Financial services and online enterprises are subject to complex and overlapping regulations and evolving levels of customer awareness and sensitivities. Both policy and technology are necessary to drive security in an increasingly decentralized environment in which consumers with limited technical expertise and desire to manage security/privacy play a central role.

- **Health Infrastructures.** Healthcare has been characterized as a "trillion dollar cottage industry" dependent upon paper records and fragmented, error-prone approaches to service delivery. Recently, however, the healthcare industry is changing, including: the dramatic increase in the amount of information required for making health decisions, the rapidly growing use of Internet worldwide, genome research that opens up opportunity to provide personalized healthcare, and medical errors caused by failures in information management.

  Information technology enables the creation of disruptive technologies that can change health care, for example the transition from paper to digital Personal Health Records (PHRs), the growing deployment and use of real-time medical decision support systems and online patient portals, and the emphasis on robust Health Information Systems (HISs). These technologies offer unique opportunities for both improving the delivery of care in medical facilities and shifting healthcare from traditional clinical settings to patient/home-centered settings. That said, adoption of these new, transformational technologies is predicated on the availability of technical solutions and design methodologies to solve problems such as the implementation of privacy requirements and the guarantee of safe operation of HISs. To address this, TRUST researchers are tackling fundamental issues affecting the design of trusted HISs that are composable from component technologies. A primary concern in HIS design is that privacy and security requirements are frequently expressed in vague, complex and often contradictory laws and regulations. Engineering software systems that are functionally complete, able to adapt to the changing

healthcare environment, and can comply with security and privacy laws and regulations is hard, if not impossible, using conventional software and systems design technology. As such, TRUST researchers are using model-based methods to offer a revolutionary way to formally and explicitly integrate privacy and security goals into HIS architectures. While this had led to progress in problem understanding and developing new foundations, TRUST researchers also place strong emphasis on experimental work. Taking advantage of the Center's partnership with the Vanderbilt University Medical Center, researchers have developed a testbed for Model Integrated Clinical Information Systems (MICIS) and home-based health monitoring that integrates TRUST research results in a platform used by the medical community for testing and validation.

- **Physical Infrastructures.** This area addresses next generation Supervisory Control and Data Acquisition (SCADA) and other networked embedded systems that control critical physical infrastructures (e.g., power grid, natural gas distribution, automated railroad control, water, transportation) and futuristic infrastructures such as "smart" buildings and structures (e.g., active-bridges whose structural integrity depends on dynamic control or actuators).

  In physical infrastructures using new secure SCADA systems and built on top of the emerging new technology of wireless networked embedded systems, substantive issues of ownership and control of the physical infrastructure (whether it is individuals inside their homes or the grid utility provider). Security requirements are traditionally enumerated in terms of confidentiality, availability, and integrity. In this area, confidentiality is not a primary drive. Moreover, availability is often too weak—real-time constraints must be satisfied which changes the approach for defending against denial of service attacks. Ensuring integrity, however, is important as reliable operation of critical infrastructures needs to be ensured even in cases where an adversary controls a subset of the devices (which requires addressing threats such as the physical compromise of unattended nodes deployed in the field). Additionally, privacy issues arise in this area, such as understanding what can be inferred from the use and analysis of infrastructure information (e.g., increased power draw implies somebody is at home). Moreover, when distributed networks of sensors are widely deployed, opportunities for privacy abuse arise through abuse of information that is being collected for other reasons. Future infrastructures such as smart buildings and structures portend immense data collection in places routinely occupied by individuals. TRUST researchers are addressing such privacy concerns by considering them early on in the design and development of technical solutions and in advancing policy and consumer protection awareness and understanding that will support this future.

- **Science of Security.** TRUST researchers are attempting to develop a science base for security, with hopes to ultimately leverage these views in revising course content and embodying this theory in tools for system developers. Much computer security today is primarily reactive, deploying defenses for known attacks; it needs to become proactive, which is possible only if we can build systems in a principled way. A science of security would provide, for example, mental tools for understanding:
  - How to expose trust assumptions intrinsic in a system design and how different defense mechanisms relocate trust assumptions in a system,
  - How to characterize security properties in a way that gives insight into enforcement mechanisms and verification approaches,
  - What classes of security properties can various classes of defenses support,
  - What classes of attacks can various classes of defenses resist,

and similar topics. The expectation is that this science can become a basis for an engineering discipline.

Specific research activities in each area are described in more detail in the following sections. For each area, overall objectives and a scope of work are provided as well more detailed information about specific research projects conducted.

2.4.1 Financial Infrastructures

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

In the TRUST Center approach to this area, we view the financial infrastructure as the combination of financial service providers, online retail businesses, and their customers, all linked together in a trustworthy environment supporting commercial transactions. While the World-Wide Web supports a range of financial transactions, we view the financial infrastructure as including Web browser, applications, and interfaces, and also extending beyond the largely customer-oriented Web infrastructure to include companies that use the Web and back-end systems for financial purposes, their internal and interconnected back-end computer systems, and the cultural and regulatory environments in which they operate.

The complexity of the scientific, engineering, cultural, psychological, and legal challenges facing the financial infrastructure stems from several characteristics of the current environment. Foremost among them is that *attacks against or within the financial infrastructure are prevalent and lucrative*. The FBI estimates that computer crime costs industry $400B/yr, with estimates of $50B for ID theft. Another important characteristic that distinguishes this area from other TRUST grand challenge areas is that *financial systems are not under control of one organization*: web browsers that execute critical parts of current web applications are separately administered by non-experts. In addition, the intra-enterprise financial infrastructure is highly networked. In contrast to traditional computer systems, financial systems *critically involve computers and people*. While authentication of computer systems to each other has been widely studied, websites want to authenticate a person, not a machine. In addition, the importance of the human in the loop leads to significant legal, social, policy, and human factors issues. Finally, the financial infrastructure operates in the face of *rapid technological evolution*. Web technologies are rapidly changing, server development frameworks are similarly rapidly evolving, and the rise of ubiquitous handheld platforms provides a means for development and deployment of new technologies that will replace old ones rapidly.

Based on interviews and discussions with industry leaders and others, TRUST has identified a range of pressing current problems, including:

- *Authentication*. Financial infrastructure enterprises face challenges in reliably authenticating clients (customers) to site and sites (enterprises) to clients, for both email and web.
- *Malware*. Enterprises face sophisticated direct malware-based attacks to their information systems, and indirect attacks through malware on their customer's computers.
- *Internal Operations*. Enterprises face policy, compliance, and risk management challenges as well as continuing exposure to insider threats.

Representative research activities and accomplishments for Financial Infrastructures projects during this reporting period are described below. Corresponding future plans for these projects are described in Section 2.6.1.

- Behavioral Biases in Personal Information Security: An Illusion of Control Hypothesis – This project investigates privacy and security decision making through the theoretical lenses of behavioral economics, using the tools and methodologies of experimental economics, in a series of human subjects experiments. The goal is to inform the design of privacy and security technologies through behavioral studies, in order to anticipate and mitigate potential human cognitive and behavioral biases that emerge in the context of privacy and security decisions. In particular, it focuses on an "illusion of control" hypothesis and its impact on privacy and personal information security decision making. Current work is analyzing normative implication sand practical applications of our findings (i.e., what people and organizations should do to avoid biases in security/privacy decision making and effectively use security technologies in light of biases) and extending the analysis of information control to other scenarios of interest, in particular behavioral targeting and online advertising.

- The Impact of Personal Information on Trust and Economic Behavior – This project investigates how judgment of other parties is affected by the valence and maturity of the personal information we collect about those parties. We have shown that the effect of personal information about a person or company on our trust towards that person or company follows a "differential discounting" pattern depending on the valence of the information. Namely, the effect of personal information about that person with *negative* valence tends to fade away more slowly than the effect of information with *positive* valence. As a consequence, we found that positive information about a person or company builds trust ONLY IF the information is recent, not if it is old; instead, negative information reduces trust regardless if whether the information is recent or old.

- Deep Automatic Error Checking of Critical Software Infrastructure – This project aims to statically verify security properties of large-scale, security-critical software infrastructure, such as an entire operating system or web browser. The core challenge is twofold: designing automatic analysis techniques of sufficient precision and scalability to handle real systems with millions of lines of code almost automatically and, for the inevitable small percentage of cases that cannot be fully automated to understand what crucial information the programmer can provide in the form of limited specifications that will render the task tractable. Work associated with this project includes developing KLEE, a tool that uses a variation on symbolic execution to automatically generate test cases that execute most statements in real programs.

- Building Trustworthy Medical and Emergency Response Systems using Cornell's Live Objects Platform – This effort is focused on creating a secure, trustworthy and scalable technology for constructing a new generation of collaboration tools and applications that can be applied in health and financial settings, as well as in applications such as military search and rescue. There is a growing opportunity to use Service-Oriented Collaboration Applications in ways that can slash health-care costs, improve productivity, permit more effective search and rescue after a disaster, enable a more nimble information-enabled military, or make possible a world of professional dialog and collaboration without travel. Existing web service technologies, however, focus on applications in which all data travels through a data center. Implementing collaboration features using these technologies is problematic because collaborative applications can generate high, bursty update rates and yet often require low latencies and tight synchronization between collaborating users. One can often achieve better performance using direct client-to-client (also called peer-to-peer, or P2P) communication, but in today's SOA platforms, "side-band" communication is hard to integrate with hosted content.

This project builds on earlier TRUST-funded work to develop Cornell's Live Distributed Objects platform (Live Objects for short) which allows even a non-programmer to construct content-rich solutions that blend traditional web services and peer-to-peer technologies, and to share them with others. Currently, a number of external users are working with the platform so this project focuses on enhancing the platform with powerful new techniques for automatically specifying desired reliability properties (by designing a properties framework and language that "compiles" into the needed code in a way that achieves unique scalability and yields proofs of correctness), a security framework (driven by type checking), and understanding the complex identity management problems that arise when collaboration tools are introduced into real medical settings.

- Characterizing Negative Externalities and their Effect in Security Decision-Making – Deployment of security technology or practices in a network of non-cooperative agents suffers from strong negative externalities, which attackers can use to gain the upper hand. Indeed, the security investments of each agent impact the network as a whole, but do not necessarily translate in increased security for the agent investing. For instance, an individual who spends significant time and money patching and securing her machine before connecting it to the Internet nevertheless remains at the mercy of attacks that rely on other, unprotected machines, over which she has no control.

  This project seeks a formal characterization of the impact of negative externalities on global network security, both from the attacker and the target's perspectives. We are combining formal, game-theoretic, modeling with behavioral experiments (user studies), and with data collection and analysis to make original contributions to the economics foundations of information security, and to demonstrate the practical benefits of this research.

- Combating Fraud in On-Line Advertising – Online commerce is a rapidly growing aspect of the economy and a lot of that commerce is driven by on-line advertising. Just like other aspects of the financial and commerce infrastructure are vulnerable to phishing attacks, spam, denial-of-service attacks, and so on, on-line advertising is vulnerable to various type of fraud, including click-fraud. Successfully committing ad fraud yields direct monetary gains for attackers at the expense of the victims. Thus, it is natural to consider online ad fraud in an economic context. Through this project, in collaboration with researchers at Google, TRUST is modeling online advertising and studying various fraud and pricing issues.

- Fraud Detection in Consumer Reports – This project seeks to determine empirically whether it is possible to detect identity theft by an analysis of a consumer report with no extrinsic information or interaction with the consumer. If such a determination is possible, it could drive policymakers to require consumer reporting agencies (CRAs) to engage in anti-fraud monitoring of reports (CRAs currently have negative incentives to engage in this analysis). With an affirmative fraud monitoring system in place, consumers could learn of identity theft in a positive manner (notice from a CRA) rather than the current situation, where consumers often learn of the problem in a negative way (such as being denied a loan or job, or being pursued by a debt collector, because of a polluted consumer report). Positive notification would mitigate the harms of identity theft and reduce losses to consumers and businesses.

- Path of Identity Theft – This project is deconstructing the "path" of identity theft and exploring the steps taken by identity thieves in actual situations where they attempt to take control of a victim's identity. The goal is to identify and create a taxonomy of early indicia of fraud, in order

to prevent and mitigate the harm of identity theft. Once understood empirically, this knowledge could be used to develop effective early detection systems for fraud, and guide federal regulators in the specification of identity theft "Red Flags," which are now required under the Fair Credit Reporting Act.

- User Perceptions of Uses of Personal Information Online – This project is focused on building a survey application for Facebook.com using the site's API in order to both test user comprehension of third-party applications on Facebook (and the abilities of these apps and their access to the user's Facebook data) and to focus on user opinions and experiences with privacy issues on social networks.

- Trustworthy and Dependable Platforms for Critical Ultra-Large-Scale Systems – It has become evident that a diversity of emerging software-intensive systems critical to the US financial infrastructure will need to connect huge numbers of platforms, networked together in ways that may or may not be managed centrally by a higher level point of administrative control. These mission-critical ultra-large-scale (ULS) systems present quality of service (QoS) challenges that go well beyond anything seen in today's systems and systems of systems. QoS properties required by ULS systems include (1) the low latency and jitter expected in conventional real-time systems and (2) high throughput, scalability, and reliability as expected in conventional enterprise distributed systems. Achieving these QoS properties in isolation is hard; it is even harder to achieve them simultaneously in ULS systems composed of heterogeneous and (often) undependable components.

  In this project, TRUST researchers are developing and validating trustworthy and dependable platforms for critical ULS systems. These platforms are based on Service-Oriented Architecture (SOA) technologies and associated educational material that can provide an assured software platform for critical ULS systems whose QoS support enables users and applications to process the right data in the right place at the right time over a much broader range of computers and networks than is possible using conventional SOA technologies. Work is focused on two integrated thrusts: (1) Dynamic provisioning of resources for SOA-based systems, which focuses on service placement issues, such as selecting appropriate service implementations, placing the appropriate service component implementations on the most suitable nodes in a distributed system, providing varying degrees of replication depending on the importance of the service, and, in dynamic environments, ensuring QoS during service deployment time utilizing the properties of various transport protocols; and (2) QoS and trust management for SOA-based systems, which focus on assembly-wide failover management to increase availability, dynamic swapping techniques to improve performance as well as replacing potential vulnerable components, load balancing techniques to improve the scalability of ULS systems, and resolution of QoS policies which can mutually impose constraints such as reliability and low latency.

- Object-Capability Graphs in Web Browsers – Recently, there has been a growing trend to treat JavaScript pointers as object-capabilities within web browsers in order to build safer mashups and more robust implementations of the browser's same-origin security policy. In this project, TRUST researchers are evaluating the security of this approach, suggest improvements, and, where appropriate, propose alternative techniques. The main difficulty in reasoning about systems that use object-capabilities is that one capability can lead to another. For example, if a function is given a pointer to one object, then that function is also implicitly given a pointer to all the objects pointed to by that object. Researchers are modeling these transitive grants of capabilities using a capability graph which will reveal that functions are granted more capabilities

than expected, leading to attacks, and that other functions are not given dangerous capabilities, even transitively.

- Next Generation Infrastructure for In-depth Malicious Code Analysis and Defense – Malicious code analysis is extremely important for financial infrastructures. Attackers continuously employ creatively crafted malicious code to attack the financial infrastructures for illegal financial gains. Thus, the ability to automatically dissect a malicious code and extract information from it is an important cornerstone for forensic analysis and defense in financial infrastructures. In this project, TRUST researchers are leveraging previous work to design and develop the next generation infrastructure for in-depth malicious code analysis and defense, which will be particularly beneficial to the financial infrastructure.

- Trusted Computing Platforms and Secure Network Enforcement – It is becoming increasing difficult to ensure security and availability of network operations in today's highly interconnected environments, partly because the networks consist of a large number of potentially malicious nodes. For example, end-hosts and network elements may be compromised by malicious software or mis-configured. Recently, large "botnets" consisting of hundreds of thousands of hosts controlled by malicious attackers have been used to launch DDoS attacks. Unfortunately, there is currently no mechanism to enforce correct behavior by each end-host in today's network.

  Trusted computing technologies such as TPMs (Trusted Platform Modules) or secure processors enable critical security functions to be performed in trusted hardware even when a system is compromised or physically vulnerable. Potentially, if the core security functions of networking can be implemented in trusted hardware, such hardware can enforce security properties at each node rather than implementing complex solutions inside the network. Unfortunately, today's trusted computing techniques are ill-suited for such network enforcements. First, increasing popularity of virtualization techniques complicates the use of software-only mechanisms to establish trust in remote systems. Second, even hardware mechanisms are optional and can be easily turned off if a system is compromised. This project is developing a trusted computing platform that enables trustworthy enforcement of network operations at each end-host along with network technologies to utilize that platform. Hardware-based mechanisms can serve as a good basis for trust because they cannot be tampered with by any software or even by an owner without substantial effort. For the trusted platform, this project is investigating (1) hardware authentication, (2) attestation, (3) isolation, and (4) enforcement components. For the network architecture and operating system stack, this project is investigating (1) network architecture primitives for enforcing correct end-host behavior, (2) designing the OS network stack to enable such an architecture, and (3) new security and reliability attributes that can be enabled with trusted network stacks. If successful, it is expected that this research will significantly increase the security and availability of network infrastructures in a way that is inexpensive and easy to deploy.

- Data-Oriented Computing to Secure Financial Data and Transactions – In data-oriented computing, data is associated with a policy that constrains what code can operate on that data and specifies exactly how that code may manipulate it. Since the ability to manipulate the data is tied directly to the code, the data cannot be corrupted by malicious code. Since the data is encrypted with a key protected by the hardware, it cannot be read except by code with the right authorization. This approach significantly departs from previous approaches where the enforcement of security policies often relies on the security of the operating system. In our proposed system, the data owner can exert control over the access and operations of the data in a

fine-grained and controllable manner. We are applying these mechanisms to secure financial data and financial transactions and are investigating the applicability of Data-Oriented Computing on smart phones. Since smart phones have hardware protection mechanisms that are very different from desktop or X86-based systems, it is unclear how these mechanisms apply in those contexts.

- Scaffolding for Human Computer Interfaces in Financial Infrastructures – It is well known that most computer security failures result from human error, usually attributable to poor user interfaces. In this project, TRUST researchers are building on successful work in developing robust user interfaces that are secure from attack to include both a study of end-user user interfaces (e.g., electronic banking) as well as institutional user interfaces (both inter-institutional and intra-institutional). Specifically, this project is (1) studying existing financial user interfaces, and analyzing them for weaknesses, (2) developing principles for strong user interfaces for financial applications, (3) building and analyzing prototype systems embodying those principles, (4) comparing these prototypes with existing systems and each other and evaluating them using rigorous user studies that contrast their vulnerability to attack, and (5) developing new forensic techniques to trace attacks when they do occur.

- Web Security through Safe Languages – This project is addressing an important challenge problem for the financial infrastructure: how to improve the security of the web, both on the client side and on the server side, by building upon type-safe programming languages. Activities include (1) protecting legacy web services code against data-driven attacks, using precise (character-level) tainting for Java, (2) designing secure web templating systems, for development of new web services with inherent resistance to command injection attacks, (3) architectures and languages for privilege-separated web services, and (4) work on secure extensions for browsers.

- Secure and Reliable World Wide Web – The Web has become the most successful platform for developing widely-used applications. It is constantly evolving to accommodate new demands: new features are added to browsers, new server-side programming paradigms emerge, and new networking protocols are deployed. The interactions between these features present increasingly complex security challenges; every new client-side feature can potentially break security assumptions made by existing server-side code. The result is a large number of web vulnerabilities. To address these challenges, we are working on solutions for the core scientific and engineering problems in three key areas:
    - *Security for existing web applications*: We are building the next generation of automated tools to identify vulnerabilities in web applications. This will greatly advance the state of art by leveraging our experience with program analysis and language semantics to build tools that analyze Javascript and server-side code to detect vulnerabilities.
    - *Web frameworks for new applications*: New server-side programming paradigms provide opportunities for better security designs. By embracing new paradigms such as single-page web sites and embedded web applications we are developing new frameworks and programming abstractions that will greatly simplify the task of building secure web applications.
    - *Client-side security*: While our previous work on browser security has helped strengthen current browsers, many areas in the browser still need to be improved. Examples include the browser update mechanism, JavaScript sandboxing, certificate checking, and plug-in security. We are developing the engineering concepts needed to secure these components and assist vendors in deploying them in main stream browsers.

- Economics of Managing the Interdependent Security Risks – When networked parties (individuals and organizations) make decisions about their systems' security, they impact the security of the overall networked infrastructure. Thus, Internet security is interdependent security (IDS). This project is investigating the following questions: (1) What are the networked parties' incentives about security choices, given the interdependent nature of network security; (2) How would the introduction of new policies and regulations—to mitigate the divergence of individual and socially optimal incentives—affect the networked parties' incentives, and (3) How legal and regulatory channels could be jointly used to improve information structure? In this project, TRUST researchers are using game-theoretic modeling to evaluate several options (such as disclosure rules, liability regimes, introduction of mandatory user certification, and other public policies and regulations) that could improve information with the goal to investigate which policies will be the most effective for improving information structure, focusing on several information inefficiencies and discuss how to alleviate them.

2.4.2 Health Infrastructures

Project Leaders: *Janos Sztipanovits (Vanderbilt), Ruzena Bajcsy (Berkeley)*

Over the past decade, many healthcare organizations have started embracing information technology. Since 2002, more than 90% of the approximately 5,000 member institutions of the American Hospital Association have reported having websites, with most having descriptive information about their facilities and services. A relatively small but growing fraction of health care organizations have created "patient portals" that provide secure, personalized customer services via the web. For example, Vanderbilt University's patient portal is one of the more advanced healthcare sites, providing a growing set of individualized services to more than 35,000 enrolled patients. In Europe, several national initiatives have been started to provide platforms for shared electronic health data records. For example, health@net is an Austrian initiative to develop concepts and an implementation of distributed cross-institutional health data records. The platform is targeted to support cooperation and information exchange between stakeholders in the healthcare domain like hospitals, family physicians, and pharmacies. These developments and experiences have resulted in the establishment of national goals in health information systems (HIS) that include archiving and accessing personal medical records, evidence-based personalized healthcare, and home-based healthcare delivery.

During this reporting period, four related TRUST projects targeted this area:

- Privacy and Compliance for Healthcare Organizations led by Prof. Mitchell from Stanford,
- Mining Care Provider Behaviors and Anomalies from Electronic Health Record Access Logs led by Prof. Malin of Vanderbilt,
- Experimental Platform for Model-Integrated Clinical Information Systems led by Prof. Sztipanovits from Vanderbilt, and
- Real Time Wireless Monitoring of People for Independent Living and Healthcare led by Prof. Bajcsy of UC Berkeley.

Representative research activities and accomplishments for Health Infrastructures projects during this reporting period are described below. Corresponding future plans for these projects are described in Section 2.6.2.

- Real Time Wireless Monitoring of People for Independent Living and Healthcare – This project is exploring the feasibility of wireless technology for continuous real time monitoring people in indoor and outdoor environments. The critical issues in this paradigm are privacy, reliability, security, and robustness. The ultimate goal is an integrated system which will not only

observe/monitor people in their daily activities and interactions with other people but record their location movements with sporadic or continuous feedback from either an automated system and/or a healthcare supervisor in order to encourage the user's performance goals. The information collected during this process will be stored and collide with other previously collected information in databases, such as medical records, enabling both direct feedback and later queries. While this kind of a system offers many benefits to the users and institutions, it raises serious questions about privacy, credibility, integrity of the database, and vulnerability from intruders, etc.

- Privacy, Compliance, and Risk Management – Privacy is an increasingly important business concern in healthcare, financial services, and other organizations. In this project, TRUST investigators are building on previous work to develop approaches for modeling systems that handle sensitive information, languages for specifying privacy policies, and algorithms for their enforcement. They are also developing more extensive policy examples, such as a significant portion of HIPAA in a machine-processable format, and beginning a new direction incorporating risk management concepts into security analysis and decision making.

  Specifically, activities are extending a TRUST privacy policy language, the Logic of Privacy and Utility (LPU), with internal operations (e.g., Alice uses Charlie's data to do X) to look at polices for internal use within an organization and extending LPU with data provenance concepts, which is relevant since regulations may not apply when data is publicly available.

  In addition to information about individuals, privacy policies often contain clauses that refer to aggregate or anonymized information about a group of individuals. For example, the HIPAA Privacy Rule has a clause allowing "anonymized" protected health information to be released, where "anonymized" is defined to be "as certified by a qualified statistician". In order to develop computational methods for specifying and enforcing such privacy properties, it is essential to make precise the notion of "data anonymity" or "data privacy" as used in such contexts. TRUST researchers are developing theoretically well-founded definitions for data privacy concepts and integrate these concepts into our privacy policy language and enforcement methods.

  One of the biggest problems that privacy-sensitive organizations face is designing their internal activities and information practices to simultaneously serve their customers or constituents effectively and manage risks from disclosure of sensitive information. This fundamental problem arises in hospitals and clinics, where personal health information must be used to provide effective health care, but must also be protected from indiscriminate sharing to respect the privacy of patients—a requirement made more precise by HIPAA. An organization must carefully design the way it processes and uses information to balance the competing goals of privacy and the usefulness, or utility, of the business process. Because considering utility or privacy alone does not provide enough information to make meaningful management decisions, TRUST researchers are developing a framework and model for designing, evaluating, and auditing business processes to achieve utility goals while minimizing privacy risks, including identifying how much and which parts can be automated and where to align incentives to ensure people act in a manner that ensures compliance with the privacy policy.

  In another area, TRUST researchers have found significant interest and need in privacy and legal compliance issues, in particular the need for machine-processable versions of standard legal requirements in a form that technical people can use to make operational decisions. To address this need, TRUST researchers are developing a formal (computer) language for expressing

privacy policies including the forms of rules that appear in laws like HIPAA, GLBA, COPPA, CA SB1386, etc. Challenges here include expressivity, usability, and ambiguity in laws and initial focus is on expressing the HIPAA rules in this language.

Finally, TRUST researchers are addressing some exciting research problems related to risk management and computer security, in particular modeling the risks of attack and the cost of defense in a way that supports rational decision making. Some interesting dimensions of the problem are that decision making depends on the utility function and risk tolerance/aversion of the decision maker and a goal is to develop suitable mathematical models for risk management in this context and evaluating the models by carrying out case studies involving, for example, enterprise security architectures.

- Access Control Across Distributed Systems – In recent years, there have been a number of organization in healthcare industries (e.g., Kaiser Permanente, Mayo Clinic, CVS Pharmacy) adopting centralized healthcare management systems, such as those provided by Google and Microsoft. Centralization, while providing convenience, unfortunately has the side effect of granting these for-profit organizations access to a large number of people's private health information. An alternative solution to centralization is distribution—letting organizations and individuals store healthcare information in separate repositories, while making it possible for all the information be accessible by the relevant party easily and securely. In this project, TRUST researchers are studying how to make it easy to write codes that operate on a distribution of data while ensuring confidentiality.

- Software Reliability – This project aims to improve software reliability through program analysis. TRUST researchers are working in a number of areas, including (1) automatic generation of Cross-Site Scripting (XSS) and SQL injection attacks with goal-directed model checking, (2) development of UniFI, a tool that attempts to automatically detect dimension errors in Java programs, to automate the detection of dimension errors in Java programs, (3) introduction and inference of stationary fields to better understand and detect errors in new code additions by developing an efficient algorithm for inferring which fields are stationary in a program, based on the observation that many fields acquire their value very close to object creation.

- Mining Care Provider Behaviors and Anomalies from Electronic Health Record Access Logs – The goal of this project is to develop methods, implemented in working software, that automatically monitor how users (e.g., physicians) access the records of subjects (e.g., patients) and flag potentially privacy-compromising actions (e.g., an unauthorized "peek"). The definition of such behaviors will assist healthcare organization officials in understanding how their employees function and collaborate so that policies do not preclude existing complex workflows. This project builds on previous work of TRUST researchers focused on building a software toolkit and real medical record access logs repository from the Vanderbilt University Medical Center (VUMC) and proof-of-concept pattern mining from such a repository. In this project, TRUST researchers are expanding methods to mine patterns on a larger scale with a focus on sequential patterns of record access and exploring how to translate the clinical patterns our methods learn into formal workflows for integration with model-based computing and a logical privacy specification.

- Experimental Platform for Model-Integrated Clinical Information Systems – This project is focused on the development of an experimental platform for Model-Integrated Clinical Information Systems (MICIS). The role of MICIS is to provide a common integration testbed for

security- and privacy-aware Clinical Information Systems (CIS). The MICIS architecture includes a component integration platform and model integration platform: the component integration platform is based on a standard Service-Oriented Architecture (SOA) framework that is extended with policy evaluation and enforcement capabilities and the model integration platform is built on Vanderbilt's metaprogrammable Model-Integrated Computing (MIC) toolsuite. The system models capture workflows, services, organizations, roles, messages, message attributes, deployment, and access control and security policies. The generated artifacts include workflow descriptions in WS-BPEL, web service descriptors in WSDL, and access control and privacy policies in Prolog. TRUST researchers are also applying the experimental platform in three ongoing cooperative efforts between ISIS and the Vanderbilt University Medical Center.

- DexterNet Medical Infrastructure – This project builds on prior TRUST research and links the DexterNet and the Vanderbilt University Medical Center systems. DexterNet, a small-scale wireless sensor networking environment for remote healthcare, is being extended to include a privacy-aware framework for handling information out of the Nokia N800 handheld device. TRUST researchers are leveraging other TRUST sensor networking testbed by installing the action recognition system on several DexterNet motes, generating multiple streams of data for processing by the system. This enables the system to include basic activity level, action recognition, GPS location, and potentially heart and breathing data as available streams, creating a data-rich environment from which to begin exploring privacy-enhancing mechanisms.

- Personal Healthcare Information – A challenging problem in healthcare environments is to ensure that privacy expectations of patients are respected in the collection, disclosure and use of personal health information. Access control mechanisms used to restrict access to medical records have, by design, to be permissive since wrongly denying or delaying access to a patient's medical records can hinder effective delivery of healthcare. However, a permissive access control regime opens up the possibility of records being inappropriately accessed. Indeed, recent studies reveal that many policy violations occur in the real world as employees inappropriately access records of celebrities and family members motivated by general curiosity, financial gain and other considerations. To compensate for the permissive nature of their access control mechanisms, medical record systems must, in addition, support audit mechanisms that can provide a posteriori enforcement of the desired privacy and security properties. This is achieved by recording accesses made by employees in an audit log that is then examined by human auditors to determine if accesses and transmissions were appropriate and to hold individuals accountable for violating policy. Commercial tools, such as FairWarning, are beginning to emerge to assist in this process. However, unlike access control, which has been the subject of a significant body of foundational work, there is comparatively little work on the foundations of audit. We are working to develop foundations and algorithms for audit drawing on techniques from learning and game theory.

- Foundations for Service Models in Health Information Exchanges – This project is developing a service model theme for Personal Health Records (PHR) in Health Information Exchanges (HIE). We identified four essential problems of creating privacy aware and secure service models for PHR and HIE and addressed those and focused efforts on leveraging the service models theme to overcoming security and privacy barriers through functional IT components that may be provided as separable modules or services.

HIE provides the capability to electronically move clinical information among health information systems in a secure way while maintaining the meaning and protecting the privacy of the information being exchanged. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care. HIEs are the foundation for creating health information services. The primary challenge is to overcome security and privacy barriers. Our work is addressing three interrelated technology components for creating HIEs: policies governing the use of PHR, architectures for HIE's that are secure and enforce such policies without compromising effectiveness, and software technologies that improve security in HIE's.

2.4.3 Physical Infrastructures

Project Leaders: *Steve Wicker (Cornell), Adrian Perrig (Carnegie Mellon), Shankar Sastry (Berkeley)*

The nation's critical infrastructure—the power grid, telecommunications, water transport, interstate highways, etc.—constitute an immense investment. The financial investment takes the form of sunk costs and ongoing development and maintenance, while human investment is ongoing through development, maintenance, and regulatory organizations at the state and federal level. Infrastructure is clearly critical to the national economy. National modes of production depend on the functionality of critical infrastructures. Furthermore, multiple positive externalities derived from the establishment of critical infrastructure have created secondary and tertiary dependencies (e.g., air traffic control dependence on power and telecom infrastructure).

The TRUST Center recognizes that increasing complexity and 21st century security requirements demand new approaches to control, security, and long-term maintenance. Our work has been based on multi-disciplinary, multi-institutional research projects. The effort also extends across theory, technology, policies, and testbeds. For example, Berkeley, Carnegie Mellon, and Cornell have worked together on threat models, attack detection and attack-resilient models, and control-theoretic approaches to security. Vanderbilt, Carnegie Mellon, and Berkeley have developed an experimental SCADA testbed for use by Center personnel and external researchers. Cornell, Stanford, and Berkeley have worked together on technology and science support for development of privacy policies

Representative research activities and accomplishments for Physical Infrastructures projects during this reporting period are described below. Corresponding future plans for these projects are described in Section 2.6.3.

- TRUST SCADA Testbed: Infrastructure and Experiments – The goal of this project is to provide an experimental testbed with well-documented examples for SCADA research in the TRUST community by building up tool-supported experimental machinery and prototypical experiments. Using existing generic tools available from previous research (MIC tools) and customizing them to provide experimental support, TRUST researchers are developing a fully integrated toolchain where infrastructure plant models can be created and deployed on the plant simulator and a replica SCADA system can be modeled and deployed on the platform. The resulting testbed will be modular, composable (i.e., plug-n-play capabilities), and configurability via graphical interfaces, will have remote experimentation functionality, and will be equipped with new tools and capabilities to support experiments which will be conducted, documented, and results published for other researchers to use as examples and templates to build their own experiments. TRUST researchers are also developing research challenge problems whose solutions will be evaluated via testbed experiments. The desired outcome is an accessible, shared, and easily reproducible research platform, as well as experimental results and educational materials for teaching and experimentation.

- A Low Power Hardware Platform for Secure Embedded Systems – The goal of this project is to develop an ultra low power hardware platform for secure embedded sensing. TRUST researchers are using a combination of expertise in ultra low power asynchronous processor design and rapid prototyping via an FPGA-based approach to evaluate the necessary trade-offs between hardware and software. The net result of this project will be a security-aware ultra low power asynchronous microprocessor suitable for embedded sensing.

- Empirical Investigations of Privacy – Individuals' privacy concerns emanate from both online and offline sources: information sharing on social networking sites, new location-based services such as Google StreetView, and offline venues such as video surveillance and other systems that network physical places. Often the privacy concerns and objections of individuals fall outside what existing privacy law protects. For example, public and government objections to Google StreetView motivated the company to institute facial and license plate blurring within images of public streets, sidewalks, and street side facades throughout the StreetView product. Similarly, individuals object to police use of CCTV on public streets despite a legal framework that offers little to no protection. While multiple theories of privacy—and its relationship to technology—have been proposed, little empirical effort has been undertaken to document and understand how individuals conceptualize privacy on the ground. What problems do individuals perceive as "privacy" problems? How do they frame and articulate their objections? What animates their concerns? What does this tell us about the sufficiency of existing policy and technical approaches to privacy protection?

  To that end, TRUST researchers are conducting empirical investigation of several datasets that contain information about the privacy objections individuals raise in relation to Internet applications and services. Current U.S. law provides limited protection for privacy and individuals experiencing privacy harms often shy away from the added publicity that generally attends litigation. Therefore, examining lawsuit problems provide limited insight into contested privacy issues on the Internet. Fortunately, through the collection of data and access to existing data sets about interpersonal and group efforts at norm enforcement in social networks, other forms of private ordering, dispute resolution, and other "below the radar" efforts to protect privacy TRUST researchers are assembling a rich understanding of privacy's meaning in an everyday life influenced by these new technologies.

- Intrusion Detection for Supervisory Control and Data Acquisition (SCADA) Systems – A hybrid, two-stage intrusion detection system (IDS) for mobile ad hoc networks has been developed through previous TRUST funding. The framework for this IDS has the flexibility to also monitor physical infrastructures. The goal of this project is to investigate the deployment of the IDS within Supervisory Control and Data Acquisition (SCADA) systems, leveraging the collaborative development of the SCADA testbed within TRUST (Berkeley, Carnegie Mellon, and Vanderbilt) to enhance the intrusion detection capability within the remote terminal units (RTUs) of the SCADA architecture. The approach starts with the assumption that the SCADA system has been compromised then attempts to identify the deviancy of the compromised nodes and minimize the negative consequences of those nodes on the overall SCADA system.

- Analysis tools for Classes of Attacks and Defenses of Networked Embedded Control Systems – Growing concern has recently risen on the vulnerabilities of the country's strategic physical infrastructures to security attack. The extensive use of information and communication technology (ICT) has made easier to gain access to system components, increasingly connected to

the internet. Distributed Control Systems (DCS) and SCADA infrastructures are of particular interest, as they are usually the basis for sensing and control of large critical infrastructures such as power, gas, water, and industrial plants. This project is developing system theoretic tools for the design and analysis of attack detection schemes and attack-resilient estimation and control algorithms together with an evaluation of the potential consequences of an attack. Significant advances are expected in modeling attacks, in developing model based detection schemes specific to cyber-physical systems and, in designing attack-resilient estimation and control algorithms.

- Defense-in-Depth Intrusion Detection and Intrusion Tolerant Control for SCADA Systems – The cyber-physical security of real-time, continuous systems necessitates a comprehensive view and holistic understanding of network security, control theory and the physical system. Ultimately, any viable technical solutions and research directions in securing SCADA systems must lie in the conjunction of computer security, communication network and control engineering. However, the very large installed base of such systems means that in many instances we must for a long time to come rely on retrofitted security mechanisms, rather than having the option to design them in from scratch This leads to a pressing need for deployable, robust, SCADA-specific intrusion detection systems (IDS) and intrusion tolerant control techniques.

  This project is developing IDS technology and intrusion tolerant control techniques that can (1) efficiently detect and block cyber intrusions into SCADA systems in real operational environments, and in real-time, (2) without interrupting the control performance of the protected system, (3) without creating extra operational burden or operational reservations due to false alarms, (4) in the presence of both malicious and messily benign network traffic. The resulting system must operate in a real-time, robust fashion, with performance adequate to meet the demands of the dynamic cyber-physical interactions inherent to SCADA systems.

- Data Aggregation Schemes for SCADA – This project is developing a theory of aggregation of SCADA data through in-network processing and combining it with a routing scheme. Given the potentially enormous quantities of data collected by SCADA systems, it would be useful to utilize an aggregation scheme that considers spatial correlation of information. This project is investigating variations of direct diffusion and related content-aware routing schemes as well as a network using nodes with IP addresses, given the ample support to such networks and the all-IP features of next-generation cellular systems.

- Privacy-Aware Design Rules for Networking Infrastructure – This project is developing a framework for privacy-aware engineering design. The Fair Information Practices proposed in Records, Computers, and the Rights of Citizens (HEW 1973) can be translated into privacy-aware engineering design rules. These rules begin with an absolute imperative to limit information collection to explicit and publicly expressed mission requirements. This simple imperative flows into a mandate for distributed information processing, anonymity-preserving information routing and tracking functions, and strong distinctions between identifying active equipment and identifying operators and owners. This project will result in a set of clear design rules and several test cases, including 3G cellular, which demonstrate that full functionality can be retained without the massive accumulation of personal information.

- Privacy Concerns in Upcoming Demand-Response Systems – TRUST researchers are exploring the confluence of sensor networking, power distribution, privacy, and security issues that will emerge from a substantial increase in power system monitoring at the consumer level.

- Vulnerability Analysis of Phasor Measurement Units – TRUST researchers are conducting a vulnerability analysis of Phasor Measurement Units (PMUs) also known as Synchrophasors. PMUs measure voltages and currents at very disperse locations on a power grid and can output accurately time-stamped voltage and current phasors at a relatively high sampling rate. In order to guarantee accurate synchronization, they use timing information from GPS. Because these phasors are truly synchronized, synchronized comparison of two quantities is possible in real time. These comparisons can be used to assess system conditions. In power engineering, PMUs are considered one of the most important measuring devices in the future of power systems. Because of their expected critical role in the smart grid (e.g., PMUs could enable fine-grained, real-time control to avoid transient instability), it is imperative that their measurements are trustworthy. The use of GPS may induce vulnerabilities that can lead to timing attacks where a malicious agent could disrupt the synchronization of some sensors to induce the network into taking corrective measures that could compromise system's stability. In this project we are investigating the resilience of the system to timing attacks and explore effective countermeasures.

- IP Geolocation and an End to the Need for Safe Harbors – Safe harbors for online service providers have been set up in a number of jurisdictions (domestically and internationally) as a compromise that allows a "marketplace of ideas" to flourish online without interference to user activity on the part of service providers. In exchange for limited liability, OSPs often are subject to a "notify and remove" regime that requires them to remove allegedly infringing material when it is brought to their notice. Specific examples of this can be seen in the DMCA in the U.S. and Electronic Commerce Directive Articles 14 and 15 in the EU. The subjects of these regimes commonly include copyright, speech, and privacy. However, there is a notable exception in the United States in Section 230 of the Communications Decency Act. This section appears to provide blanket immunity without any exceptions for tort liability, often practically taking away any ability of users to pursue claims when their privacy is violated. We are exploring the extent to which such safe harbors may be modified or removed in return for technology that identifies the location from which an IP packet has been sent to the OSP, or conclusively shows that the sender is attempting to mask their location. In the former case, OSPs will be able to make transmission decisions that are appropriate for the jurisdiction of the sender. In the latter case, the OSP can refuse service.

2.4.4 Science of Security

Project Leaders: *Shankar Sastry (Berkeley), Fred Schneider (Cornell), John Mitchell (Stanford), Anupam Datta (Carnegie Mellon)*

TRUST researchers are attempting to develop a science base for security, with hopes to ultimately leverage these views in revising course content and embodying this theory in tools for system developers. Much computer security today is primarily reactive, deploying defenses for known attacks; it needs to become proactive, which is possible only if we can build systems in a principled way. A science of security would provide, for example, mental tools for understanding:

- How to expose trust assumptions intrinsic in a system design and how different defense mechanisms relocate trust assumptions in a system,
- How to characterize security properties in a way that gives insight into enforcement mechanisms and verification approaches,
- What classes of security properties can various classes of defenses support,
- What classes of attacks can various classes of defenses resist,

and similar topics. The expectation is that this science can become a basis for an engineering discipline.

Representative research activities and accomplishments for Science of Security projects during this reporting period are described below. Corresponding future plans for these projects are described in Section 2.6.4.

- Towards a Science of Security: Models, Logics, and Languages – The overall goal of this project is to make progress towards a science of security by developing precise security models, and reasoning methods based on logics and languages to prove security properties of system designs and implementations.

  In the area of Compositional Security, we develop a formal framework for compositional reasoning about secure systems. A key insight is to view a trusted system in terms of the interfaces that the various components expose: larger trusted components are built by combining interface calls in known ways; the adversary is confined to the interfaces it has access to, but may combine interface calls without restriction. Compositional reasoning for such systems is based on an extension of rely-guarantee reasoning for system correctness to a setting that involves an adversary whose exact program is not known. At a technical level, we present an expressive concurrent programming language with recursive functions for modeling interfaces and trusted programs, and a logic of programs in which compositional reasoning principles are formalized and proved sound with respect to trace semantics. The methods are applied to representative examples of web-based systems and network protocols. In ongoing work, we are carrying out comprehensive case studies of web browser models and trusted computing platforms, building on our previously published results (http://www.truststc.org/pubs/821.html). The technical work is reported in http://www.truststc.org/pubs/822.html and an article for a broader audience appears in the May/June 2011 special issue of *IEEE Security and Privacy* on Science of Security.

  In the area of Language-Based Security, we propose a programming language, called PCML5, for building distributed applications with distributed access control. Target applications include web-based systems in which programs must compute with stipulated resources at different sites. In such a setting, access control policies are decentralized (each site may impose restrictions on access to its resources without the knowledge of or cooperation with other sites) and spatially distributed (each site may store its policies locally). To enforce such policies PCML5 employs a distributed proof-carrying authorization framework in which sensitive resources are governed by reference monitors that authenticate principals and demand logical proofs of compliance with site-specific access control policies. The language provides primitive operations for authentication, and acquisition of proofs from local policies. The type system of PCML5 enforces locality restrictions on resources, ensuring that they can only be accessed from the site at which they reside, and enforces the authentication and authorization obligations required to comply with local access control policies. This ensures that a well-typed PCML5 program cannot incur a runtime access control violation at a reference monitor for a controlled resource.

- Trust Allocation and Information Flow –We investigated two, related thrusts. The first thrust focuses on ways to describe and reason about how trust is allocated among the components of a system when building a system that is more trustworthy than any of its components. Our goal here is to understand whether and what logics can help; we conjecture that the deductive apparatus they provide can lead to insights about engineering trade-offs that system builders might make during system design. Part of this work requires developing and understanding connections between classes of trustworthiness properties, enforcement mechanisms, and attacks.

The second thrust concerns creating a rigorous basis for enforcing information flow at the source-code level but in a realistic execution model. Here, we are concerned about caching, processor scheduling, and other aspects of the run-time environment that have previously been ignored by security researchers but nevertheless provide covert avenues for information flow. To start, we aim to develop precise formal characterizations of what information is leaked through caching channels, and to use these characterizations to explore new methods for controlling these channels. Among these methods is static analysis to help decide when to prefetch or to evict data.

A paper describing the proof theory for NAL (Nexus Authorization Logic) was completed (http://www.truststc.org/pubs/901.html). It is now in print, along with applications illustrating how the logic can be used for authorization in some surprising settings (document integrity and document confidentiality).

NAL, however, is proving useful for more than specifying authorization. A second thread of our investigation has been the use of NAL for describing the design of systems that pervasively employ mutual suspicion and the principle of least privilege. Some have argued that run-time costs would render systems structured along these lines impractical. By designing and implementing example systems, we hoped to better understand the issues. So with this in mind, we built and measured a file system and we discovered:

- NAL is an ideal language for describing system designs, because of the way it forces trust assumptions intrinsic to an architecture to become apparent.
- The performance costs associated with the necessary fine-grained authorization are indeed quite manageable.

We also investigated quantitative measures of information flow. One focus was on characterizing and controlling timing channels. The work on predictive mitigation develops a new way to control timing channels by limiting the amount of timing leakage to a user-specified bound. The bound is a function of time, and we have demonstrated that leakage can be sublinear in time.

Another focus of this effort was the development of new, more accurate mathematical models of the security properties that are enforced using an information flow type system with declassification and endorsement. In particular, we developed a semantic model for robust declassification and robust endorsement, and we showed that a type system like that used in Fabric does enforce that semantic security property. In the process, we gained a better understanding of the interaction between confidentiality and integrity, and the ways in which they are not duals.

The final focus of our quantitative information flow investigations was understanding how our new approach to quantifying integrity could be used for comparing and contrasting different algorithms for database privacy. We had earlier developed measures for integrity in terms of contamination, channel suppression, and program suppression. With these, we were able to prove a theorem characterizing the relationship between quantitative integrity, confidentiality, and database privacy. The theorem allows a quantitative comparison of differential privacy to other approaches like K-anonymity and L-diversity.

- Language-based Techniques for Web Security – This project focuses on language-based methods for isolation and integrity, foundational theory of security properties, and understanding the consequences of malicious behavior in incentivized environments. In many kinds of systems, it is useful to isolate independent components from each other. This is an important part of applying

the principle of least privilege, for example: in order to meaningfully give different privileges to different portions of a system, those components of the system must be isolated so that privileges granted to one component are not immediately available to others. However, meaningful systems are generally composed of interacting components. Therefore, once we find ways to isolate components, we must find ways for separate components to interact, while maintaining the security advantages of isolation. We have explored this general idea in the context of Web browser execution of JavaScript programs over the last few years. While our initial papers were on isolation, we have now made enough progress on isolating portions of JavaScript from each other than we have now turned our attention to secure interaction between isolated sections of JavaScript.

JavaScript is widely used to provide client-side functionality in Web applications. To provide services ranging from maps to advertisements, Web applications may incorporate untrusted JavaScript code from third parties. The trusted portion of each application may then expose an API to untrusted code, interposing a reference monitor that mediates access to security-critical resources. However, a JavaScript reference monitor can only be effective if it cannot be circumvented through programming tricks or programming language idiosyncrasies. In order to verify complete mediation of critical resources for applications of interest, we define the semantics of a restricted version of JavaScript devised by the ECMA Standards committee for isolation purposes, and develop and test an automated tool that can soundly establish that a given API cannot be circumvented or subverted. Our tool reveals a previously-undiscovered vulnerability in the widely-examined Yahoo! ADsafe filter and verifies confinement of the repaired filter and other examples from the Object-Capability literature.

We also wrote a paper on Security Modeling and Analysis for the May/June 2011 special issue of *IEEE Security and Privacy* on Science of Security. The purpose of this article is to explain a scientific process for security modeling and analysis that is widely applicable. Three examples are used to explain the method, is value, and its applicability. Our article describes a uniform approach for evaluating the security of systems and illustrates the approach by summarizing three past case studies. Security modeling centers on identifying the behavior of the system of interest (including any security defenses), the power of the system adversary, and the properties that constitute security of the system. Once a security model is clearly defined, security analysis proceeds by evaluating whether the adversary, interacting with the system, is able to defeat the desired security properties. While we illustrate security analysis using model checking, various forms of analysis methods and tools can be used to evaluate system security, including manual and automated theorem proving tools that provide assurance about absence of attacks within a specified threat model. Security modeling and analysis also provide a basis for comparative evaluation and some forms of security metrics.

- Security of Control Systems for Physical Infrastructures – Growing concern has recently risen on the vulnerabilities of the country's strategic physical infrastructures to security attack. The extensive use of information and communication technology has made easier to gain access to system components, increasingly connected to the internet. Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) infrastructures are of particular interest, as they are usually the basis for sensing and control of large critical infrastructures such as power, gas, water, and industrial plants. In this project on the security of control systems for physical infrastructures, we develop system theoretic tools for the design and analysis of attack detection schemes and attack-resilient estimation and control algorithms together with an evaluation of the potential consequences of an attack. Significant advances are required in modeling attacks,

developing model based detection schemes specific to cyber-physical systems and finally in designing attack-resilient estimation and control algorithms. We also develop taxonomy of the vulnerabilities of control systems, and outline the current security posture and current efforts for securing control systems.

Over the past decade, many concerns have been raised about the vulnerabilities of infrastructure systems to both random failures and security attacks. Cyber-security of SCADA systems is especially important, because these systems are employed for sensing and control of large physical infrastructures. So far, the existing research in robust and fault-tolerant control does not account for cyber attacks on networked control system (NCS) components. Also, the existing research in computer security neither considers the attacks targeting NCS components nor accounts for their interactions with the physical system. We are bridging this gap by focusing on (1) security threat assessment, (2) model-based attack diagnosis, and (3) resilient control design.

First, we have performed cyber-security assessment for SCADA systems based on well-defined attacker and defender objectives. The mathematical model of SCADA systems considered in this work has two control levels: regulatory control using distributed proportional-integral (PI) controllers and supervisory fault diagnosis based on approximate dynamical system models. We studied the performance of a PI control based regulatory scheme and a model-based supervisory diagnostic scheme under a class of deception attacks. We also analyzed a class of stealthy attacks which can evade detection by SCADA systems.

Second, we designed attack diagnosis schemes that incorporate the knowledge of physical dynamics of the system. For SCADA systems used to manage water canal networks, we developed an observer-based attack diagnostic scheme, in which each observer estimates the state of a reduced-order flow model. We computed the observer parameters, tested this scheme on a number of attack scenarios, and demonstrated an application of the theoretical results by a field operational test performed on the SCADA system of the Gignac water canal system. A successful experimental cyber-attack on the sensors and actuators of this canal network revealed new vulnerabilities of the current SCADA system implementation. Another illustration includes security analysis of two benchmark scenarios: the Tennessee Eastman process control system (TE-PCS) and a power system state estimator (PSSE). In both these cases, we used model-based statistical detection schemes to study stealthy deception attacks.

Third, we studied the stability of linear hyperbolic systems of PDEs when the boundary control actions and the system parameters switch discontinuously between a finite set of modes. We derived a new condition for stability of linear hyperbolic systems of PDEs under arbitrary switching of boundary control actions and system parameters and applied this result to analyze a class of switching attacks.

Fourth, we considered the problem of controlling stochastic systems for networked settings when the sensor-control data is prone to packet loss or jamming. For a class of packet drop models, we synthesized feedback control policies which minimize a given objective function subject to safety constraints.

Finally, we considered a class of games involving discrete interdependent risks when each player is a NCS, and their security is interdependent due to the exposure to network induced risks. We formulated the problem of security decisions of individual players as a two-stage non-cooperative game and characterized the equilibria of the game, which includes the determination of the

individually optimal security levels. The presence of interdependent security causes a negative externality, and the individual players tend to under invest in security relative to the social optimum. From these results, for a wide parameter range, public policy incentivising higher security investments is desirable.xxx

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 research areas is to set the Center's strategic research agenda and align individual projects in such a way that they support the strategic research objectives. Because trustworthiness is an extremely broad field and TRUST does not have the resources to cover the entire spectrum of challenges, we have annually strived to focus TRUST research in areas where the Center could have the most impact. During the first three years, the research areas enabled TRUST researchers to both pursue specific research directions that the Principal Investigators believed were important and study application areas with an eye towards better understanding the landscape. The sections below provide a description of the planned TRUST research areas for the next reporting period. For each center thrust, the name(s) and institution(s) of the lead TRUST faculty member(s) is included.

2.6.1 Financial Infrastructures

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

Representative research projects in the Financial Infrastructures area were described in Section 2.4.1; representative future plans for the next reporting period for those projects are summarized below.

- Behavioral Biases in Personal Information Security: An Illusion of Control Hypothesis – We propose to investigate privacy and security decision making through the theoretical lenses of behavioral economics, and using the tools and methodologies of experimental economics, in a series of human subjects experiments. Our goal is to inform the design of privacy and security technologies through behavioral studies, in order to anticipate and mitigate potential human cognitive and behavioral biases that emerge in the context of privacy and security decisions. In particular, we will focus on an "illusion of control" hypothesis and its impact on privacy and personal information security decision making.

  The PI has already obtained Institutional Review Board (IRB) approval for two studies and is negotiating approval with Carnegie Mellon IRB for the third study. With sufficient budget to recruit and pay human subjects to participate in the studies, the researchers expect to be able to run the studies within the first 3-5 months from the start of the project, leaving sufficient time for possible follow-up studies (based on the results of the first three studies), as well as the writing and dissemination of the results. The researchers expect to submit the completed results of at least a subset of the studies within the 12 months since the start of the project, and submit a cumulative journal article (combining the different studies) by the end of the project.

- The Impact of Personal Information on Trust and Economic Behavior – We plan to extend three studies based on *hypothetical* experiments common in experimental psychology (i.e., we measured trust by asking subjects "how much do you trust this individual") with an experiment involving *actual economic incentives*, more common in experimental economics. Specifically, we intend to run a real-life version of the Dictator game, in which each subject is instructed to split a sum of money ($1) between him/herself and the opponent. The subject has to decide how to split the money with the other player, who has no chance to reject the offer or retaliate afterwards. Consistent with the results of empirical research (see Camerer, 2003 for an overview), initial instructions also specify that previous studies showed that dictators on average keep for themselves 70% of the sum. Thus, we prime subjects to regard a 70-30 split as simply fair. After reading the initial instructions, subjects will be randomly be assigned to one of seven conditions, which differ from each other in the fairness of the opponent (valence information) and the time in which the described fair or unfair behavior occurred (maturity information). Unknown to the real subjects of the experiment, their opponents are actually computer agents. Subjects will be told that their opponent has already played seven rounds of the game in the past seven weeks, holding the role of the dictator, and will be shown a table summarizing the allocations the opponent had decided in these seven previous weeks. This experiment consists in a 3 (time: old vs. middle vs. recent) x 2 (valence: positive vs. negative) + 1 (neutral condition) between-subjects design. Our dependent variable will be how our subject chooses to allocate her $1 between herself and the opponent.

  We have already run the hypothetical version of this experiment with great success (confirming our differential discounting hypothesis: subjects are generous to opponents who have also been generous with their allocations in recent rounds, but not when the opponent was generous in earlier rounds; instead, subjects punish opponents who chose a "greedy" allocations regardless of when those allocations took place).

- Deep Automatic Error Checking of Critical Software Infrastructure – TRUST researchers have been developing KLEE, a tool that uses a variation on symbolic execution to automatically generate test cases that execute most statements in real programs. The long term goal is to be

able to take programs of 100K-1M lines and automatically run most statements in them. We are currently in the 10K or less size. Adding another zero or two will mainly require:

- More clever search heuristics: While the set of paths is exponential, the number of "interesting"' paths is not. We have developed (and will further develop) ways to merge equivalent paths (even when they differ superficially) and to reach unexecuted statements.
- More clever constraint solver tricks: While constraint solving in general is NP-hard, people program in particular, not in general. Thus, exploiting the regularities in the constraints generated by code can give exponential speedups.

In the short term, TRUST researchers are taking 50+ network applications and extending the techniques in KLEE to obtain 90%+ coverage on them. Given that this code is network exposed, improving its security in a non-trivial way will be a significant practical result. For each bug found, KLEE is able to generate an attack that will trigger it—i.e., the concrete packet sequence that when sent to an un-instrumented copy of the program will crash it. Researchers will use this ability to focus developer attention on fixing those errors.

In the next reporting period, TRUST researchers also plan to focus on scaling the new buffer overrun techniques up to both the entire Linux OS and Firefox. The goal is to automatically check at least 90% of buffer accesses automatically, and to understand what the limits of static analysis are with respect to any remaining, unverified buffer accesses.

- Building Trustworthy Medical and Emergency Response Systems using Cornell's Live Objects Platform – TRUST researchers will expand by using real problems derived from dialogs with the health, financial, and military sectors as drivers. They will build simple applications but will extract new challenge questions from them, which can then be tackled through a mixture of theoretical and practical methods and ultimately used to push the envelope on the platform, motivate papers and research talks, and to help other educators get these sorts of ideas and solutions into the hands of their students. TRUST researchers are also hoping to create a wide-area "second life" environment, based on live objects: a potential killer application for this work that could attract a very high level of interest in our effort.

- Characterizing Negative Externalities and their Effect in Security Decision-Making – TRUST researchers plan to further combine some of the measurement-based initiatives that have been conducted with formal economic modeling. Specifically, we have collected and analyzed corpora of several metrics (spam email and peer-to-peer traffic volumes) and cross-referenced them with network routing topology updates (e.g., BGP updates). We have observed so far an absence of correlation between these metrics and dynamic routing policies, which indicates that minimal intervention against undesirable traffic is being conducted by ISP at the routing level. We are currently in the process of evaluating the effect of different intervention policies on undesirable traffic volumes and will extend this work further and look into additional case studies using a similar methodology, for instance the impact of compromised SSL certificate authorities on certificate trust chains; and the cost of associated intervention policies (e.g., blacklisting a certain authority).

- Combating Fraud in On-Line Advertising – TRUST researchers plan to continue work on online advertising and fraud and continue to study a variety of privacy issues related to large scale data management.

- Fraud Detection in Consumer Reports – TRUST researchers have developed a strong working relationship with ID Watchdog and have gained a greater understanding of the company's data modeling. Additional milestones include meeting with the ID Watchdog's data team to create a system for collecting this data for empirical analysis, analyzing the data collected, and writing a report detailing the results—one measure of success being empirical observations about the ability to detect fraud from consumer reports. A future impact is also significant public policy outcome by showing that if it is possible to detect fraud in this way, this report could build a record that would support creating greater incentives for CRAs to perform anti-fraud analyses.

- Path of Identity Theft – Planned work in this project is similar to the previous project with one measure of success being the ability to make empirical statements concerning the initial steps impostors take when stealing identities.

- User Perceptions of Uses of Personal Information Online – Future activities of this project focus on the completion of a Facebook survey application using the site's API, including (1) finalizing survey questions, (2) completing the application design, including: user interface design, question delivery logic, database creation, installation "incentive" (whether we straightforwardly appeal to our subjects' sense of duty to take a survey or provide an incentive for installing the app and taking the survey, such as a prize or user feedback/game), (3) data gathering and analysis, and (4) identification of potential publishing venues based upon findings.

- Trustworthy and Dependable Platforms for Critical Ultra-Large-Scale Systems – Proposed future work builds on current accomplishments by incorporating and enhancing the following technologies and research to support maintaining QoS for pub/sub middleware via autonomic adaptation:
    - Supervised machine learning to address timely adaptation to dynamic environments and managing multiple interacting QoS requirements by selecting in a timely manner an appropriate transport protocol and protocol parameters given specified QoS and a particular environment configuration. The machine learning component will include features for several different environment configurations and supervised training to learn the correct protocol and parameters for a given environment configuration. The machine learning will interpolate and extrapolate its learning based on the current environment configuration, which might not have been included in the supervised training.
    - Environment monitoring to address timely adaptation to dynamic environments by providing environment configuration information. Relevant environment configuration values will be monitored as needed such as the number of subscribers, the percentage of network packet loss, and the sending rate of the data. These monitored values will be input to the machine learning component to determine an appropriate network transport and accompanying parameters.
    - Autonomic adaptation to address timely adaptation to dynamic environments and managing multiple interacting QoS requirements by (1) querying relevant values from the environment monitoring, (2) activating the machine learning component which will determine an appropriate transport protocol and parameters, (3) retrieving the recommended protocol settings, and (4) transitioning the adaptive network transports to use the recommended settings.
    - Incorporation of common general and domain-specific data distribution profiles to determine system behavior and performance, e.g., when certain data types are more popular or in higher demand than others. Cornell personnel (e.g., Ýmir Vigfússon) are

conducting research to characterize data distribution profiles, while Vanderbilt personnel are researching behavior of QoS-enabled pub/sub middleware utilizing the profiles.

- Object-Capability Graphs in Web Browsers –This project will evaluate the security of object-capability systems used in web browsers. Using a common set of techniques, TRUST researchers will investigate the object-capability systems used at distinct layers in web browsers. TRUST researchers plan to build a number of tools for extracting capability graphs from web browsers. For example, instrumenting the JavaScript heap to record the points-to relation among JavaScript objects and implementing an XPCOM interface parser and type inference system to deduce the relation between XPCOM types in Firefox. It is expected that these tools will be useful for future research projects and for automated testing of web browsers.

- Next Generation Infrastructure for In-depth Malicious Code Analysis and Defense –TRUST researchers plan to enhance and apply the analysis infrastructure in several different directions to take on a variety of further security threats. First, in the area of automatic directed testing, TRUST researchers will apply the infrastructure for symbolic execution and test input generation to search for vulnerabilities in security-relevant software of both defensive and offensive varieties. For instance, vulnerabilities in defensive software like virus checkers or intrusion detection systems could allow malicious software to escape detection or even allow compromise themselves. On the other hand, vulnerabilities in malicious software such as botnet clients could allow new possibilities for containing their spread or preventing them from doing harm. Second, building on existing work in understanding the protocols that malicious binary programs use for network communication, TRUST researchers want to apply related techniques to automatically understand the internal communications between functional elements in a malicious code sample. Such information about internal structure could, for instance, allow a decryption function used by a botnet to be extracted and reused for network monitoring, and understanding the functional decomposition of a binary would allow many other kinds of analysis to be applied in a more scalable way. Third, TRUST researchers plan to move beyond simple heuristics for control dependencies and develop techniques that apply more generally in both dynamic and static analysis contexts to address control dependencies, another challenging area for tainting and symbolic-execution based code analysis, in which one part of a program affects the execution of a later part not by directly modifying data that it reads, but by making control decisions that have an indirect effect on later execution. Finally, TRUST researchers plan to use the analysis infrastructure to investigate architectures for building more secure systems in the future. For instance, one reason that present systems are difficult to secure is software at many different levels must access and process sensitive information, and implementation or design flaws at any of these levels might allow compromise (e.g., allowing confidential information to be revealed, or allowing an attacker control of data he should not have). It is widely agreed that these difficulties could be ameliorated by shrinking the amount of code that must be trusted in this way, but it is difficult to do so while preserving all of the complex functionality of modern systems. In order to better understand the design possibilities for future secure systems, TRUST researchers plan to study how sensitive information is processed in large systems (e.g., the combination of JavaScript code, a web browser, a windowing system, and an operating system that are involved in using an e-commerce web application). By examining which software accesses sensitive data in current-generation systems, the goal is to look for patterns of unnecessary access and evaluate the prospects for reducing the amount of trusted code in new architectures.

- Trusted Computing Platforms and Secure Network Enforcement – TRUST researchers plan to focus more on the network aspect of the project and further develop the hardware platform based on the needs that are more specific to the network enforcement.

- Scaffolding for Human Computer Interfaces in Financial Infrastructures – A near-term milestone is the implementation of prototype systems based on design principles proposed and a refined list of forensic techniques. Longer-term milestones include user studies on various prototype systems (and contrast with existing systems), user studies on forensic techniques, seminar presentations on secure interface design, and the release of final version of educational modules. Additionally, a release is planned for defense mechanisms for learning systems in hostile environments as is the spin-off of a commercialized version of the usability testing system and an open source version of the testbeds.

- Web Security through Safe Languages – This project aims to provide strong security for the web, including securing both servers and clients—and as type-safe languages are a powerful foundation for this work, plan are to build upon Java (on the server-side) and JavaScript (on clients) and study both how to retrofit legacy code for security, as well as how to design new systems that are inherently resilient to certain classes of attacks. On the server side, work will (1) develop methods for securing legacy web application code written against a broad variety of data-driven attacks, including cross-site scripting attacks, SQL injection attacks, path manipulation attacks, and others, (2) facilitate construction of new web services code, in a way that ensures security against these and other attacks, and (3) demonstrate how new languages and system architectures can provide improved security for server-side web application code. On the client side, work will (1) study how to provide security for browser extensions, in particular how tools could partially automate and make more efficient the current manual process of analyzing new browser extensions, and (2) develop new models for extension construction that better support this kind of review process, using ideas derived from proof-carrying code (particularly, policy-carrying code).

- Secure and Reliable World Wide Web – This project aims to address the interactions between web applications and the increasingly complex security challenges they pose. Planned work will address three areas:
    - *Security for Existing Web Applications*: The are many ways that the security of existing web applications may be improved. In order to systematically understand the vulnerabilities of existing applications, we plan a concerted effort to evaluate and improve tools for testing existing applications. We will conduct an substantial study of existing commercial and open-source tools to determine how well existing tools work. Based on the outcome of this evaluation, we will then target specific classes of known vulnerabilities where we see an opportunity to dramatically improve the effectiveness of tools, and develop methods for more effective testing. Through this process, we believe we can raise awareness about existing vulnerabilities, educate our students and researchers and industrial web developers by identifying problems in existing sites, and improve the state-of-the-art of scanning tools. Based on our past experience with research and commercial tools, we are confident that substantial scientific and intellectual challenges will arise in developing new methods for improving web vulnerability analysis tools. Three directions for tool improvement are: improvements in black-box scanning for server side vulnerabilities related to server state and stored XSS or SQL, for example; improvements in scanning of client-side JavaScript and other active content sent from servers, and synergy between black-box methods and code analysis methods

applied to server-side code. In addition, as we discover new web attacks through other project activities, we will develop new methods aimed at detecting the presence of these new attacks.

- *Secure Frameworks for New Applications*: Virtually all large-scale web systems today are built on top of web application frameworks that automate the mundane tasks of building a web application. In recent years, the trend has been to put more "smarts" into the framework, where the effort expended can be re-used across multiple applications. For example, ASP.NET manages user sessions for the application and Ruby-on- Rails provides a model-view-controller abstraction that maps HTTP methods on URLs to Ruby methods on Ruby objects. These frameworks provide a powerful leverage point for building security into the foundation of applications. We plan to develop programming abstractions implemented in a web framework that will greatly help in developing secure web applications. There is considerable room for innovation in this area and industry is barely scratching the surface. This is an opportune time to undertake such an effort due to shifts in programming paradigms for web apps, specifically the move to single page applications and the prevalence of embedded web servers. These shifts present a unique opportunity to build rich security primitives into application frameworks.
- *Web Client Security*: As web developers push the limits of what is possible with current browsers, web clients are evolving to provide additional functionality and enable new web applications that were never before possible. As the web platform becomes more complex, the potential for introducing security risks increases thus slowing down the rate of innovation. We plan several research thrusts to increase the pace of innovation in web client functionality without putting users at risk. By designing extensible delivery mechanisms for security policies, we will allow servers to better communicate their expected behavior to clients and prevent attacks. By helping vendors push security updates to users quickly and securely, we will help them protect their customers if a vulnerability is discovered. By ensuring the security of browser extensions and plug-ins, we will allow developers to demonstrate revolutionary ideas while still allowing users to browse safely. Finally, by providing mechanisms for rigorously evaluating the security consequences of web features, we will allow new ideas to be deployed more quickly without introducing new vulnerabilities.

- Economics of Managing the Interdependent Security Risks – During the next reporting period, the focus will be on modeling the effects of asymmetric information in the presence of user and provider heterogeneity and considering various forms of regulatory interventions, such as disclosure rules, liability regimes, and the introduction of mandatory user certification. The legal component of this work relates to exploring how a legal framework should evolve to facilitate enabling prosecution of international crimes (e.g., bank fraud and identity theft) driven by Internet insecurity and reducing inefficiencies driven by the separation of rights for information ownership and its control in application to privacy and data collection issues.

2.6.2 Health Infrastructures

Thrust Leader: *Janos Sztipanovits (Vanderbilt University), Ruzena Bajcsy (Berkeley)*

Representative research projects in the Health Infrastructures area were described in Section 2.4.2; representative future plans for the next reporting period for those projects are summarized below.

- Real Time Wireless Monitoring of People for Independent Living and Healthcare – TRUST researchers plan to strengthen the collaboration between this project and the "Experimental

Platform for Model-Integrated Clinical Information Systems" project. The planned joint effort will include the following key components:

- Targeting post-operative home-based monitoring of Congestive Heart Failure (CHF) patients.
- Extending the system to collect, analyze, give feedback, and securely transmit heart failure patient medical data from different home medical devices to the clinical information system.
- Developing a decision support system for the treatment management of CHF patients based on the STEEP (Sepsis Treatment Enhanced through Electronic Protocolization) toolset developed by TRUST researchers at Vanderbilt.
- Supporting the delivery of treatment recommendations from decision support system to the patients.

- Privacy, Compliance, and Risk Management – In the area of Logical Specification and Enforcement of Privacy Regulations, TRUST researchers plan to continue work on logical expression and enforcement of privacy regulations. Specifically, continue efforts to formalize substantial fragments of HIPAA, GLBA and FERPA, building on prior work and extending the logic with features that appear in such regulations—dynamic and parametric roles, delegation, real-time, exceptions and cross-references, to name a few. In the area of Privacy-Preserving Aggregate Information Sharing, TRUST researchers plan to investigate a systematic foundation for privacy guarantees building on prior work on differential privacy for probabilistic systems and reasoning about privacy-preserving aggregate information sharing in organizational processes and distributed systems. This is particularly relevant in the context of processes in health care institutions that deal with both individual and aggregate information, and privacy policies (e.g., HIPAA) impose constraints on flows of both kinds of information. In the area of Information Risk Management, TRUST researchers plan to address issues associated with privacy violations that occur when organizational processes and controls in place to ensure that privacy expectations are respected by employees are violated. Since enforcing controls comes at a cost, and complete monitoring is typically infeasible, organizations have to manage their privacy risks by designing and taking into account the incentives of the employees and the external auditor. TRUST researchers view this as a mechanism design problem and are currently working on a repeated game model with reputation effects to model the interaction among the organization, its employees, and the external auditor with plans to evaluate the model by carrying out case studies of organizational processes in hospitals and BPO's. Finally, in the area of HIPAA Formalization and Demonstration, TRUST researchers will continue to develop formalization of HIPAA and to develop demonstrations systems based on this and make the Prolog presentation of HIPAA an open-source project so that any researcher or user (hospital or clinic) can use it—allowing others to contribute, hopefully leading to greater confidence in the accuracy of the formalization of HIPAA.

- Access Control Across Distributed Systems – TRUST researchers plan to create an application development platform and a reference implementation to demonstrate how it should be done. The ideas to be explored include (1) a distributed semantic web of information where access control is provide at the granularity of individual data tuples, (2) a distributed data base query language that hides the details of distribution from the end user, (3) a distributed database system that automatically enforces the compliance of access control policies, (4) a programming language that uses information flow control to safeguard against application coding errors, and (5) an integration between the application and query language to implement access control and

information flow control. The plan is to create an open API so others can build inter-operable components independently

- Software Reliability – Many modern software platforms today, including browsers, middleware server architectures, cell phone operating systems, and web application engines support third-party software extensions. TRUST researchers plan to develop an object-oriented approach that enables platform developers to efficiently enforce fine-grain safety checks on third-party extensions without requiring their cooperation. This enable harnessing the true power of third-party software by giving it access to sensitive data while ensuring that it does not leak data.

- Mining Care Provider Behaviors and Anomalies from Electronic Health Record Access Logs – Future activities are planned in four areas: (1) Develop noise filtering methods to maximize signal strength (i.e., workflows discovered) and minimize false positives (i.e., access anomalies detected); (2) Evaluate how various temporal and sequential pattern mining algorithms for categorical data function in the context of medical record access logs. Then, based on the results, determine how best to adapt such algorithms to incorporate organization-specific knowledge (e.g., clinical features and user-department assignments); (3) Investigate how to transform probabilistic workflows within the clinical environment into model-based computing. This will entail the docking of workflows to service-oriented computing languages; (4) Investigate how to transform workflows into temporal logic-based languages to specify and detect deviations from (or conflicts with) workflows in a formal manner.

- Experimental Platform for Model-Integrated Clinical Information Systems – TRUST researchers plan to strengthen the collaboration between this project and the "Privacy and Compliance for Healthcare Organizations" project. The planned joint effort will include the following key components:
  - Separating static and dynamic structural and policy constraints, where static constraints can be checked design time, while dynamic constraints need to be checked runtime.
  - Developing consistency checking tools for resolving conflicts between functional models and policies.
  - Introducing constructive modeling in the design flow for repairing functional models that contradict policy requirements.
  - Developing a suite of model transformation tools that can translate dynamic structural and policy constraints into Horn logic.

  TRUST researchers also plan to strengthen the collaboration between this project and the "Real Time Wireless Monitoring of People for Independent Living and Healthcare" project as described in that project's future plans.

- DexterNet Medical Infrastructure – Work will continue to strengthen the link between DexterNet and the Vanderbilt University Medical Center systems, while further developing connections in the privacy work at Cornell and Vanderbilt.

- Foundations for Service Models in Health Information Exchanges – This project is developing a service model theme for Personal Health Records (PHR) in Health Information Exchanges (HIE). Our work is addressing three interrelated technology components for creating HIEs: policies governing the use of PHR, architectures for HIE's that are secure and enforce such policies without compromising effectiveness, and software technologies that improve security in HIE's. PHRs broadly involve a range of possible systems, including integrated PHRs in which patients can enter and export data from systems maintained by their healthcare providers, and third-party

systems such as those advanced by Google and Microsoft. PHRs currently face many challenges: properly grasping their fundamental aims, developing technology for tracking the flow and use of medical data they hold, establishing ways for healthcare professionals to interpret the origin and integrity of this data, and formulating model privacy and security policies appropriate for third-party providers.

We plan to investigate the incentives and concerns of patients, healthcare enterprises, and third parties, and articulate and evaluate potential privacy policies that further productive use of health information systems and are socially acceptable. Based on our study of privacy and security requirements in this area, this component will explore ways that technology can be developed and public policy shaped to support appropriate privacy practices.

We will also investigate several security considerations: (a) connecting PHRs with EHRs, which is critical given the HIPAA+HITECH requirement that covered entities provide patients with their personal health data in digital form; (b) managing patient consent for using personal health information in medical studies using PHRs, which is one significant example of meaningful use of health IT; (c) using PHRs as the basis of health information exchange; and (d) empowering patients by supporting sharing of PHR data in web forums (e.g., with other patients undergoing similar treatment) with adequate control over access to and use of such data.

2.6.3 Physical Infrastructures

Thrust Leaders: *Steve Wicker (Cornell), Adrian Perrig (Carnegie Mellon), Shankar Sastry (Berkeley)*

Representative research projects in the Physical Infrastructures area were described in Section 2.4.3; representative future plans for the next reporting period for those projects are summarized below.

- TRUST SCADA Testbed: Infrastructure and Experiments – TRUST researchers plan to expand a working prototype testbed. While the current setup is operational, it is difficult to use and it does not have remote access capability so in order to overcome such limitations, TRUST researchers will develop software tools to increase ease of use, such as graphical tools, a remote access capability, and an attack models interface and create experimental research examples to demonstrate the testbed's flexibility. Expected deliverables are (1) testbed implementation available on the web, (2) a website documenting all testbed details and providing interface to the experiment documentation and repository, (3) documentation for the use of the testbed, (4) tools to configure, deploy, execute, and analyze the testbed experiments, and (5) sample experiments (stored in some form of repository).

- A Low Power Hardware Platform for Secure Embedded Systems – Future activities are focused on a SNAP2 Implementation and an FPGA-Based Prototype. For the SNAP2 Implementation, the primary activity is to complete the implementation of the SNAP processor with AES support. The physical chip implementation is underway and a complete transistor-level description of the modified SNAP processor is complete. Work on optimizing the transistor sizes to reduce power consumption while maintaining the current operating frequency of the processor is planned as preliminary results indicate that the power consumption can be significantly reduced even compared to what is currently reported. Planned work will also investigate the susceptibility of the SNAP2 implementation to side-channel attacks and the development of a mode to support a larger external ROM to "fake" the presence of on-chip FLASH memory for instruction storage. For the FPGA-Based Prototype, plans are to complete the full verification of the RTL model for SNAP which will require some back-annotation to match the model to the enhanced version of SNAP that supports the extended instruction set. Additional planned activities will enhance the

integration with the compiler tools developed by TRUST researchers at Cornell and emulating the behavior of SNAP to reduce the execution time of applications and possibly using the FPGA-based prototype to interface with other components pending the final chip fabrication. For elliptic curve cryptography, planned activities will further evaluate the hardware and software costs in support of SNAP, the limiting factor for ECC in SNAP being the memory size, including investigating techniques to reduce the memory requirements for ECC in order to encrypt the AES keys for network transmission.

- Empirical Investigations of Privacy –This project will use available data sets and, through surveys and interviews, generate new data to understand existing conceptions of privacy and the privacy management strategies employed by individuals. Planned activities include examining complaints and notices sent to search engines and service providers as well as to the third-party clearinghouse ChillingEffects.org for privacy concerns and performing a content analysis to identify privacy concerns and violations both according to type of service offered (search, photo sharing, etc.) and across all services. Also planned are surveys and interviews to document the practices individuals on social networks use to manage information about themselves. This work will explore three specific conceptions of privacy: control over presentation of self, intrusion upon seclusion or solitude or into private affairs (including family life), and public disclosure of embarrassing private facts. Activities will explore three distinct sets of strategies: how individuals manage information under their control, how they attempt to manage information about them controlled by peers (such as photos, stories, buddy lists etc.), and how they attempt to manage information about them in relation to application and service providers.

- Intrusion Detection for Supervisory Control and Data Acquisition (SCADA) Systems – One of the challenges of protecting the SCADA system is providing fault tolerance and recovery within the network. While TRUST researchers have examined intrusion detection, the natural extension is to provide some mechanism to reassign network tasks if some nodes are compromised. TRUST researchers have developed a task reallocation strategy that will optimally identify nodes that can provide identical resources of the compromised node, and reassign the network tasks accordingly. A caching scheme helps to minimize the network traffic overhead. This reallocation process is based upon information obtained from the application layer instead of monitoring all network traffic, thus minimizing the cost of monitoring all network packets. This work will leverage the TRUST SCADA testbed to provide sample underlying network traffic patterns for analysis, including the following:
  - Network recovery vs. network demands
  - Network recovery vs. power demands
  - Maintenance overhead costs for reliable reallocation methods

- Analysis tools for Classes of Attacks and Defenses of Networked Embedded Control Systems – Planned activities will (1) identify and classify known cyber-incidents to control systems based on three categories: accidents, non-targeted attacks (e.g., worms spreading in control systems software) and targeted attacks, (2) develop a taxonomy of the vulnerabilities of control systems, and outline the current security posture and current efforts for securing control systems, (3) identifying the incentives for asset owners and vendors for deploying systems with the best security practices, and (4) outline a research plan for defense in depth of control systems.

- Defense-in-Depth Intrusion Detection and Intrusion Tolerant Control for SCADA Systems – Future plans will further develop "normalcy checking", that is, a combination of techniques designed to capture two envelopes of possible system activity: (1) definitely safe operations and

(2) definitely unsafe operations. When identifiable, the first of these can be safely ignored; the second merits immediate attention/blocking; and the middle ground between the two requires additional analysis. The first technique will draw upon in this regard is specification-based intrusion detection that constructs the control system's overall allowable behavior, that is, as seen from the application level, and reflecting the monitored plant dynamics, including its valid extreme cases. The second uses encodings of misuse signatures and their possible variants. The third draws upon models derived from the control system's formal dynamics; this aspect is unique to the problem domain and holds great promise.

- Data Aggregation Schemes for SCADA – Work will continue to develop a theory of aggregation of SCADA data through in-network processing and combine it with a routing scheme.

- Privacy-Aware Design Rules for Networking Infrastructure – Planned activities will advance the development of a privacy-aware telecommunication system. Areas to be addressed are providing full disclosure of data collection, requiring consent to data collection, minimizing the collection of personal data, minimizing the identification of data with individuals, and minimizing and securing data retention. These guidelines will be applied to the development of a privacy-aware cellular network, showing how functionality can be retained without accumulating user location information.

- Privacy Concerns in Upcoming Demand-Response Systems – Planned future work includes further improving behavior extraction algorithms by using Markov Chain and Lempel-Ziv based predictive algorithms originally used, and already proven to be effective, within the context of home automation. It is also planned to further develop the disclosure metric, which associates data quality (accuracy of readings, time resolution, types of readings, etc.) from a particular source with the information that may potentially be disclosed by the data.

- Anonymity and Protection of Collected Data – In the past year, several cellular equipment manufacturers have admitted to collecting user location data through their smart phones. The manufacturers have asserted that no harm has been done, as the data was "anonymized." Independent investigators have been unable to assess this claim for at basic reasons: first, the companies involved have been unwilling to go into more detail. But more importantly, we lack a basic science of anonymity – a critical element to any science of user data security. Anonymity is the first defense against database hacking. We propose the development of a fundamental theory of anonymity that can be applied to a wide variety of data collection functions in information networks. Using information-theoretic techniques, we will develop strategies for estimating the extent to which a given dataset reveals personally identifiable information. We will then extend this effort to include correlation attacks. Using mutual information metrics as a stating point, we will develop means for characterizing the extent to which a dataset is amenable to de-anonymization through a correlation attack.

- AMI: Advanced Architectures and Policy Development – "Smart meters" (more formally known as Advanced Metering Infrastructure, or AMI) are a highly promising technology includes design choices made for purely functional reasons that may invade individual privacy on a large scale. AMI has a powerful role to play in the development of demand response systems and the smart grid, but our research team has shown that power consumption data at the granularity available to AMI can reveal detailed information about activities within the home. The question of how AMI data is to be collected, transmitted and processed is fraught with privacy concerns. Privacy-aware design practices may determine the long-term social acceptability and thus viability of this

technology. In the coming year we will continue our development of a privacy-aware architecture that combines anonymization and public key cryptography to meet the mission goals of demand response without privacy risk to the consumer. We will continue to address the question of how to motivate the adoption of privacy-aware architectures. A game-theoretic approach has been developed to identify the critical policy parameters that might drive the market to a privacy-aware Nash equilibrium. To this we have added an experimental psychology effort, in conjunction with Cornell faculty in the economics and communications departments, with the goal of determining how individuals value privacy.

- Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures – The problem of constructing malicious data attack of smart grid state estimation will be considered together with countermeasures that detect the presence of such attacks. For the adversary, using a graph theoretic approach, an efficient algorithm with polynomial-time complexity can be obtained for the design of unobservable malicious data attacks. When the unobservable attack does not exist due to restrictions of meter access, attacks will be constructed to minimize the residue energy of attack while guaranteeing a certain level of increase of mean square error. For the control center, a computationally efficient algorithm will be derived to detect and localize attacks using the generalized likelihood ratio test regularized by an L1 norm penalty on the strength of attack

- Malicious Data Attack on Real-Time Electricity Markets – Malicious data attacks to the real-time electricity market will be studied. In particular, an adversary launches an attack by manipulating data from a set of meters with the goal of influencing revenues of a real-time market. The adversary must deal with the tradeoff between avoiding being detected by the control center and making maximum profit from the real time market. We will derive an optimal attacking strategy through an optimization of a quasi-concave objective function. We will show that the probability of detection of optimal attack will always be less than 0.5. Attack performance will be evaluated using simulations on the IEEE 14-bus system.

- Next-Generation Low Power Microprocessor Prototype – There are two goals for the upcoming year: one along the chip-design thrust and a second along design methodologies for secure asynchronous systems.
    - *Chip Design*: The AES circuit will be integrated into the processor for a new version of the chip next year. Since the AES design is complete, and the processor will be completed in a month, we expect that this integration will not be a major task as we plan to develop automation tools for the physical design of asynchronous circuits this summer (using other funding).
    - *Design Methodologies*: Our design methodology for asynchronous VLSI uses a formal synthesis approach, starting with the chip described in a CSP-like notation with strong typing. One of the projects we plan to pursue in this upcoming year is the incorporation of analysis techniques such as language-based security to statically determine the security of an asynchronous chip during its design phase. By incorporating security constraints from the beginning, we believe a robust methodology can be developed with strong guarantees about information flow properties through the primary inputs and outputs of a chip, and also possibly about the vulnerability of a design to side-channel attacks.

2.6.4 Science of Security

Thrust Leaders: *Shankar Sastry (Berkeley), Fred Schneider (Cornell), John Mitchell (Stanford), Anupam Datta (Carnegie Mellon)*

Representative research projects in the Science of Security area were described in Section 2.4.4; representative future plans for the next reporting period for those projects are summarized below.

- Secure Composition for C – We plan to examine secure composition of software systems written in C. The technical approach will build on our prior work on composition of system designs. We expect to prove correspondence theorems between properties of the design level language and C source code. We will validate the theory by analyzing isolation properties of security hypervisors written in C. This work will build on our design level treatment of composition and our design level verification of security hypervisors.

- Understanding Cyber Security Metrics – There is great interest in metrics for cyber security, but little has been done towards formulating what properties these should exhibit. We plan to undertake such a study. Our goal will be to clarify in a mathematically rigorous way (i.e., axiomatically) what we might expect from reasonable cyber security metrics and to derive results about the feasibility and non-existence of functions (i.e., cyber security metrics) that exhibit certain of these desirable properties.

- Quantitative Security Logics – We plan to explore the security science of comparative computational effort for network protocols and other systems that use cryptography in various ways. We aim to develop scientific laws that will be applicable to determining, for example, how frequently a new cryptographic key must be regenerated, based on how the key is used in a communication protocol, disk encryption system, or cloud computing environment. In an effort to lay the groundwork for a more general theory, we have begun the development of Quantitative Protocol Composition Logic (QPCL), a symbolic logic for proving exact security properties of cryptographic protocols. QPCL is based on Protocol Composition Logic (PCL), previously proved sound, applied in case studies, and documented in a number of publications. The quantitative meaning of assertions in QPCL is based on a probabilistic logic introduced by Halpern, which in turn is based on the epsilon-semantics of Goldszmidt, Morris, and Pearl. We plan to develop proof rules indicating quantitative security bounds and sample axioms for digital signatures, random nonces, and other cryptographic primitives. The soundness proof for this logic will be carried out using conventional cryptographic reduction arguments and therefore imply that derivable properties are guaranteed in a conventional computational model of protocol execution and resource-bounded attack. However, the concept of deriving measurable concrete security bounds from symbolic correctness proofs is novel and fundamentally different from prior work.

- Mutliplayer Games and Team for Cyber Security of Physical Infrastructures – We plan to focus on the design of reliable and secure control for upcoming efficient infrastructure networks. Of particular interest are NCS/SCADA systems for power grid, water and gas distribution, road and air transportation, and energy management infrastructures. We will develop a comprehensive analytical framework and practical tools for building secure and resilient NCS, with focus on the survivability of networked infrastructures against both reliability failures and security attacks. We will work on the following issues: (1) Cyber-security threat assessment for NCS; (2) Model-based diagnostic tools for stealthy attacks; (3) Resilient control algorithms for survivability in the presence of security attacks and random faults; (4) Design of incentive compatible security mechanisms to reduce network risks; and (5) Testing and evaluation of diagnostic tools and resilient control algorithms.

We plan to introduce taxonomy of attack models with a primary focus on availability and integrity of NCS components. To address stealthy attacks, we will develop new diagnostic tools such as model-based intrusion detection systems. We will develop control algorithms which can withstand a wide range of attack/fault scenarios, and adaptive mechanisms to reconfigure the NCS operations in response to extreme attacks. We believe that these control-specific detection and response mechanisms will increase the survivability of NCS/SCADA systems, and reduce risks of cascading failures. In the design of control algorithms, we will also address privacy concerns. We will integrate current emulation-based testing capabilities of the cyber-DEfense Technology Experimental Research (DETER) laboratory test bed with NCS simulations and emulations which will allow us to investigate the effect of common-mode failures on NCS/SCADA systems. Finally, we will develop tools to identify and realign cyber economic incentives for security of critical infrastructures, which are predominantly managed by profit-driven, private entities. The presence of incomplete and asymmetric information results in a gap between the individually and socially optimal security levels. Thus, we will use game theoretic models to characterize the respective optima of security and control decisions for both individual and social settings. Such analysis will provide new tools to evaluate the effects of regulatory impositions aimed at improving security levels. Our main contribution in this area will be the design of incentive-compatible control algorithms for security and resilience of NCS/SCADA systems.Planned activities will (1) identify and classify known cyber-incidents to control systems based on three categories: accidents, non-targeted attacks (e.g., worms spreading in control systems software) and targeted attacks, (2) develop a taxonomy of the vulnerabilities of control systems, and outline the current security posture and current efforts for securing control systems, (3) identifying the incentives for asset owners and vendors for deploying systems with the best security practices, and (4) outline a research plan for defense in depth of control systems.

3 EDUCATION

3.1 Goals and Objectives

In education, TRUST is generating learning materials, providing dissemination structures, and establishing broad educator communities. Our education activities have reached undergraduate and graduate students, postdoctoral scholars and junior faculty, and industry professionals to address the technical, policy, and economic issues essential to improving cyber security and trustworthy systems.

Affiliated with TRUST is a multi-disciplinary team of students, post doctoral scholars, research scientists, and faculty from a world class research group of universities providing a unique breadth and depth of research expertise and accomplishment in cyber security and critical infrastructure protection. The Center research team is supported by students and faculty from partner institutions with whom the Center collaborates to provide unique opportunities for female and underrepresented minority students and faculty to engage in cross-institutional activities.

The TRUST education mission is to educate the next generation of computer scientists, engineers, lawyers, policy makers, and social scientists in the field of cyber security and trustworthy systems. Specific TRUST education goals are to:

1. Provide graduate students with research opportunities in cyber security and trustworthy systems topics.
2. Provide academic-year and summer research opportunities to undergraduate students.
3. Increase the number of women and underrepresented students that pursue graduate education in cyber security and trustworthy systems.
4. Provide academic courses and degree programs supporting TRUST research and education mission.
5. Prepare and support HSIs, MSIs and HBCUs faculty in the teaching of TRUST related research topics.
6. Develop technology to assist with the dissemination and outreach efforts of the Center.

Research and education are interwoven into all Center activities. TRUST summer programs, workshops, technical series, seminars, and internships leverage the materials and tools developed in our research projects. These materials and tools also become module content and project profiles distributed on the TRUST Academy Online (TAO). A goal of TRUST is to disseminate education materials for engineering, computer science, law, public policy, economics, and social science students working in cyber security. In the TAO we have developed teaching modules that can be incorporated into diverse curricula, ranging from privacy modules that can be taught to engineers working on SCADA control systems to cryptography modules that introduce digital rights management concepts to law students.

3.2 Performance and Management Indicators

To support both quantitative and qualitative analysis of TRUST education programs, we continue to use participant and mentor surveys, focus groups, in-depth interviews, rubrics, program metrics, and electronic portfolios as methods for data collection. These are intended to capture the effectiveness of TRUST programs and the educational and professional development value added to participants. We are also working to expand our participant tracking efforts, especially for Center students after graduation, to continue contact with participants, monitor where they are in their careers, and better understand the impact affiliation with TRUST had on their professional development and advancement. Working with organizations like the National Center for Women and Information Technology (NCWIT), the Anita Borg

Institute for Women and Technology, and the Assessing Women and Men in Engineering Project (AWE), will support our assessment efforts while disseminating our results to a broader audience as well as our TRUST Academy Online community.

The TRUST Academy Online (TAO) continues to grow as a repository for TRUST research results and course materials. User survey feedback is used to refine the portal's technology and user functions, as necessary, and data collection strategies track the use and dissemination of TRUST education materials from the TAO. Analysis of the TAO online access statistics indicates that approximately 25% of people accessing the TAO download a resource in the repository, however we will further develop portal survey and user-rating technologies to help us better understand our online community and their usage of the TAO.

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

During this reporting period, the Center education activities expanded the learning technology infrastructure, continued the work of successful undergraduate and graduate programs, and expanded academic course development and teaching opportunities. The items below describe in more detail specific education activities of the TRUST Center during this reporting period.

Activity Name	TRUST Academy Online (TAO) Portal
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

The Trust Academy Online (TAO) Portal (http://tao.truststc.org) is a vehicle for online community outreach for the TRUST Center. Its initial emphasis was to provide educators access to sets of learning materials contributed by center investigators, institutions, and partners and is used to disseminate learning materials developed or contributed by educators participating in the TRUST Center.

TAO content is bundled into "profiles" that provide descriptions, metadata, and complementary scaffolding resources such as guides to their use for teaching and learning in the classroom, lab, or online. The profiles include a variety of learning materials such as PowerPoint presentations, lecture notes, case studies, class assignments, related web site links, video clips, and "rich" media content.

During this reporting period, we continued our effort in the development of "visual storytelling" as the vehicle for this communication. In project profiles, lightweight multimedia shorts are used to

Figure 1: The TAO Portal Front Page

quickly present the essential details of a project's work in a way that is accessible to a broad audience. We used a small group of TRUST research projects at Vanderbilt to "prototype" and refine this concept. TAO media designers then collaborated with project graduate students to identify story elements and produce multimedia resources. The profiles were then established and fully populated by the project teams. Given that TRUST projects comprise a fairly stable portfolio, we feel this strategy is scalable to incrementally include all TRUST projects, resulting in a rich information flow.

Accompanying this extension in audience, we enhanced the user experience on TAO. A keystone element in our strategy was the introduction of "visual browsers" as an alternative way of presenting and selecting profiles from collections. This navigation vehicle was influenced by innovations such as Apple's "cover flow" browsers and its distinct quality makes a significant contribution to the visual impact of the portal. At the same time, we have retained the tabular, text-based browser of the courseware profiles as a navigation alternative. These changes resulted in significant increases in TAO portal usage and in the number of learning modules and courseware available.

Figure 2: The Visual Browser for TAO Courseware Profiles

To further our continuing commitment to provide educators and other users online access to materials and resources produced by TRUST researchers, the TAO has been registered as a collection in the National Science Digital Library (NSDL), the Nation's online library for education and research in Science, Technology, Engineering, and Mathematics. Using the OAI-PMH metadata harvesting protocol, the NSDL now will routinely import metadata from the TAO's courseware and project profiles and will support searching this metadata from within the digital library. Registration of the TAO in the NSDL is part of our ongoing efforts to broaden awareness of the Center's research and education missions. Membership in the NSDL and support for the OAI-PMH metadata resulted in a three-fold increase in the number of search engine visits (e.g., accessing the TAO via a Google search result) and promotion of the portal at TRUST education seminars and workshops has significantly increased the exposure of the TAO and greatly increased usage.

Activity Name	TRUST Courseware Modules and Projects
Led by	Larry Howard (Vanderbilt), Kristen Gates (Berkeley)
Intended Audience	TRUST portal users: students, faculty, researchers, and industry professionals
Approx Number of Attendees (if appl.)	Unlimited. Portal and content is open access via the Internet.

The TRUST Academy Online (TAO) is an online repository for TRUST Courseware Modules and Projects. Accessible by the public, the TAO contains learning materials available at no cost and enables educators access to leading-edge research and teaching materials specific to trusted systems technology and policy issues. The purpose of the courseware modules is to provide learning

materials that are assessable via the TAO portal that are usable by teaching faculty as course content, lecture material, and supporting information for higher education courses. Modules consist of a variety of learning materials, including PowerPoint presentations, lecture notes, case studies, class assignments, related web site links, and video clips.

TRUST researchers incorporate their findings and methods, whenever possible, into the standard curricula addressing operating systems, programming languages and compilers, analysis of algorithms, networking protocols, and databases. The primary goal for the TAO Portal is to make a body of these curricular materials available to the larger educational community. Courseware development aims at three areas of research: Security Technology, Systems Science, and Social Sciences. It is anticipated that curriculum development based on this courseware will follow different trajectories resulting in materials of different granularities, from individual modules to complete courses and lower division to the advanced graduate level. Building on our current inventory, the portal now hosts 55 contributing members and 53 projects and courseware profiles.

Activity Name	Women's Institute in Summer Enrichment (WISE)
Led by	Kristen Gates (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, with a focused recruitment effort toward underrepresented minority groups and women.
Approx Number of Attendees (if appl.)	30 participants with 11 speakers

WISE is an annual one-week residential summer program 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. WISE participation is open to U.S. professors and post-doctoral fellows, and Ph.D. candidates studying at U.S. 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 were cataloged on the TAO Portal for reference.

The program was held June 15-19, 2011 on the campus of Carnegie Mellon University. For the summer 2011 program, invited speakers were:

- Lorrie Cranor (CyLab, Carnegie Mellon University)
- Brenda Fellows (Fellows Corporate Consortium)
- Deb Frincke (National Security Agency)
- Dorothy Glancy (Santa Clara University Law)
- Leslie Lambert (Juniper Networks)
- Brad Malin (TRUST, Vanderbilt University)
- Priya Narasimhan (Carnegie Mellon University)
- Michelle Nix (McKesson)
- Joan Peckham (University of Rhode Island)

- Adrian Perrig (TRUST, Carnegie Mellon University)
- Theodora Titonis (TTI Technologies Inc.)

The summer 2011 participants included 18 faculty and 12 graduate students. The group was composed of 28 women and two men. Twelve of the participants were Underrepresented Minorities.

Tuition for WISE 2011 was $2,500; however, TRUST fellowships were available to U.S. professors, post-doctoral fellows, and Ph.D. candidates studying at U.S. universities. A total of 30 fellowships with travel stipends were awarded.

Program Evaluation: Each WISE fellow completed a program evaluation. WISE participants are tacked over a several year period to evaluate the program impact on research, teaching, professional development, job placement, and retention. This was the sixth year for WISE and WISE 2012 will be hosted by Berkeley.

An evaluation of first-year WISE participants was conducted with a follow-up survey scheduled for years one, three, and five. Recommendations from the WISE 2006 survey were put into place for the WISE 2007 program. The WISE 2007 cohort was surveyed at the end of the program and again one year out. The cohort will also be surveyed again at three and five years out. TRUST also set up a program group on LinkedIn for the WISE 2010 and 2011 cohorts. The LinkedIn sites, along with survey instruments, will facilitate the tracking of the WISE cohorts to help 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 WISE participants.

Activity Name	TRUST Research Experiences for Undergraduates (TRUST-REU)
Led by	Kristen Gates (Berkeley), Chris Hoofnagle (Berkeley), John Mitchell (Stanford), David Wagner (Berkeley), Hakim Weatherspoon (Cornell), Steve Wicker (Cornell), Yuan Xue (Vanderbilt)
Intended Audience	Undergraduate students, underrepresented minority groups, and women.
Approx Number of Attendees (if appl.)	13

The TRUST Research Experiences for Undergraduates (TRUST-REU) offers a group of talented undergraduate 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. The program provides students with the opportunity to gain research experience by participating in TRUST-related research projects with TRUST faculty and graduate students and affirms their motivation for graduate study and strengthens their qualifications. Upon completion of this program, it is expected that TRUST-REU students will be better prepared and motivated to attend graduate school.

TRUST-REU is an annual eight-week program, last year conducted June 6 – July 29, 2011. In 2011, TRUST had 13 students participating in the REU. Each student was given a $4,000 stipend for the period, travel allowance, and provided on-campus housing. In addition to the research experience,

TRUST-REU students participated in educational activities including lab tours and industry field trips, received graduate school advising, and took part in a subsidized GRE test preparation course.

The table below lists the names of the TRUST-REU 2011 participants and their research projects:

Participant Name (Home Institution)	Project Title
Michael Ayenson (Worcester Polytechnic Institute)	Analysis of FLASH,HTTP, and HTML5 Data
Patrick Baxter (Clemson University)	Automated Election Auditing from DRE Logs
Robert Carlson (California State University, Chico)	Privacy Policy Language
Anne Edmundson (Cornell University)	Automated Election Auditing from DRE Logs
Jovanni Hernandez (Drexel University)	Understanding Web Advertising Privacy Through Browser Instrumentation
Hector Tosado Jimenez (University of Puerto Rico-Mayaguez)	Hector Codes – SoNIC Steganography
Ryan Kaczowka (Youngstown State University)	Opt-in Procedures of Web Sites Selling Information to Third Parties
Keishla Ortiz López (University of Puerto Rico, Arecibo)	Automated Election Auditing from DRE Logs
John Mela (Youngstown State University)	Generating Attack Traffic using DETERLab in an Emulation-Simulation Environment
AnaMaria Quevedo (Miami Dade College)	Automated Election Auditing from DRE Logs
Cody Rigney (Youngstown State University)	Third Party Information Sharing Disclosure Practices
Samuel Rodriguez (University of Puerto Rico-Mayaguez)	Automated Election Auditing from DRE Logs
Dietrich Wambach (University of Wyoming)	Analysis of FLASH,HTTP, and HTML5 Data

Program Evaluation: TRUST-REU students are evaluated at midterm and at the end of the program. They also report their research progress at the regular weekly meetings. They receive feedback on their work from faculty advisors at the weekly meetings and after the midterm evaluation. At the end of the program, the TRUST-REU students evaluate the program via a questionnaire, the results of which are distributed to faculty advisors and graduate student mentors as feedback and for program development. TRUST-REU participants are also tracked over time to identify those students considering graduate school and those that have been accepted into graduate school programs.

Activity Name	TRUST Academic Courses
Led by	Various TRUST Faculty
Intended Audience	Undergraduate and graduate students
Approx Number of Attendees (if appl.)	Varies by course

During this reporting period, a number of academic courses were developed or updated by TRUST faculty across the Center partner institutions. Listed below is information on each course, including

the title, faculty teacher(s), intended audience, enrollment (per semester), when the course was or will be first offered, and a brief description.

Course Name:	Privacy in the Digital Age (94806)
Taught By:	Alessandro Acquisti (Heinz School - CMU)
Audience:	Graduate standing
Enrollment:	40 per semester
First Offered:	Spring 2011: Revised
Description:	The reduction of the cost of storing and manipulating information has led organizations to capture increasing amounts of information about individual behavior. New trade-offs have emerged for parties involved with privacy-enhancing or intrusive technologies: individuals want to avoid the misuse of the information they pass along to others, but they also want to share enough information to achieve satisfactory interactions; organizations want to know more about the parties with which they interact, but they do not want to alienate them with policies deemed as intrusive. Is there a "sweet" spot that satisfies the interests of all parties? Is there a combination of technological solutions, economic incentives, and legal safeguards that is acceptable for the individual and beneficial to society? Privacy is a complex and multi-faceted concept. This course combines technical, economic, legal, and policy perspectives to present a holistic view of its role and value in the digital age. It begins by comparing early definitions of privacy to the current information-focused debate. It then focuses on: • Technological aspects of privacy (privacy concerns raised by new IT such as the Internet, wireless communications, and computer matching; tracking techniques and data mining; privacy enhancing technologies and anonymous protocols; • Economic aspects (economic models of the market for privacy; financial risks caused by privacy violations; the value of customer information; • Legal aspects (laissez-faire versus regulated approaches; US versus EU legal safeguards; • Managerial implications (the emerging role of Chief Privacy Officers; compulsory directives and self-regulative efforts; • Policy aspects (trade-offs between individual privacy rights and societal needs.

Course Name:	Technology & Policy Lab (INF290)
Taught By:	Deirdre Mulligan (Berkeley)
Audience:	Graduate majors in Information Science, Law & Computer Science
Enrollment:	8 per semester
First Offered:	Spring 2011: New
Description:	In this lab course, students will engage in hands-on examinations of the policy implications of technical standards currently under consideration, the technical andpolicy impacts of legislation before state and federal government, and ongoing efforts to address policy implications of the introduction of new technology into government processes. Through research, analysis and direct participation in standards setting and other processes, students will gain experience applying law and policy theory to real world cases. The course will begin with regular meetings for discussion of various standard setting bodies and their practices and processes, the history and current status of legal doctrine and the underlying theory of technology and delegation. The remainder of the course will be project based: students may bring their own projects or contribute to ongoing collaborations with organizations such as the World Wide Web Consortium (W3C), the Organization for the Advancement of Structured Information Standards (OASIS), the Internet Architecture Board (IAB) and the Digital Due Process Coalition (ddp); or research related to the Smart Grid, eVoting, net neutrality and other complicated issues facing policymakers.

Course Name:	Graduate seminar in high assurance cloud computing architectures (CS514)
Taught By:	Ken Birman (Cornell)
Audience:	Upper division majors in computer science and engineering
Enrollment:	16 per semester
First Offered:	Spring 2011: Revised
Description:	An advanced graduate course exploring consistency issues seen in large-scale computing environments such as modern cloud-computing data centers. The course will read papers on this and related topics, looking at the major scalable computing applications, such as scalable storage systems, web services built using Google AppEngine or Azure, and internal tools like MapReduce (Hadoop), GFS, BigTable, ZooKeeper, Amazon's shopping cart, etc. In each case we'll look at what has been done, and then will try to tease out the underlying consistency assumptions, model and properties or guarantees of the solution. Cloud computing doesn't have much of a theoretical basis right now, so one might think of a course like this as laying the foundation for trying to tackle that question (namely, what would a theory of scalable consistency look like, if we had one?).

Course Name:	Data Privacy in Biomedicine (BMIF-380/CS-396)
Taught By:	Bradley Malin (Vanderbilt)
Audience:	Graduate: Biomedical Informatics and Computer Science
Enrollment:	7 per semester
First Offered:	Spring 2011: Revised
Description:	The integration of information technology into biomedical environments has enabled unprecedented advances in the collection, storage, analysis, and rapid dissemination of patient-specific data. Many organizations need to share data for various purposes, such as quality assurance, public health, and basic research. In today's complex networked environments, it is increasingly difficult to share biomedical data due to concerns about patient privacy and anonymity. The goal of this course is to introduce students to the computational challenges, as well as formal solutions, for data privacy in healthcare and biomedical environments. Data privacy is an interdisciplinary problem, so this course will touch on issues in computer science, law and policy, and biomedicine.

Course Name:	Computer Crime Law (Law 278.78)
Taught By:	Chris Hoofnagle (Berkeley)
Audience:	Graduate Law students
Enrollment:	25 per semester
First Offered:	Fall 2011: New
Description:	"Computer crime" has been with us since the 1960s, but our society's dependence upon, and the evolution of, networked communications has changed computer crime dramatically in recent decades. With the aid of a computer, individuals now can levy sophisticated attacks at a scale typically available to organized crime rings or governments. As a result, all 50 states and the federal government have enacted laws prohibiting unauthorized use of computers, and in recent years, governments have tried to harmonize these laws internationally. Computers can be the means, target of, or the source of information about a crime, and increasingly, those interested in all aspects of criminal law must have some working knowledge of computer crime to effectively investigate, prosecute, and defend cases. This course will explore the policy and law of computer crime and consider how "cybercrimes" are different from and similar to transgressive behavior in physical space. Topics will include the Fourth Amendment, forensics, electronic surveillance, cyberbullying, identity theft, computer hacking and cracking, espionage, cyberterrorism, privacy, and the challenge of cross-jurisdiction enforcement.

3.5 Professional Development Activities

During this reporting period, TRUST students were involved 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. The following sections list the various professional development activities of TRUST students.

The TRUST Center provides a unique opportunity for a wide range of cyber security issues to be addressed from many points of view—technological, scientific, social, policy, and legal. The diverse academic and professional interests of TRUST students are a major contribution to the Center's success. TRUST students have a wide range of academic and professional interests reflected by the conferences attended, workshops supported, personal development courses taken, and social and professional society

memberships. These professional development activities increase student cross-domain and multi-domain knowledge, professional growth, academic success, and overall retention–all of which benefit TRUST and the student learning experience and impact provided by the Center.

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

- Internship at eBay, San Jose, CA
- Internship at Fortinet, Sunnyvale, CA
- Internship at Intel, Oregon
- Internship at Intel Research Pittsburgh, PA
- Internship at Intuit, Mountain View, CA
- Internship at McKesson, San Francisco, CA
- Internship at Microsoft Research, Redmond, WA
- Internship at Salesforce, San Francisco, CA
- Internship at Yahoo! Research, Santa Clara, CA
- Fellowship to Anita Borg Institute
- NSF Graduate Research Fellowship

TRUST students have membership in the following organizations:

- ACM: Association for Computing Machinery
- GWIS: Graduate Women in Science
- HKN: Eta Kappa Nu National Electrical Engineering honor society
- IEEE: Institute of Electrical and Electronics Engineers
- KDP: International Education Honor Society
- PME: Psychology of Mathematics Education - International
- PMENA: Psychology of Mathematics Education - North America
- SIGMA XI: International Honor Society of Science and Engineering
- SWE: Society of Women Engineers
- Tau Beta Pi: The Engineering Honor Society
- USENIX: Advanced Computing Systems Association
- W3C: The World Wide Web Consortium
- WICSE: Women in Computer Science and Electrical Engineering

TRUST students have participated in the following workshops, conferences, and symposiums:

- ASIACCS: ACM Symposium on Information, Computer and Communications Security, Hong Kong
- Browser Privacy Mechanisms Roundtable, Berkeley, CA
- BSN: International Conference on Body Sensor Networks, London, UK
- CCS: ACM Conference on Computer and Communications Security, Chicago, IL
- CDSIA: Curriculum Development in Security and Information Assurance, San Jose, CA
- CIST: Conference on Information Systems and Technology, Charlotte, NC
- CSF: Computer Security Foundations, Abbaye des Vaux de Cernay, France
- DEBS: ACM International Conference on Distributed Event-Based Systems, New York, NY
- DEFCON and Black Hat, Las Vegas, NV
- Grace Hopper Celebration of Women in Computing, Portland, OR
- HealthSec: USENIX Workshop on Health Security and Privacy, San Francisco, CA

- HiCoNS: ACM International Conference on High Confidence Networked Systems, Beijing, China
- ICEIT: International Conference on Educational and Information Technology, Paris, France
- ICSTE: International Conference on Software Technology and Engineering, Kuala Lumpur, Malaysia
- IPTC: International Symposium on Intelligence Information Processing and Trusted Computing, Wuhan, China
- ITSEF: IT Security Entrepreneurs' Forum, Stanford, CA
- ITTC: Identity Theft Technology Council, DHS-SRI International, San Mateo, CA
- NDSS: Network and Distributed System Security Symposium, San Diego, CA
- SACMAT: Symposium on Access control Models and Technologies, Innsbruck, Austria
- SSP: IEEE Symposium on Security and Privacy, San Francisco, CA
- W3C: World Wide Web Conference, Seattle, WA
- WEIS: Workshop on the Economics of Information Security, Fairfax, VA
- WISE: Women's Institute in Summer Enrichment, Pittsburgh, PA

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	Curriculum Development in Security and Information Assurance (CDSIA)
Led by	Sigurd Meldal (San Jose State)
Intended Audience	California State University System and Hispanic Association of Colleges and Universities member institutions
Approx Number of Attendees (if appl.)	60

On April 29, 2011 TRUST hosted the fifth annual Workshop on Curriculum Development in Security and Information Assurance (CDSIA 2011) at San Jose State University.

The objectives were to (1) reach out to the many universities of the California State University system and to other universities whose mission is focused on work-force preparation and undergraduate education, (2) to share with faculty members of these institutions material and support structures developed by the TRUST partners, (3) to strengthen the TRUST-related community of educators, and (4) to facilitate the education of members of underrepresented communities in the domain of secure technologies.

CDSIA 2011 had 60 participants from 29 universities. Half of those universities are Hispanic Serving Institutions (HSIs) and the remainders are all Associate members of the Hispanic Association of Colleges and Universities (HACU). Ten of the 23 California State University (CSU) schools were represented. Three TRUST partner institutions (Carnegie Mellon, San Jose State (host), and Berkeley) also participated in CDSIA 2011. The workshop topics included:

- Security, information assurance, and policy in the general education curriculum
- Tools support for teaching IA and security curriculum components
- Sharing and delivering curricula through the TRUST Academy Online (TAO)
- What preparation does industry require?
- Certification and accreditation - where are we with respect to security?

- What role (if any) should the teaching of "malware" play in the curriculum?

Program materials generated by this program were cataloged on the TAO Portal.

Activity Name	TRUST Seminar Series
Led by	Galina Schwartz (Berkeley)
Intended Audience	Graduate level (MS & Ph.D.) students in computer science, faculty and industry professionals
Approx Number of Attendees (if appl.)	1,260 over 26 week series (Fall and Spring semesters)

The TRUST Speakers Series began in the fall of 2007. The program is a weekly event on the Berkeley campus that brings in well-known speakers who are experts in the fields of security, privacy, and trustworthy systems. The event is focused toward graduate students in computer science, industry professionals, and campus community at large. Next year we are investigating both broadcasting the TRUST Seminar talks live via the Web and archiving the talks for offline viewing—both of which will make the talks available to a much wider audience.

Activity Name	SoNIC Workshop
Led by	Hakim Weatherspoon (Cornell)
Intended Audience	Graduate level (MS & Ph.D.) students in computer science, faculty and industry professionals
Approx Number of Attendees (if appl.)	6

TRUST researcher Hakim Weatherspoon from Cornell led a week-long summer workshop for six URM undergraduate students. The students, all Computer Science majors, were exposed to research of the TRUST SONIC (SOftware defined Network InterfaCe) project which is exploring how information is encoded into packets of digital bits for transmission and how networking hardware sends and receives those packets with the goal of improving the reliability of cloud computing, where data is stored and processed in remote data centers. Participants included five students from Howard University and one student from the University of Puerto Rico.

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 portal as are workshops and symposiums such as TIPPI and WISE archived presentations.

Activity Name	DHS-SRI Infosec Technology Transition Council (ITTC)
Led by	John Mitchell (Stanford), Larry Rohrbough (Berkeley)
Intended Audience	Academics and Industry Professionals
Approx Number of Attendees (if appl.)	Total of 300 over the meetings in 2011-2012

The DHS-SRI Infosec Technology Transition Council (ITTC) is a working forum that brings together experts and leaders from the government, private sector, financial industry, information technology

services, venture capital, and academia and science sectors to address the problem of information security and related activity.

Workshops are held three times per year (during this period they were held in June 2011, September 2011, and February 2012) and are used to identify proactive IT security solutions and assist in the acceleration of its development and deployment into the marketplace. Seasoned IT security practitioners, law enforcement professionals, and representatives from academia and science have strategically aligned themselves with subject matter experts and organizations to accomplish this goal. A key component to the success of this public-private partnership is the ability to actively work with leaders in the community who are principals of change in an effort to better protect our communities and corporations from attacks against their critical infrastructures. The subject matter experts of the ITTC seek to share information that will assist in the discovery, due diligence, development, and deployment of next generation technologies best suited to protect our critical infrastructures and serve our communities.

John Mitchell from Stanford and Larry Rohrbough from Berkeley are the TRUST liaisons to the DHS-SRI ITTC and meetings are attended by various TRUST researchers.

Activity Name	IT Security Entrepreneurs' Forum (ITSEF)
Led by	John Mitchell (Stanford), Larry Rohrbough (Berkeley)
Intended Audience	Academics and Industry Professionals
Approx Number of Attendees (if appl.)	275 for the March 20-21, 2012 meeting

The Department of Homeland Security and Kauffman Foundation IT Security Entrepreneurs' Forum (ITSEF) is a Public Private Partnership initiative is designed to "bridge the gap" between IT security solution providers and the end users of our nation's IT and Telecommunications critical infrastructures. The ITSEF believes that innovative solutions developed by entrepreneurs' can best be promoted through collaborative efforts between the public and private sectors.

A key component to the success of such relationships is to identify and bring together public and private sector "change agents" who can drive education and awareness programs through forums that will promote lasting and permanent relationships between all levels of government and the full range of emerging and established private sector companies. This year's forum occurred during a critical time as attacks and emerging threats continue to increase in sophistication and frequency against our nation's IT and telecommunication infrastructures. The ITSEF strives to accelerate the search for and implementation of "best of class" solutions to address such threats.

John Mitchell from Stanford and Larry Rohrbough from Berkeley are the TRUST liaisons and Stanford is a sponsor of the ITSEF.

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 Professional Workshops and Symposiums.

Learning Materials and Technology

During this reporting period, there was a continued effort to reconfigure the TRUST Academy Online (TAO) Portal, including metadata technology and information architecture, as well as the further development of TAO courseware modules and projects. Since 2009, this effort has resulted in a three-fold usage increase of the TAO portal. TRUST researchers have created learning modules and courseware, currently 326 resource files produced by 55 TRUST contributors.

We have implemented data collection strategies that will track the use and dissemination of TRUST education materials from the TAO. Further analysis of the TAO online access statistics indicates that approximately 25% of people accessing the TAO download a resource in the repository. That said, we will further develop portal survey and user rating technologies to help us better understand our online community and their usage of the TAO. Additionally, the TAO has been registered as a collection in the National Science Digital Library (NSDL), the nation's online library for education and research in Science, Technology, Engineering, and Mathematics. Registration of the TAO in the NSDL is part of our ongoing efforts to broaden awareness of the Center's research and education missions.

Professional Development Workshop and Symposiums

TRUST professional development activities are designed for graduate students, post-doctoral scholars, industry researchers, and faculty from various disciplines working and conducting research in cyber security and trustworthy systems. In addition to education and learning opportunities, these programs support professional growth, especially for female and URM faculty, with the goal of ultimately expanding the number female and URM researchers in cyber security and trustworthy systems.

TRUST faculty and staff have participated at education and outreach conferences through panels, associated workshops, or a series of presentations, including: Computer Alliance for Hispanic Serving Institutions (CAHSI), Richard Tapia Celebration in Diversity in Computing, Grace Hopper Celebration of Women in Computing, Executive Women's Forum (EWF), Bay Area Council Cyber Security Education/Workforce Subcommittee, Berkeley EECS Annual Research Symposium (BEARS), Bay Area Council and the Bay Area Science & Innovation Consortium (BASIC), EE and CS Education Days at UC Berkeley, and the Richmond High School Engineering Partnership Academy.

The assessment process is both qualitative and quantitative and will include pre- and post-evaluation surveys, focus groups, participant assessments, and program evaluations for the education, human resource development, and underrepresented minority student uptake initiatives of TRUST. Evaluation rubrics will be developed for assessment of course materials, electronic portfolios, and research activities.

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 TAO will continue to develop. Course modules and learning objects will be developed as educational deliverables of each TRUST research area. As the review process continues, refinement will be made to the module design and the portal. The TAO is making an impact by providing TRUST Center learning materials for use by teaching faculty as course content, lecture materials, and program support for the development of their computer science or related higher education courses. TRUST has created a significant number of learning modules across a wide range of topical areas, providing educators access to a substantial amount of leading-edge research and teaching material. The Center will continue to place materials generated by our education, outreach, and diversity programs on the TAO to be shared with other teachers and researchers.

TRUST visibility and influence in education community continues to grow as TRUST researchers and staff participation in educational conferences, workshops, panel discussions, and industry workgroups take hold.

The Women's Institute in Summer Enrichment (WISE) is a signature program for TRUST and consistently receives excellent evaluations form participants. WISE is hosted at TRUST partner institutions (the summer 2012 will be held on the Berkeley campus) and the Center will continue to offer this program each summer. To meet the program's increasing demand, TRUST will expand WISE to 30 participants per summer with a greater emphasis on recruiting female URM scholars.

The TRUST-REU 2012 will host 10-15 undergraduate students at TRUST partner institutions Berkeley, Carnegie Mellon, Cornell, Stanford, and Vanderbilt, increasing the number of undergraduate students exposed to research in general and the TRUST Center in particular. The TRUST-REU will continue to support the Center's goal of increasing the number of underrepresented minority groups and women that are conducting research in cyber security and trusted systems.

During the summer 2012, TRUST REU students will participate in the following research projects:

- *A Study of Captcha Security*: Human interaction tests (better known as Captchas) are used to distinguish human activity from automated activity on websites. The main goal is to prevent various forms of online abuse like spam messages, fake registrations, automatic login attempts, poll rigging. Captchas are traditionally in the form of a visual or audio test in which the users are asked to recognize a sequence of distorted alphanumeric characters. Such recognition is assumed to be hard for machines while being relatively easy for humans. Studying Captcha security (e.g., breaking captchas), requires a large effort from the attackers in terms of labeling thousands of captcha samples by hand, in order to train the classifiers. In this project, we want to explore the possibility of using semi-supervised learning approaches to break captchas. With only a small number of solved captchas given, semi-supervised learning can exploit a huge corpus of unsolved captchas. First, we transfer the unlabeled observations to a low-dimensional representation, then the few available labels are distributed to close-by observations.

- *On the Usage of Brainwave Data in Safety and Security Applications*: This project focuses on neuro-based safety bounds for human-machine interactions. We want to use brainwave signals to help us determine whether subjects are able and qualified to perform complex tasks, such as safety-critical operational decisions about network control systems or electric dispatch. This research relates to a broader agenda of investigating the possibilities to utilize brainwave data in safety and security applications.
    - Experiments: Conduct studies with human subjects, including designing experiment protocols and collecting data from human subjects using brain wave equipment and controls to measure the subject's vital signs, most likely using hardware from NeuroSky.
    - Statistical Data Analysis: Learn to analyze the experimental data collected via the experiments and perform statistical analysis of the data.
    - Working with Literature: Review the current state of art of brain wave data applications in various domains by researching the literature and summarize the existing studies about the possible uses of brainwave data including limitations and constraining problems of brain wave usability. An emphasis will be on applications targeting non-traditional, non-diagnostic (non-medical) purposes (e.g., games and neuromarketing) and special attention will be paid to privacy issues and the privacy repercussions of using brain wave signals.

- Equipment Testing: Design and perform a series of tests to collect comparative performance statistics (signal quality and precision) of existing, commercially-available brainwave hardware.

- *Managing Exhaustion: An Analysis of Regional Variations in IPv4 Allocation Strategies*: The amount of free IPv4 address space is currently running out, resulting in a coordinated push to transition to IPv6, which will offer substantially more address space. However, the shortage of IPv4 addresses varies quite radically by region, due to both historical and market conditions. For instance, North America holds a substantial chunk of so-called legacy address space, allocated in the early days of the Internet, while emerging economies in Asia are rapidly exhausting their available address space. Accordingly, policies for handling the exhaustion of IPv4 address space have also varied amongst the five Regional Internet Registries responsible for handling the allocation of critical Internet resources in their regions of the world. In the face of scarcity, recurrent debates about IP address allocations have gained in prominence: whether IP addresses are to be viewed as resources to be held in common, or property to be exchanged in markets. This has crucial implications for the nature of trust in ICANN and the Regional Internet Registries, the institutions of Internet governance – are they to be viewed as guarantors of property rights in IP addresses, or shepherds of common pool resources? The relationship between institutional structures, policy design and the trustworthiness of large scale computing systems is a core concern of this research project.

  In this project, we will examine variations amongst regional IPv4 allocation policies, with particular focus on how these policies have changed in the last few years, as IPv4 exhaustion became a more pressing concern. This will involve qualitative research into the language and implications of policies, analysis of conversations on policy mailing lists that led to particular policy decisions, and a quantitative examination of actual IPv4 allocations as a consequence of these policy variations. This research project will provide important insights into the functioning of the global Internet governance regime, over a crucial period of reaction to IPv4 address space exhaustion.

- *RACS: Research in Cloud Storage Diversity*: The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud. However, success for cloud storage providers can present a significant risk to customers; namely, it becomes very expensive to switch storage providers. In this project, we make a case for applying RAID-like techniques used by disks and file systems, but at the cloud storage level. We argue that striping user data across multiple providers can allow customers to avoid vendor lock-in, reduce the cost of switching providers, and better tolerate provider outages or failures. We will work on a project called RACS (redundant array of cloud storage), a proxy that transparently spreads the storage load over many providers. We will build and evaluate a prototype of RACS system and estimate the costs incurred and benefits reaped.

- *SoNic Boom*: State-of-the-art networks require state-of-the-art methodologies to understand and secure them, and use them efficiently. Our SoNIC-enabled (software defined network interface) networks are a crucial enabling step. Informed by the improved understanding, control, and flexibility given by being able to control the entire network stack in software, we expect to develop better protocols for moving large quantities of data securely and reliably in modern networks. In this project, we will investigate end-to-end system dependability, focusing on the flow dynamics introduced by a state-of-the-art 10 Gbps wide-area network carrying a variety of extremely steady data streams. We intend to show that the burstiness introduced by this network

causes endpoint buffer overflows and resultant packet loss, and that the degree of loss can be far more severe than would be expected purely on the basis of the packet chain lengths. Further, we plan to investigate ways in which data transfer protocols, like TCP, could be modified to remedy the problem. The issue is important since enterprises ranging from geographically dispersed scientific projects that move large data sets to cloud computing applications shipping data between data centers (or directly to end-users) are building networks of the sort we used in our studies. As a result, a substantial community faces the performance issues we investigate, and would benefit from the remedial steps we would research and suggest.

- *Securing Web Applications from Logic Flaws*: The World Wide Web has evolved from a system that delivers static pages to a platform that supports distributed applications, known as web applications, and has become one of the most prevalent technologies for information and service delivery over Internet. Web applications usually interact with back-end database systems, which may store sensitive information (e.g., financial, health) and are increasingly used to deliver security critical services. Web applications also become a primary and valuable target for cyber attacks which raises serious security concerns for all the users and corporations that rely on web applications. A breach report from Verizon shows that web applications now reign supreme in both the number of breaches and the amount of data compromised. For instance, in June 2010 it was reported that a vulnerability of the AT&T website allowed an attacker to harvest Apple iPad subscribers' emails by enumerating ICC-ID numbers which affected over 100,000 Apple customers. As web applications get deeply embedded in business activities and required to support sophisticated functionalities, the design and implementation of web applications are becoming more and more complicated. The increasing complexity is confronted with the fact of insufficient security assurance from both currently widely-used web application development and testing frameworks and developers with insufficient security skills or awareness. As a result, a high percentage of web applications deployed on the Internet are exposed to security vulnerabilities. The goal of this research project is to harden web applications and secure them from logic flaws and state violation attacks. In particular, we aim to develop a software testing technique that is able to identify potential logic vulnerabilities within web applications so as to prevent successful state violation attacks.

- *Evaluating the Impact of Security Attacks on Cyber-Physical Systems*: Cyber-physical systems (CPS) are characterized by the tight coupling and coordination among sensing, communications, computational and physical resources. As CPS become more complex through distributed architectures and expanded mission capability, it becomes more challenging to assure the performance, stability, safety, and security properties of their behavior. There is a pressing need to evaluate both cyber- and physical systems together and holistically in the realistic network environments, especially under security attacks. The goal of this project is to perform an experimental study for CPS systems in an integrated environment of simulation tools (e.g., Matlab) and emulation environments (e.g., DETERlab). Specific tasks will include (1) implement/run a simple networked control system in DETERLab, (2) use network attack generation tools to generate network attacks during the execution of the network control system, and (3) collect traces, measure NCS system performance, and study the results.

CDSIA has received excellent reviews from faculty participants. CDSIA is creating a community of TRUST scholars and has merged it with the IACBP into one annual event called the Annual Symposium on Curriculum. Going forward, we will continue to leverage CDSIA to engage community colleges and broaden participation. The 2012 program is scheduled for May 11, 2012 at San Jose State.

In 2012, we will offer the Summer Experience, Colloquium and Research in Information Technology (SECuR-IT), a 10-week summer internship for M.S. and Ph.D. students having a degree emphasis in cyber security and trustworthy systems. The SECuR-IT 2012 program will begin on June 11 and conclude on August 17, 2012. SECuR-IT is a collaborative effort between TRUST and industry/academic partners in the San Francisco Bay area. The summer cohort consists of graduate students studying information technology: computer science, electrical engineering, software engineering, and information assurance at U.S. higher education programs. Participants are paid by the sponsoring organization as employee interns and will receive a relocation stipend (if they reside outside California) and a housing stipend. Students are paid for a 40-hour work week and will spend Tuesday through Friday at the sponsoring company and spend Mondays participating in a TRUST-organized seminar hosted at a participant location. Those weekly seminars will cover topics germane to the cyber security industry and will be presented by TRUST faculty from Berkeley, San Jose State, and Stanford together with leading industry experts in an exciting lecture format.

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 stakeholders, and the research community.

TRUST knowledge transfer objectives are to: (1) develop strong liaison with the concerns of industry and infrastructure stakeholders; (2) produce legislative and legal policy papers and amicus briefs; (3) leverage testbeds for demonstrating Center research project results; (4) enable student internships and support entrepreneurial clubs; and (5) convene 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 Center's 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 and support technology transfer from the research community to government and industry partners. 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., Cisco, HP, IBM, Intel, Microsoft, Symantec), and infrastructure providers (BellSouth, Boeing, Qualcomm, Raytheon) 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) Seminars and workshops held at major conferences and 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, development of significant TRUST spin-offs, and exploratory discussions regarding additional activities such as a center focused on research, development, and deployment of technologies for trustworthy cyber-infrastructure and systems.

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. Items are grouped by the lead institution(s).

Technology Transition to the U.S. Air Force		
Led by	Cornell University	
Organizations Involved		
	Name	Address
1	Cornell University	Ithaca, NY 14850

At the request of the Chief Information Officer of the U.S. Air Force, Mr. Tilotson (and the AF/XC, Mr. Werner), Birman and Schneider organized a workshop to study risks associated with Air Force deployment of Windows Vista as a single solution on client platforms. Although the workshop did identify some risks, we also identified a number of cutting edge risk management options that seem to address most issues. For example, TRUST research on artificial diversity seems to be a powerful remedy for the potential creation of a viral "target" associated with the very homogeneous deployment model, and indeed Windows Vista itself incorporates stack randomization, which is a very important first step. AF/XC was extremely pleased with the outcome and is acting on our recommendations for next steps, including early deployment suggestions and longer term research proposals. Contact: Dr. Sekar Chandersekaran (cchander@ida.org)

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

The TRUST research team has had prominent 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 cyber security 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. Finally, TRUST researchers have taken the lead to start new workshops and conferences focused around TRUST research themes. Of note during this period was the second annual Model-Based Trustworthy Health Information Systems (MOTHIS) workshop which was established by TRUST research Janos Sztipanovits.

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

Under the direction of Professor Ken Birman at Cornell, work is underway on helping the Red Hat Linux community develop a new, open-source technology for time-critical event-driven computing. Many applications, such as financial systems or medical systems, are "event driven" in that some form of external data source (a ticker plant, or medical telemetry) must drive a reaction by the system. Today, there are surprisingly few technical options for building such systems: users are forced to purchase message middleware products from vendors and complain that the solutions are complex, expensive, and unstable in scaled-out deployments. Cornell's Ricochet protocol addresses these requirements in a simple, lightweight manner that offers extremely good real-time properties and involves minimal infrastructure. We're now working to produce a version matched to the needs of the Red Hat community, with the hope that the IP might enter their public-source distribution early in the 2009 timeframe. Patents on Ricochet would be transferred to OIN and licensed, for free, to any organization wishing to implement a new solution using the same ideas, and the Ricochet platform itself would become an open source component. We're also working on a new research paper reflecting some of the innovations needed to address practical deployment issues posed by the folks at Red Hat. Our main contact is Carl Trieloff (cctrieloff@redhat.com), the Chief Technology Officer of Red Hat.

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.

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. Additionally, we have made available open source software releases of our Doppelganger code (http://www.umeshshankar.com/doppelganger/).

Privacy Issues in Electronic Medical Records		
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.

Industry Technology Collaboration and Consulting		
Led by	University of California, Berkeley and Stanford University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	University of California, Berkeley	Berkeley, CA 94720

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. David Wagner also consults for Fortify Software, an HP company that produces software security tools. Fortify Software has commercialized research into program analysis from several TRUST participants, including Alex Aiken and Dawson Engler from Stanford and Dawn Song and David Wagner from Berkeley.

Model Integrated Clinical Information Systems (MICIS)		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Vanderbilt University Medical Center	Nashville, TN 37235

Vanderbilt researchers have developed MICIS, a software toolkit that is based on model-based design techniques and high-level modeling abstractions to represent complex clinical workflows in a service-oriented architecture paradigm. MICIS models are enriched with formal security and privacy policy specifications, which are enforced within the execution environment. One of the application domains of MICIS is the management of sepsis in acute care settings at the Vanderbilt Medical Center. The Sepsis Treatment Enhanced through Electronic Protocolization (STEEP) is a joint effort between TRUST at Vanderbilt and the Health Tech Lab of Vanderbilt Medical Center. MICIS is also being applied is the Emergency Department (ED) of the Vanderbilt Medical Center. The goal in any ED is the rapid turnaround of patients while maintaining a high quality of care and reducing cost by not ordering unnecessary tests. Privacy and security is achieved using the policy languages developed by TRUST.

Sepsis Treatment Enhanced through Electronic Protocolization (STEEP)		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Vanderbilt University Medical Center	Nashville, TN 37235

STEEP is a joint effort between TRUST at Vanderbilt and the Health Tech Lab of Vanderbilt University Medical Center. It is an on-line patient management and advisory system using evidence-based guidelines for managing septic patients in Emergency Departments. The use of model-based techniques for specifying and implementing guidelines as coordinated asynchronous processes has proved to be a promising new methodology for providing advanced clinical decision support. STEEP is currently deployed and being used by clinicians at the Vanderbilt University Medical Center.

Health Education Relational Network Extraction Toolkit (HORNET)		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Carnegie Mellon University	Pittsburgh, PA 15213
2	Stanford University	Stanford, CA 94305
3	University of California, Berkeley	Berkeley, CA 94720

Vanderbilt, Carnegie Mellon, and Stanford researchers have developed this open source electronic medical record access surveillance toolkit which can detect suspicious behavior with respect to usage of medical records. HORNET incorporates a suite of algorithms and statistical techniques for building social, or interaction networks in a temporal setting which is platform independent and can be integrated with existing health records infrastructures. It is currently being piloted with real-world access transaction logs from the Vanderbilt University Medical Center.

Architectural Modeling and Policy Languages		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	Vanderbilt University	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.

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

We have developed security co-design tools that couple security with the initial design stages of sensor networks. The basic 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.

Workshop on Internet Tracking, Advertising, and Privacy (WiTAP)		
Led by	Stanford University	
Organizations Involved		
	Name	Address
1	Stanford University	Stanford, CA 94305
2	University of California, Berkeley	Berkeley, CA 94720

TRUST researchers from Stanford and Berkeley organized and hosted the Workshop on Internet Tracking, Advertising, and Privacy (WiTAP) July 22, 2011 on the Stanford campus.

WiTAP focused on the tension between Internet privacy and the desire to track users for targeted advertising or fraud prevention. The workshop covered technical challenges and research and development opportunities in this space. The organizing committee included TRUST research Dan Boneh and John Mitchell from Stanford and Dawn Song from Berkeley. The program included research talks by TRUST researchers Arvind Narayanan and Jonathan Mayer, both of Stanford.

4th International Symposium on Resilient Control Systems		
Led by	University of California, Berkeley	
Organizations Involved		
	Name	Address
1	Carnegie Mellon University	Pittsburgh, PA 15213
2	University of California, Berkeley	Berkeley, CA 94720
3	Vanderbilt University	Nashville, TN 37235

TRUST researchers from Berkeley, Carnegie Mellon, and Vanderbilt organized a special workshop at the 4th International Symposium on Resilient Control Systems (ISRCS) sponsored by the Idaho National Laboratory August 9-11, 2011 in Boise, Idaho. The session, titled Workshop on Game Theoretic Approaches to Network Security and Reliability, included research presentations by TRUST researchers and technical panel discussions led by TRUST researchers. Additionally, TRUST PI S. Shankar Sastry from Berkeley gave a keynote presentation titled "Towards a Theory of High Confidence Networked Control Systems."

Dagstuhl Seminar on Science and Engineering of Cyber-Physical Systems		
Led by	Vanderbilt University	
Organizations Involved		
	Name	Address
1	Carnegie Mellon University	Pittsburgh, PA 15213
2	Vanderbilt University	Nashville, TN 37235

TRUST researchers from Carnegie Mellon and Vanderbilt participated in a seminar focused on the need for a new science and engineering approach for building cyber-physical systems—systems that combine physical processes with computational control. The seminar, held November 1-4, 2011 in Wadern, Germany, was co-organized by TRUST researcher Janos Sztipanovits from Vanderbilt. It focused on the scientific foundations and the engineering aspects of cyber-physical systems and brought together researchers from both academia and industry to discuss the new scientific foundations and engineering principles for the vastly emerging field of CPS and included research presentations by TRUST researchers.

1st ACM International Conference on High Confidence Networked Systems (HiCoNS)		
Led by	University of California, Berkeley	
Organizations Involved		
	Name	Address
1	Carnegie Mellon University	Pittsburgh, PA 15213
2	Cornell University	Ithaca, NY 14850
3	University of California, Berkeley	Berkeley, CA 94720
4	Vanderbilt University	Nashville, TN 37235

TRUST researchers in collaboration with government officials from the National Science Foundation and the National Security Agency organized the ***1st ACM International Conference on High Confidence Networked Systems (HiCoNS)*** on April 17-18, 2012 in Beijing, China as part of CPSWeek 2012. The focus of the conference is on system theoretic approaches to address fundamental challenges to the confidence of networked cyber-physical systems (CPS) by making them more secure, dependable, and trustworthy. The conference emphases the control and verification challenges arising as a result of complex interdependencies between networked systems, in particular those at the intersection of cyber and physical areas, and aims to advance the development of a principled approach to high confidence networked CPS.

HiCoNS is being led and organized by a world-class group of experts from multiple disciplines, including control and systems theory, embedded systems, game theory, software verification, formal methods, and computer security. TRUST PI S. Shankar Sastry as conference General Chair, Vanderbilt researcher Gabor Karsai as Program Chair, and researchers from TRUST partner institutions Berkeley, Carnegie Mellon, Cornell, and Vanderbilt serving as Program Committee members. These subject matter experts are not only leaders in their fields and the CPS community but they bring to bear experience that will allow the conference to link work being done in applied areas with foundational work to advance a science base for high-confidence networked systems that aims to provide a means of building CPS systems in a principled way.

The HiCoNS program will contain presentations from the accepted paper submissions, invited keynote talks, Work-In-Progress talks, and poster presentations from leading researchers, practitioners, and subject matter experts. Accepted papers will be published by ACM in a printed proceedings and included in an electronic proceedings distributed by the CPSWeek organizers. The paper presentations and invited talks will also be posted to the HiCoNS website after the conference to ensure the research results are widely disseminated.

This conference is sponsored by the ACM Special Interest Group on Embedded Systems (ACM SIGBED). Information on the conference is available at http://www.hi-cons.org/.

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 cyber security 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 many research and education activities that have been established in the first five years of the Center.

Additionally, the Center plans to build on previous programs that brought together TRUST researchers with U.S. and international researchers to develop security technologies, increase security public awareness, and foster security partnership among government organizations, academic institutions, and private sector companies. The hope is to see 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

The items below describe external partnership activities of TRUST researchers.

Partnership Activity		Industrial Research Partnership	
Led by		UC Berkeley	
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	San Jose State University		
5	Stanford University		
6	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 External Advisory Board, or collaborate actively with TRUST researchers. Current TRUST industrial partners are:

- BT
- Cisco Systems
- DoCoMo USA Labs
- EADS
- ESCHER Research Institute
- Hewlett Packard
- IBM
- Intel
- Microsoft
- Oak Ridge National Laboratory
- Pirelli
- Qualcomm
- SELEX Sistemi Integrati
- Sun
- Symantec
- Tata Consultancy Services
- 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		BITS	
Led by		Stanford University	
Organizations Involved			
	Name of Organization	Shared Resources (if any)	Use of Resources (if applicable)
1	Cornell University		
2	Stanford University		
3	University of California, Berkeley		

TRUST has established a partnership with BITS an organization that supports member institutions in the financial services industry by sponsoring noncompetitive, collaborative R&D of interest to the financial services community and promoting activities that sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions.

TRUST investigators John Mitchell from Stanford and Ken Birman and Fred Schneider from Cornell have been most active in engaging senior BITS personnel and industry executives. Initial dialogue between TRUST researchers and BITS personnel has identified a number of areas of active research within TRUST that is also of interest to BITS member institutions. Currently, Dan Schutzer from the FSTC is working to establish a special interest group (SIG) within the organization to bring together academic researchers and industry practitioners to share research results and operational and technical needs and TRUST is working to identify promising research areas relevant to the financial services industry and topics to be presented at future BITS SIG meetings. It is expected that this partnership will increase exposure to TRUST research activities and identify opportunities for future industry and government collaboration.

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. Industrial partners new to TRUST during this reporting period are DoCoMo USA Labs, EADS, and Tata Consultancy Services. These partnerships provide an opportunity to leverage fundamental cyber security 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.

We also hope to increase the center's global presence by identifying international partners with whom the Center can partner to broaden our research, education, and knowledge transfer impact. Initial discussions

have taken place with cyber security researchers and centers, government organizations, and commercial companies in Belgium, Denmark, Finland, India, Korea, Singapore, Sweden, Taiwan, and the United Kingdom.

6 DIVERSITY

6.1 Goals and Objectives

In TRUST, our diversity efforts will take a "grass roots" approach by building strong partnerships with faculty and institutions that will help us achieve our goals of inclusion of women and underrepresented minorities (URM). These partnerships will help us to cultivate the role models and mentors necessary to meet the diversity goals and objectives of the Center. Our programs can be grouped under the following goals:

- Infuse the computer science and engineering pipeline with new, diverse, and talented individuals
- Retain those individuals within TRUST research areas
- Prepare those individuals for successful careers, especially as researchers and educators in academia

Our objectives are quantified by the level of participation of women and underrepresented minorities within the Center. We seek to achieve 30% women among the Center's participants (i.e., faculty, students, research scientists, and Center staff). We also seek to achieve 10% underrepresented minorities among the Center's participants. The Center conducts assessments to track our progress towards these objectives.

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
Minority Faculty Research	Guided Summer Program	Number of faculty, Exit Surveys, Tracking surveys of alumni	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
SUPERB-TRUST	Research opportunities for minority undergraduate 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 TRUST summer programs 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, Quality Education for Minorities Network (QEM) and Integrative Graduate Education and Research Traineeship (IGERT) website program portal.

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

The sections below describe some of the Center's activities which are contributing to the development of U.S. 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.

Bridges to Underrepresented Institutions for Long-term Development in Information Technology (BUILD-IT) – This program selects faculty mentors from Historically Black Colleges and Universities (HBCUs) and Hispanic Serving Institutions (HSIs) and provides them with the opportunity to (a) learn about TRUST research thrusts, (b) meet TRUST faculty and graduate students, and (c) discuss the Center's diversity mission, objectives, and programs. Target institutions are among the largest producers of undergraduates in computer science and engineering from traditionally underrepresented groups. Selected HBCU/HIS faculty participate in a TRUST-organized conference that connects them with TRUST researchers to explore opportunities for joint research, graduate student placement, and technical conference travel support.

TRUST Summer Faculty Fellowship – This program enables TRUST to host faculty from Historically Black Colleges and Universities (HBCUs) and Hispanic Serving Institutions (HSIs) at Center partner institutions enabling TRUST to forge lasting relationships based upon research collaborations which could then be leveraged to create R1-HBCU research pods as well as graduate student recruiting.

TRUST Recruiting Scholarships for Incoming Graduate Students – This program provides supplemental scholarships to help TRUST partner institutions recruit top graduate student applicants from traditionally underrepresented groups, thus increasing opportunities for those students and the diversity among the Center's graduate student population. The scholarship supplements the base award made by a TRUST partner institution, thus enhancing admission offers.

TRUST Post-Doctoral Fellowships – This program supports a post-doctoral position at any TRUST partner institution that seeks a qualified candidate from an underrepresented group. The post-doctoral position gives a potential faculty candidate an opportunity beyond their dissertation to connect with TRUST researchers, complete additional publications, collaborate on new research topics, and hone skills (e.g., proposal-writing), thus making the candidate more competitive for a tenure-track position.

TRUST Research Experiences for Undergraduates (TRUST_REU) – This program supports a cohort of URM undergraduate students for an eight week summer residential program at TRUST partner institutions. The program allows undergraduate students to work with TRUST faculty and graduate students in a TRUST-related research area, experience firsthand a rigorous academic research environment, participate in technical seminars, participate in professional development activities, and present the results of their research.

Women's Institute in Summer Enrichment (WISE) – This is a one-week residential summer program 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 Institute emphasizes the inclusion of women and underrepresented graduate students, post-doctorates, and junior faculty.

6.5 Diversity Activity Impact

"[The] under-participation in CS [computer science] by large segments of our society represents a loss of opportunity for individuals, a loss of talent in the workforce, and a loss of creativity in shaping the future of technology. Not only is it a basic equity issue, but it threatens our global economic viability as a nation."

> P. A. Freeman and J. Cuny, "Common ground: A diverse CS community benefits all of us," Computing Research News, vol. 17, 2005.

TRUST seeks to address the grand challenge as described by Freeman and Cuny. Our efforts in computer science and engineering must make strides to diversify the workforce in order to meet the future demands of our technical profession. To that end, TRUST faculty and staff are engaged in a number of diversity activities:

Women's Institute for Summer Enrichment (WISE): WISE has now become a signature program of TRUST to attract women researchers.

TRUST Research Experiences for Undergraduates (TRUST-REU): During summer 2011, TRUST faculty and graduate student mentors across partner institutions led research projects for 13 undergraduate students. Participants were from diverse backgrounds and cultures, including a large number of female and URM students—most from undergraduate institutions with limited research programs giving them an opportunity to be exposed to cutting edge of academic research in general and projects tightly integrated with ongoing research of TRUST faculty and graduate students, in particular.

Curriculum Development in Security and Information Assurance (CDSIA): The CDSIA is a capacity building program with the objective to (1) reach out to the many universities of the California State University system and to other universities whose mission is focused on work-force preparation and undergraduate education, (2) to share with faculty members of these institutions material and support structures developed by the TRUST partners, (3) to strengthen the TRUST-related community of educators, and (4) to facilitate the education of members of underrepresented communities in the domain of secure technologies.

Community Outreach: Programs like the TRUST Security Seminar provide information and technology transfer to the community at large. In addition to providing on-campus presentations, TRUST archives speaker presentations on the TAO Portal. This program is learning exchange for professionals and academics in the security field.

6.6 Diversity Metrics/Indicators

As stated previously, the Center has established the goals of 30% participation by women and 10% participation by members of underrepresented groups. Figure 3 and Figure 4 provide the historical participation within the Center by gender and by race/ethnicity respectively. For gender, the Center is near the goal and for race/ethnicity the Center has exceeded the goal. Specifically, the within the Center

there are 24% women and 14% URM. For a perspective in computer science and engineering, the Taulbee Survey reports approximately 20% participation by women and approximately 5% participation by underrepresented minorities.

The gender and race/ethnicity for the WISE, TRUST-REU, SECuR-IT, and CDSIA programs during this reporting period are as follows:

- WISE (30 participants): = 93% Women, 40% URM
- TRUST-REU (13 participants): 23% Women, 46% URM
- SECuR-IT (15 participants): 40% Women, 20% URM
- CDSIA (60 participants): 25% Women, 18% URM.

6.7 Next Reporting Period Diversity Plans

We plan to continue our successful activities such as WISE, TRUST-REU, CDSIA, and BUILD-IT. To that portfolio, we will continue our outreach scholarship/fellowship programs targeting HBCU and HIS faculty, post-doctoral scholars, and graduate students.

We have identified the Computing Alliance for Hispanic-Serving Institutions (CAHSI) and the Association of Computer/Information Sciences and Engineering Departments at Minority Institutions (ADMI) as potential partners to aid us in reaching a new generation of researchers in the area of security. We also plan to work with the Coalition to Diversify Computing to support their programming efforts, such as participating in the Richard Tapia Celebration of Diversity in Computing Conference, and leverage our affiliation with the Empowering Leadership Alliance to connect our students with a larger community of scholars and mentors.

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 Berkeley. Center leadership is provided by the Chief Scientist, Prof. Fred Schneider from Cornell; the Executive Director, Mr. Larry Rohrbough from Berkeley; the Outreach Director, Prof. William Robinson from Vanderbilt; and the Policy Director, Prof. Deirdre Mulligan from Berkeley. Additional Center administrative and operational support is provided by the Program Manager, Dr. Aimee Tabor from Berkeley; the Financial Manager, Ms. Annie Ren from Berkeley; the Webmaster, Mr. Christopher Brooks from Berkeley, the Technical Administrator Ms. Mary Stewart from Berkeley; and the Program Coordinator, Ms. Jessica Gamble from 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, Diversity Director, Policy Director, Program Manager, and university Principal Investigators.

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, Adrian Perrig, 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.

7.4 Current and Anticipated Problems

During the reporting period, a new TRUST Education Director joined the Center, replacing the former Education Director who left the Center and UC Berkeley. The Center performed an extensive national search that identified over 60 candidates. The new Education Director is Dr. Aimee Tabor and we are very excited to have her on board. Aimee has a Doctorate in Education and extensive education program development and evaluation experience—in addition to her knowledge of TRUST from serving as the Center's Program Manager for the past 10 months. During the Education Director search period, Aimee was instrumental in helping plan and organize the Center's summer education programs in addition to her program management duties. Aimee brings a lot of enthusiasm and energy to her work as well as fresh ideas and plans for advancing the Center's education programs, partnerships, and results.

As a result of Aimee's appointment as Education Director, the Center is in the process of recruiting a new Program Manager and we anticipate having someone on board very soon.

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. New during this reporting period is the added use of WebEx to share documents among the geographically-dispersed Executive Board membership and the inclusion of a non-Executive Board TRUST investigator at each meeting to report on recent research results and outcomes. 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

TRUST receives outside advice, guidance, and counsel from our External Advisory Board (EAB). The TRUST EAB is a distinguished group of experts in research, education, technology, 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 knowledge transfer accomplishments, goals, and plans. EAB input also 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
Tamer Başar	University of Illinois at Urbana-Champaign
Rebecca Base	Infidel, Inc.
Marjory Blumenthal	Georgetown University
Brian Chess	Fortify Software
David Clark	Massachusetts Institute of Technology
Alissa Cooper	Center for Democracy & Technology
Úlfar Erlingsson	Google
Richard Kemmerer	University of California, Santa Barbara
Jay Lala	Raytheon Integrated Defense Systems
Leslie Lambert	Juniper Networks
Dough Maughan	Department of Homeland Security
Mike Schroeder	Microsoft Research Silicon Valley
Dan Schutzer	Financial Services Technology Consortium
Valerie Taylor	Texas A&M University
Noam Ziv	Qualcomm

7.7 Center Strategic Plan Changes

Changes to the TRUST Strategic Plan are indicated within that document. The TRUST Strategic Plan was last updated September 18, 2008.

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. Publications are listed in reverse chronological order and are grouped into the following categories based on their publication type: Peer Reviewed Publications, Journal Articles, Books and Book Chapters, and Non-Peer Reviewed Publications. For each publication, a link to the TRUST publications database is provided as reference.

8.1.1 Peer Reviewed Publication

- On the Nonlinearity Effects on Malicious Data Attack on Power System, Jia Liyan, Robert J. Thomas, Lang Tong, To appear in 2012 Power and Energy Society general meeting, July, 2012
- Formalizing and Enforcing Purpose Restrictions in Privacy Policies, Michael Tschantz, Anupam Datta, Jeanette Wing, Proceedings of 33rd IEEE Symposium on Security and Privacy, IEEE, May, 2012
- Alvaro Cardenas, Saurabh Amin, Galina A. Schwartz. Privacy-Aware Sampling for Residential Demand Response Programs, Proceedings of the 1st International ACM Conference on High Confidence Networked Systems (HiCoNS), April, 2012.
- Alefiya Hussain, Saurabh Amin. NCS Security Experimentation Using DETER, Proceedings of the 1st International ACM Conference on High Confidence Networked Systems (HiCoNS), April, 2012.
- Provable De-Anonymization of Large Datasets with Sparse Dimensions, Anupam Datta, Divya Sharma, Arunesh Sinha, Proceedings of ETAPS Conference on Principles of Security and Trust, March, 2012
- A Critical Look at Decentralized Personal Data Architectures, Arvind Narayanan, Vincent Toubiana, Solon Barocas, Helen Nissenbaum, Dan Boneh, CoRR, February, 2012
- ACCessory: Keystroke Inference using Accelerometers on Smartphones, Emmanuel Owusu, Jun Han, Sauvik Das, Adrian Perrig, Joy Zhang, To appear in Proceedings of The Thirteenth Workshop on Mobile Computing Systems and Applications (HotMobile), ACM, 28, February, 2012
- Metrics for Measuring ISP Badness: The Case of Spam, Benjamin Johnson, John Chuang, Jens Grossklags, Nicolas Christin, To appear in Proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC'12, International Financial Cryptography Association, 12, February, 2012
- Impacts of Malicious Data on Real-time Price of Electricity Market Operations, Jia Liyan, Robert J. Thomas, Lang Tong, 45th Hawaii International Conference on System Sciences, pp.1907-1914, 4, January, 2012
- Community-based web security: complementary roles of the serious and casual contributors, Pern Hui Chia, John Chuang, Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work, ACM, 2012
- Colonel Blotto in the Phishing War, Pern Hui Chia, John Chuang, Lecture Notes in Computer Science, GameSec 2011, Springer, pp.201-218, 2012
- The case for prefetching and prevalidating TLS server certificates, E. Stark, L.S. Huang, D. Israni, C. Jackson, D. Boneh, To appear in Proceedings of Network & Distributed System Security (NDSS), 2012

- Android Permissions Demystified, Adrienne Porter Felt, Dawn Song, David Wagner, Steve Hanna, 18th ACM conference on Computer and communications security, ACM, 2012
- Cyber–Physical Security of a Smart Grid Infrastructure, Y. Mo, K. Brancik, D. Dickenson, H. Lee, Proceedings of the IEEE, IEEE, pp. 195-209, 2012
- Adaptive Regret Minimization in Bounded-Memory Games, Jeremiah Blocki, Nicholas Cristin, Anupam Datta, Arunesh Sinha, COLT, 2012
- Targeted malleability: homomorphic encryption for restricted computations, Dan Boneh, Gil Segev, Brent Waters, Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, 2012
- NCSWT: An Integrated Modeling and Simulation Tool for Networked Control Systems, Emeka Eyisi, Jia Bai, Derek Riley, Jiannian Weng, Jan Wei, Yuan Xue, Xenofon Koutsoukos, Janos Sztipanovits, Hybrid Systems: Computation and Control 2012, 2012
- Declarative privacy policy: finite models and attribute-based encryption, Susan Landau, John C. Mitchell, Andre Scedrov, Sharada Sundaram, Frank Wang, Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium (IHI'12), 2012
- Sponsored search auctions with conflict constraints, Panagiotis Papadimitriou, Hector Garcia-Molina, Proceedings of the fifth ACM international conference on Web search and data mining, 2012
- SENTINEL: securing database from logic flaws in web applications, Xiaowei Li, Wei Yan, Yuan Xue, Proceedings of the second ACM conference on Data and Application Security and Privacy, 2012
- On the Interdependence of Reliability and Security in Networked Control Systems, Saurabh Amin, Galina A. Schwartz, S. Shankar Sastry, 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), IEEE, pp 4078-4083, 12, December, 2011
- Understanding and Protecting Privacy: Formal Semantics and Principled Audit Mechanisms, Anupam Datta, Jeremiah Blocki, Nicolas Christin, Henry DeYoung, Deepak Garg, Limin Jia, Dilsun Kaynar, Arunesh Sinha, 7th International Conference on Information Systems Security, 1-27, December, 2011
- Network Security Games: Combining Game Theory, Behavioral Economics, and Network Measurements, Nicolas Christin, Proceedings GameSec 2011, November, 2011
- Fashion Crimes: Trending-Term Exploitation on the Web, Tyler Moore, Nektarios Leontiadis, Nicolas Christin, Proceedings ACM CCS 2011, October, 2011
- Congestion Pricing Using a Raffle-Based Scheme, Patrick Loiseau, Galina A. Schwartz, John Musacchio, Saurabh Amin, S. Shankar Sastry, Network Games, Control and Optimization (NetGCooP), 5th International Conference, IEEE, 1-8, 12, October, 2011
- Policy Auditing over Incomplete Logs: Theory, Implementation and Applications, Deepak Garg, Limin Jia, Anupam Datta, ACM Conference on Computer and Communications Security, October, 2011
- A Survey of Mobile Malware in the Wild, Adrienne Porter Felt, Mtthew Finifter, Erika Chin, David Wagner, ACM Workshop on Security and Privacy in Mobile Devices (SPSM), ACM, 17, October, 2011
- Revisit Dynamic ARIMA Based Anomaly Detection, Bonnie Zhu, S. Shankar Sastry, SocialCom/PASSAT 2011, IEEE, pp.1263-1268, 9, October, 2011

- Linking Computer Vision with Off-the-Shelf Accelerometry through Kinetic Energy for Precise Localization, Eladio Martin, Victor Shia, Posu Yan, Philip Kuryloski, Edmund Y.W. Seto, Venkatesan Ekambaram, Ruzena Bajcsy, 5th IEEE International Conference on Semantic Computing (ICSC), IEEE, pp.239-242, 18, September, 2011
- Enhancing context awareness with activity recognition and radio fingerprinting, Eladio Martin, Victor Shia, Posu Yan, Philip Kuryloski, Edmund Y.W. Seto, Venkatesan Ekambaram, Ruzena Bajcsy, 5th IEEE International Conference on Semantic Computing (ICSC), IEEE, pp.263-266, 18, September, 2011
- Interference channel with binary fading: Effect of delayed network state information, A. Vahid, M.A. Maddah-Ali, A.S. Avestimehr, 49th Annual Allerton Converence on Communication, Control, and Computing, pp.894-901, 28, September, 2011
- Incentive schemes for internet congestion management: Raffles versus time-of-day pricing, Patrick Loiseau, Galina A. Schwartz, John Musachhio, Saurabh Amin, 49th Annual Allerton Conference on Communication, Control and Computing, IEEE, 103-110, 28, September, 2011
- Network design game with both reliability and security failures, G. A. Schwartz, S. Amin, A. Gueye, J. Walrand, 49th Annual Allerton Conference on Communication, Control, and Computing, IEEE, pp 675-681, 28, September, 2011
- Audit Mechanisms for Privacy Protection in Healthcare Environments (Position Paper), Jeremiah Blocki, Nicolas Christin, Anupam Datta, Arunesh Sinha, 2nd Usenix Workshop on Health Security and Privacy, August, 2011
- Measuring and Analyzing Search-Redirection Attacks in the Illicit Online Prescription Drug Trade, Nektarios Leontiadis, Tyler Moore, Nicolas Christin, Proceedings USENIX Security 2011, August, 2011
- Audit Mechanisms for Privacy Protection in Healthcare Environments, Jeremiah Blocki, Nicolas Christin, Anupam Datta, Arunesh Sinha, Proceedings USENIX HealthSec 2011, August, 2011
- Beyond Power Proportionality: Designing Power-Lean Cloud Storage, Lakshmi Ganesh, Hakim Weatherspoon, Ken Birman, IEEE 10th International Symposium on Network Computing and Applications, IEEE, 25, August, 2011
- Netquery: A Knowledge Plane For Reasoning About Network Properties., Alan Shieh, Emin Gun Sirer, Fred Schneider, Proceedings of the SIGCOMM Conference, August, 2011
- "I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook, Yang Wang, Saranga Komanduri, Pedro Leon, Gregory Norcie, Alessandro Acquisti, Lorrie Faith Cranor, Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS), ACM, July, 2011
- Unshackle the Cloud!, Dan Williams, Eslam Elnikety, Mohammed Edehiry, Hani Jamjoon, Hai Huang, Hakim Weatherspoon, Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud),, June, 2011
- Regret Minimizing Audits: A Learning-Theoretic Basis for Privacy Protection, Jeremiah Blocki, Nicolas Christin, Anupam Datta, Arunesh Sinha, 24th IEEE Computer Security Foundations Symposium, June, 2011

8.1.2 Journal Articles

- A Path-Based Approach for Web Page Retrieval, Jian-qiang Li, Yu Zhao, Hector Garcia-Molina, World Wide Web, 15, 3, pp.257-283, May, 2012

- Detecting Anomalous Insiders in Collaborative Information Systems, Yu Chen, Steve Nyemba, Bradley Malin, IEEE Transactions on Dependable and Secure Computing, 9, 3, pp.332-344, May, 2012
- Specializing Network Analysis to Detect Anomalous Insider Actions, You Chen, Steve Nyemba, Wen Zhang, Bradley Malin, Security Informatics, February, 2012
- Maelstrom: Transparent Error Correction for Communication Between Data Centers, Mahesh Balakrishnan, Tudor Marian, Ken Birman, Hakim Weatherspoon, IEEE/ACM Transactions on Networking (ToN), 19, 3, pp.617-629, 2012
- Malicious Data Attacks on the Smart Grid, Oliver Kosut, Jia Liyan, Robert J. Thomas, Lang Tong, IEEE Trans. Smart Grid Special Issue on Cyber, Physical, and System Security for Smart Grid, 2, 4, pp. 645-658, 2012
- Do Interruptions Pay Off? Effects of Interruptive Ads on Consumers' Willingness to Pay, Alessandro Acquisti, Sarah Spiekermann, Journal of Interactive Marketing, 25, 4, pp. 226-240, November, 2011
- Cellular Telephony and the Question of Privacy, Stephen Wicker, Communications of the ACM, 54, 7, July, 2011
- Loci of competition for future internet architectures, John Chuang, Communications Magazine, 49, 7, pp. 38-43, July, 2011
- Tweakable Block Ciphers, Moses Liskov, Ronald L. Rivest, David Wagner, Journal of Cryptology, 24, 3, July, 2011

8.1.3 Books and Book Chapters

- PIA Requirements and Privacy Decisionmaking in U.S. Government Agencies PRIVACY IMPACT ASSESSMENTS: ENGAGING STAKEHOLDERS IN PROTECTING PRIVACY, Deirdre Mulligan, Kenneth A. Bamberger, De Hert and Wright, 10, 225-250, Springer, 2012
- A Symbolic Logic with Exact Bounds for Cryptographic Protocols, John C. Mitchell, 6642, SpringerLink, 2011
- Next-Generation Internet: Architectures and Protocols, John Musacchio, Galina Schwartz, Jean Walrand, Byrav Ramamurthy, George Rouskas, and Krishna M. Svialingam, pp 378-402, Cambridge University Press, 2011

8.1.4 Non-peer Reviewed Publications

- DefAT: Dependable Connection Setup for Network Capabilities, Soo Bum Lee, Virgil D. Gligor, Adrian Perrig, Carnegie Mellon University, CMU-CyLab-011-018, 2012
- Exploiting Privacy Policy Conflicts in Online Social Networks, Akira Yamada, Tiffany Hyun-Jin Kim, Adrian Perrig, Carnegie Mellon University, CMU-CyLab-012-005, 2012

8.2 Conference Presentations

The following is a list of conference presentations made by TRUST Center personnel during this reporting period. For each presentation, a link to the TRUST publications database is provided as reference.

- Virtualization of R&D Driving New Health IT Requirements, Vijay Pillai, 2, November, 2011
- SCION: Scalability, Control and Isolation On Next-Generation Networks, Xin Zhang, Hsu-Chun Hsiao, Geoffrey Hasker, Haowen Chan, Adrian Perrig, 2, November, 2011

- Mechanism Design for Network Decongestion: Rebates and Time-of-Day Pricing, Galina A. Schwartz, Saurabh Amin, Patrick Loiseau, 2, November, 2011
- Game theoretic analysis of Advanced Metering Infrastructure adoption, Dipayan P. Ghosh, Stephen Wicker, Dawn Schrader, William Schulze, Lawrence Blume, 2, November, 2011
- Trust in Anarchy? Problems in the Governance of Distributed Computing Systems, Ashwin Jacob Mathew, 2, November, 2011
- Realizing intrinsically cyber secure large systems, Massimo Scipioni, 2, November, 2011
- Federal Cyber Security Research & Development, Brad Martin, 2, November, 2011
- SCRUB Intel Science and Technology Center: Secure Computing Research for Users' Benefit, Anthony Joseph, 2, November, 2011
- Uncovering Anomalous Usage of Medical Records via Social Network Analysis, You Chen, Bradley Malin, Steve Nyemba, Wen Zhang, 2, November, 2011
- Sensor Systems for Monitoring Congestive Heart Failure: Location-based Privacy Encodings, Edmund Seto , Posan Yu, Ruzena Bajcsy, 2, November, 2011
- Context-aware Anomaly Detection for Electronic Medical Record Systems, Yuan Xue, Xiaowei Li, You Chen, Bradley Malin, 2, November, 2011
- Declarative Privacy Policy: Finite Models and Attribute-Based Encryption, Ellick Chan, 2, November, 2011
- Regret Minimizing Audits: A Learning-Theoretic Basis for Privacy Protection, Jeremiah Blocki, Nicolas Christin, Anupam Datta, Arunesh Sinha, 2, November, 2011
- Securing Interaction for Sites, Apps and Extensions in the Browser, Brad Miller, Doug Tygar, 2, November, 2011
- Privacy in the Age of Augmented Reality, Alessandro Acquisti, Ralph Gross, 3, November, 2011
- A Little Too Smart: Location Privacy in the Cellular Age, Stephen Wicker, 3, November, 2011
- Incorporating Cybersecurity Education into the CS curriculum, Jonathan Mayer, Steve Cooper, 3, November, 2011
- Do Not Track, or Musings of a Graduate Student, Jonathan Mayer, 3, November, 2011
- Integrated Modeling, Simulation and Emulation Environment for Security Assessment of Cyber-Physical Systems, Yuan Xue, 3, November, 2011
- Secure Detection in the Presence of Integrity Attacks, Yilin Mo, 3, November, 2011
- Ultra Low Power Computation For Secure Embedded Systems, Rajit Manohar, 3, November, 2011
- Privacy: Is There an App for That?, Jennifer King, 3, November, 2011
- Network Design Game with Reliability & Security Failures, Saurabh Amin, Galina A. Schwartz, 3, November, 2011
- Logical Attestation: An Authorization Architecture for Trustworthy Computing, Emin Gun Sirer, Willem de Bruijn, Patrick Reynolds, Alan Shieh, Kevin Walsh, Dan Williams, Fred Schneider, 3, November, 2011
- Broadening Participation in Cyber Security, William H. Robinson, Kristen Gates, Sigurd Meldal, 3, November, 2011
- ENGRI 1280: Security, Privacy, and Information Network Design: Wiretaps to Facebook, Stephen Wicker, 3, November, 2011

- The Failure of Noise-Based Non- Continuous Audio Captchas, Hristo Paskov, Elie Bursztein, Romain Beauxis, Daniele Perito, Celine Fabry, John C. Mitchell, 2, November, 2011
- Faces of Facebook: Privacy in the Age of Augmented Reality, Alessandro Acquisti, Ralph Gross, Fred Stutzman, 18, August, 2011
- Privacy: Is There An App For That?, Jennifer King, Airi Lampinen, Alex Smolen, July, 2011

8.3 Other Dissemination Activities

Details of dissemination activities associated with TRUST Center personnel during this reporting period are covered elsewhere in this report.

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
Dan Boneh	"Outstanding teaching and exemplary leadership in industry education" through his teaching of Advanced Computer Security, Computer and Network Security, and Introduction to Cryptography delivered online by the Stanford Center for Professional Development.	Stanford's "Dean's Award for Industry Education Innovation"	June 2011	Scientific
Fred Schneider	For outstanding contributions in the field of information processing, in relation to computer science.	IEEE Emanuel R. Piore Award	July 2011	Scientific
Vern Paxson	The highest honor from ACM SIGCOMM, for Paxson's lifetime contributions to Internet measurement and security.	ACM Special Interest Group on Data Communications (SIGCOMM)	August 2011	Scientific

Recipient	Reason for Award	Award Name and Sponsor	Date	Award Type
Salman Avestimehr	Recognized as one of the Nation's "most meritorious scientists and engineers whose early accomplishments show the greatest promise for assuring America's preeminence in science and engineering and contributing to the awarding agencies' missions."	Presidential Early Career Award for Scientists and Engineers (PECASE)	September 2011	Scientific
Hakim Weatherspoon	NSF's most prestigious awards in support of junior faculty who exemplify the role of teacher-scholars through outstanding research, excellent education and the integration of education and research within the context of the mission of their organizations	National Science Foundation CAREER Award	October 2011	Scientific

8.5 Graduates

The following undergraduate, graduate, and Ph.D. students from across all TRUST universities graduated during this reporting period. Students are listed alphabetically by last name along with their institution name and degree.

#	Student Name / Affiliation	Degree(s)
1	Saurabh Amin (Berkeley)	Ph.D.
2	Kumar Avijit (Carnegie Mellon)	Ph.D.
3	Jaiganesh Balasubramanian (Vanderbilt)	Ph.D.
4	Coalton Bennett (Cornell)	Ph.D.
5	Sergio Bermudez (Cornell)	Ph.D.
6	John Bethencourt (Berkeley)	Ph.D.
7	Joe Hoffert (Vanderbilt)	Ph.D.
8	Deepti Kundu (San Jose State)	M.S.
9	Adrian Lauf (Vanderbilt)	Ph.D.
10	Mikhail Lisovich (Cornell)	Ph.D.
11	Bryan Parno (Carnegie Mellon)	Ph.D.
12	Blaine Nelson (Berkeley)	Ph.D.
13	Sharada Sundaram (Stanford)	M.S.
14	Amulya Yedugur (San Jose State)	M.S.

8.6 General Knowledge Transfer Outputs

Details of knowledge transfer outputs are provided in Section 4.

8.7 Institutional Partners

The following table lists all TRUST Center research, education, knowledge transfer, and other institutional partners.

Org. Name	Org. Type	Address	Contact Name	Type of Partner	160+ Hrs?
Air Force Office of Scientific Research	Federal Government	Arlington, VA	Bob Herklotz	Research	Y
Air Force Research Laboratory	Federal Government	Rome, NY	Rick Metzger	Research	Y
Cisco Systems	Company	San Jose, CA	Ken Watson	Research Knowledge Transfer	N
Department of Homeland Security	Federal Government	Washington, DC	Doug Maughan	Research	Y
DoCoMo USA Labs	Company	Palo Alto, CA	Svetlana Radosavac	Research	Y
EADS	Company	Paris, France	Cedric Blancher	Research	Y
eBay	Company	San Jose, CA	Rinki Sethi	Education	Y
Fortinet	Company	Sunnyvale, CA	Ken Xie	Education	Y
Hewlett-Packard	Company	Palo Alto, CA	Rich McGeer	Research Knowledge Transfer	N
Intel	Company	Santa Clara, CA	Anand Rajan	Research Knowledge Transfer	N
Intuit	Company	Mountain View, CA	Samantha Scott	Education	Y
McKesson	Company	San Francisco, CA	Michelle Nix	Education	Y
Microsoft Research	Company	Redmond, WA	Mike Schroeder	Research	N
Oracle	Company	Redwood Shores, CA	Mary Ann Davidson	Knowledge Transfer	N
Salesforce	Company	San Francisco, CA		Education	Y
SELEX Sistemi Integrati	Company	Rome, Italy	Emanuela Barbi	Research	Y
Sun Microsystems	Company	Menlo Park, CA	Katherine Hartsell	Research Education	Y
Symantec	Company	Santa Monica, CA	Marc Dacier	Research Knowledge Transfer	N
Tata Consultancy Services	Company	Chennai, India	Sanjay Bahl	Education	N
United Technologies	Company	East Hartford, CT	Clas Jacobson	Research Knowledge Transfer	N
Visa International	Company	San Francisco, CA	George Sullivan	Research Knowledge Transfer	N

9 INDIRECT/OTHER IMPACTS

9.1 International Activities

None to report.

9.2 Other Outputs, Impacts, and Influences

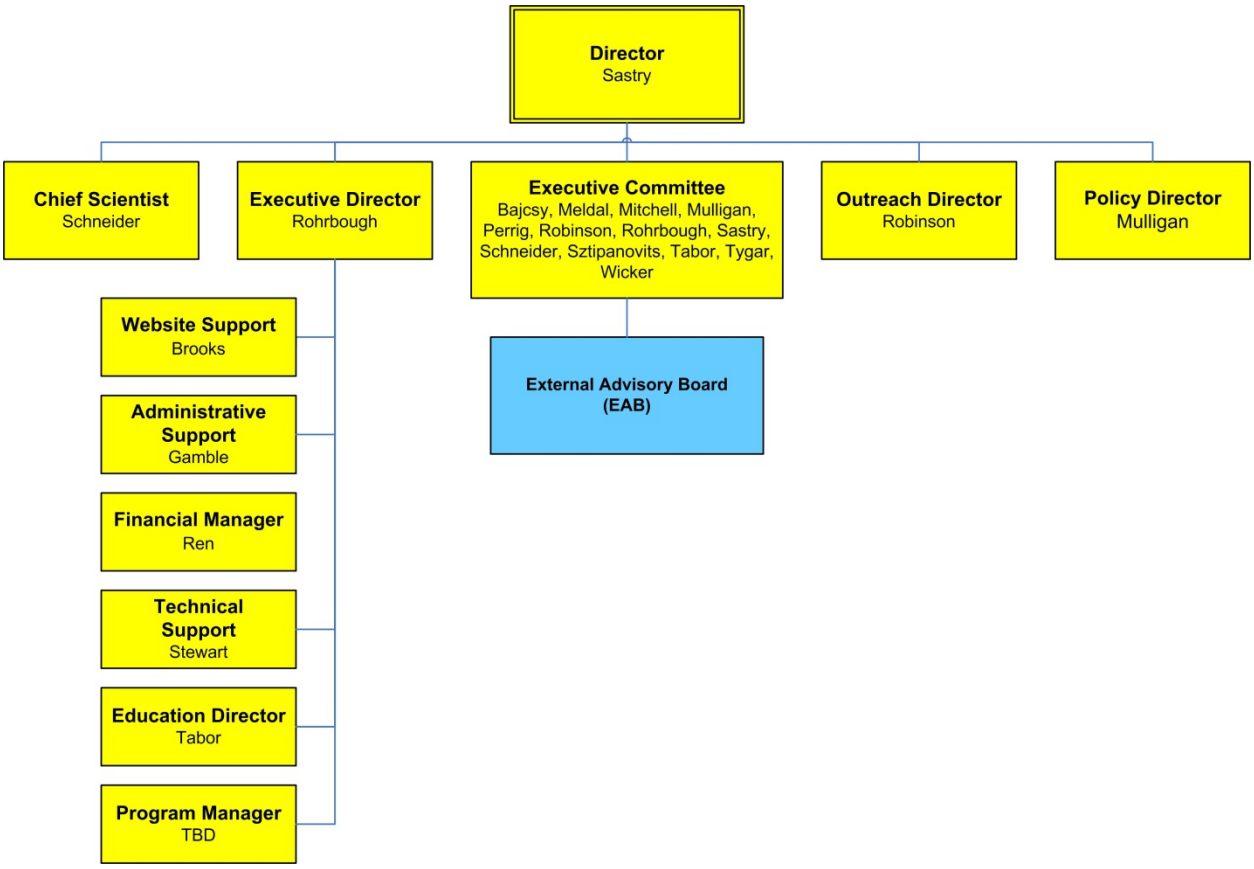
None to report.

10 ATTACHMENTS

Appendix A: Biographical Information of New Faculty

During the reporting period, there were no new faculty investigators not previously been involved with TRUST added from across the Center's partner institutions.

Appendix B: Center Organizational Chart



Appendix C: Minutes of External Advisory Committee Meetings

Minutes are in the form of PowerPoint slides. The slides below are from the November 3-4, 2011 TRUST External Advisor Board meeting in Washington, DC. There are a total of ten (10) slides for that meeting.

TRUST EXTERNAL ADVISORY BOARD MEMBERS

Tamer Başar
Professor, Electrical and Computer Engineering, University of Illinois at Urbana-Champaign

Rebecca Bace
President and CEO, Infidel, Inc.

Emanuela Barbi
Head of Intangible Capital Management
SELEX Sistemi Integrati

Marjory Blumenthal
Assistant Provost of Academics, Georgetown University

Brian Chess
Chief Scientist, Fortify Software

David Clark
Senior Research Scientist, CSAIL, Massachusetts Institute of Technology

Alissa Cooper *
Chief Computer Scientist, Center for Democracy & Technology

Úlfar Erlingsson
Manager, Security Research, Google

Richard Kemmerer *
Professor, Computer Science, University of California, Santa Barbara

Jay Lala
Senior Engineering Fellow, Raytheon Company

Leslie Lambert
Chief Information Security Officer, Juniper Networks

Doug Maughan
Program Manager, Cyber Security R&D, Department of Homeland Security

Mike Schroeder
Assistant Director, Microsoft Research Silicon Valley

Dan Schutzer
President, Financial Services Technology Consortium

Valerie Taylor *
Professor, Computer Science and Engineering, Texas A&M University

Noam Ziv
Vice President of Engineering, Health & Life Sciences, Qualcomm

* Unable to attend the meeting

4 Nov 2011 TRUST EAB Out-Brief 2

EAB CHARTER*

The primary goal of the EAB is to offer an independent assessment of TRUST research, education, outreach, and diversity accomplishments, goals, and plans.

The EAB's guidance supplements the strategic planning by TRUST management and the TRUST Executive Committee and EAB input plays a crucial role in the annual revision of the TRUST Strategic Plan.

The EAB also communicates the perspectives and research needs of both industry and the government and helps the Executive Board develop and execute a successful Public/Private partnership model.

* TRUST Proposal 2008

4 Nov 2011 TRUST EAB Out-Brief 3

4th EAB Meeting
Washington, DC

- Part I: Overview of TRUST Research and Report on Research, Education, and Outreach, Nov 3 – 4, 2011
- Part II: EAB Deliberations, Nov 4th
- Part III: Out brief to TRUST Exec Committee, Nov 4th

4 Nov 2011 TRUST EAB Out-Brief 4

Out-Brief Topics

- TRUST Strengths
- EAB Recommendations

TRUST Strengths

- Based on research selected for presentation to EAB, more work has been focused on contribution to SoS
- Work on metrics shows great promise in foundational science for security
- Heightened combination of technology and policy starting to bear fruit
  - Connected to appropriate policy influentials
- World class team of researchers
- Passionate & committed leadership & effective management structure
- Education and Outreach continue to perform well
  - Emphasis on URM and woven is good even though it may not be reflected using NSF guidelines (160 hrs min)

4 Nov 2011 TRUST EAB Out-Brief 6

Recommendations (1 of 4)

- More effort needed towards a holistic body of work; a taxonomy of SoS may help
- Continue to push on capturing, preserving, and disseminating the SoS Laws in a concise and precise way

Recommendations (2 of 4)

- Use policy progress to inform an ongoing program of technical research
- And, use SoS to advance policy agenda

Recommendations (3 of 4)

- EAB would like to see a concise summary of the extensive research activities to-date.
- Progression, evolution, and interaction of ideas and projects across universities.
- Ensure that inter-disciplinary projects have collaborators from relevant domains.

Recommendations (4 of 4)

- Good to see that TRUST Leadership is starting to plan for the future
- Need to lay out drivers: continued research, maturation of 6.1 concepts and SoS; transition to use; etc.
- Draft white papers can be circulated to EAB for iteration before the next annual EAB meeting

4 Nov 2011 TRUST EAB Out-Brief 10

Appendix D: Media Publicity Materials (if any)

Below are flyers for TRUST-sponsored events and programs, including:

- Summer 2011 TRUST Research Experiences for Undergraduates (REU) program.
- Summer 2011 TRUST Women's Institute for Summer Enrichment (WISE) program.
- Summer 2011 TRUST Summer Experience, Colloquium and Research in Information Technology (SECuR-IT) program.
- 1st ACM International Conference on High Confidence Networked Systems (HiCoNS) at CPSWeek 2012


TRUST
Team for Research in Ubiquitous Secure Technology
TRUST-REU 2011
NSF
An Eight-Week Summer Research Experience for Undergraduates
in Cybersecurity and Trustworthy Systems
eBaY
CYBERSECURITY AND TRUSTWORTHY SYSTEMS
TRUST is addressing technical, operational, privacy, and policy challenges with interdisciplinary projects that combine fundamental science and applied research to deliver breakthrough advances in trustworthy systems in three "grand challenge" areas:
Financial Infrastructures
Health Infrastructures
Physical Infrastructures
REU students work in small groups on TRUST research projects with faculty and graduate mentors.
Apply by
March 1, 2011 at:
www.truststc.org/reu
RESEARCH PROGRAM LOCATIONS
UC Berkeley (Berkeley, CA)
Carnegie Mellon University (Pittsburgh, PA)
Cornell University (Ithaca, NY)
Stanford University (Palo Alto, CA)
Vanderbilt University (Nashville, TN)
The Team for Research in Ubiquitous Secure Technology (TRUST) is a National Science Foundation sponsored Science and Technology Center, Cooperative Agreement No. 0424422 with headquarters at the University of California, Berkeley.

TRUST-REU 2011

An Eight-Week Summer Research Experience for Undergraduates in Cybersecurity and Trustworthy Systems

RESEARCH ACTIVITIES

- Define a research problem
- Conduct a scientific research
- Summarize your results in a scientific paper
- Present your finding in oral and poster presentations

PROGRAM BENEFITS

- 8-week research experience: June 6 – July 29, 2011
- Program dates may vary depending on location
- Research guided by faculty mentors and graduate students
- Guest speakers, lab tours and industry field trips
- Graduate school advising and subsidized GRE prep course
- $4,000 Stipend
- Travel allowance up to $600
- Room and board provided

Contact Information

Dr. Kristen Gates
TRUST REU Program Office
University of California
337 Cory Hall
Berkeley, CA 94720

510-642-3737
kgates@eecs.berkeley.edu
URL: www.truststc.org

"This program helped me realize not only that I definitely want to pursue graduate school, but also where I'd like to apply and what I'd like to study!" – REU Participant

WHO SHOULD APPLY?

- Must be a US Citizen or US Permanent Resident
- Completed Sophomore year of study in Computer Science, Computer Engineering or related field
- Good programming knowledge in an Object-oriented language (C++ or Java)
- GPA of 3.0 or above with an upward trend
- Underrepresented students are encouraged to apply

HOW DO I APPLY?

On-line application with additional information and instructions is available at: **www.truststc.org/reu**
Application deadline is **March 1, 2011**

The Team for Research in Ubiquitous Secure Technology (TRUST) is a National Science Foundation sponsored Science and Technology Center, Cooperative Agreement No. 0424422 with headquarters at the University of California, Berkeley.

WISE 2011: Women's Institute in Summer Enrichment

Sponsored by the Team for Research in Ubiquitous Secure Technology (TRUST)

July 15th through 19th, 2011: Carnegie Mellon University, Pittsburgh, PA

Program Description

WISE is a one-week residential summer program on the Carnegie Mellon University 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.

We are inviting scholars who are willing to share their knowledge, experience and skills with women faculty and graduate students in the various computer science, electrical engineering, and civil engineering disciplines associated with sensing systems for critical infrastructure, with an emphasis on the security and privacy issues that arise from the use of sensing systems in public places.

Topics may include but are not limited to:
Electronic Medical Records and Health Record Portals * Secure Sensor Networking * Sensor Information Processing * mobile and sensor cloud computing * Public Surveillance, Privacy, and the 4th Amendment * Rights and responsibilities of data, data owners and data users

Seminar Speakers (a partial list)

- Lorrie Cantor: CyLab, Carnegie Mellon University
- Chris Hoofnagle : TRUST, Berkeley Center for Law and Technology, UC Berkeley
- Leslie Lambert: Juniper Networks
- Brad Malin: TRUST, Biomedical Informatics, School of Medicine, Vanderbilt University
- Priya Narasimhan: CyLab, Carnegie Mellon University
- Adrian Perrig: TRUST, Carnegie Mellon University
- Bruno Sinopoli: TRUST, Carnegie Mellon University
- Dawn Song : TRUST, UC Berkeley
- Yuan Xue: TRUST, Electrical Engineering and Computer Science, Vanderbilt University

WISE 2011 at Carnegie Mellon University in Pittsburgh, Pennsylvania

The seminar will be held on the campus of Carnegie Mellon University. The seminar will last one week and begin on July 15, 2011 and includes lodging and meals.

WISE Tuition

Tuition for WISE 2011 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 for Ph.D. candidates, post-doctoral fellows, and professors of all levels for the Institute.

Application Process

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.

- **On-line application** only (available December 1, 2010) at **http://www.truststc.org/wise/apply**
- Application deadline: **April 1, 2011 at 11:59 PM (Pacific Time)**
- Women will be given strong consideration although everyone is encouraged to apply

Contact Information

Dr. Kristen Gates, Executive Director of Education
Team for Research in Ubiquitous Secure Technology (TRUST)
337 Cory Hall
University of California, Berkeley CA 94720
(510) 642-3737 :: email: kgates@eecs.berkeley.edu :: URL: www.truststc.org

Team for Research in Ubiquitous Secure Technology (TRUST) :: URL: www.truststc.org
National Science Foundation Cooperative Agreement No. 0424422
University of California, Berkeley :: Carnegie Mellon University :: Cornell University
San Jose State University :: Stanford University :: Vanderbilt University

SECuR-IT

Summer Experience, Colloquium and Research in Information Technology with UC Berkeley, Stanford University and San Jose State University

SUMMER 2011: Graduate Student Academic Immersion with Internship Program
June 13th through August 19th, 2011

The Team for Ubiquitous Secure Technology (TRUST) is proud to announce the Summer Experience, Colloquium and Research in Information Technology (SECuR-IT). This is a ten-week paid internship with academic seminars, sponsored by TRUST partners UC Berkeley, Stanford University and San Jose State University with internships located in Silicon Valley and the San Francisco Bay Area.

Program Overview

- Paid internship at a Silicon Valley technology company
- Learning cohort of 24 graduate students
- Seminars and presentations in security topics at Stanford University, UC Berkeley and industry partner campuses
- College units for summer educational program

Graduate student internship opportunities available in

Security Architecture • Security Awareness and Security Management • Host and OS Security • Mobile and Cloud Security • Application Security • Network Security • Secure Software Engineering • Risk Management • Policy and Legal Compliance

Participating Technology Companies

Juniper Networks • Fortinet • Broadcom • eBay • SalesForce • McKesson • Intuit • Symantec

Program Structure

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 University, University of California, Berkeley and San Jose Sate University
- Informal social gatherings that provide a relaxed setting for students and faculty to exchange ideas and share experiences;
- Ten week, paid 40-hour per week internship.

Application Process

SECuR-IT participation is open to graduate students (M.S. & Ph.D). Participation is limited to 30 people and will be selected from a nationwide pool of applicants, who have demonstrated, outstanding academic talent.

- **On-line application only at http://www.truststc.org/securit/apply**
  Applications review as received—with deadline: **February 18, 2011 at 5pm PST**
- Women and historically underrepresented ethnic minority groups will be given strong consideration although everyone is encouraged to apply.

Contact Information

Dr. Kristen Gates, Executive Director of Education
Team for Research in Ubiquitous Secure Technology (TRUST)
337 Cory Hall
University of California, Berkeley CA 94720
(510) 642-3737 :: email: kgates@eecs.berkeley.edu :: URL: www.truststc.org

---

Team for Research in Ubiquitous Secure Technology (TRUST) :: URL: www.truststc.org
National Science Foundation Cooperative Agreement No. 0424422
University of California, Berkeley :: Carnegie Mellon University :: Cornell University
San Jose State University :: Stanford University :: Vanderbilt University

1st INTERNATIONAL CONFERENCE ON HIGH CONFIDENCE NETWORKED SYSTEMS (HiCoNS)

The 1st International Conference on High Confidence Networked Systems (HiCoNS) aims to bring together novel concepts and theories that will help in the development of the science of high confidence networked systems, in particular those considered cyber-physical systems (CPS).

The conference will focus on system theoretic approaches that increase the confidence of networked CPS by making them more secure, dependable, and trustworthy.

Topics of interest include

- Taxonomy of attacks and attack models
- Novel security challenges
- Testbeds for critical infrastructures
- Decision and game theory
- Design architectures
- Risk assessment and verification
- Detectability and diagnosis of attacks
- Economics based studies of security
- Resilience/robustness against attacks
- Response and reconfiguration methods

Other topics are welcome!

Initial submission is a 3-5 page extended abstract

April 17-18, 2012
CPSWeek 2012






Important Dates:
November 30, 2011 Extended Abstracts Due
January 6, 2012 Authors Notified
February 3, 2012 Camera Ready Papers Due
April 17-18, 2012 Conference Dates

Conference Website:
http://www.hi-cons.org/

Association for Computing Machinery

TRUST