TRUST

Team for Research in Ubiquitous Secure Technology

Autumn 2009 Conference

October 29 – 30, 2009

Hamilton Crowne Plaza
Washington, DC

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

CONTENTS

WELCOME MESSAGE

It is with great pleasure that we welcome you to the ***TRUST Autumn 2009 Conference*** in Washington, DC.

This is one of two major conferences each year that highlights activities of the TRUST Center. Specifically, work of the Center is focused on:

- Advancing a *leading-edge research agenda* to improve the state-of-the art in cyber security and critical infrastructure protection;
- Developing a *robust education plan* to teach the next generation of computer scientists, engineers, and social scientists; and
- Pursuing *knowledge transfer* opportunities to transition TRUST results to end users within industry and the government.

This conference provides an opportunity to hear firsthand about recent research results and future plans of TRUST faculty and students across all TRUST-affiliated universities. We hope you will find the conference educational, engaging, and insightful.

We are honored this time to have two keynote speakers. On Thursday, Donna Dodson from the National Institute of Standards and Technology will provide an overview of cybersecurity-related activities at NIST and their links to other government initiatives and work within the research community. On Friday, Fred Schneider, a professor of Computer Science at Cornell University and the TRUST Chief Scientist, will discuss the TRUST Center's plans to help define a science-base for security, including the kinds of questions one might expect such a science base to address and examples of how such questions have been answered.

For those of you not affiliated with TRUST, or new to TRUST, I encourage you to use this conference to meet the TRUST team and find out more about the Center and its projects.

Sincerely,

S. Shankar Sastry
Director, Team for Research in Ubiquitous Secure Technology
Dean of Engineering, University of California, Berkeley

TRUST OVERVIEW

The **Team for Research in Ubiquitous Secure Technology (TRUST)** is focused on the development of cyber security science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure. Established as a National Science Foundation Science and Technology Center (STC), TRUST is addressing technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems.

TRUST activities are advancing a leading-edge *research* agenda to improve the state-of-the art in cyber security; developing a robust *education* plan to teach the next generation of computer scientists, engineers, and social scientists; and pursuing *knowledge transfer* opportunities to transition TRUST results to end users within industry and the government.

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:

Financial Infrastructures – Creation of a trustworthy environment that links and supports commercial transactions among financial institutions, online retailers, and customers.

Health Infrastructures – Technology that advances "Healthcare Informatics" to enable engaged patients, personalized medicine, providers as coach-consultants, and agile evidence-based care.

Physical Infrastructures – Advances that support Next Generation Supervisory Control and Data Acquisition (SCADA) and control systems, including power, water, and telecommunications.

TRUST is led by the University of California, Berkeley with partner institutions Carnegie Mellon University, Cornell University, Mills College, San Jose State University, Smith College, Stanford University, and Vanderbilt University. TRUST projects have a holistic view that addresses computer security, software technology, analysis of complex interacting systems, and economic, legal, and public policy issues. As such, TRUST draws on researchers is such diverse fields as Computer Engineering, Computer Science, Economics, Electrical Engineering, Law, Public Policy, and the Social Sciences.

More information on TRUST is available at **http://www.truststc.org**.

CONFERENCE AGENDA

THURSDAY, OCTOBER 29, 2009

TIME	*TOPIC*
0800 – 0845	**Breakfast**
0845 – 0900	Conference Welcome
0900 – 1000	Keynote Address – Overview of NIST Cybersecurity Activities *Donna F. Dodson (National Institute of Standards and Technology)*
1000 – 1030	**Break**
Session1: Physical Infrastructures *Chair: Steve Wicker (Cornell University)*	
1030 – 1040	TRUST Physical Infrastructures Overview *Steve Wicker (Cornell University)*
1040 – 1100	TRUST for SCADA: A Simulation-Based Experimental Platform *Gabor Karsai (Vanderbilt University)*
1100 – 1120	Secure Control Against Replay Attacks *Bruno Sinopoli (Carnegie Mellon University)*
1120 – 1140	Critical Infrastructure Protection and Privacy-Aware Design *Steve Wicker (Cornell University)*
1140 – 1200	Stealthy Deception Attacks on Water SCADA Systems *Saurabh Amin (University of California, Berkeley)*
1200 – 1330	**Lunch / TRUST Poster and Demonstration Period**
Session 2: Financial Industry/TRUST Collaboration Roundtable *Chair: John Mitchell (Stanford University)*	
1330 – 1400	Session Overview and Financial Infrastructures Workshop Outbrief *John Mitchell (Stanford University), Brian Peretti (Department of Treasury), Dan Schutzer (FSTC)*
1400 – 1445	Financial Industry/TRUST Roundtable Introductions
1445 – 1530	Financial Industry/TRUST Collaboration: *Financial Industry Goals and Needs* *Warren Axelrod (FSTC), Craig Froelich (Bank of America), Mike McCormick (Wells Fargo), Dan Schutzer (FSTC)*
1530 – 1600	**Break**
1600 – 1645	Financial Industry/TRUST Collaboration: *TRUST Technologies and Research* *Alessandro Acquisti (Carnegie Mellon University), Mike Reiter (University of North Carolina at Chapel Hill), Dawn Song (University of California, Berkeley), Janos Sztipanovits (Vanderbilt University), Hakim Weatherspoon (Cornell University)*
1645 – 1700	Wrap Up / Next Steps *John Mitchell (Stanford University), Ken Birman (Cornell University), Fred Schneider (Cornell University)*
1700	**Conference Attendee Reception (TRUST Posters/Demonstrations on Display)**

CONFERENCE AGENDA (cont.)

FRIDAY, OCTOBER 30, 2009

TIME	*TOPIC*
0800 – 0900	**Breakfast**
0900 – 1000	Keynote Address – Agenda for a Science of Security *Fred Schneider (Cornell University)*
1000 – 1030	**Break**
Session 3: Financial Infrastructures *Chair: Anupam Datta (Carnegie Mellon University)*	
1030 – 1050	Reintroducing Consistency Guarantees in Cloud Computing Systems *Ken Birman (Cornell University)*
1050 – 1110	Efficient Character-Level Taint Tracking for Java *Erika Chin (University of California, Berkeley)*
1110 – 1130	A Logic of Secure Systems and its Application to Trusted Computing *Jason Franklin (Carnegie Mellon University)*
1130 – 1150	JavaScript Heap Analysis: From Exploiting Browsers to Building Safe JavaScript Subsets *Joel Weinberger (University of California, Berkeley)*
1150 – 1210	Competitive Cyber-Insurance and Network Security *Galina Schwartz (University of California, Berkeley)*
1210 – 1230	Reasoning about Concrete Security in Protocol Proofs *Arnab Roy (Stanford University)*
1230 – 1330	**Lunch / TRUST Poster and Demonstration Period**
Session 4: Health Infrastructures *Chair: Janos Sztipanovits (Vanderbilt University)*	
1330 – 1400	Stratified Negation and HIPAA Compliance *John Mitchell (Stanford University)*
1400 – 1430	Learning Privacy Policy from Audit Logs *Brad Malin (Vanderbilt University)*
1430 – 1500	Guideline Driven Patient Management Systems *Janos Mathe (Vanderbilt University), Jason Martin (Vanderbilt University Medical Center)*
1500 – 1530	Body Sensors for In-Home Patient Monitoring *Yuan Xue (Vanderbilt University), Posu Yan (University of California, Berkeley)*
1530 – 1545	**Wrap Up / Conference Closing**

PRESENTATION ABSTRACTS

Thursday, October 29

0900 – 1000 **Keynote Address – Overview of NIST Cybersecurity Activities**

Donna F. Dodson (Deputy Chief Cybersecurity Advisor, National Institute of Standards and Technology)

NIST provides standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and information systems. Through its diverse research agenda and participation in many nation priority initiatives, leading to the development and implementation of high-quality, cost-effective security and privacy mechanisms, NIST helps improve information security across the federal government and the nation. This talk will provide an overview of NIST's Cyber Security research and development activities. It will also describe NIST's related standards, metrics and test programs.

1030 – 1040 **TRUST Physical Infrastructures Overview**

Steve Wicker (Cornell University)

A brief overview of ongoing TRUST research into the monitoring, controlling, and securing of critical infrastructure. An emphasis will be placed on the overlapping roles of engineering, computer science, and public policy in this TRUST thrust.

1040 – 1100 **TRUST for SCADA: A Simulation-Based Experimental Platform**

Gabor Karsai (Vanderbilt University)

Designing SCADA systems in general and control algorithms in particular that are robust against realistic security attacks on the network and the computing infrastructure is non-trivial as realistic evaluation is necessary. Today, high-fidelity dynamic simulations of plants and controllers, as well as networks are available, but they can rarely be used together. This talk will present an approach for building such integrated simulation platforms that leverages results from a related project on C2 systems. The approach is based on a model-based paradigm for integrating dynamic simulators and has been used to construct a simulation-based testbed to evaluate plant-specific control algorithms together with networks and network attack models. The testbed is highly configurable through the domain-specific simulation models and the integration models.

1100 – 1120 **Secure Control Against Replay Attacks**

Bruno Sinopoli (Carnegie Mellon University)

This work analyzes the effect of replay attacks on a control system. We assume an attacker wishes to disrupt the operation of a control system in steady state. In order to inject an exogenous control input without being detected the attacker will hijack the sensors, observe and record their readings for a certain amount of time and repeat them while carrying out his attack. This is a very common and natural attack (we have seen numerous times intruders recording and replaying security videos while performing their attack undisturbed) for an attacker who does not know the dynamics of the system but is aware of the fact that the system itself is expected to be in steady state for the duration of the attack. We assume the control system to be a discrete time linear time invariant Gaussian system applying an infinite horizon Linear Quadratic Gaussian (LQG) controller. We also assume that the system is equipped with a Chi Square failure detector. The main contributions of this work, beyond the novelty of the problem formulation, consist in 1) providing conditions on the feasibility of the replay attack on the aforementioned system and 2) proposing a countermeasure that guarantees a desired probability of detection (with a fixed false alarm rate) by trading off either detection delay or closed loop system performance.

1120 – 1140 **Critical Infrastructure Protection and Privacy-Aware Design**

Steve Wicker (Cornell University)

During this talk I will discuss recent advances in sensor networking and their potential for monitoring, controlling, and securing physical infrastructure. As part of this presentation I will discuss current efforts to secure and control the U.S. electrical power grid. I will then present a series of design rules for exploiting these new technologies while minimizing the potential threat to privacy. I will conclude with a brief outline of the ethical and pedagogical implications of these design rules.

1140 – 1200 **Stealthy Deception Attacks on Water SCADA Systems**

Saurabh Amin (University of California, Berkeley)

Dynamics of water flow networks, such as irrigation canal systems, can be modeled by differential equations evolving on graphs. Water flow networks are monitored and controlled at boundary nodes by supervisory control and data acquisition (SCADA) systems. Recently, there have been significant developments in the suite of automatic control methods for water SCADA systems such that a user specified performance criteria as well as certain robustness guarantees are achieved in closed-loop. Water SCADA systems often use commodity information technology (IT) solutions and are now being made accessible to remote users via corporate networks and the Internet. Thus, they inherit many of known IT vulnerabilities and threats. Indeed, recent incidents have confirmed that cyber-attacks on water SCADA systems have become a more attractive choice for the attackers in comparison to physical attacks; they are cheaper, less risky, and are becoming easier to execute.

We believe that in order to increase the resilience of SCADA systems under attacks, a system theoretic characterization of cyber-attacks is needed. Motivated by this challenge, we will discuss stealthy deception attacks on a typical water SCADA system managing an irrigation canal network. We study scenarios in which an adversary—with financial or malicious intent—can carry out deception attacks on certain sensor and control processes. In particular, we focus on analysis of stealthy deception attacks in which the adversary degrades the intended purpose of commonly used proportional (P) or proportional-integral (PI) controllers by compromising certain sensor measurements and/or control actions. We use the theory of switching dynamical systems to model adversary's actions and show that due to the slow and distributed nature of these systems, detection of these attacks can be difficult for the SCADA system. We illustrate a deception attack scenario implemented on a real SCADA system that manages the Gignac canal in France.

1330 – 1400 **Session Overview and Financial Infrastructures Workshop Outbrief**

John Mitchell (Stanford University)
Brian Peretti (Department of Treasury)
Dan Schutzer (FSTC)

The session will kick off with an overview of the goals and objectives, a discussion on recent collaboration between the financial services industry, the government, and the research community, and an outbrief on topics discussed and issues raised during a recent financial infrastructures workshop.

1400 – 1445 **Financial Services / TRUST Roundtable Introductions**

Alessandro Acquisti (Carnegie Mellon University)
Warren Axelrod (FSTC)
Craig Froelich (Bank of America)
Mike McCormick (Wells Fargo)
Mike Reiter (University of North Carolina at Chapel Hill)
Dan Schutzer (FSTC)
Dawn Song (University of California, Berkeley)
Janos Sztipanovits (Vanderbilt University)
Hakim Weatherspoon (Cornell University)

Roundtable panelists from the financial industry and academic research community will be introduced. Each will speak briefly about their work, in particular activities associated with securing financial systems, networks, and other infrastructure.

1445 – 1530 **Financial Services / TRUST Collaboration: *Financial Industry Goals and Needs***

Warren Axelrod (FSTC)
Craig Froelich (Bank of America)
Mike McCormick (Wells Fargo)
Dan Schutzer (FSTC)

Panelists from the financial services industry will present several topics that address industry's needs and long-term goals for secure, trustworthy financial infrastructures.

1600 – 1645 **Financial Services / TRUST Collaboration: *TRUST Technologies and Research***

Alessandro Acquisti (Carnegie Mellon University)
Mike Reiter (University of North Carolina at Chapel Hill)
Dawn Song (University of California, Berkeley)
Janos Sztipanovits (Vanderbilt University)
Hakim Weatherspoon (Cornell University)

Panelists from the research community will present work focused on improving security and trust in financial infrastructures, including recent research results, relevant technologies, and future research directions.

1645 – 1700 **Wrap Up / Next Steps**

John Mitchell (Stanford University)
Ken Birman (Cornell University)
Fred Schneider (Cornell University)

The session will conclude with a wrap up of the topics discussed, highlighting key points of interest to both the financial services industry and the research community, and will propose next steps for follow-up actions and areas of collaboration.

Friday, October 30

0900 – 1000 **Agenda for a Science of Security**
Fred Schneider (Cornell University)
For this second term, TRUST will focus on helping define a science-base for security. This talk will discuss the kinds of questions one might expect such a science base to address. It will also give examples of how such questions have been answered.

1030 – 1050 **Reintroducing Consistency Guarantees in Cloud Computing Systems**
Ken Birman (Cornell University)
Modern cloud platforms have begun to "embrace inconsistency" for reasons of scalability. Yet consistency guarantees are at the core of security and reliability and if we are ever to host medical records or banking records in cloud settings, clearly will be required. This talk will look at the reasons for the trend, and some reasons to believe that researchers should be able to overcome the underlying issues.

1050 – 1110 **Efficient Character-Level Taint Tracking for Java**
Erika Chin (University of California, Berkeley)
Over 80% of web services are vulnerable to attack, and much of the danger arises from command injection vulnerabilities. We present an efficient character-level taint tracking system for Java web applications and argue that it can be used to defend against command injection vulnerabilities. Our approach involves modification only to Java library classes and the implementation of the Java servlets framework, so it requires only a one-time modification to the server without any subsequent modifications to a web application's bytecode or access to the web application's source code. This makes it easy to deploy our technique and easy to secure legacy web software. Our preliminary experiments with the JForum web application suggest that character-level taint tracking adds 0-15% runtime overhead.

1110 – 1130 **A Logic of Secure Systems and its Application to Trusted Computing**
Jason Franklin (Carnegie Mellon University)
We present a logic for reasoning about properties of secure systems. The logic is built around a concurrent programming language with constructs for modeling machines with shared memory, a simple form of access control on memory, machine resets, cryptographic operations, network communication, and dynamically loading and executing unknown (and potentially untrusted) code. The adversary's capabilities are constrained by the system interface as defined in the programming model (leading to the name csi-adversary). We develop a sound proof system for reasoning about programs without explicitly reasoning about adversary actions. We use the logic to characterize trusted computing primitives and prove code integrity and execution integrity properties of two remote attestation protocols. The proofs make precise assumptions needed for the security of these protocols and reveal an insecure interaction between the two protocols.

1130 – 1150 **JavaScript Heap Analysis: From Exploiting Browsers to Building Safe JavaScript Subsets**
Joel Weinberger (University of California, Berkeley)
Many JavaScript security issues revolve around the delicacy of the same-origin policy. The basic concern is that information from one origin should not leak to another. We develop a technique that uses JavaScript heap analysis to analyze the behavior of different origins on the heap and identify a new class of vulnerabilities which we call "cross-origin JavaScript capability leaks". We discover several instances of these vulnerabilities and propose a solution to mitigate them in web browsers. Additionally, we use these techniques to identify problems in safe JavaScript subsets. In particular, we discuss ADsafe and several problems identified with it and propose an alternative safe JavaScript subset with the same properties but more security guarantees.

1150 – 1210 **Competitive Cyber-Insurance and Network Security**

Galina Schwartz (University of California, Berkeley)

This paper, joint with Nikhil Shetty, Mark Felegyhazi, and Jean Walrand, investigates how competitive cyber-insurers affect network security and welfare of the networked society. In our model, a user's probability to incur damage (from being attacked) depends on both his security and the network security, with the latter taken by individual users as given. First, we consider cyber-insurers who cannot observe (and thus, affect) individual user security. This asymmetric information causes moral hazard. Then, for most parameters, no equilibrium exists: the insurance market is missing. Even if an equilibrium exists, the insurance contract covers only a minor fraction of the damage; network security worsens relative to the no-insurance equilibrium. Second, we consider insurers with perfect information about their users' security. Here, user security is perfectly enforceable (zero cost); each insurance contract stipulates the required user security. The unique equilibrium contract covers the entire user damage. Still, for most parameters, network security worsens relative to the no-insurance equilibrium. Although cyber-insurance improves user welfare, in general, competitive cyber-insurers fail to improve network security.

1210 – 1230 **Reasoning about Concrete Security in Protocol Proofs**

Arnab Roy (Stanford University)

Concrete security analysis of network protocols is a refinement of complexity theoretic analysis where the aim is to provide quantitative security guarantees instead of asymptotic ones. This provides valuable insight into answering such questions as how frequently should we refresh keys and what is the exact trade-off between security and efficiency given known methods to attack the cryptographic primitives. We are developing a logical framework which supports reasoning about concrete security. We demonstrate the system by proving concrete authentication guarantee of a signature based challenge response protocol. This is joint work with Anupam Datta, Joseph Y. Halpern, John C. Mitchell, and Riccardo Pucella.

1330 – 1400 **Stratified Negation and HIPAA Compliance**

John Mitchell (Stanford University)

The complexity of regulations in healthcare, financial services, and other industries makes it diffcult for enterprises to design and deploy effective compliance systems. We believe that in some applications, it may be practical to support compliance by using formalized portions of applicable laws to regulate business processes that use information systems. In order to explore this possibility, we use a stratified fragment of Prolog with limited use of negation to formalize a portion of the U.S. Health Insurance Portability and Accountability Act (HIPAA). As part of our study, we also explore the deployment of our formalization in a prototype hospital Web portal messaging system.

1400 – 1430 **Learning Privacy Policy from Audit Logs**

Brad Malin (Vanderbilt University)

The healthcare community has made considerable strides in the development and deployment of information systems, with particular gains in electronic health records (EHRs). Many EHRs are equipped with role-based access control, but it is seldom practical in mission-critical environments, such as point-of-care hospitals, where roles lack clear and static definitions. The overarching objective of our research is to build technologies that protect patient privacy in complex primary care environments. The goal for this work specifically is in the development of methods that automatically monitor how users (e.g., physicians) access the records of subjects (e.g., patients). We model the system as dynamic teams participating in healthcare business processes and subsequently apply the learned models to score the "safety" of each recorded EHR access. Our pilot study with six-months data from the Vanderbilt University Medical Center, which contains over seven million accesses, has revealed

that though there is churn in the teams, there are clear patterns of information use, as well as statistically confirmable anomalies of access. This presentation will illustrate some of the methods our tools apply and the open source framework that is available for evaluation and extension by the research community.

1430 – 1500 **Guideline Driven Patient Management Systems**

Janos Mathe (Vanderbilt University)

Jason Martin (Vanderbilt University Medical Center)

Using evidence-based guidelines to standardize the care of patients with complex medical problems is a difficult challenge. In acute care settings, such as intensive care units, the inherent problems of stabilizing and improving vital patient parameters is complicated by the division of responsibilities among different members of the health care team. Computerized support for implementing such guidelines has tremendous potential. The use of model-integrated techniques for specifying and implementing guidelines as coordinated asynchronous processes is a promising new methodology for providing advanced clinical decision support. Combined with visual dashboards, which show the status of the implemented guidelines, a new approach to computer-supported care is possible. These techniques are being applied to the management of sepsis at the Vanderbilt Medical Center (VMC).

1500 – 1530 **Body Sensors for In-Home Patient Monitoring**

Yuan Xue (Vanderbilt University)

Posu Yan (University of California, Berkeley)

The cost of health care has become a national concern. Recent advances in wireless communication, networking and information technology have made it possible to monitor rehabilitation outcomes across diverse health care environments (such as hospital, rehabilitation facility, nursing facilities, or home care). This provides a unique opportunity for evidence-based medical practice where a large amount of medical information can be collected to help determine the most effective strategies for treating chronic illness, reducing disability and secondary conditions, improving health outcomes, and reducing the healthcare expenses by more efficient use of clinical resources. To facilitate this process, existing technologies on wireless communication, sensor platform, networking, and database have to be fully integrated with the existing clinical enterprise practice to become part of the overall chronic disease management process.

This talk presents our work on supporting remote congestive heart failure (CHF) patient monitoring and management via an integration of biosensor technology, mobile wireless communication platform and clinical enterprise system. In the remote patient monitoring and management, a sensor-based networking system captures and analyzes the medical data of a patient and securely transmits in real time the relevant information to the clinical patient management system. It is built on top of open-source software and readily available hardware. The system is designed to be generic -- it not only monitors CHF patients but supports mobile health applications in general. The design of the remote patient monitoring and management system employs a Model-Integrated Computing (MIC) approach, where the formal models of treatment protocols is built to manage the overall medical processes. Using a model-based approach, security becomes an integral part of the overall system design, where formal models of the security policies are integrated into the clinical workflow models. This talk will present our system design, its end-to-end security support, and the experiments on the monitoring and treatment of congestive heart failure (CHF) patients.
We will also present a second BSN system, WAVE and Berkeley Fit, which aims to leverage social networking to promote physical fitness.

KEYNOTE SPEAKER BIOGRAPHIES

Donna F. Dodson

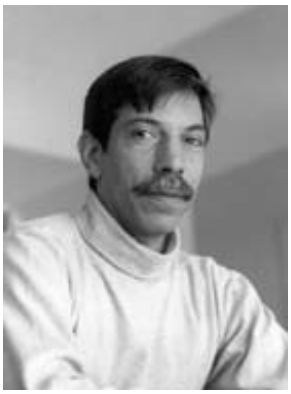
Deputy Chief Cybersecurity Advisor
National Institute of Standards and Technology

Donna Dodson is the Deputy Cyber Security Advisor at the National Institute of Standards and Technology (NIST). As part of the management team, Donna helps direct the development of NIST's standards, technology and research for the protection of information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems.

She is also an active contributor in the areas of authentication and cryptography. Donna has also managed programs including the Advanced Encryption Standard, key management, PKI, authentication and security testing.

Fred Schneider

Samuel B. Eckert Professor of Computer Science,
Cornell University
Chief Scientist, TRUST Center



Fred Schneider is a professor in Cornell's Computer Science Department and director of the AFRL/Cornell Information Assurance Institute. Professor Schneider has a B.S. from Cornell, an M.S. and Ph.D. (1978) from SUNY Stony Brook, and a D.Sc. [honoris causa] from the University of Newcastle upon Tyne (2003). He is a fellow of AAAS and ACM, and was named Professor-at-Large at University of Tromso (Norway) in 1996.

Professor Schneider is author of the graduate text *On Concurrent Programming*, and is co-author (with David Gries) of the undergraduate text *A Logical Approach to Discrete Math*. In addition to chairing the National Research Council's study committee on information systems trustworthiness and editing *Trust in Cyberspace*, Professor Schneider is co-managing editor of Springer-Verlag's Texts and Monographs in Computer Science, associate editor-in-chief of "IEEE Security and Privacy", and serves on several other journal editorial boards.

A member of industrial technical advisory boards for FAST ASA, CIGITAL, and Fortify, Professor Schneider co-chairs Microsoft's Trustworthy Computing Academic Advisory Board. Professor Schneider also serves on the NSF CISE Advisory Board and the National Research Council's CSTB. He was founding chief scientist of New York State's Griffiss Institute cybersecurity consortium and currently serves as a member of the Board of Directors and as its Science Advisor.

Professor Schneider's research concerns problems associated with making distributed and concurrent systems trustworthy. His early work was in formal methods and methodologies for concurrent programming and in protocols for fault-tolerance. More recently, his attention has turned to topics in computer security.

SPEAKER BIOGRAPHIES

Saurabh Amin

University of California, Berkeley

Saurabh is a fifth year graduate student in the Civil and Environmental Engineering systems engineering program. Before coming to UC Berkeley, Saurabh studied civil engineering at the Indian Institute of Technology, Roorkee (formerly, University of Roorkee). He then studied transportation engineering at the University of Texas at Austin, where he obtained an M.S.E. in the area of infrastructure systems. He moved to Berkeley in fall 2004 for his Ph.D. studies and is currently interested in control of hybrid systems, robust optimization, boundary control of hyperbolic PDEs, and reachability analysis for stochastic systems. His research has been supervised by Prof. S. Shankar Sastry and Prof. Alexandre M. Bayen.

Ken Birman

Cornell University

Ken Birman is Professor of Computer Science at Cornell University. He currently heads the QuickSilver project, which is developing the world's fastest and most scalable publish-subscribe system and a new, highly automated, platform aimed at making it dramatically easier to build scalable clustered applications.

Previously he worked on fault-tolerance, security, and reliable multicast. In 1987 he founded a company, Isis Distributed Systems, which developed robust software solutions for stock exchanges, air traffic control, and factory automation. For example, Isis currently operates both the New York and Swiss Stock Exchanges, the French air traffic control system, and the US Navy AEGIS warship. The technology permits these and other systems to automatically adapt themselves when failures or other disruptions occur, and to replicate critical services so that availability can be maintained even while some system components are down.

In contrast to his past work, Birman's recent work has focused on issues of scale, self-management and self-repair mechanisms for complex distributed systems, such as large data centers and wide-area publish-subscribe. The very large scale of these kinds of applications poses completely new challenges. For example, while protocols for data replication on a small scale are closely tied to database concepts such as two-phase commit, these large scale applications are best viewed as probabilistic systems, and the most appropriate technologies are similar to techniques seen in peer-to-peer file sharing applications.

Birman is the author of several books. His most recent textbook, *Reliable Distributed Computing: Technologies, Web Services, and Applications*, was published by Springer-Verlag in May of 2005. Previously he wrote two other books and more than 200 journal and conference papers, including one that appeared in Scientific American in May, 1996. Dr. Birman was also Editor in Chief of ACM Transactions on Computer Systems from 1993-1998 and is a Fellow of the ACM.

Erika Chin

University of California, Berkeley

Erika Chin is a Ph.D. student in Computer Science at the University of California, Berkeley. She received her B.S. degree in Computer Science from the University of Virginia. Her current research interest is in improving web security. In particular, she is interested in taint tracking and server-side solutions to prevent web-based attacks. She is currently the Vice President of the Computer Science Graduate Student Association (CSGSA), the Siebel Scholar Ambassador to Berkeley, and a member of Women in Computer Science and Electrical Engineering (WICSE).

Jason Franklin

Carnegie Mellon University

Jason Franklin is a 5th year Ph.D. student in the Computer Science Department at Carnegie Mellon University. He received a B.S. in Computer Science and Mathematics from the University of Wisconsin-Madison in 2005. He is the recipient of the 2005 USENIX Security Best Paper Award, 2009 SOSP Best Paper Award, Department of Homeland Security Fellowship, and NSF Graduate Research Fellowship.

His research focuses on the application of principled techniques to improve system and network security.

Gabor Karsai

Vanderbilt University

Dr. Gabor Karsai is a Professor of Electrical Engineering and Computer Science at Vanderbilt University, and Senior Research Scientist at the Institute for Software-Integrated Systems. He has over twenty-five years of experience in software engineering. He conducts research in the design and implementation of embedded systems, in programming tools for visual programming environments, in the theory and practice of model-integrated computing, in resource management and scheduling systems, and in real-time fault diagnostics. He received his B.Sc., M.Sc., and Dr. Tech degrees from the Technical University of Budapest, Hungary, in 1982, 1984 and 1988, respectively, and his PhD from Vanderbilt University in 1988. He has published over 100 papers, and he is the co-author of four patents. He has managed several large DARPA projects in the recent past: advanced scheduling and resource management algorithms that resulted in a technology being transitioned into all tactical aviation squadrons of the USMC, fault-adaptive control technology that has been transitioned into the J-UCAS program, and model-based integration of embedded systems whose resulting tools are being used in embedded software development toolchains. He is Senior Member of IEEE, and serves as on the Editorial Board of Journal of Software and Systems.

Bradley Malin

Vanderbilt University

Bradley Malin is an assistant professor of biomedical informatics at the Vanderbilt University Medical Center. His primary research focus is on data privacy and management issues in biomedical research and clinical management systems. He is the author of numerous scientific articles on data privacy, fraud detection, and surveillance within various technologies, including text databases, biomedical databases, and face recognition systems. His research on the re-identification and privacy protection of patient-specific genomic database records has received several awards from the American Medical Informatics Association and International Medical Informatics Association. Brad holds a bachelor's in molecular biology, a master's in public policy and management, a master's in computer science ("data mining and knowledge discovery"), and a doctorate in computer science ("computation, organizations, and society") from Carnegie Mellon University.

Prior to joining Vanderbilt, he was a graduate researcher in the Data Privacy Laboratory at Carnegie Mellon University.

Janos Mathe

Vanderbilt University

Janos L. Mathe received his M.Sc. degree in Computer Science at the Technical University of Budapest in 2004. He continued his studies by enrolling to the Department of Electrical Engineering and Computer Science at Vanderbilt University where he is currently pursuing his Ph.D. under the guidance of Janos Sztipanovits. Janos is interested in applying Model-Integrated Computing techniques to address the security and privacy requirements in healthcare settings. His current research focuses on the model-based development of clinical information systems where he investigates how modeling, validation, verification and deployment of treatment protocols can be performed by using the example of sepsis management.

John Mitchell

Stanford University

John Mitchell is a Professor of Computer Science and (by courtesy) Electrical Engineering at Stanford University. Professor Mitchell's research interests are in computer security (access control, network protocols and software system security) as well as programming languages, type systems, object systems, formal methods, and applications of mathematical logic to computer science.

Professor Mitchell has a B.S. from Stanford University and an M.S. and Ph.D. from the Massachusetts Institute of Technology in 1984.

Arnab Roy

Stanford University

Arnab Roy is a Ph.D. candidate at the Stanford University Department of Computer Science and a Siebel Scholar, Class of 2006. Prior to joining Stanford, he completed undergraduate studies at Indian Institute of Technology Kharagpur obtaining the Prime Minister of India Gold Medal for graduating at the top of his class.

Galina Schwartz

University of California, Berkeley

Galina Schwartz is a researcher in the Department of Electrical Engineering and Computer Sciences, at the University of California, Berkeley. She focuses game theory applications to Internet commerce, specifically Internet security and service quality (network neutrality). Galina Schwartz received her Ph.D. in Economics from Princeton University. Prior to joining TRUST, she taught economics in the Department of Economics, UC Berkeley and UC Davis, and finance in the Department of Finance at the University of Michigan, Ann-Arbor, Ross School of Business. She collaborates with University of Michigan Center for Information Technology Integration (CITI).

Bruno Sinopoli

Carnegie Mellon University

Bruno Sinopoli received the Dr. Eng. degree from the University of Padova in 1998 and his M.S. and Ph.D. in Electrical Engineering from the University of California, Berkeley in 2003 and 2005, respectively, along with the Management of Technology Certificate from the Haas Business School. After a postdoctoral position at Stanford University, Dr. Sinopoli joined the faculty at Carnegie Mellon University where he is an assistant professor in the Department of Electrical and Computer Engineering with courtesy appointments in Mechanical Engineering and in the Robotics Institute.

Dr. Sinopoli was awarded the 2006 Eli Jury Award for outstanding research achievement in the areas of systems, communications, control and signal processing at UC Berkeley.

His research interests include networked embedded control systems, distributed estimation and control with applications to wireless sensor-actuator networks and system security.

Joel Weinberger

University of California, Berkeley

Joel Weinberger is a Ph.D. student in Computer Science at the University of California, Berkeley. Joel Weinberger received a B.S. and M.S. in Computer Science from Brown University in 2007. From 2007 to 2008, Joel worked in the Fishworks group at Sun Microsystems as a software engineer. At UC Berkeley, his research with his advisor, Dawn Song, has primarily focused on JavaScript security and creating tools for programming secure systems with greater ease.

Stephen Wicker

Cornell University

Stephen B. Wicker is a Professor of Electrical and Computer Engineering at Cornell University, and a member of the graduate fields of Computer Science and Applied Mathematics. Professor Wicker was awarded the 1988 Cornell College of Engineering Michael Tien Teaching Award and the 2000 Cornell School of Electrical and Computer Engineering Teaching Award. As of early 2007, he has supervised thirty doctoral dissertations.

Professor Wicker is the author of *Codes, Graphs, and Iterative Decoding* (Kluwer, 2002), *Turbo Coding* (Kluwer, 1999), *Error Control Systems for Digital Communication and Storage* (Prentice Hall, 1995) and *Reed-Solomon Codes and Their Applications* (IEEE Press, 1994). He has served as Associate Editor for Coding Theory and Techniques for the *IEEE Transactions on Communications*, and is currently Associate Editor for the *ACM Transactions on Sensor Networks*. He has served two terms as a member of the Board of Governors of the IEEE Information Theory Society, and chaired the Technical Program Committee for the Fifth International Conference on Information Processing in Sensor Networks (IPSN 2006).

Professor Wicker teaches and conducts research in wireless information networks, digital systems, self-configuring systems, and artificial intelligence. His current research focuses on the use of probabilistic models and game theory in the development of highly distributed, adaptive sensor networks. He is also conducting joint research with the Berkeley School of Law on privacy policy and the impact of the deployment of sensor networks in public spaces. Professor Wicker is the Cornell Principal Investigator for the TRUST Science and Technology Center – a National Science Foundation center dedicated to the development of technologies for securing the nation's critical infrastructure.

Professor Wicker heads the Wireless Intelligent Systems Laboratory, whose focus is on the field of wireless networks, including traditional cellular networks, ad-hoc networks, and sensor networks.

Yuan Xue

Vanderbilt University

Yuan Xue received her B.S. in Computer Science from Harbin Institute of Technology, China in 1998 and her M.S. and Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign in 2002, and 2005. Currently she is an assistant professor at the Department of Electrical Engineering and Computer Science of Vanderbilt University. She is a recipient of the Vodafone fellowship. Her research interests include wireless and sensor networks, peer-to-peer and overlay systems, QoS support, and network security. She is a member of the IEEE and ACM.

Posu Yan

University of California, Berkeley

Posu is currently a staff engineer in the Electrical Engineering and Computer Sciences department at the University of California, Berkeley. After graduating from EECS at UC Berkeley and receiving an M.S. in computer science at UCLA, he is now mainly involved in the areas of wireless camera motes and wireless body sensors. Aside from engineering, he spends his free time pursuing music and other artistic endeavors.

NOTES

NOTES (cont.)