Kenneth Birman, computer science professor at Cornell University and TRUST coordinator for knowledge transfer

Fred B. Schneider, computer science professor at Cornell University and chief scientist of TRUST

TRUST education director Kristen Gates

SCADA FACILITY

Critical infrastructure, including power plants, water systems, and electric power networks, are controlled by devices that measure parameters of the system and activate controllers. Those devices are referred to as SCADA networks—Supervisory Control and Data Acquisition. “We feel these SCADA networks need to be replaced by more secure sensor networks, which is why it is one of the marquis grand challenge problems in the center,” says Sastry.

The center’s work on secure sensor networks responds to the need to build a new generation of technology to control our nation’s physical infrastructure. TRUST researchers have developed new wireless network embedded systems with secure protocols built into them. They have developed models of attack and corresponding solutions, based on the mathematics of game theory, says Sastry. These solutions are built into the network embedded systems as security safeguards. Prototypes and software are now being transferred into practice, starting with oil and gas networks and power networks. “Those are the lead adopters,” says Sastry. “Initial deployments were made on a 500-node network at Berkeley.” The technology is now being transitioned to an oil company, he notes.

CENTER TACKLES GRAND CHALLENGES IN CYBERSECURITY

Computing technologies are part of our nation’s critical infrastructure. They form a part of everything from financial systems and the energy grid to telecommunication and transportation systems. Enhancing cybersecurity and computer trustworthiness is therefore of increasing importance as a scientific, economic, and social problem.

In response to this need, the Team for Research in Ubiquitous Secure Technology (TRUST) aims to transform the ability of organizations like software vendors, utilities, and government agencies to design, build, and operate trustworthy information systems.

Headquartered at the University of California, Berkeley, and led by center director S. Shankar Sastry, the center is working to catalyze collaboration between computing experts, social scientists, and the legal and policy communities in support of strengthening the security and trustworthiness of our nation’s computing and critical infrastructures. Academic partners in TRUST with UC Berkeley include Carnegie Mellon University, Cornell University, Stanford University, Vanderbilt University, Mills College, San Jose State University, and Smith College.

Sastry, whose research is in the area of secure sensor networks and network defense, is a professor in the Departments of Electrical Engineering and Computer Sciences and Bioengineering at the University of California, Berkeley. He is the NEC Distinguished Professor of Engineering.

Researchers at TRUST are working on three major research thrusts: security of physical infrastructure; combating identity theft and Web security; and access and privacy issues pertaining to electronic medical records. “The theme of the center is restoring trust to all infrastructures: physical, electronic, and information,” says Sastry.

Over the last decade, the world has seen a rapid increase in computer security attacks at all levels, from the so-called “phishing” scams that lure people into revealing sensitive information to Internet attacks that paralyze Web sites. The center has developed many kinds of improved technologies to combat phishing, spyware, botnets, and related threats. But new technologies are only part of the answer.

“The solutions to today’s cybersecurity ills or trustworthiness problems are not going to come only from the technical side or from the policy side of the house—but rather, from both sides working together,” says Fred B. Schneider, computer science professor at Cornell University and chief scientist of TRUST.

These advances may come from research in computer science and engineering—but “sometimes the answer involves changing the law instead of changing the technology,” says Kenneth Birman, computer science professor at Cornell and TRUST coordinator for knowledge transfer. Birman’s research has focused on fault tolerance and distributed computing. He developed software used at the New York Stock Exchange and by the French air traffic control system, among other applications. But better technology sometimes won’t be adopted unless the potential users face strong incentives to do so.

For example, TRUST researcher and clinical law professor Deidre Mulligan of UC Berkeley worked closely on California legislation that requires companies to track down and inform anybody whose private information was disclosed as a result of company negligence. The law passed, and now many other states are trying to enact similar legislation. “This has had an enormous nationwide impact,” says Birman.

When the center started, the kind of connections happening at Berkeley, with legal scholars partnering with technology researchers, was relatively rare, says Sastry. “Now, each one of the partner campuses has an activity in terms of public policy, public health, or social sciences rolled into their agenda which adds to the richness of the issues being discussed,” says Sastry. “It’s gratifying to see all the wonderful links and connections that wouldn’t have happened without the center.” □

TRUST researcher and clinical law professor Deidre Mulligan of the University of California, Berkeley

EDUCATING THE NEXT GENERATION OF CYBERSECURITY EXPERTS

Educational efforts at TRUST, led by Kristen Gates, focus on the enhancing the experience of graduate students by bringing them into contact with leaders in cybersecurity. "Not only are we helping to educate and inspire students but we're also helping to energize and invigorate younger faculty that are bringing these cybersecurity and technology issues into their classrooms at our partner institutions," she notes.

"We're seeing that these perspectives appeal to a diverse range of students," says Kenneth Birman of Cornell University. "They're drawn by the opportunity to have a very positive impact on society," he says. "We wonder if by engaging in this broader way, we may actually appeal to a larger community of students."

A new program staring summer 2007 combines a seminar experience combined with an internship in Silicon Valley companies. It's called SECuR-IT, short for Summer Experience Colloquium and Research in Information Technology, and it's a learning community of 20 graduate students who have applied from all over the country.

These students will be matched with companies that specialize in information technology, such as Cisco, Yahoo, eBay, and Intel, among others. Participants will live at San Jose State University in the dormitory as a learning community, and they will work at organizations in Silicon Valley four days per week. On Fridays, they attend Stanford seminars on cybersecurity given by faculty from partner institutions.

The program is an outgrowth of an industry group of chief security officers organized by John Mitchell, TRUST principal at Stanford, and Robert Rodriguez, a consultant, formerly of the Secret Service. The informal working group has met periodically to talk about issues in cybersecurity education and curriculum. "In addition to college curriculum recommendations from industry, two things came out of that process," says Mitchell, "the industry contacts for the summer internship program, and a speaker series, which we plan to record and archive on the Web."

ELECTRONIC MEDICAL RECORDS: SECURITY, PRIVACY, AND ACCESS

TRUST researchers Janos Sztipanovits and colleagues at Vanderbilt University are involved in efforts to automate health care records. But there is an inherent tension between the goals of providing access to information to those who ought to have it, and protecting information from those who ought not to have it.

"Because Vanderbilt is at the forefront of this research nationally, we have a unique window into a laboratory where cutting edge work is going on," notes Schneider.

A health portal at the Vanderbilt medical school with some 10,000 patient records has been made available to TRUST as a test bed for research on access and privacy issues. Called "MyHealthAtVanderbilt," the system is one of the largest operational healthcare portals in the world, according to the center. "MyHealthAtVanderbilt" gives patients secure messaging with their providers. They can make appointments online and see the contents of their medical records.

TRUST researchers are working to develop a theory of privacy that is amenable to automation. "The challenge is to help organizations understand how to treat sensitive data, what they can and can't use it for, and how to track its use," says Mitchell. "We want to help organizations build information systems a with a privacy policy that helps them manage sensitive information correctly."

A CONVERSATION WITH THE DIRECTOR

Shankar Sastry

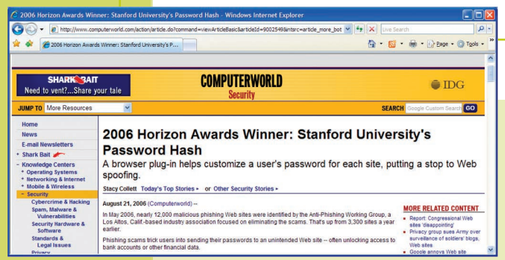
When it comes to cybersecurity and computer trustworthiness, "the problems are so big, there is not the talent in any one university to put this together. So I thought we needed a coalition," says center director S. Shankar Sastry.

"I'm operating on a sense of conviction that the science and technology is important, but getting it out before it's too late is *as* important. So to do that means a combination of someone with research credentials and committed to getting the results out to stakeholders.

"Some researchers feel they come up with the best technologies and they just throw it over the wall, and then they get frustrated the world doesn't change.

"But the reason it doesn't is that there are important social, legal, economic, privacy considerations that do need to be addressed. And I think an STC needs to be a place to do that."

> **"The problems are so big, there is not the talent in any one university to put this together. So I thought we needed a coalition."**
>
> — SHANKAR SASTRY



GONE: PHISHIN'

A user inadvertently visits a Web site thinking that it's a trusted service provider, like a bank, when in fact it's a "fake" site set up by criminals to capture sensitive information for illegal purposes. This is the scam called "phishing."

TRUST researchers have developed several freely distributed software prototypes that are run with a Web browser to help protect passwords designed for ordinary Web users. "Our goal is to get these ideas picked up in industry and the main browser distributors," says John C. Mitchell, who is the Mary and Gordon Crary Family Professor of Computer Science at Stanford University.

In the abstract, the problem is one of "authentication"—establishing the identity of the entity you're talking to. Whenever you log into a computer and give your password, that's part of a protocol by which you authenticate your identity to the computer.

"We're used to having people prove their identity to machines. We're also actually pretty good at protocols for machines to prove their identity to other machines. But nobody appreciated that there's this other technical problem of having machines prove their identity to people—because really what you want is the web site to somehow prove to you it is who you think it is," says Schneider.

In one scheme, called Dynamic skins, developed by Doug Tygar of UC Berkeley and colleagues, the Web site displays for you a picture that is a secret you share with the site: a sailboat, a cat. Whenever you log in it shows you this picture. A phishing site won't know what your favorite picture is, and therefore it won't be able to reproduce the look of this site of your service provider.

Another scheme is based on the realization that a stolen password only has value if the phishers can reuse the password someplace else. "Most people, having bad memories, have a very small number of passwords that they use at the sites they visit," notes Schneider.

But TRUST researchers realized they could automatically take the password you typed and transform it—by applying a mathematical function called a cryptographic hash to a combination of the password and the name of the site you're visiting—and use that as the password they send to the site. Now, in effect you have a different password at each site but have to remember only one. Phishers get a password, but they cannot decompose it into your password and the word inserted into it. Why not? By analogy, "five plus two is seven, but if I tell you seven, you have no way to know if it was three plus four, one plus six, and so on," explains Schneider.

This development of this method inside a protective browser extension, called PwdHash, was done by Mitchell, Dan Boneh of Stanford, and colleagues. It was honored with an award from *Computerworld* in 2006.

Anti-phishing methods are but one example of many other research projects at the center addressing the general theme of identity theft and security of information systems. Companies are picking up these anti-phishing approaches, among other areas of center research. "We've seen enormous interest from industry," says Birman. "If you're a company out there and having a tough time overcoming a reliability or security problem and start to browse around, the appeal of an NSF STC is that it offers a kind of one stop shopping," he says. "Here's a group of tremendously talented researchers who have come together to do a coherent job of focusing on these questions."