SECURE TECHNOLOGY

TEAM FOR RESEARCH IN UBIQUITOUS SECURE TECHNOLOGY TRUST

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 healthcare, telecommunication, and transportation systems. Enhancing cyber security 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 to strengthen 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, San Jose State University, Stanford University, and Vanderbilt University.

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 and is the NEC Distinguished Professor of Engineering and the Dean of the College of Engineering.

Researchers at TRUST are working on three major research thrusts aimed at improving the trustworthiness of information systems for the nation's critical infrastructures, including the financial sector (banking and financial services), healthcare delivery (health IT systems and medical data), and physical infrastructures (power, water, gas, telecommunications). "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

Kenneth Birman, computer science professor at Cornell University

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

Steve Wicker, Cornell University

CRITICAL INFRASTRUCTURE PROTECTION

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 (Supervisory Control and Data Acquisition) networks and Industrial Control Systems (ICS). "Control systems are at the heart of our nation's critical infrastructure," says Sastry. "As such, we feel it is vitally important that existing networks are secured and next-generation infrastructure is designed, developed, and deployed to ensure trustworthy, high-confidence operations."

To this end, 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 models of attack and corresponding solutions, leveraging traditional security concepts but also areas such as game theory, says Sastry. These solutions are built into the infrastructure systems as security safeguards. Prototypes and software are now being transferred into practice, starting with oil and gas networks and power networks.

At the same time, the center is exploring privacy concerns with emerging technologies in areas such as energy consumption. TRUST researchers at Cornell, led by Stephen Wicker, professor of computer and electrical engineering, are addressing such concerns through novel system architectures that enable the benefits of emerging technologies such as Advance Metering Infrastructure (AMI) while protecting individual consumer privacy. "We are developing a set of privacy-aware design practices for next-generation infrastructures such as demand response," says Wicker. "While there are many related technical and policy issues, we see this work serving as a roadmap for embedding privacy awareness into information networks."

of improved technologies to combat phishing, spyware, botnets, and related threats. But new technologies are only part of the answer.

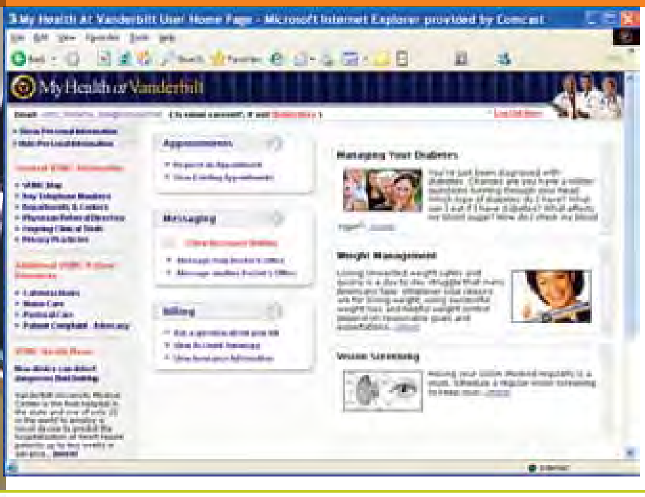
"The solutions to today's cyber security ills or trustworthiness problems are not going to come only from the technical side or from the policy side of the house—but rather, from both sides working together," says Fred B. Schneider, computer science professor at Cornell University and chief scientist 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. For example, TRUST researcher and School of Information 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 have enacted similar legislation. Recent TRUST policy work is addressing issues such as paths to identity theft, privacy in social networking and social media, and the use of web browser tracking technologies for targeted advertising. In such areas, TRUST is conducting research that is addressing technology and policy by crafting solutions that address both business functionality and privacy.

When the center started, the kind of connections between legal scholars and 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."

Another planned legacy of the center is the establishment of a science base for security to move computer security from a reactive to proactive mode and beyond deploying defenses for known attacks but building secure systems in a principled way. The goal of such a "science of security" is to create networks where security is not an afterthought. According to Schneider, such a science of security "would articulate and organize a set of abstractions, principles, and trade-offs for building secure systems, given the realities of the threats and of our cyber security needs." Adds Sastry, "these new capabilities will require the architecture of the infrastructure to change. The idea is that what ultimately replaces them will be more secure and resilient."□

Deirdre Mulligan, TRUST policy director and professor of information at the University of California, Berkeley



TRUSTED HEALTH INFORMATION SYSTEMS

Janos Sztipanovits,
Vanderbilt University

TRUST researchers Janos Sztipanovits and colleagues at Vanderbilt University are involved in efforts to develop secure and trustworthy health information systems. Given the nature of these systems, 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 thousands of 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.

More broadly, TRUST researchers are working on things such as 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 John Mitchell, Stanford principal investigator and professor of computer science. "We want to help organizations build information systems a with a privacy policy that helps them manage sensitive information correctly."

John Mitchell,
Stanford University

EDUCATING THE NEXT GENERATION OF CYBERSECURITY EXPERTS

TRUST education director Kristen Gates

Educational efforts at TRUST, led by Kristen Gates, place an emphasis on enhancing the experience of undergraduate and graduate students by bringing them into contact with leaders in cyber security. "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 cyber security and technology issues into their classrooms at our partner institutions," she notes.

A core program of the center is its Research Experiences for Undergraduates (REU). This eight-week program held annually in the summer offers talented undergraduate students from across the country the opportunity to gain research experience. The center places undergraduate students in cohorts at all partner campuses, working with a faculty advisor and graduate student mentors on topics directly related to TRUST research thrusts. "The REU students were enthusiastic, motivated, and jumped right into the research," says Berkeley law professor and TRUST-REU faculty advisor Chris Hoofnagle, whose REU students researched online tracking techniques. "They were quite successful at uncovering practices that raised a number of privacy issues," says Hoofnagle. "Their work was covered in the press but, more importantly, resulted in privacy improvements on some of the Internet's most popular websites."

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. That requires people with research credentials who are also committed to transitioning results 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 is a place to do that.”

“The STC is also enabling researchers to think broadly about projects of national importance. For example, we are working to advance a science base for security—a means of moving computer security from a reactive mode to a proactive mode, taking the field beyond the current approach of deploying defenses for known attacks to building secure systems in a principled way.”

> “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

2006 Horizon Awards Winner: Stanford University’s Password Hash

A browser plug-in helps customize a user’s password for each site, putting a stop to Web spoofing.

WEB BROWSING: TO TRACK OR NOT TO TRACK

The Internet makes available large amount of information to anyone, anytime, usually for free. While beneficial to users, organizations that produce and make available that content incur costs in doing so. Thus, most websites make use of online advertising. To maximize the effectiveness of advertising, many websites track the activities of users who visit their sites, often by using “cookies”—small files stored on users’ computers—to capture that information.

This presented an interesting opportunity for TRUST researchers to address privacy concerns of end users and policy issues about what information websites should collect and how it is used.

“The political consensus was, if you don’t want to be tracked you can take steps to opt out,” says Chris Hoofnagle, a TRUST researcher and Berkeley law professor. Awareness of issues in this area by TRUST and others led to web browser features that allow users to limit or prevent the storage of cookies from websites.

Lately, though, websites have made use more sophisticated means of tracking that circumvent conventional web browser cookies, for example employing software that “respawns” browser cookies that have been deleted by the user. TRUST research in this area highlighted such practices, prompting a number of popular websites to change their tracking activities and privacy policies. “All of this is about is whether your technical actions, your privacy-seeking behavior, will be affected by advertisers,” says Berkeley’s Hoofnagle. “It’s a major issue that will get more and more attention in the months ahead.”

Related research at Stanford by Jonathan Mayer and Arvind Narayanan, security researchers working with professor John Mitchell, has led to the development of web browser technology that supports a “do not track” mechanism—a means by which web browsers tell websites and online advertisers not to track their activity. “People get creeped out by some of the advertising that happens online,” says Mayer, who, along with Narayanan has created software that can be installed as an add-on to web browsers and is working on ways web servers can process request by users not to be tracked.

This work has not only raised public awareness of online tracking activities, but it has gotten the attention of the Federal Trade Commission and Obama administration, which is pushing for legislation that would compel organizations and online advertisers to respect opt-out mechanisms. “We’re really excited about what we’ve created,” says Mayer. “Do Not Track has the ability to make a meaningful impact in the protection of online privacy.”