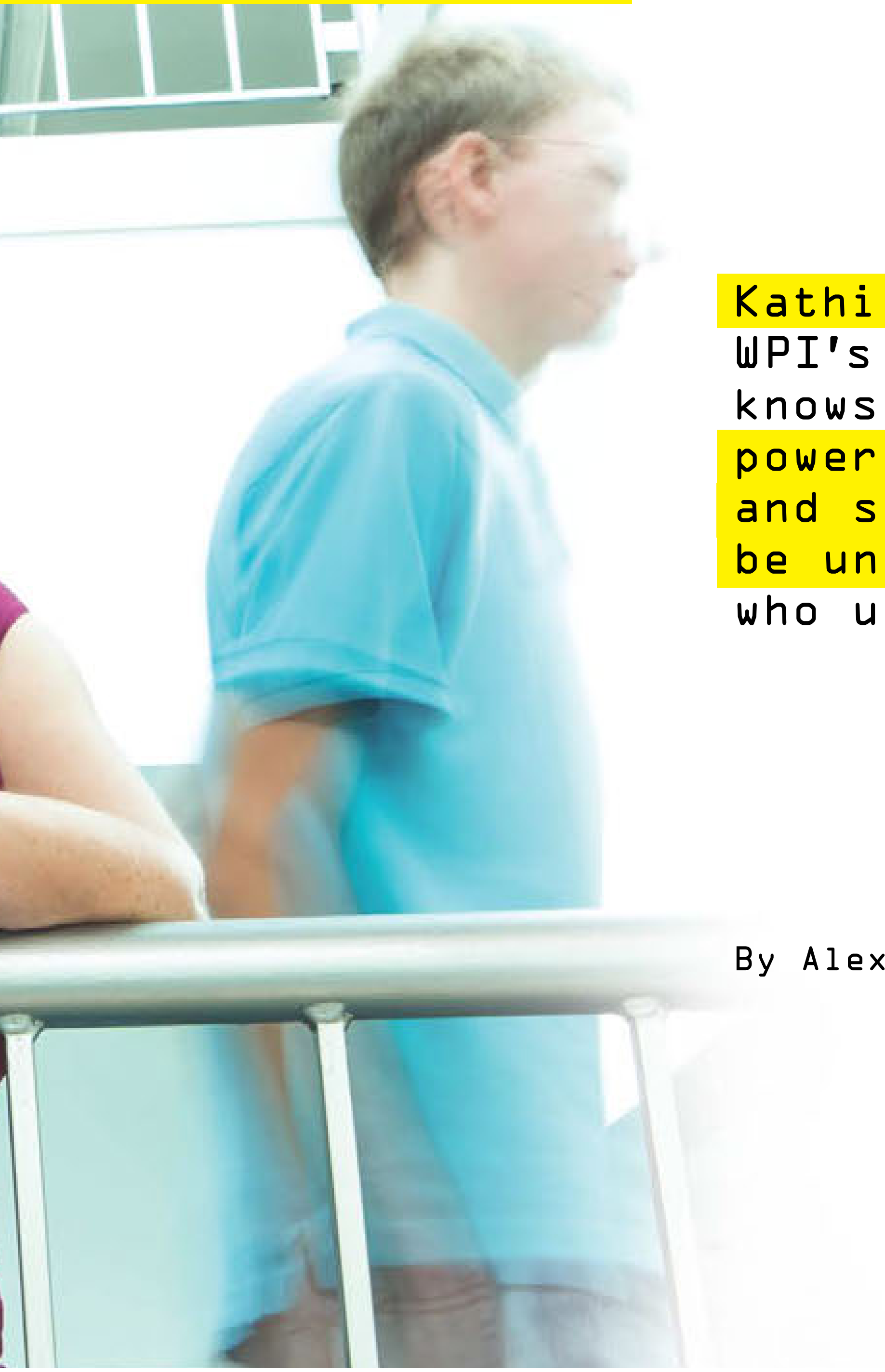
The Weak

Photography by Patrick O'Connor

est Link



Kathi Fisler, director of WPI's Cybersecurity Program, knows that even the most powerful cryptographic tools and security practices can be undone by the people who use them.

By Alexander Gelfand

Security: a complicated business

Engineers and computer scientists have established cryptographic protocols to hide data from prying eyes. They have invented techniques for shielding wireless networks from intrusion. And they've developed guidelines for limiting access to sensitive information.

But every measure and countermeasure comes with its own costs and its own inherent weaknesses. Some of the weaknesses stem from the human factor: the fact that people use technology in ways that can lead to inadvertent leaks or attacks by malicious actors. WPI's new Cybersecurity Program (see sidebar) draws together experts from computer science, electrical and computer engineering, mathematical sciences, and the social sciences to find new and innovative approaches to protecting digital data — approaches that take the human factor into account in one way or another.

"People are the weakest link in just about any security system," says program director **Kathi Fisler**, associate professor of computer science. That's why students in the new program are required to take at least one class that deals with human factors. It's also why Fisler says it's important "to not bug users with stuff they don't want to think about" (and might, therefore, ignore), but instead bug them just enough so they will avoid compromising their own security.

Fisler herself has been building tools to help users understand the implications of their own security and privacy settings, and to help developers understand the security limitations of the systems they design. One of those tools, an application called Margrave, grew out of work she did with her husband, Shriram Krishnamurthi, a professor of computer science at Brown University, her WPI colleague Dan Dougherty, and Tim Nelson, a 2013 PhD recipient who is currently a postdoctoral research associate at Brown.

Margrave interrogates and compares access control policies, the sets of rules that govern who can see and manipulate the various data in a given system. Access control policies specify who can view patient records at a hospital, for example, or who has permission to change student grades in a university database. Such policies can be quite complicated, and are typically managed by human resources personnel who might not understand their full

Preparing Tomorrow's Cyber Watchdogs

In recent years, the need for professionals to defend the nation's information technology from increasingly sophisticated attacks—and from careless users —has been growing at a steep pace. WPI has responded in kind with new academic initiatives, new faculty expertise, and a growing reputation for excellence.

WPI's emerging Cybersecurity Program is driven by nine core faculty members, four of whom arrived during the last two years. They are actively engaged in well-funded research on such topics as software and network security, cryptography, and online privacy.

Having long offered cybersecurity research projects and courses for students pursuing a PhD in either computer science or electrical and computer engineering, the university added a cybersecurity specialization for its existing MS program in computer science. Both programs, as well as a number of new graduate courses in cybersecurity, are seeing rising student interest, according to program director Kathi Fisler, associate professor of computer science.

Also attracting attention is a new graduate certificate in cybersecurity developed expressly for power engineering professionals —the first such program in the nation. The program is designed to help the power industry guard against threats to the electric grid. "This is an exciting program that combines WPI's historic strengths in power engineering with its emerging focus on cybersecurity," Fisler says.

WPI students have expressed their enthusiasm for cybersecurity by forming a cybersecurity club and participating on the WPI Cyber-Defense Team, coached by Craig Shue, assistant professor of computer science. In just its second year, the team took third place, out of 14 teams, in the 2013 Northeast Collegiate Cyber Defense Competition.

WPI's growing momentum in cybersecurity has not gone unnoticed. The university was recently recognized as a National Security Administration/Department of Homeland Security Center of Excellence in Information Assurance Research, Fisler says. "This is a testament to the diverse research and other academic efforts by our security-related faculty."

Krishna Venkatasubramanian develops solutions to security, privacy, and safety concerns raised by interoperable medical devices—pacemakers, sensors, and other medical technology that can communicate over networks.

implications — or the unintended consequences that can ensue when they are altered.

Margrave, however, can run through all of the various roles in an organization and determine precisely who has access to what. It can also compare different access control policies, or different versions of the same policy, to show how changes to the rules can affect privacy and security. That would be a boon to people who must configure their own privacy settings on platforms like Facebook, but have trouble understanding what those settings actually mean. (The "leakage" of private information from Facebook and other websites is one focus of cybersecurity research by Craig Wills, head of WPI's Computer Science Department.)

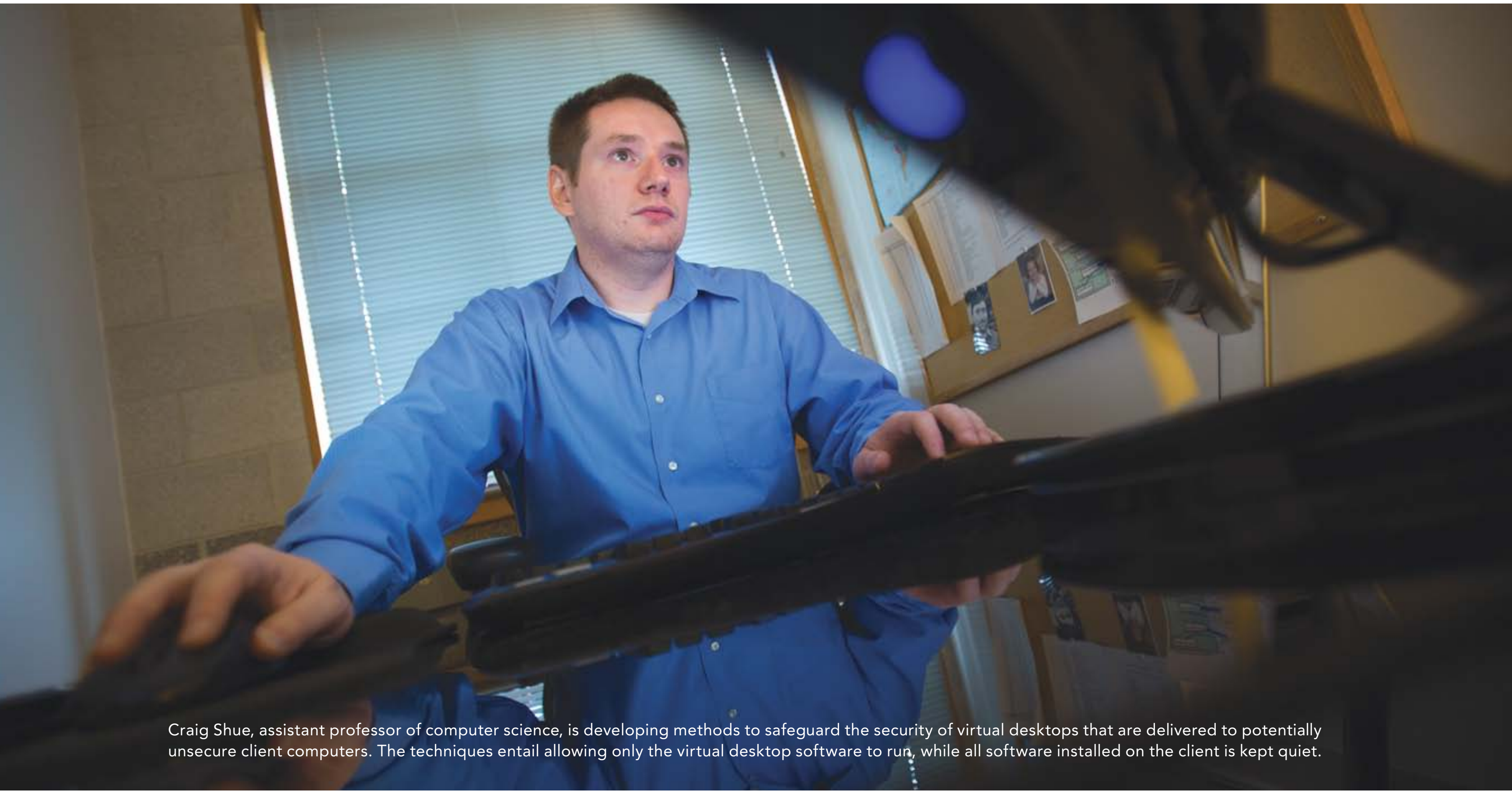
Fisler has also been developing methods for mathematically analyzing applications to verify that they conform to the principles of usable security — principles that are meant to ensure that users actually have the ability to maintain their security on a practical basis. The principle of revocability, for example, might require that a user who has decided to share information can also choose to "unshare" it.

Cyberattacks get personal

Krishna Venkatasubramanian, assistant professor of computer science, is also trying to develop security solutions that are both effective and user-friendly. In particular, Venkatasubramanian is looking for methods for securely coordinating medical devices, like x-ray scanners and heart monitors. Such devices have traditionally operated in standalone fashion, but are now beginning to communicate with one another across networks.

These interoperable medical devices (IMDs) can provide useful information to doctors and nurses, but they also raise a whole host of new security concerns. A sophisticated attacker could eavesdrop on an IMD network to glean sensitive patient information or interfere with specific devices; researchers have already hacked a pacemaker, for example, and fed it faulty instructions. IMDs, therefore, present a case in which cyberattacks could potentially lead to physical harm, or even death.

Consequently, IMDs need to generate alarms not only when a patient's health is at risk, but also when security has been breached — alarms that won't just add to the noise



Craig Shue, assistant professor of computer science, is developing methods to safeguard the security of virtual desktops that are delivered to potentially unsecure client computers. The techniques entail allowing only the virtual desktop software to run, while all software installed on the client is kept quiet.

and confusion of a busy operating room or intensive care unit, but will help hospital staff make informed decisions. The devices also need to be able to enter some kind of safe mode until the problem has been solved, without simply shutting down or failing in a way that could harm a patient.

Together with colleagues at the University of Kansas and the University of Pennsylvania, Venkatasubramanian is working to improve IMD alarm systems with the help of a software "coordinator" — middleware that can interpret the data flowing from multiple devices, determine what kind of alarm should be sounded, and communicate that alarm to healthcare providers in a helpful way.

Isolating the problem

Sometimes, however, it's best to remove users from the security equation completely. That's one of the goals behind a system designed by **Craig Shue**, assistant professor of computer science, and graduate student Evan Frenn.

Shue notes that desktop virtualization services like Citrix can deliver entire virtual desktops to client PCs over the Web. But while the applications and services delivered to the client from the server may be secure, the operating system and applications that live on the client remain vulnerable to infection by malware. In a corporate environment, that can be a serious problem — especially when untrained users are largely responsible for their own security settings, and when more and more people are bringing their own devices to work.

Shue and Frenn have proposed a system in which only the software supplied by the server is allowed to run on the client machine. Everything else, including the client's operating system — millions of lines of code rife with potential security vulnerabilities — is kept quiet, so that even if the client machine is loaded with malware, none of it can cause trouble. The client is able to attest, or prove, via cryptographic means that nothing but the served applications are running; and responsibility for security stays in the hands of the trained IT professionals who work on the server side.

Shue and Frenn's scheme was made possible by recent improvements to secure microprocessors called trusted

WPI's new Cybersecurity Program draws together experts from computer science, electrical and computer engineering, mathematical sciences, and the social sciences to find new and innovative approaches to protecting digital data—approaches that take the human factor into account in one way or another.

platform modules (TPMs) that are installed in many desktop and notebook computers. But what about all of the chips that live in the smartphones and smart cards that, increasingly, are being used to access bank account information, make purchases, and provide proof of identity?

While some of those chips employ cryptographic protections like digital signatures, which rely on both public and private keys, they are far from bulletproof. The cryptographic algorithms currently in use, for example, use the same private keys over and over again. By monitoring the electromagnetic emissions from the chips that process those keys, a clever attacker could, over time, collect enough information to crack the private key.

Building elusive keys

According to **Thomas Eisenbarth**, assistant professor of electrical and computer engineering, there are two ways to fend off such attacks: develop countermeasures to protect the standard cryptographic algorithms; or come up with entirely new algorithms that are less vulnerable in the first place. Having already investigated the former approach, Eisenbarth is currently working on the latter in his own laboratory and in the Vernam Lab, a new partnership between Eisenbarth and fellow ECE cybersecurity researchers Berk Sunar and Lifeng Lai, and William Martin, professor of mathematical sciences (the lab is named for Gilbert Vernam, WPI Class of 1914, who discovered the only unbreakable encryption algorithm).

In a forthcoming paper, Eisenbarth and his collaborators investigate key evolving cryptosystems: algorithms whose private keys change over time, making them more resilient to attack. Such systems have existed in theory for some time, but the trick is to implement them so that they will work in small, low-power devices. And researchers don't yet know what would be less costly, and therefore more viable: equipping the old algorithms with fresh countermeasures, or replacing those algorithms altogether with new and improved ones.

"It's always a trade-off between cost and security," says Eisenbarth, who explains that cryptographic enhancements can increase CPU usage, power consumption, and even chip size.

That may be so. But the need for better, cheaper, and less burdensome security measures will only increase. And Eisenbarth and his colleagues in the Cybersecurity Program will continue to help find them, using all the means at their disposal.

>
Thomas Eisenbarth, assistant professor of electrical and computer engineering, develops key evolving cryptographic algorithms that will make small networked devices more secure.