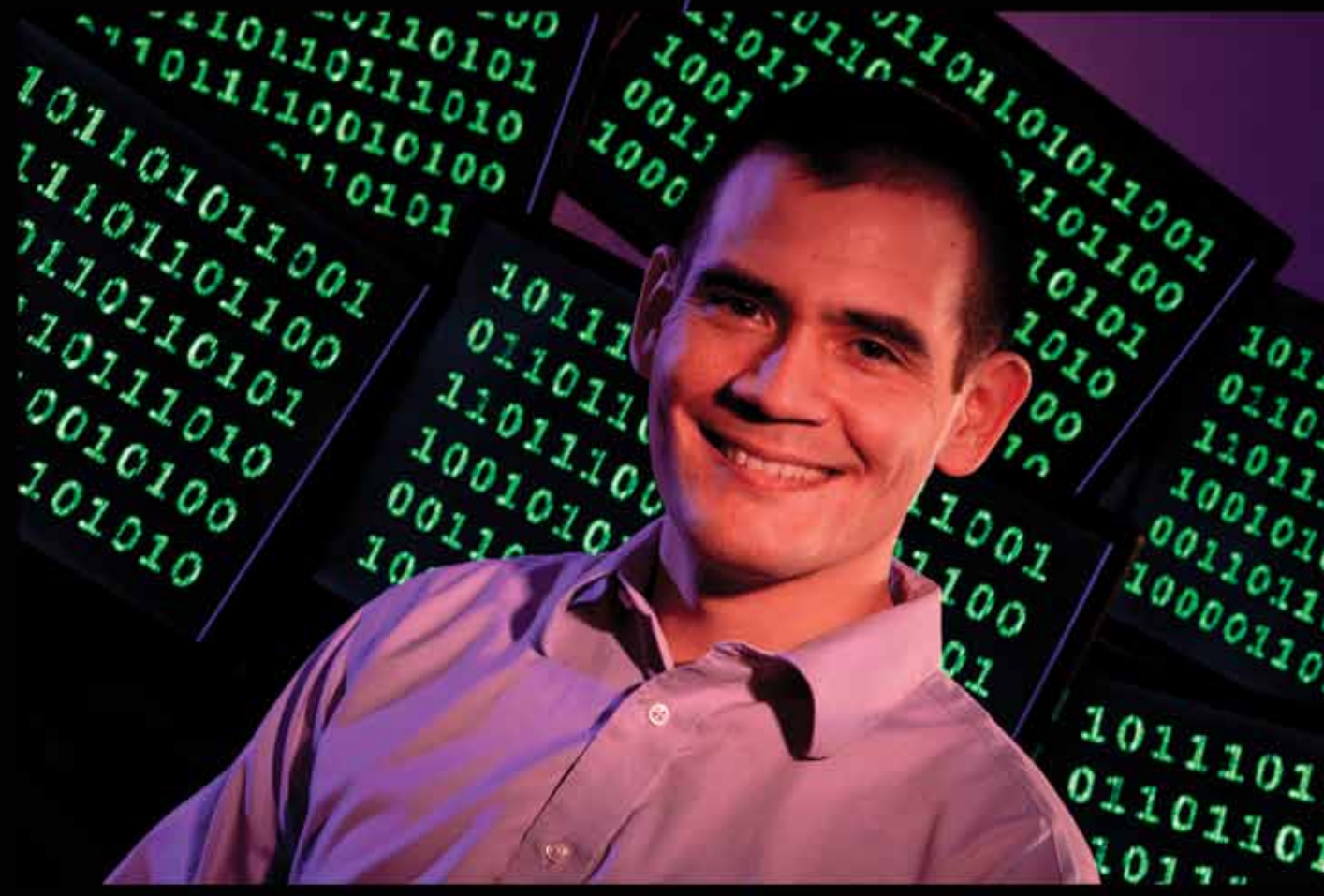
Hackers can play havoc in our lives, but a UW professor is working to make sure you are safe

VIRTUAL GUARDIAN

BY DAVID VOLK



TADAYOSHI

Kohno's experiments are the stuff of science fiction movies: using a kid's Erector Set to spy on its owner, tracking a runner using his mileage monitor or even hackers taking over a car while it's driving and forcing it to brake to a stop. The only difference between Hollywood make-believe and reality is that this white hat hacker doesn't need special effects to make them reality.

He's already overcome all those challenges and he's constantly looking for more. And thanks to the increased use of computer chips that send out or receive information digitally in even seemingly simple devices like toys, ski goggles, cars and pacemakers, there will be no shortage of challenges in the foreseeable future.

The reason is simple, really.

Adding computers to items that haven't been online before makes them hackable. As an example, Kohno points to an Erector Set that came with a built-in wireless connection and a web camera that would allow the owner to control the resulting homemade contraptions via the Internet. While it may sound like innocent fun, its connection to the Internet might also give a less-than-well-intentioned-hacker the ability to spy on the child and her family.

"We actually looked at a number of children's toy robots. You'd be surprised at the number that even have video cameras and wireless connections," Kohno says. The 34-year-old associate professor of in the Department of Computer Science and Engineering doesn't want to be a killjoy, though. The school's only cybersecurity expert just wants to raise public awareness of potential concerns most consumers haven't even considered, but should. "We really need to get people to think about security proactively. People are not thinking about it [now] because they haven't been burned in the past," he says.

The same goes for product makers who are adding the chips, he adds. Although some folks within companies have expressed concern about possible security implications, the worry hasn't translated into action because many of the manufacturers involved haven't had to worry about computer security before.

If the experiments he and his researchers have conducted are any indication, there's plenty of room for concern. The smart meters people have installed in their homes to monitor energy usage are a case in point. While the level of communication between consumers and utilities is a good thing because it can help them be more energy efficient and save money, Kohno's team discovered a potential lack of security could allow a hacker to learn more about a family's habits all the way down to what television shows they watch.

In another experiment, Kohno's team also hacked into a car, flashed its lights, unlocked the power locks and started the ignition without a key. They also managed to put on the brakes while the car was moving. In a far more sobering development, he's even shown that it's possible to hack into pacemakers, insulin pumps and other medical devices. "I think the risk today is pretty small. If someone needed a medical device I would absolutely get one. The point is to understand these vulnerabilities," he says.

Although he enjoys thinking up new targets and experiments, he isn't doing it for fun. Instead, he's trying to stay several steps ahead of the hackers and find other potential problem areas. "We try to anticipate what will be the new hot technologies over the next 10 years" and look for their vulnerabilities so they can point them out to the manufacturers and the government to make products more secure.

Once he and his team successfully hack a device, they try to get manufacturers to plug security holes. Two major organizations within the auto industry, the automotive engineering group SAE International and the U.S. Council for Automotive Research, responded to his car experiment by setting up task forces to study ways to increase car security. Fortunately, most hackers don't have the same level of sophistication as Kohno's team.

Another way to put pressure on manufacturers to pay attention to security concerns is to educate shoppers. Although most try to prevent computer viruses and identity theft, the issue of cybersecurity for everyday, household consumer goods hasn't yet resonated with most people.

"It's safe to say that the average consumer of these technologies doesn't think about it. My hope is that that changes. I would love it if Consumer Reports started analyzing security" and parents start asking, "Is this toy that I'm buying for my child going to compromise his security?" Kohno has already started to push the needle in that direction by developing a card game centering on security. He also covers many of the same issues in his senior level security class, of course. Since security is an issue that crosses all of science and many different disciplines he says he believes that it should be covered long before students are in their final year.

"Our introduction to computer programming classes are taken by a huge number of people, not just people interested in computer science. I would love it if security was available to undergrads and all people taking computer science," he says, adding, "I would love it if we could integrate security as early as we can into the curriculum."

Until he can convince consumer magazines to focus on the issue of cybersecurity, his classes are the best way to have an impact on the problem in the long term. And not a moment too soon.

As he said on a recent episode of *NOVA scienceNOW* in which he was featured, "Our privacy is slowly eroding over time and we need to make a conscious decision to let it happen or try to stop it." ■

—David Volk is a Seattle freelancer writer. His last piece for Columns *was on Huskies in the wine industry.*

Cybersecurity expert Yoshi Kohno wants to raise public awareness of potential concerns most consumers haven't even considered.

MICHAEL MOORE / MR. PIX.COM

UW TACOMA TO OFFER MASTERS IN CYBERSECURITY

A new cybersecurity masters degree program set to start this summer at UW Tacoma offers aspiring computer industry professionals something they won't find at similar programs—a background in business. Launched partly in response to a request from the National Guard at Camp Murray, the year program has five 8-week sessions, each featuring a business class and security class side-by-side. The pairings include Principles of Cybersecurity and Business Communication, as well as Building an Information Risk Management Toolkit and Organization Change. Students will also have an internship where they'll act as a cybersecurity consultant for a local company.