Yoshi Kohno, associate professor of computer science and engineering at the University of Washington, talks about how academic security impacts commercial security, car hacking, and consumer understanding about privacy implications.

You’ve been a consultant, a graduate-level cryptographer, and a professor. How much impact does academic security have on the commercial world, and what are you doing about that? Academia has the potential to have a huge impact in industry. That’s not to say that every project has a lot of impact, but we have a few diamonds in the rough. One recent example is automotive security. Both at University of Washington and in collaboration with University of California, San Diego, we purchased two automobiles, experimentally tried to understand their vulnerabilities, and then disseminated the results of our research. It had a tremendous amount of impact in the automotive industry and even in government, too.

Most of your publicized work involves hacking things that normal people use every day. What motivated your lab to look into cars in the first place?

One of the underlying themes in our lab is trying to figure out what will be the hot new technologies over the next 5, 10, or 15 years that might have potential security and privacy issues. Can we start looking at those technologies now, so that we can have a leg up on the adversary, so that we can proactively address security issues? What drew us to automobiles was the observation that the modern car is pervasively computerized, which raises the question of whether one of its components is compromisable. I haven’t described the vulnerability that we uncovered or our actual adversarial capability, but there are numerous fraud-detection techniques that automotive manufacturers could do on the back end to detect people either mounting an attack or exploring the attack surface to develop attack capability.

I’ve read most of your car hacking work in the popular press. Can you be a little more technical about what you did with the brake controller?

At the highest level, our work was focused into two phases. In the first phase, we asked, “What might an attacker be able to do if he or she could somehow connect to the car’s internal computer network?” That’s a big if, but there’s actually a port underneath the dash called the OBD-II port—the onboard diagnostics port—that’s federally mandated for emission testing purposes. We plugged directly into that port and tried to figure out what we could do from there. The first step is familiar to some of your listeners: eavesdropping. We sat in the car, turned on the lights, and sniffed the packets being sent over that internal network, trying to see which one was sent with different lights turning on or off. From there, we did a playback attack, which gave us the capability to mimic any sort of operation that we saw on the vehicle during its normal operation. Nothing cryptographic prevented us from replaying packets whenever we wished, and that gave
INTERVIEW

About Yoshi Kohno

Yoshi Kohno is an associate professor in the Computer Science and Engineering Department at the University of Washington. His research often garners widespread attention because it focuses on computer security for emerging and consumer technologies, security and privacy for mobile and cloud systems, the human element in computer security systems, and computer security education.

us pretty significant control. I mean, we could set the speedometer to whatever we wanted. We could turn all the lights off if we wanted, including brake lights, and so on.

From there, we wanted to explore another class of capabilities, such as disabling the brakes or forcibly engaging them. We knew we wouldn’t see those messages sent over the car’s internal network during its normal course of operation, so we turned to fuzzing. We made specially crafted packets that were constrained in some areas and had random data in others, sent those packets over the car’s internal network, and then watched what happened. Through that process, we learned how to forcibly disengage the brakes so that if someone put pressure on the brake pedal, the brakes wouldn’t engage. We also learned how to create packets that would forcibly engage the brakes so that if someone were driving, the brakes would suddenly lock up.

This involves access to the bus directly. How did you do that through a wireless transmission?

In the second phase of our research, we wanted to explore how someone might gain access to the car without ever physically touching it, and we found maybe four or five different ways to do that. I’ll start with one of the coolest ones.

The CD player is connected to the car’s internal computer network, and we found two problems with it, one of which being how the car’s CD player handled WMA audio files. Give us any song—in our demo, we used Beethoven’s Ninth Symphony—and we could run it through scripts that would produce a WMA file that would play perfectly on a Windows or a Mac machine, but if you burned it on a CD and put that CD in the car, the doors unlock.

There’s so much focus on the external wireless interface, but we really need to think about all the interfaces, even something as simple as a CD player. The risk for this might be low, but it’s still worth keeping in mind that if I post a WMA file on the Internet and someone downloads it, burns it to a CD, and puts it in their car, this type of thing could happen.

Here’s another example. Because our car has a built-in telematics unit that can effectively call 911 if it gets in an accident—a benefit that most major manufacturers now offer—it means it has a cell phone inside it, which means that we can call it. Once we dialed our car’s phone number, we found that we could play the appropriate tone to switch to the in-band modem and then exploit an authentication vulnerability. Once we did that, we could inject a very small payload to do a buffer overflow and get our own code running on the car.

One of the interesting things for us was that this telematics service—again, in an unmodified car purchased off a lot—basically runs a variant of Unix. The car’s cell phone has 3G data and the Internet. We connected to an FTP server at the University of Washington, which downloaded another, much larger program to run on the car—in this case, an IRC client. We started that client, which then connected to our IRC channel at UW, making the car part of our IRC botnet.

When we have a computer company that learned the hard way that security is an important issue and it moves into an emerging space, it tends to think more proactively about security. But when you have an industry that’s succeeded in its own field—automotive, medical, home automation, toys—and starts thinking, “Hey, let’s bring in computers and wireless to boost our business,” you can bet that it hasn’t learned the hard way to think about security. These systems suffer from the same vulnerabilities that Microsoft and others learned to address back in the mid-1990s.

People are attracted to stories about hacking, but they aren’t as interested in how well a company is building its products. How do you get the media to cover good software and system security?

We’ve had some success with the media looking at our educational efforts. I’m very passionate about trying to figure out new ways to teach computer security. I focus on what some people call professional paranoia and others call the security mindset. I prefer the latter term. When people see a new system or product, they say, “Oh, I can’t wait to use it.” Someone with a security mindset sees that product and says, “Oh, I can’t wait to use it. But I’m also curious about how I could abuse it.” I want to give people enough insight into the security mindset that when they go into industry and start working on their own products, they have this memory of the security mindset, just a little bit of a buzz, so that when something that has a potential security issue arises, maybe they themselves don’t know how to address it, but they’re aware of the
fact that they might need to bring in outside experts.

I believe this kind of thinking can be taught, but I believe also that some people are more natural at it than others. I don’t know if we can bring everyone to a level of expertise that a security expert would have, but I do think we can teach people to have a little bit more of a security mindset.

Let’s assume that you can teach somebody to notice that something’s broken. That doesn’t necessarily teach them how to build it properly in the first place. What do you do about that?

The amount of education involved in how to design secure software is pretty intense. I have students for one 10-week quarter, so I have to drill down into what will have the highest impact. If I focus on exploiting one specific technology, like cross-site scripting or buffer overflow, they might learn it, but in 10 years, that knowledge might be dated. If I can teach them to have a security mindset, then I feel like I’ve done my job for that course. My goal is to teach people to know when to involve someone in security, the security expert will then help with the actual design or evaluation of that system. I’m not expecting that everyone from this course is fully equipped to go it alone.

The “Internet of Broken Things” seems particularly rife with invasion-of-privacy problems. How do we get people to understand the kind of privacy invasion that a lot of these products involve?

I think awareness plus action is the key. One example I like to give is when Facebook changes its privacy policy. There’s usually a lot of public outcry, but then a few weeks later, it dies down and people go back to using Facebook again, seemingly having forgotten about this privacy change.

CHAIR AND TENURED FULL PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, THE GEORGE WASHINGTON UNIVERSITY, WASHINGTON, D.C.

The George Washington University invites applications for a tenured full-professor position as Chair of the Department of Computer science, to begin as early as Summer 2014. This is an exciting opportunity for an outstanding person to lead and expand an established, thriving and growing department.

GW is the largest university in the nation’s capital with close access to many Federal funding agencies and research laboratories. The University offers comprehensive programs of undergraduate and graduate liberal arts studies as well as degrees in engineering, law, medicine, public health, education, business and international affairs. Thanks to a recently adopted strategic plan, GW is committed to creating several multidisciplinary research institutes, including three computation-centric institutes with up to 18 new faculty lines to be filled. Also, in support of its emphasis on research in science and technology, the University is constructing a new 500,000 square foot Science and Engineering Hall in the heart of campus, which includes state-of-the-art research and instructional laboratories, clean rooms, imaging facilities, and much more. The School of Engineering and Applied Science, including the CS Department, will move into the building in Spring 2015.

The Department of Computer Science has 20 full-time faculty members, a large adjunct faculty pool, and 650 students, and offers B.S., B.A., M.S. and Ph.D. degree programs in Computer Science, and an M.S. degree program in Cybersecurity. Its educational and research programs span core as well as cutting-edge areas, with funding from various agencies. Additionally, the University is a federally-designated Center of Academic Excellence in Research in security. Embarked on rapid growth, the Department has hired nine tenure-track professors in the past five years, and plans to continue hiring for the next several years. For further information please refer to http://www.cs.gwu.edu.

Responsibilities

The new Chair will be expected to lead the Department, supervise all of its resources, and promote and support excellence in teaching and research. Equally, the new Chair will lead in effective recruiting of talented faculty and students, and vigorously catalyze and develop further the Department’s collaborations and relationship across the University and with Government and industry. The new Chair will be an active promoter of diversity, an enthusiastic proponent of creativity, innovation and outreach, and an effective advocate and spokesperson for the Department, both within and beyond the University.

Basic Qualifications

Applicants must have a doctorate in Computer science or a closely related field, evidence of outstanding research and academic achievements with a strong reputation in the research and professional community, and a demonstrated ability to teach effectively at both graduate and undergraduate levels.

Inquiries and Application

Inquiries will be accorded the utmost discretion. To inquire, please email Tom Mazzuchi, Chair of the Search Committee (cschsearch@gwu.edu). To apply, complete the online faculty application, at http://www.gwujobs.postings/17254 and upload a detailed CV or resume, full contact information for five professional references and a cover letter that describes your research and teaching accomplishments and your views of growth opportunities in computer science. References will be expected to address research and teaching skills necessary for appointment at the full professor rank as well as skills for the chair position including leadership, interpersonal, administrative, and mentoring abilities. Only complete applications will be considered. Review of applications will begin on April 18, 2014 and will continue until the position is filled.

EEO/AA Policy

The George Washington University is an Equal Opportunity and Affirmative Action Employer. Applications from women and underrepresented minority groups are strongly encouraged.

www.computer.org/security
INTERVIEW

When you break something, and you go back to the people who built it, have you been able to see how products have improved because of your work? Different industries respond in different ways. We’ve looked at home automation systems, medical devices, children’s toys, and automobiles, and I have to say the automotive industry has had an incredibly positive response. The Society of Automotive Engineers created a new task force focused specifically on computer security and privacy for vehicles. I know that a number of manufacturers have significantly ramped up their efforts with a lot of hiring and security. It takes time to reengineer our future automobiles, but I know they’re really proactively thinking about security. The US National Highway Transportation Safety Administration’s focus on security is a result of the work that we did.

What’s your view of the Edward Snowden revelations, and dragnet surveillance, and the way technology is trending now?
It’s hard for me to step back and think about all these revelations and know crisply what I feel. But one of the things that I think security researchers have known for a long time is that these types of things are possible. I don’t know if my worldview has changed significantly, but I do think that we’re seeing a lot more interest in computer security and privacy, which I think is good for the security and privacy community. People are more demanding of the security technologies out there now.

What kind of security education should all engineers and designers be forced to take?
I think threat modeling and the security mindset. We’ve created a new toolkit at the University of Washington with this goal in mind—we originally called them “the Security and Privacy Threat-Discovery Cards,” but now we’re calling them “the Security Cards.” Visit securitycards.cs.washington.edu for a free PDF that lets you download and print these cards, which are designed to help people brainstorm and learn about threat modeling, who the adversaries might be, what the adversary targets are, and so on.

Is that related to Control-Alt-Hack?
No, Control-Alt-Hack is a game that we did a couple years ago; the Security Cards are something completely different. We have four suits: Adversary Method, Adversary Motivation, Adversary Resources, and Human Impact. We’ve targeted this for AP computer science courses, so someone who has a very cursory introduction into computer science can get some exposure to security. We’re also targeting industry training as well.

There are many ways of using these cards, one of which is to present people with an example system—maybe it’s something they’re working on in industry, or maybe it’s a concocted system that we’ve created for the purpose of the class. We can now take this system and go through the Adversary Motivation cards based on applicability: What might attackers want to do, and why? We can also look at pairings between cards, so if I pick up the Adversary Motivation card, along with the Human Impact card with personal data, how might these two cards relate to the system that we’re analyzing? If any educators are interested in using this system, contact me—we have a grant and can give them away!

The Silver Bullet Podcast with Gary McGraw is cosponsored by Cigital and this magazine and is syndicated by SearchSecurity.

Gary McGraw is Cigital’s chief technology officer. He’s the author of Software Security: Building Security In (Addison-Wesley 2006) and eight other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.