

Interview

Silver Bullet Speaks to Avi Rubin

BY GARY MCGRAW
Cigital

Avi Rubin is a professor of Computer Science at Johns Hopkins University, where he's the technical director of the Johns Hopkins' Information Security Institute. Professor Rubin is also the Director of the National Science Foundation-funded AC-CURATE Center, which focuses on secure electronic voting. He's also the coauthor of three very popular security books. His newest book, *Brave New Ballot* (Random House, 2006), will be published later this year.

Rubin and our host Gary McGraw recently recorded a podcast that can be heard in its entirety at www.computer.org/security/podcasts/. Their conversation ranged widely, from Avi's most fun (and famous) projects all the way to his favorite breakfast cereal and what he's currently reading. Featured below is an excerpt adapted from the interview.

Gary McGraw: You've done some outstanding work on security and privacy throughout the years—from Crowds [a system for protecting users' anonymity on the World Wide Web] to the RFID hack [which impacted the ExxonMobil Speedpass and common car-based antitheft systems], to critical work in electronic voting. What was the most fun?

Avi Rubin: I'd say that the RFID project was the most fun at the time that we did it, because we were able to actually go to gas stations and buy gas without Speedpasses and start cars. It made a tremendous demo.

McGraw: How long did it take to break the RFID system once your group at Johns Hopkins decided to do it?

Rubin: It took three months, but not a normal three months because once the guys got into it, they started working around the clock on it. They weren't getting much sleep and they were pretty much obsessed. The hardest part was figuring out what cryptographic algorithm was on the Speedpass because it was a proprietary algorithm that Texas Instruments had designed.

McGraw: So you had to reverse that algorithm and then fabricate some hardware?

Rubin: Right. We had pretty much only black-box access to RFIDs, so we got a kit from Texas Instruments (they sold evaluation kits), and we were able to send challenges to the device and get back responses. We were also able to program in a [test] key. We got lucky when one of the guys was at the library and found a high-level diagram of what the algorithm might be like in a Texas Instruments conference presentation. It turned out that the diagram was pretty wrong, but it was close enough so that once we were able to feed in some test keys and run some experiments, we were slowly able to reverse-engineer the entire algorithm.

McGraw: I think there's an important lesson there. Attackers actually

Introducing the Silver Bullet Security Podcast



The *Silver Bullet Security Podcast with Gary McGraw* series debuts with this issue. A complete audio version of the Silver Bullet interviews in podcast form can be found at www.computer.org/security/podcasts/. This series of in-depth interviews with prominent security experts features Gary McGraw as anchor. *IEEE Security & Privacy* magazine will publish excerpts of the 20-minute conversations in article format each issue.

use their resources more than some people let on. People talk about hackers being these guys who do random fuzzing (arbitrarily sending input to Web applications), but it turns out that hackers use libraries, go look stuff up, and understand algorithms better than some people think.

Rubin: That's right. I think that when people make assumptions about attackers—like one of my favorites, “surely no one will try that”—that's where you run into trouble. When you decide how to secure something, you need to know that the attacker might just be a disgruntled former employee. I've seen that happen before. You can't make any assumptions about what the attackers know or don't know, or what they have or don't have.

McGraw: I really like that point. In fact, Dan Geer has an excellent little story that I stole and put in my latest book, which described the ultimate scenario to think about when you're thinking about your own system security. That is, you fire your best engineers after really insulting them, then you throw them out on the street—what can they do to break your system?

Rubin: For most people, the answer is “everything.”

McGraw: One of the things that's interesting about you is that you look like the boy next door, and yet

Rubin: I think that it started out early in my career when I became a security person. I was working at the University of Michigan, where most of the work is funded by the auto industry. The only thing about vehicle research that I found interesting was looking at the proposed automatic toll-collection systems—which now are pretty widespread, but in those days it was just kind of a futuristic idea—and coming up with ways that you could steal from it or drive through without paying. I made kind of a hobby of looking through the designs that were being proposed and saying “Wow, here's how people could cheat.”

My advisor didn't know what to do with me, because I kept trying to break the rules. Finally, he introduced me to Peter Honeyman, who was doing research in security, among other things. We spoke about security and breaking systems. My philosophy is that the best way—and really, I think, the only way—to learn how to make secure systems and design things so that they can withstand attack, is to know how to think like an attacker. You have to actually be an attacker in the white hat sense, where you're not really stealing from people or breaking systems and maliciously causing them to fail, but you're breaking them for pedagogical reasons.

McGraw: Does it worry you that in order to do security properly, you really do need to think like an attacker,

Rubin: Well, I don't think so. I think there are always people that can go wrong, but in an academic setting, the students that I get in my classes at least are much more likely to find themselves in a job where they have to defend against attackers than to actually carry out attacks. That doesn't mean that some of them won't go bad. But it's just like teaching people to use weapons when they're going to school for law enforcement. Yes, one of them could go use that weapon against someone; but more likely, they're going to use that skill and knowledge to protect society.

McGraw: Tell me about some of the fun things that you've done with your classes to help get points across about security and privacy. I know you've done some really fun exercises. What was your favorite?

Rubin: My favorite was the one that I did about a year ago in my class. I like to make the project sort of adversarial—where some groups are competing against the other groups. So I broke them up into groups of four students, and I gave them the assignment of learning from public sources as much as they could about the residents of Baltimore City.

Then, they had to challenge each other in front of the class. So they had to build databases that they could access easily.

McGraw: Are you a resident of Baltimore City?

Rubin: I'm not a resident of Baltimore City. Otherwise, I probably wouldn't have assigned it that way! But it was unbelievable what they were able to come up with. When they were being tested at the end of the semester, I threw out names of people—just people that I knew who lived in Baltimore City—and they could give me their name, their spouse, their income, how much they paid for their house, how many

My philosophy is that the best way to learn how to make secure systems ... is to know how to think like an attacker.
—Avi Rubin

under that mild-mannered exterior lies the mind of a very devious attacker. So the real question is, how did you learn to break things?

even if you're wearing your white hat? Does it worry you to teach kids in a university setting how to be devious and underhanded?

children they had, details about their shopping habits. The groups that did really well all came up with exactly the same number of residents, which was something like 495,000.

McGraw: What do you think the students learned by doing this exercise?

Rubin: I believe the students learned about the exposure of personal information and how little privacy there actually is. They were not permitted to spend money to dig into illegal sources—although several of them told me about offers they had from clerks in government offices to sell them lists of social security numbers. They could only follow legal means using publicly available databases. Of course, real attackers in the real world don't restrict themselves that way.

McGraw: Let's switch gears a little bit. A lot of your work has sort of a political, almost libertarian, bent to it. I'm thinking about things like Crowds, where you're working on peer-to-peer privacy, or your work on electronic voting. Can you work on things like that without being politicized?

Rubin: You know, it's funny that you mention that because it did occur to me, after a while, that that was the case. I've actually never considered myself a particularly politically active person. The Crowds project came up because it was technically interesting and I thought it would be good for society. The problems attract me for their technical reasons—at least that was true until I got into voting.

You know, voting is, by its nature, political. This is the first time in my life that I got really engaged in a project for a public cause. I noticed that the electronic voting machines that were being used across the country were not only insecure, but they weren't re-countable and were rigid (that may be a word that I

About Avi Rubin



Prior to joining Johns Hopkins, Avi Rubin was a research scientist at AT&T Labs. He is also cofounder of a security consulting firm, Independent Security Evaluators. Rubin is an associate editor of *IEEE Transactions on Software Engineering*, associate editor of *ACM Transactions on Internet Technology*, associate editor of *IEEE Security & Privacy*, and an advisory board member of Springer's Information Security and Cryptography Book Series. He also serves on the Darpa Information Science and Technology Study Group. In January 2004, *Baltimore Magazine* named Rubin a Baltimorean of the Year for his work in safeguarding the integrity of our election process. He is also the recipient of the 2004 Electronic Frontiers Foundation Pioneer Award. Rubin has a PhD in computer science and engineering from the University of Michigan.

invented). That is, they could have been rigged by the people that made them with no way to discover that. I became very, very concerned as a citizen, and the role that I've been playing in the electronic voting arena has gone from initially looking at the technical aspects to what could be called activism.

McGraw: Do you hold out hope that electronic voting eventually can be as good as what we have now?

Rubin: I do think there's a lot of hope for electronic voting; and I by no means believe that we shouldn't use computers in our voting process. But it's important for us to realize what computers are good at and when computers can be dangerous. Computers are very good at providing nice interfaces for people, and computers are very good at performing repeatable tasks that can be difficult for humans.

But voting machines and computers consist of a lot of software. Software, as you very well know and as you've pointed out in your books, is something that is definitely guaranteed to have bugs in it. It's going to behave in ways that aren't expected, and if we know that and if we design our systems to tolerate that, then we're going to be okay. We simply can't just throw electronic voting machines that are built like dot-com applications into our

voting booths and expect everything to be okay.

McGraw: So, some assurance work is necessary and probably with the right amount, we can do electronic voting?

Rubin: I do believe so.

More of this interview can be found in audio form at www.computer.org/security/podcasts/.

Gary McGraw is chief technology officer of Cigital. His real-world experience is grounded in years of consulting with major corporations and software producers. McGraw is the coauthor of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), *Java Security* (John Wiley & Sons, 1996), and four other books. His latest book is *Software Security: Building Security In* (Addison-Wesley, 2006). 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.

We welcome your thoughts on this interview or the podcast. Send a letter to Kathy Clark-Fisher at kclark-fisher@computer.org.

You can also discuss this and other topics on our community forum at www.ieee.comunities.org/securityandprivacy/.



\$29

New Lower Subscription Price!

IEEE
SECURITY & PRIVACY

Subscribe to our
magazine today
for only \$29—
our lowest price ever!

You'll receive 6 issues of today's
leading-edge, peer-reviewed
software development information.

Ask us how
you can get this great deal on
IEEE Security & Privacy magazine!

S&P is the premier magazine
for security professionals.
Every issue is packed with
tutorials, best practices, and
expert commentary on:

- attack trends
- cybercrime
- security policies
- mobile and wireless issues
- digital rights management
- and much more.

Subscribe at www.computer.org/services/nonmem/spbnr