Gary McGraw: What on earth got you interested in computer security? Did it have anything to do with what you studied in school?

Adam Shostack: What actually got me started in computer security was Frank Abagnale’s book. I was maybe eight or nine when Catch Me If You Can [Broadway Books, 1980] came out and I was enthralled by the way in which Abagnale gained an understanding of how the financial system worked, where the checks and balances were, where the security policy was implemented, and then how to bypass it. That captured my imagination at a young age.

Gary McGraw: Is that what turned you into an Evil Genius in the first place?

Adam Shostack: I would hate to blame Frank for that. To the other half of your question, I was going to be an environmental scientist.

McGraw: How does that inform your work in computer security?

Shostack: One is the multidisciplinary nature. Environmental science is not biology, it’s not ecology. It’s the intersection of those fields with public policy and economics.

When I was studying how we might clean up air pollution, for example, there were all sorts of lessons in economics, public policy, and public-choice theory that I think apply directly to computer security.

McGraw: That makes a lot of sense. I’m sure you’ve chatted with Dan Geer about his idea of what I call the Security Renaissance—the notion that we have so many people with so many diverse backgrounds that it’s a great time to be in security. [Check out S&P’s May/June 2008 ClearText column to read more about that. —Ed.]

Shostack: Absolutely. I think that a field does better when there’s a plethora of different ideas and different approaches; when you have a diverse toolbox of ways that people have approached problems in the past and ways that you can bring them to bear on the problems that you’re facing.

McGraw: How does your interest in art and literature inform your work?

Shostack: That’s an interesting question, and I’ve thought about this. I’m not sure how to formulate it except perhaps that art can remind us that we’re human or inform on how people interact with each other. A lot of the focus of any good novel has, at its heart, some sort of conflict between two people or multiple people or a person and themselves, and how they think about that and how they resolve that.

At the end of the day, as security professionals, it’s easy to talk about technology. But we’re doing this because of the impact that security issues or a lack of security or that good security have on people and the way they interact with the world.

McGraw: I think there’s some aspect of analogy and metaphor in art that can help inform our work as well. Your answer, “I’m not sure how to explain it but” captures it.

At RSA this year, I bought a copy of your book [The New School of Information Security, Addison-Wesley, 2008] for its cover, which features a print from Kandinsky in his less formal musical phase. I planned to give your book to a friend who’s a Kandinsky fan. I started reading it on the way to delivering it and I found out it’s really very interesting.
Tell us briefly about *The New School*. What’s the basic idea behind the book?

**Shostack:** There are three big ideas in the book. The first big idea is that there’s this conversation which has moved away from technology. When you and I were getting started in security—actually, I’m not sure this is when you got started—but I remember reading the work you did with people like Ed Felten and attacking Java.

**McGraw:** That was back in 1995 when I got started.

**Shostack:** I did some work and I attacked the Security Dynamic Secure ID protocol and the way that went back and forth. We were very technology-focused. As we’ve solved some of the technology problems, we’ve gotten to a point where the interesting problems are more related to human beings and the way that they intersect with the technology rather than the technology itself.

**McGraw:** That’s true of software, too.

**Shostack:** I hate to speak about something as broadly as software, but I think the interesting thing in software is how it intersects with a business process.

**McGraw:** Exactly.

**Shostack:** The second big idea that we present in *The New School* is that if we’re going to succeed, we need to actually test our ideas about what it is we should do. It’s not enough to say, “I am a smart guy or you are a smart guy and therefore you will come up with the right answer of how to address this problem.” We need to be able to, like scientists, test our ideas and understand whether or not they’re actually having the impact that we’d like them to have. We need to be able to test our processes and say for example, “If you’d like to deploy a security awareness program, does it actually change people’s behavior at the end of the day if that’s its goal?”

**McGraw:** Right. A little bit of empiricism.

**Shostack:** A little bit of empiricism. Then the third big idea is that we don’t actually have the data that we need to test our ideas because we’re very afraid to talk about things that go wrong. And in being unwilling to discuss what goes wrong, we find ourselves making similar mistakes over and over again. So *The New School* is really this idea that we need to discuss what’s happening, be willing to discuss our successes and our failures, and analyze what we’re doing in such a way that can advance the science and the state of the art.

**McGraw:** You harken back to the ’90s. Back then, security research in the scientific literature, which is peer reviewed and empirical (theoretically), really changed radically in my view. I was there to witness this and to participate on the Java security front as you mentioned. I think that the change in the research community was fundamental and pretty permanent. I wonder if you agree with that and whether *The New School* is a continuation of that process that started in the research community and is now getting wider and spreading into commercial security.

**Shostack:** Could you say a little bit more about how you perceive that change?

**McGraw:** Absolutely. For example, when I got started in ’95, I was reading papers about multilevel security, database security, and reviewing the transactions of what was going on at Security and Privacy in Oakland [IEEE Symposium on Security and Privacy, or the Oakland Conference].

Then we wrote a paper about software fault injection that was about how to break stuff. The committee had a really hard time with that paper because it was breaking something.

The same thing with the Hot Java paper [“Java Security: From HotJava to Netscape and Beyond,” www.cs.princeton.edu/sip/pub/secure96.html] that Felten wrote with Dan Wallach and Drew Dean, which was really about a new technology and how it was broken. For a while, there was a kind of repositioning around the scientific literature about how you talk about how to build things and how you talk about how to break things. It became much more empirical and a little bit less about spook systems that people had been working on in cryptography.

**Shostack:** I think there’s still valu
We’ve gotten to a point where the interesting problems are more related to human beings and the way that they intersect with the technology rather than the technology itself. — Adam Shostack

Understanding these things is great, and I think that the empiricism is the growing awareness that we needed to actually test these systems. It wasn’t sufficient to say, “I’m going to prove that this system has this property.” You have to say, “As the system is moved from a description of an algorithm to an implementation, does it retain the properties that you think it retains?”

Then, does it actually deliver in the real world the properties that the customers want? Or that the customers should want?

McGraw: My feeling is that that exact thing happened in the mid-’90s but only in the scientific community. Now, The New School is a reflection of the widening of that kind of wave.

Shostack: I think some of it happened in the scientific research community, some of it happened in the applied, hands-on research community. One of the interesting things which has grown out of that is the beginning of a taxonomic effort to analyze the ways in which attacks actually succeed. That we can talk about stack smash attacks, heap overflows, and integer overflows is a result of a growing corpus of examples.

If you think back to the way The Royal Society [UK’s academy of science] started out, they were collecting all sorts of bizarre things. They were trying to expand the scope of the universe that they could look at so they could say, “Here’s a duck-billed platypus, what the heck is that?”

McGraw: We still aren’t sure what the heck it is. I read the other day about scientists trying to sequence those genes and find out what it is.

Shostack: Yes, the reductionist analysis, and I don’t mean to slam gene sequencing in any way. It’s brilliant, it’s wonderful, it’s useful. But just knowing what those genes are isn’t enough to understand how it all comes together and what the heck this duck-billed platypus is.

McGraw: Magazines such as IEEE Security & Privacy try to make security science of the sort that you’re describing practical and useful. I’m wondering what role magazines have in The New School. Have you thought about the role a magazine like S&P plays versus a trade magazine?

Shostack: I haven’t thought incredibly deeply about what role IEEE S&P should play. But my feeling is that there’s tremendous room for analysis of the data that we have and there’s a tremendous amount of room through the choice of editorials and the choice of news to help shape the way people perceive what’s going on.

One of the examples I’ve been coming back to a lot recently is what happened to Tylenol in the 1980s. Someone put cyanide in their capsules, people died. The makers of Tylenol took on that problem, they engaged with the public, and the company is still in business even though no one was ever caught or prosecuted for the crime.

The problem which they [the makers of Tylenol] experienced—and I don’t mean to say this in a way which diminishes the very real pain people experience when their systems are broken into—but most computer security incidents don’t actually lead to death.

McGraw: You can conceive of ways in which they could, but most of them haven’t happened.

Shostack: Most of them have not happened and if Tylenol is able to spring back—actually it’s used as a case study in crisis management now—should we really be so unwilling to discuss the things that are going wrong for us today?

McGraw: That’s a good example. Here’s an easy one, but it’s also a deep question. Why do you think that The New School is radical? Why is it new?

Shostack: Why is it new? Before I say why it’s new, I want to make clear that when we talk about The New School of Information Security, what we’re doing is capturing and trying to help shape some conversations that are going on in the field. I look to the workshop on Economics and Information Security as a prime example of this.


Shostack: We’re applying economics and Bruce Schneier has talked about psychology and there’s this trend towards empiricism. And what we’re trying to do with The New School is not to claim inventorship over all of this; but we’re trying to pull forward these possibly disparate threads and turn them into, if you will, a tapestry and say, “If you take the
empiarism and if you take the willingness to draw on other sciences and the need for a diverse toolbox, then what you get is not the sum of its parts but you get something that's greater.”

**McGraw:** So one of the key tenets of The New School is to get good data and analyze it. You use the CardSystems breach in which about 40 million card numbers were compromised as an example in several places. I thought it might be good to use that to turn our attention to regulation.

Though CardSystems complains that they “followed Visa rules to the letter,” they were still compromised. Isn’t the problem a focus on the letter of PCI versus the spirit of PCI?

**Shostack:** I actually don’t believe it is. Let’s say you or I were advising CardSystems. We would start out by saying, “Comply with the PCI requirements because you have to by contract.” Then they say, “Well, what else should we do?” You might have some advice; we might even agree on some of this advice—that they should engage in a program to analyze the security of their source code of the custom software which they’re building.

**McGraw:** The spirit in this case would be the notion of wanting to protect customer data because it’s the right thing to do. Their customers expect it.

**Shostack:** Where I’d like to go is the question of—no one has infinite resources—so how do you allocate your resources most effectively?

I don’t believe that we have a defensible answer. We could sit down and argue at great length anything you would like to propose, but I could find a way to undercut because neither of us has data that shows 100 organizations did X and 100 organizations didn’t do X, and the ones that did X suffered 96 percent less break-ins.

**McGraw:** It’s kind of like psychology before statistics.

**Shostack:** Yes. When you asked what CardSystems should have done differently, it’s very easy to exhort and suggest that they should have done more. But it’s very difficult to justify the spending on what more they should have done and select what it is that they should have done. I think that raises a real dilemma for a regulator who might want to exhort people to do more and to spend more. The regulator also wants an efficient market in which people invest their money well. And saying that you should invest your money in, say, application firewalls or security awareness training or password change policies. How do the organizations which have these things compare to the ones that don’t? Without an answer to that, when you sit down and say, “Let’s put more regulation in place,” I want to say, “Well hang on.”

**McGraw:** I tend to agree with that. I’m just trying to understand whether it’s even possible to try to capture spirit in a simple regulation which seems to always devolve to letter very quickly.

**Shostack:** I think that it may be possible to capture the spirit. I think it may be easier—and I’m not an accountant—but I’ll go out on a limb here. We used to have a relatively simple set of accounting principles and the goal of the accounting principles was to provide high-level guidance to ensure that someone reading the accounts of an organization could understand its financial position.

As we tried to become more prescriptive to address the ways in which people have done bad things, the ability to understand accounting principles becomes harder.

**McGraw:** Right, so we get principles versus particular prescriptive guidance. But then we still end up with Enron.

**Shostack:** Well, we do. And even surgeons make mistakes. There are awful stories of instruments left in people, or a few years ago, someone had the wrong leg amputated. It’s easy to pass a law that prohibits another Enron. Just forbid Ken Lay from becoming CEO again and you don’t have another Enron. You might have something very similar, so you look to the accounting practices or you look to the way in which the company operated. But at the end of the day, I believe that what happened with Enron was that people chose to commit a fraud. And then they did it and that’s already illegal.

**McGraw:** I wanted to ask you a couple of questions about software security before we run out of time. You spent some time in software security when you were at Reflective, and in your role at Microsoft you do that, too. What do you think of the SANS idea of certifying developers as secure coders?

**Shostack:** I think it’s an interesting idea and the empiricist in me would love to actually see what happens when an organization which has certified its developers compares itself to an organization which is investing its money in other ways.

**McGraw:** Oh, that’d be super. I’d like to see that, too.

**Shostack:** For example, at Microsoft, we don’t have certification...
or tests, but we do have a process that all of the code goes through. So rather than focusing on the developer, we focus on the output, which is better. My personal opinion is that focusing on the output is a good idea. I’m glad that we’re seeing experimentation and I hope we’ll get interesting data.

McGraw: That’s a good answer. In your book, you also eviscerate the term “best practice,” which I think is hilarious. I’m not sure what we should call whatever those things are. What are the things that everybody agrees we should do for software security if you stand back from the Touchpoints and SDL [Secure Development Lifecycle] and CLASP [Comprehensive, Lightweight Application Security Process]. Don’t you think there are some things we all sort of agree on?

Shostack: I do, and I think there’s a set of things which we might call received wisdom or we might call evolved practice. We might even call it best practice. My trouble with the term “best practice” is that it means so many different things and it’s such an easy label to apply to something.

McGraw: It’s probably the “best” part that you don’t like.

Shostack: It’s the lack of testability. I think of back-ups as a great best practice. There are definitely things which are simply so sensible and so reasonable that they are best practices and if you’re not doing them, there’s a question.

Then there’s a tremendous set of things that people have put the best practices label on which I don’t think qualify and I don’t think people often enough challenge the assertion that this is really a best practice; that it’s really been through that testing and honing and validation.

McGraw: Well, maybe you guys can help with some data from the SDL results.

Shostack: That’s possible. There’s some difficulty in doing that because even between different teams you have different practices. I’ll give you a personal example of just one of my current challenges in gathering data: someone came and said, “I’m trying to threat model this component.” We went back and forth through email a couple of times, we analyzed the problem a little bit, and they went out and they had a decent threat model at the end of all of that. How do I capture data about the fact that their initial design had some issues?

I want people to go ahead and fix their designs more than I want to spend the energy to capture the data. Again, it becomes where do you put your resources and where do you put your energy?

McGraw: Yes. We have a ways to go in our field.

Shostack: I’d prefer they get the thing fixed and not have as much data because that’s the right result.

McGraw: You’re going to get kicked out of the new school.

Shostack: No, no. I can go to the end of the process and count design issues that make it all the way to the end. I just can’t do the precision measurement at the beginning.

McGraw: One last question, kind of front left field. It appears that you like Infinite Jest [David Foster Wallace, 1996] way more than The Crying of Lot 49 [Thomas Pynchon, 1966]. What are you, nuts?

Shostack: I think Infinite Jest should be a hacker classic.

McGraw: You just like it because it was about your neighborhood.

Shostack: Well, there is the bizarre coincidence that I lived in Cambridge, Mass., where a good chunk of it is set and then moved from there to Montreal. But really I like it because it’s recursive in so many different dimensions. It’s recursive in that the book is infinitely long and is a joke about an infinitely long set of jokes. I like the recursive footnoting and the way the footnotes refer to one another within the novel.

McGraw: I still like the little trumpet from The Crying of Lot 49.

Shostack: I’m confused as to why you think I didn’t like The Crying of Lot 49.

McGraw: I just get to throw these questions out so I can make false accusations and then that’s the last word.

Shostack: Aha. Well, all right. Well, thank you.

You can find additional podcasts in the series, including those featuring Gunnar Peterson and Chris Wysopal, at www.computer.org/security/podcasts or www.cigital.com/silverbullet.

Gary McGraw is Cigital’s chief technology officer. His real-world experience is grounded in years of consulting with major corporations and software producers. McGraw is the author of Exploiting Online Games (Addison-Wesley, 2007), Software Security: Building Security In (Addison-Wesley, 2006), and Exploiting Software (Addison-Wesley, 2004). McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. He is a member of the IEEE Computer Society Board of Governors. Contact him at gem@cigital.com.
New Lower Subscription Price!

$29

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 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!

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