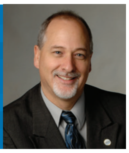

Bruce Schneier: The Security Mindset

Charles Severance, University of Michigan

Security guru Bruce Schneier talks about what it takes to think like a security expert.

Networked technology increasingly touches all aspects of our lives. When essential systems are connected to a networked environment, it becomes important to make sure that they're protected from attack. We continue improving the mathematics and algorithms used to secure these systems, but attackers tend to exploit weaknesses in how the mathematics and technologies are used.

As effective security becomes more vital, many computer science students are becoming interested in making security part of their education. I talked to Bruce Schneier, a leading cybersecurity thinker, and asked him how students might prepare themselves for a career in this field. See the entire interview at www.computer.org/computingconversations.

See **www.computer.org/computer-multimedia** for multimedia content related to this article.

WHY STUDY SECURITY?

In some ways, the security field is different from other traditional areas of computer science like hardware, compilers, or OSs:

> *I think computer security is the most exciting part of computing right now, because it has something that nothing else has: an adversary relationship between the parties. When you do graphics or operating systems or anything else, there's no one trying to thwart you at every turn. That's what you have in security, and that's what makes it exciting and interesting. Security involves psychology, economics, computing, law, policy, and so many other things. It's a constantly evolving arms race between attacker and defender.*

In many other areas of computer science, we're iteratively improving something, such as the algorithms that power databases. We gain new understanding of the underlying problems and then improve our solutions to the problems. But because the "underlying problems" in security are often creative, highly motivated human adversaries, there are always surprising new twists and turns. We simply can't know in advance what skills we'll need to succeed as security professionals:

> *Security is a mindset. It's a way of thinking about the world. Think about the definition of "hacker." A hacker is someone who cobbles stuff together and makes it work. You could hack a tool that works one way, and add some other piece to it, and suddenly it does something else—maybe something it wasn't intended to do.*

Those with the intent to break security don't follow rules; they don't stay in a well-defined box. We can't just tell folks to behave.

> *If I'm the hacker, I get to attack whenever I want. I get to do it at the most inopportune time [for you]. I get to do it in a way that makes your system fail as badly as possible. And you have to think about security that way. Not about how to build something and make it work, but how to make it fail in precisely the right way to do precisely the right sort of damage.*

To get into the security mindset is to try to understand the unexpected directions from which attacks might come:

> *I remember a class in security where one of the assignments was to come in the next day and write down the first hundred digits of pi. There are two aspects to this test. First, you can't memorize a hundred digits of pi overnight, so you had to cheat. Second, if the students were caught cheating, they would fail. Students were forced to think outside the box and explore the security mindset.*

The security mindset isn't something that can be taught directly. There's no "principles of the security mindset" section in a textbook that we can all learn and then apply to become security experts. But a security expert must understand many different topic areas, because adversaries are looking for any way to break into systems:

> *I'm often asked, "Should I study forensics or cryptography or network security or protocols or embedded devices or SCADA systems?" Study what you want. Follow whatever interests you, because what you're really learning is how to think like a security expert. Honestly, if you get a job where you're securing VPNs, you can easily pick up how VPNs work. The hard part is how to think about security, and not the technical details of the problem.*

Students interested in a career in security need to expose themselves to open-ended challenges to develop the security mindset:

> *A lot of hacker conferences have Capture the Flag contests [where participants] build their own private network to cut down on both network latency and federal law violations. You're going to learn a lot by breaking other people's systems. And that's probably going to involve illegal activity. We have this clash between the technology imperative and what society wants. You can go in and try to hack your own smartphone or computer and there's a lot of stuff you can learn. But it's going to be more fun if you can hack somebody else's phone or computer. I prefer things to be open ended.*

Over the years, Schneier has written many books that explain security concepts and issues to a nontechnical audience including *Secrets and Lies: Digital Security in a Networked World* (Wiley, 2000) and *Liars and Outliers: Enabling the Trust that Society Needs to Thrive* (Wiley, 2012). His most recent book is about surveillance and data:

> *My latest book is called* Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World *[W.W. Norton, 2015]. It discusses what's going on in the world of surveillance and how we can regain security. All of my books are general interest, for those who want to learn more about the topic. I always hope my books spark different interests in different directions. They're going to give people ideas that they research further. That's how you get your passion; that's how you get your calling.*

The good news for students who aspire to join the security field is that demand is growing for people with expertise in this area. Although it's important for a student to master core skills in computer science, those skills must be placed in the context of a security mindset. Because this takes a long time to develop, and draws from many diverse areas of study, students can think of their entire education as preparation for a career in security. C

CHARLES SEVERANCE is a clinical associate professor and teaches in the School of Information at the University of Michigan, and is *Computer*'s multimedia editor. Follow him on Twitter @drchuck or contact him at csev@umich.edu.