Silver Bullet Talks with Becky Bace

Gary McGraw
Cigital

Becky Bace, one of the luminaries of computer security, grew up in Birmingham, Alabama. She spent 12 years at the US National Security Agency (NSA), where her work focused on intrusion detection and cryptography. Currently, Bace is a venture consultant with the venture capital firm Trident Capital in Palo Alto, California.

Featured here is an excerpt adapted from the full interview between Bace and Silver Bullet host Gary McGraw. Their conversation ranged widely, from explosives to vulnerability disclosure to venture capital. You can listen to the podcast in its entirety at www.computer.org/security/podcast/ or www.cigital.com/silverbullet, and you can subscribe to the series on iTunes.

Gary McGraw: I'm always pleased to come across security gurus who grew up in the country. Did your experiences as a girl blowing up tree stumps with ammonium nitrate have any impact on your choice of computer security as a career?

Becky Bace: Aside from fostering a sense of enjoying the perverse, I suspect it probably did. Actually, I think there's an aspect of security that marks the evolution of folks who end up in security in that, at some point, you're interested in how things fail. Obviously, explosives push that envelope.

McGraw: They help things fail more quickly. It's funny—you and I know a lot of people in computer security who are into explosives and firearms and stuff like that.

Bace: Well, it's fun. I remember chatting with folks when I first got involved in security in the mid to late '80s. It seemed that most of them had an almost orderly progression into information security: they were ham radio operators early on, got enchanted with the whole notion of coding, and developed an avid interest in picking locks.

We were far enough out in the woods and far enough removed from the ham radio operators that aside from the occasional keying, I didn't really get enchanted with that. But I did love to pick locks. It was part of that set of interests.

McGraw: The other thing that got you started was being sent to college by the teamsters.

Bace: Originally, I went to the University of Alabama in Birmingham, and that was sort of a hurry-up situation. I came from rather humble means—large family, single-wage earner—and it wasn't particularly clear that I would go to college immediately. It looked as if I was going to take a year or two off and work to afford tuition. Lo and behold, not only the teamsters, but also General Mills, of all people, anteed up scholarships at the last minute, which allowed me to go to college.

McGraw: Where you discovered math, and that's all she wrote.

Bace: Absolutely. I went in believing that I was going to do something reasonably nailed-down compared to computer security. I was actually going to be a medical records administrator and got waylaid on the way.

I remember going into the guidance counselor, and the guy telling me that it's the first time in his career that he's ever encountered anyone coming through the door saying, "I want to sign up for a major that requires more math, not less."

McGraw: Back then, I bet that if you wanted to study things like computer security and cryptography, you had to do math, and there probably wasn't much offered in terms of courses about computer security.

Bace: No, at that point, there was no such thing as a computer major, let alone a computer security major.

McGraw: You played a pivotal role in the apprehension of Kevin Mitnick. What was that like?

Bace: It was insane, purely insane. I

About Becky Bace

Becky Bace spent 12 years at the US National Security Agency (NSA), where she created the Computer Misuse and Anomaly Detection (CMAD) research program. For her achievement, Bace received the NSA's Distinguished Leadership Award. She then served as the deputy security officer of the computing division at Los Alamos National Laboratory. Currently, she's the chief executive officer (CEO) of Infidel, a network security consulting firm, and a venture consultant for Trident Capital.

Bace is the author of *Intrusion Detection* (MacMillan, 2000) and coauthor of *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness* (Addison-Wesley, 2002). She has an MS in engineering with a concentration on digital systems engineering from Loyola College in Baltimore, Maryland.

was in a situation where I knew a fair amount about the domain—about the investigative capabilities of all the parties involved—and had a sense of what an actual, successful apprehension represented in terms of a very convincing proof of concept.

I think, to a degree, people believed that the folks who alleged that hackers were actually getting into these major systems were in some way delusional or victims of their own wishful thinking. At the same time, I think there were folks who believed that a lot of the curative measures and the investigative measures and so forth were also similarly fluff. I thought it was interesting and emblematic of a point in which folks got to demonstrate that, yes, bad things were going on, victims were compelled to come forward and characterize the nature of the problems that they had, and we were able to demonstrate that some of the things that were put forth as potential ways of apprehending someone actually worked.

McGraw: The rubber meeting the road, so to speak.

Bace: Absolutely. Up to that point, there was a great deal of violent debate as to whether the trace back and capture were doable.

McGraw: What do you think about Mitnick's budding career as a consultant?

Bace: Hey, as long as he stays on the straight and narrow—as far as I can recall, he got a sentence. He served it. If the courts say that they're fine with that, then I'm fine with that.

McGraw: Do you have strong feelings about the glorification of hackers in computer security?

Bace: I think they are always going to be part of an almost elicit pleasure in the same way that I'll probably continue to read spy thrillers even though I may not advocate someone spying on me or some entity I care about.

McGraw: It's kind of nice as observed from a distance?

Bace: Yes, absolutely. It's intriguing—it represents a convergence of a human subversive pleasure and a little bit of intellectual tickle as well.

McGraw: I think that's right. In fact, I think that black hats, to some extent, have a very important role to play in computer security—not necessarily as carried out by criminals—but certainly as part of assurance activities while you're taking a look at a system that's been stood up. What's your opinion about those kinds of activities? Should we describe and write about attacks?

Bace: I think so. It doesn't make any sense to attempt to constrain that information. I've never found the constraining of that information by design to actually work. I think it virtually eliminates those in a position to put forth the functional protection from entering into the fray.

It was only when we got to a point where people were comfortable with wading knee-deep into the morass of vulnerabilities that we were able to actually isolate patterns.

McGraw: When I first got started in computer security, the research guys were still hoarding vulnerability information as if it were too radioactive to talk about and too secret to share. I found that very disconcerting because I wanted to study the stuff. What were we supposed to study? Were we supposed to just sit around and contemplate theories?

Bace: Well, I find it sort of entertaining that they talked about real hacks while the vast majority of them were actually quite good hackers themselves, much more elegant than most anything you and I see on the street these days.

They also had a great deal of decorum built around their practice of discussing these [hacks] with each other. You would get knowing looks. I think you see the same sort of dynamic when you have cryppies [cryptologists] talking about various fundamental problems in crypto.

McGraw: It's just a club, really. It involves knowing the vocabulary and proving your stripes and all that jazz.

Bace: It is, and I think that that dynamic remains in security. Frankly, I think it's healthy for security. There is a guild sort of feel, at least among security practitioners on the commercial side. I think that's something that I would not be necessarily happy to see set aside.

McGraw: We have an awful lot to learn from each other in terms of sharing information about events that are going on or possible vulnerabilities or even best practices when it comes to things like software security—there's still a ton of sharing that needs to go on.

> **…there's an aspect of security that marks the evolution of folks who end up in security in that, at some point, you're interested in how things fail.**

Bace: One interesting note is that divulging attack information in general forced us to get a lot crisper about our characterization of vulnerabilities. At the same time, I think that perhaps there's a bit of tension—a bit of friction—involved in differentiating attacks or attack information and publishing attacks versus publishing the vulnerabilities that perhaps enable those attacks.

McGraw: It's hard to do one without the other sometimes. Another way of putting it is when you do one, you sort of by caveat do the other. As a discipline, in terms of managing the knowledge that we have, we do an okay job as a collective with our myths and stories, but we don't do a very good job as academicians writing it down in a way that other people could use if they aren't part of the club.

Bace: Being able to lay things down in stone is really important in a couple of specific areas that I deal with daily on the commercial side. The first of those is actually pushing the whole discipline forward. It makes a difference between me being able to educate someone over a four- or six-year academic program—

McGraw: As opposed to being an apprentice?

Bace: Yes. I think this becomes absolutely critical with the advent of things of value residing on computer systems and with legal remedies.

I do a lot of business right now in the legal realm, in particular for things like intellectual property. And that's actually what forced me to get real about the practice of security.

McGraw: I have to mention that I broke my leg, and I'm on Percocet, which makes my questions particularly ridiculous. I was talking with Becky before we started and she said that when she was taking Vicodin for a problem that she had, it ended up making her write book proposals. I suppose one of those was for *A Guide to Forensic Testimony* [with Fred Smith, Addison-Wesley, 2002]?

Bace: Oh, absolutely. It's come to be a morbid joke. The first time this happened was by sheer coincidence. I was trying to decide whether to write my first book [*Intrusion Detection*, MacMillan, 2000] and was suffering a great paralytic angst. I had an abscessed tooth, and the endodontist couldn't get to it for a couple of days. They gave me a fair snoot full of Vicodin, and to my great surprise, I absolutely, positively had to get that proposal out. Wrote it all out, sent it in, and the next morning woke up and went, "Oh, my God."

I called up the editor, and the editor said, "That was perfect. That was absolutely brilliant. Of course we're going to do this book." On the second one, I ironically developed a second abscessed tooth when Fred and I were muddling through the proposal.

McGraw: Switching gears, you've had a big interest in women's issues over the years and are especially active in creating opportunities for women in computer security. Are there any organizations that you think are doing advocacy work for women in the field?

Bace: We have one group that I love. I've worked with Joyce Brocaglia at Alta Associates on the Executive Women's Forum [www.infosecuritywomen.com], and it's turned out to be just a fabulous organization. We're close to 200 women now—all are director level or above, on all sides of the aisle. We have some academics, some commercial solution providers, as well as commercial computer information security officers, security officers, risk officers, and privacy officers.

McGraw: What exactly do you do all day as a VC [venture capitalist]?

Bace: I'm not a VC per se; I am a venture consultant for a venture capital firm. Venture capitalists are basically investors. They're effectively folks who function as a commercial bank might, except that they do things that by nature are higher risk, hopefully for a higher return. So far, we've been fortunate with Trident. And really good VCs—this was sort of a revelation to me—don't sit around like Simon Legree [Ed. note: Legree is a fictional plantation owner in American literature] and cackle wildly at the thought of impoverishing poor technical entrepreneurs. They spend a lot of time and energy exploring the nature of evolving markets and also exercise a fair amount of resource and guidance for entrepreneurs. In the best of cases, a good VC is one who studies the area, knows the market cold, does a good job of identifying fast-evolving markets, and then identifies the movers and shakers in those markets.

McGraw: One last completely unrelated question. What kind of music do you listen to?

Bace: Oh, goodness gracious—a total mishmash. For Christmas, I usually play Santa Claus for my two preteen nephews—who are a trip and one of the joys of my life. So this year, I was Santa Claus, and we bought iPods. Just for jollies, I threw my library onto their iPods as a starting point, and one of them—the younger one—came to me and confessed that he's so thrilled because I had Tony Bennett and Frank Sinatra. The other one came to me and was thrilled because I had a rather edgy group out of San Francisco called The Kinsey Sicks, who do very satirical, very gay humor, and Garrison Keillor's *A Prairie Home Companion* [radio variety show]. Apparently, both of them found what they liked.

McGraw: Do you have a favorite that you're listening to now?

Bace: Oh, heavens—nothing in particular. I do an alarming amount of Frank Sinatra as far as I'm concerned, seeing it as an impending sign of age.

You can find additional podcasts in the series, including those featuring Ross Anderson or Bruce Schneier, at www.computer.org/security/podcasts or www.cigital.com/silverbullet/. □

***Gary McGraw** is chief technology officer of Cigital. His real-world experience is grounded in years of consulting with major corporation and software producers. McGraw is the author of* Software Security: Building Security In *(Addison-Wesley, 2006),* Exploiting Software *(Addison-Wesley, 2004),* Building Secure Software *(Addison-Wesley, 2001), and five 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. He is a member of the IEEE Computer Society Board of Governors. Contact him at gem@cigital.com.*