Editor: Gary McGraw, gem@cigital.com

Silver Bullet Talks with Deborah Frincke

Gary McGraw | Cigital

Hear the full podcast at www.computer.org/silverbullet. Show links, notes, and an online discussion can be found at www.cigital.com/silverbullet.

Deborah Frincke is currently a member of the Defense Intelligence Senior Executive Service and deputy director for research at the National Security Agency (NSA). This interview was conducted while she served as Chief Scientist of Cybersecurity at the Department of Energy's Pacific Northwest National Laboratory (PNNL). Prior to PNNL, she was a professor at the University of Idaho, where she cofounded the academic Center for Secure and Dependable Systems and also TriGeo Network Security. Frincke is active in the US Department of Energy's cybersecurity grassroots community and an affiliated professor with the University of Washington's iSchool.

You've worked as a professor, an entrepreneur, and a researcher. What are the similarities and differences between those three professions, and which do you like the most?

"Which do you like the most?" is a hard question. I think the similarity is that it helps to be entrepreneurial in all three. If you wait for someone to tell you what to do, you won't have any fun in any role.

What about the differences between, say, being a professor and being a researcher?

Being a professor, the main goal that I had was to educate students, and after that, to make scientific discoveries. At the University of Idaho, I wanted to help the next generation of researchers learn what was next, so my emphasis was more on what they were able to uncover as opposed to what I was able to do. What I found moving over to Pacific Northwest National Lab was that science was a business, so the emphasis had to be on utility as well as on science [for its own sake], which makes a difference in the kinds of problems that you approach and the way you go about approaching them.

What have you learned about what it takes to do a startup?

Doing a startup is hard. I think what I learned is that it takes a great deal of focus on who is going to use your stuff, who is going to pay for it, and how to get people to realize that they want it. Again, that's not something you normally think about as a professor, so we didn't really get much traction until we brought in people who were very good at the business and marketing end, who knew how to phrase what we were doing instead of emphasizing how wonderful this research is for science, emphasizing how much of an improvement it would make in the daily life of somebody else who would be willing to pay for it.

Much government cybersecurity information is classified, sometimes for no apparent reason. In your view, is classification used to mask incompetence in cybersecurity, or do some things really need to be classified?

For me, much of what's classified has to do with methods and methodologies. I'm not certain that I've seen it used to mask incompetence, but I wouldn't necessarily be looking at any program that would have that as an issue. At least let's hope I would recognize it if I saw it! When I see things classified, it really does have more to do with some kind of

About Deborah Frincke

Deborah Frincke is currently a member of the Defense Intelligence Senior Executive Service and deputy director for research at the National Security Agency. This interview was conducted while she served as Chief Scientist of Cybersecurity at the Department of Energy's Pacific Northwest National Laboratory (PNNL). Prior to PNNL, she was a professor at the University of Idaho, where she cofounded the academic Center for Secure and Dependable Systems and also TriGeo Network Security. Frincke is active in the US Department of Energy's cybersecurity grassroots community and an affiliated professor with the University of Washington's iSchool. She works on intrusion detection, system defenses, and collaboration and distributed systems. Frincke lives in Idaho, where she oversees a forest full of daffodils with her husband. She has a PhD in computer science/security from the University of California, Davis. Contact her at dafrinc at nsa dot gov.

a method that's being kept secret or some particular thing that if it were released would endanger our specific system.

That makes sense. I just worry that science and classification seem to work at cross purposes. I know we have to have some secrets, but the whole idea behind science is to be peer reviewed and to have people criticize your work and try to fix it.

Exactly, and I've actually been on a bit of a crusade about that. What I've noticed is that people do a little less publishing on the classified side than I'd like to see. There are some things where if a person put in that extra mile, he or she could do more in publishing. Now, that's not to say that the work as is couldn't go forward, but with a little extra effort, you can sanitize. A few of us are trying to find some way of having a classified journal or a peer-reviewed publication that comes out regularly in the government cybersecurity community, so that it can enjoy the advantage of peer review.

The US Department of Energy should be all over smart-grid cybersecurity implications, but I worry that it's not. Who's in charge of that? Who's supposed to be watching the smart grid from a security perspective?

Smart grid is one of those things that's going to challenge us as a culture, and I'm saying that because much of what's going to go on in smart grid is owned by industry. Smart grid illustrates better than almost anything I know the tie that has to happen in an industry-owned infrastructure that's benefiting the public. Citizens and government need to keep the infrastructure safe.

But what I see is this big push to basically hang a naked PC off of everybody's house, which has a whole bunch of incredibly cool things that can happen as a result but also, from a security perspective, is problematic.

It is. I think that this is a little bit like the iPods we're all hanging nakedly off of our PCs right now, except the implications of misusing them are a little bit greater.

We have a lot of work to do there, but in the interest of making a big impact in the efficiency of energy distribution in going from one to one to many. I don't know how to explain it exactly, but we're making some tradeoffs when we do that.

Yes, and I really think that we do need to focus on that. Now, there are some bright spots: I like what I'm seeing in TCIPG [http://tcipg.org/resources], the study of infrastructures that it did. I really like seeing the new NETL program coming out of the Department of Energy, which is investing in some long-term thinking about cybersecurity structures [www.netl.doe.gov/about/index.html]. Part of the problem we've got is that in some cases with smart grid, the train has already left the station. We're working right now on smart-grid meters that are intended to meet today's needs, so we aren't projecting into the future. It could be 10 years before we can make use of a new technology we invest in today.

And some of the things that we're hanging off of houses today you can order off eBay, which is what some of hackers have done—decompiling the code, finding buffer overflows, and rooting the boxes.

Yes, and given that I live in a rural environment, we're even generating some of our own energy, and we can sell it back to the grid. I do a lot with solar; we use some geothermal to heat the house, and our meter is read by us and phoned in, so we'll want to think about that model. It's a little different than the city reading the meter.

Next, a question about your research. The "fog of war" is a well-known situational awareness challenge, and in my view, cyberwar will add a dimension of speed, fast-forwarding things like we've never seen before. How does your situational awareness work in network security deal with the issue of speed?

Speed is probably the second greatest challenge in the next generation

of war. The first is where it's being fought, which is essentially in the living rooms and the smart devices we have in our homes. For speed, there are a couple of challenges, and one approach that we're working on is how to be as proactive and predictive as possible.

You're actually looking at multiple futures when you're doing prediction. Coupling that with some form of resilience so that when your guess is wrong, as it inevitably is, you have some way of riding the situation out. The human involvement is going to need to be from the big picture view, taking a look at what the broad scheme of things is and trying to set up goals and directives as opposed to being hands-on management.

At human-level speed.

Exactly. Human level compared with Internet speed and real-time speed is an entirely different way of dealing with warfare.

We're dealing with that in trading systems as well, with the market crash that was caused by super-fast trading systems—this is something that most people who built these markets didn't anticipate. We're definitely going to see it in cyberwar as well.

The more you look, the more you see it. Think of autopilots and airlines, where sometimes the autopilot saves a plane from a crash, and other times the autopilot makes exactly the wrong move. We're going to see the same thing in cyberwarfare.

Clearly we need more people with a computer security clue in this country and in our government, so how can we address that need?

Of course, as an academician, I'd love to see a lot more of this taught in our institutions, and by that, I don't mean necessarily just at the college level. I think we need a lot more going on at K through 12, just helping people be digitally savvy and look both ways before they cross the cyber street. If our kids are a bit more understanding of some of the tradeoffs, they'll make better adults and more informed citizens. But, in the meantime, we've got a major problem in that most of the people who run things at the government level, of course, didn't come up with a technology background, and they're learning about it, and the devices are evolving underneath them. So, outreach from people that understand—people like ourselves—is going to be absolutely critical. I'm very much hoping that our politicians and community leaders will listen to those of us with something to offer from the technology side.

Do you think we've made reasonable progress there? I know you were involved in the NSA Centers of Excellence, talking about curricula and things like that, for quite a long time. Do you think we're going in the right direction?

Sometimes, I say yes, but the problem's gotten harder faster than we've gotten good at it. I think that if most disciplines looked at how much we've advanced, they would think this is terrific, but when you think of the adversary, who's advancing exactly as fast or faster in many cases, and the opportunity space is moving by leaps and bounds … I'm not convinced that we're doing much more than keeping our head above water most of the time. Still, I think that what we are trying is good. I don't see us as having given up. I think that the reemergence of looking at secure software and safe building of systems, which was out of fashion for a while, is heartening.

What's your view on professional certifications for cybersecurity versus academic degrees?

From a research standpoint, I have to say that we haven't found them particularly useful. When we've hired people on the research side, of course we're looking more at their capacity to do research and to think broadly, not always for cybersecurity skills. In fact, some of our best people come from other sciences—the certification isn't buying us that much in terms of extra added value. And, in some ways, certification is a bit more tied to the current system, which is a hindrance when you're trying to look 10 years downstream.

Do you think that academic degrees do a reasonable job preparing the workforce for doing what needs doing in cybersecurity?

Some do, and some don't. I would say that we're getting some excellent students out of places like Tulsa who have a good feel for what's going on. We've hired some very good people out of Virginia Tech, too. I've looked at some other institutions, and I'm a little less happy with what I'm seeing. They are, I think, more geared toward compliance, which is a valuable thing, but it's not so much a useful thing for me on the research side.

I see a lot of that in the government in what's known as the assurance community, where assurance, in many cases, means a whole lot of bureaucracy. Is your view the same, or have I just not looked in the right places?

Some of it's useful. What I do find happens, unfortunately, with assurance, is that we set a standard, and it's intended to be, in most cases, the least amount of security that's acceptable for that system. And that's what we mean when we set the standard there: if everyone meets the standard, they will at least have the basics. But, unfortunately, assurance culture tends to be, "this is the maximum" that's required. And that's a bad mindset. If what we consider the minimum now becomes the

maximum, we're not really meeting the basics in all cases. We're going through a lot of effort and not necessarily being more secure than we would be if we had a bit looser view of what was required and a little bit higher standards.

We still don't have enough women in computer science, much less computer security, so if you were to go back and chat with yourself about becoming a scientist before you became one, how would you motivate yourself?

Now, that is an interesting question, especially since I'm not certain that I listened to people too well when I was deciding what I wanted to do with my career.

I think you would listen to yourself, though, wouldn't you?

I'd hope so. What would've worked with me then is what did work with me, which is that I saw this huge need for improvement in cybersecurity. I've mentioned before to others that I was drawn to this field at about the time of the Morris worm, and I was just so angry that a technology that was supposed to help people communicate with one another was instead being used to harm systems. I was furious, and I think that a lot of people, a lot of women, for instance, like fields where they feel they can make a difference, they can improve things, they can help protect, and that's what drew me in. I'd go back and say, "Hey, Deb, you know, this is a field where you actually could make a difference if you stick with it."

I do think that there's a pretty big difference between why men tend to get involved in computer security and why women tend to get involved, having asked this question in the podcast over the last few years.

I've been interested in the answer when I've heard you interview men. A lot of times I'm hearing them discuss how much they enjoyed playing with gadgets and so on, and I did too, but that wasn't enough to get me interested in computer security. It wasn't until I had a cause, so to speak, that I felt like this is the profession that I wanted to stick with. ■

Gary McGraw is Cigital's chief technology officer. He's the author of *Exploiting Online Games* (Addison-Wesley, 2007), *Software Security: Building Security In* (Addison-Wesley, 2006), and seven 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.