

# Interview

## Silver Bullet Talks with Dorothy Denning

GARY MCGRAW  
Cigital

**D**orothy Denning is a professor in the Department of Defense Analysis at the Naval Postgraduate School (NPS) in Monterey, California. Denning has also worked at the Stanford Research Institute and Digital Equipment Corporation.

Featured here is an excerpt adapted from the full interview between Denning and Silver Bullet host Gary McGraw. Their conversation ranged widely, from teaching computer security to the Big Sur Power Walk. You can listen to the podcast in its entirety at [www.computer.org/security/podcasts/](http://www.computer.org/security/podcasts/) or [www.cigital.com/silverbullet](http://www.cigital.com/silverbullet), or you can subscribe to the series on iTunes.

**Gary McGraw:** You've been in academia for much of your career, teaching at Purdue and Georgetown and now NPS. What's the best way to teach computer security?

**Dorothy Denning:** I don't know what the best way is. I honestly don't. I can only tell you how I do it, which is to look at both the attack side and the defense side and try to make some sense out of the field and why we need certain kinds of defenses.

**McGraw:** Do you think that teaching particular courses on security is the best way, or is it better to have a little bit of security in all courses?

**Denning:** I think you need to have courses that are dedicated to security, particularly topics such as cryptography, which would be hard to integrate into another class. The field is just way too big to squeeze a little bit here and there into other courses. If you've got a course on computer networks, to do justice to the security part really requires another course.

On the other hand, you do want to cover some security in courses, particularly courses on software development. Students have to understand why it's important to check your input parameters and do various other things so that the software doesn't end up being shipped with vulnerabilities.

**McGraw:** Greg Hoglund and I cited your book, *Information Warfare and Security* [Addison-Wesley, 1998], on page five of our book, *Exploiting Software* [Addison-Wesley, 2004]. We did that because we wanted people to understand that the things we were talking about in that book could in fact be applied during wartime. What role does describing and understanding real attacks play in computer security?

**Denning:** You need to understand how attacks work because you need to understand how IP spoofing works, what happens during denial-of-service attacks, and how packets get past firewalls, and so on. How can you build a firewall if you don't

understand what the threats are against that firewall?

**McGraw:** Some people claim that we should only let specialists have that knowledge because it's too dangerous and that it shouldn't be written, published, or talked about. What's your position?

**Denning:** Again, I don't think you can do good defense without understanding offense. I don't see how you can teach defense without teaching offense. If you're talking about how you want to do authentication, you've got to understand what the threats to password files are and how they're cracked and sniffed off of networks.

**McGraw:** I think sometimes people believe, for whatever reason, that if you just talk about building defect-free software or how cryptography works or security functionality that you can ignore the attack part because it would become irrelevant. I don't think that's really true.

**Denning:** Right, because the whole field is evolving. There's constantly new attack methods and they're outside of the models that we design our security around. You're constantly having to invent new defenses to go with the new attacks. Then new software is rolling out continuously, which people find vulnerabilities in, so you're getting

## About Dorothy Denning



**D**orothy E. Denning is a professor in the Naval Postgraduate School's Department of Defense Analysis. She previously taught at Georgetown University, where she was the Callahan Family Professor of Computer Science and Director of the Georgetown Institute of Information Assurance, and Purdue University.

She has published 120 articles and four books, including *Information Warfare and Security* (Addison-Wesley Professional, 1998). She is an ACM Fellow and recipient of several awards, including the Augusta Ada Lovelace Award and the National Computer Systems Security Award. In November 2001, *Time* magazine named her to its innovators list. Her past leadership positions include president of the International Association for Cryptologic Research and chair of the National Research Council Forum on Rights and Responsibilities of Participants in Network Communities.

Denning has a PhD in computer science from Purdue University. Her research interests include terrorism and crime, conflict and cyberspace, information warfare and security, and cryptography.

more new attacks and you need more defenses. The two are coupled. It's like the front and back of your hand. You can't talk about one without talking about the other.

**McGraw:** Possibly one of the biggest controversies you've been involved in professionally was the whole Clipper chip dustup [the Clinton administration's 1993 encryption proposal, which used a US National Security Agency-created computer chip that provided a government backdoor to encrypted files using escrowed keys, for which Denning was an advocate]. What was it like being dubbed the "Clipper chick"?

**Denning:** Actually, it was a friend of mine who gave me that name.

**McGraw:** Well, it certainly got picked up and flung around. What was it like being in the middle of that controversy?

**Denning:** It was really rough. I felt like it damaged a lot of my relationships with people in the field.

**McGraw:** Did you think that to some extent some of the arguments were caricaturing things or making them ridiculously simple to make a political point?

**Denning:** Yes, there was a lot of that going on. The hardest part for me was the ad hominem attacks. From my perspective, I just wanted people to have a rational debate on the topic but that didn't happen. I was rarely in a setting where it looked like that. It was such an emotionally charged issue.

**McGraw:** Switching gears, you're widely regarded as the inventor of geoencryption. Do you think that this spatial concept will escape the defense community and move into areas such as geographic marketing?

**Denning:** Geoencryption, first of all, really wasn't my idea. Even location-based security wasn't my idea. I originally got involved because Pete MacDoran had a company and he was doing location-based authentication. He later got involved with folks who were interested in location-based encryption and already had a concept. So I tried to provide greater security and methods for doing it, but I don't really deserve credit for the idea.

**McGraw:** Do you think geolocation is going to catch on with the general public with GPS devices such as those in cell phones and cars?

**Denning:** Yes. Location is certainly

taking off now as an important concept in computing and networking. To the extent that information will be encrypted based on location, or that people will be authenticated based on their geographical location—I don't know to what extent those might become more prevalent.

**McGraw:** One of the trade-offs—and there are always trade-offs involved in security—is that it could be dangerous to broadcast your location.

**Denning:** You wouldn't have to broadcast your location. That communication could go encrypted.

**McGraw:** And then come to you and only be decrypted if you happen to be in the right place?

**Denning:** Right.

**McGraw:** I suppose a lot of people aren't aware of the fact that many of the gizmos that they carry around have this geolocation capability built into them. Do you think that we should make a point of making people more aware of that, or is it just something that happens and you just live with it?

**Denning:** It will probably happen at the rate that's needed to understand what's happening with the technology. I think a lot more people are aware of it—many people know that if they're in an emergency situation, somebody can find out where they are through their cell phones.

**McGraw:** I was talking to some cell phone vendors and they don't want to advertise the fact that you can be geolocated. Not because people might be worried about privacy, but because they're worried about liability in case it doesn't work. Imagine that someone kidnaps your kids and you're trying to use a cell phone to geolocate them and it doesn't work. Then whose fault is it if it doesn't work after the vendors make claims

that it does? Strangely, that's one of the things that's holding that kind of technology back right now.

**Denning:** That could be.

**McGraw:** You and I have very similar opinions about cybercriminals. We both think that cybercriminals are bad and that we shouldn't spend time hyping these guys up into rock stars. But your view on that seems to have evolved pretty radically over the years. What changed your mind? Did it happen all at once or gradually?

**Denning:** I don't think my views have evolved all that much.

**McGraw:** Okay. So what is your view now?

**Denning:** There's a lot of bad guys out there. A lot of them are doing it for money. It's just plain old crime. In my early work, I honestly didn't pay too much attention to who the bad guys were and the methods they used. I was looking at security from a totally theoretical perspective. It was in the late '80s, around 1990, that I did a study where I interviewed some hackers. The hackers I interviewed, about a dozen of them, were all pretty decent folks, I thought. I wrote an article about them and I probably came across as sounding like they were fairly decent folks, but without trying to necessarily endorse their behavior of breaking into systems. I never endorsed it.

But then Don Parker and others got to me and said, "You really should go and talk to the security administrators and the law enforcement folks and get their perspectives on that." I did and that reminded me that there are a lot of folks out there that have objectives that aren't benign. Today, I think the major threat is coming from people who are interested in making money or causing damage or leaking intelligence or all kinds of things that you really don't want to happen.

**McGraw:** I was at the National Academy of Science recently and someone was talking about the way Amazon.com's systems have evolved—instead of being engineered in a top-down fashion, they've emerged as this chaotic soup. They were one of the first to adopt this new service-oriented architecture idea. It's interesting when you have a system that's in some sense an organic thing—defending it can be a lot more difficult than if engineered a system in a top-down way.

**Denning:** Well, that's what we've got today. The whole Internet and computer networks and everything have just emerged over time. So that's probably the reason why it's very hard. People have attempted this top-down design of secure operating systems since the very early days, probably the '60s. That's hard to do; when you finally get your product put together and certified and all that, it's going to be very expensive. It's going to be obsolete. It's going to be slow.

**McGraw:** People used to the edge of technology will say, "My goodness, that seems like an Apple II from 1981."

**Denning:** Right. In the meantime, the rest of the technology has marched on and you want it because it's a productivity enhancer. It allows you to do things that you couldn't do before. You can communicate in ways you couldn't before.

This top-down approach to building systems and security is great and maybe works well in some small, rather confined kinds of environ-

doomed—maybe not doomed, but at least relegated—to co-evolution in terms of security, where we're caught in this constant arms race, this attack-defense thing. Which, I suppose, is why you believe that we have to understand attacks as much as we understand defense.

**Denning:** It's the same in the physical world. In the physical world, things evolve. You get new technologies. Automobiles came along and then airplanes; all this comes along and it introduces new security issues. They don't all get solved. So the world is a vulnerable place and we just kind of accept that and we try to achieve a reasonable level of security and stability and so on, but it's not perfect.

**McGraw:** We seem to be bubbling along pretty well.

**Denning:** Yes, but the difference is that there seems to be this expectation with our computer networks that we could do it all right and that there are no vulnerabilities. To me, that's just crazy; it's not realistic and we have to accept that there's always going to be security issues. It's not just Microsoft's problem. It's not their fault.

**McGraw:** Oh, they're going to solve it with Vista, haven't you heard?

**Denning:** They're adapting. I've been very impressed with what Microsoft has done over the years.

**McGraw:** Absolutely. Mike Howard's work has been good. I don't know if

**'We have to accept that there's always going to be security issues. It's not just Microsoft's problem. It's not their fault.'**

ments, but for the world at large and the Internet it's never going to work.

**McGraw:** I guess we're sort of

you know Mike or not, but he was a previous Silver Bullet victim back in episode six. I want to switch gears pretty radically. I noticed your time

# New nonmember rate of \$29 for S&P magazine!

IEEE Security & Privacy magazine is the premier magazine for security professionals. Each issue is packed with information about cybercrime, security & policy, privacy and legal issues, and intellectual property protection.

S&P features regular contributions by noted security experts, including Gary McGraw & Bruce Schneier.

Top security professionals in the field share information you can rely on:

- Wireless Security
- Intellectual Property Protection and Piracy
- Designing for Infrastructure Security
- Privacy Issues
- Legal Issues
- Cybercrime
- Digital Rights Management
- Securing the Enterprise
- The Security Profession
- Education



Save 59%!

[www.computer.org/  
services/nonmem/spbnr](http://www.computer.org/services/nonmem/spbnr)

on the Big Sur Power Walk, which is a 21-mile walk, is trending down over the last two years.

**Denning:** No! It's been about the same!

**McGraw:** I wonder whether 2007 is going to be a breakthrough year. Are you going to break your 2005 record?

**Denning:** Our goal is just to enjoy it out there, we have six and a half hours. If it takes six and a half hours, it's no problem. It's a nice walk. It's beautiful. There's no reason to rush it.

**McGraw:** I'm jealous of that. Can I come?

**Denning:** It's already sold out. You can run the marathon though.

**McGraw:** I think you're talking to the wrong guy. One last question: What kind of advice would you give to a young scientist who's just starting out in security?

**Denning:** My advice would be, "Follow your interest, but follow the law." I'm very much against experiments that break the law.

You can find additional podcasts in the series, such as those featuring Becky Bace or Microsoft's Michael Howard, at [www.computer.org/security/podcasts/](http://www.computer.org/security/podcasts/) or [www.cigital.com/silverbullet/](http://www.cigital.com/silverbullet/). □

*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 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](mailto:gem@cigital.com).*