

Interview

Silver Bullet Speaks with Ed Felten

BY GARY MCGRAW
Cigital

Ed Felten is a professor of computer science and public affairs at Princeton University and director of the Center for Information Technology Policy. He's well known for his work at the intersection of privacy, security, and technology, especially regarding digital content protection. Felten's blog, Freedom to Tinker (www.freedom-to-tinker.com), is one of the Internet's best blogs on these subjects. He's also known for his work on the Microsoft antitrust trial, in which he was a star witness for the US Department of Justice.

Featured here is an excerpt adapted from the full interview between Felten and Silver Bullet host Gary McGraw. Their conversation ranged widely, from Felten's technology predictions and his thoughts on public policy and law all the way to raising kids. Listen to the podcast in its entirety at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/, or you can subscribe to the series on iTunes.

Gary McGraw: On your Freedom to Tinker blog, you made several predictions for 2006. How are you doing with those predictions?

Ed Felten: Let's take a look at what I predicted—a sort of mid-year score card. Number one: "Digital rights

management technology will still fail to prevent wide spread infringement. In a related development, pigs will still fail to fly." I'm pretty confident on that one. I predict that every year, and it turns out to be true every year.

McGraw: Are there any predictions that you felt you were going out on a limb with?

Felten: Yes. "The recording industry will quietly reduce the number of lawsuits it's filed against users." That one, I think, has not happened. "The Google Books Search case will settle." I predicted that, and it has not happened yet, although the case seems to have fallen off the front pages. "It will become trendy to say that the Internet is broken and needs to be redesigned, and this theme will be especially popular with those recommending bad policies." I think it has become a bit trendy to say the Internet is broken.

Here's another one where I went out on a limb a little bit, "Push technology, as in PointCast and the Windows Active Desktop and all that, will come back, this time with multimedia." I don't know if this has happened.

McGraw: Why did you think push technology was going to come back 10 years later?

Felten: It just seemed to me that the

way that people were moving in—delivering multimedia, audio, and video and so on—was in that area. There were people who wanted a TV-like model, and there were people who wanted to be able to choose their content. So if you think about something like a TiVO device that lets you choose your programming off a menu of recorded programs, and you put that together with delivery of material over the Net, what you get is a device that delivers a menu of stuff over the Net to your device, and then you can pick what's there. That's rather like push technology; that was the theory.

McGraw: It sounds to me like an RSS feed.

Felten: Yes, it's kind of like RSS or podcasting, but slightly friendlier for the average user's user interface. Kind of like what we're doing here.

McGraw: Let's switch gears from prognostication to something else. A lot of your career since 1995 has involved taking on huge corporations or organizations, and sometimes even governments. I'm thinking of things like taking on Sun with Java security, Microsoft with the antitrust trial, the RIAA [Recording Industry Association of America], Sony with the music CD rootkit, and sometimes even [the US] Congress. Do you ever worry about making powerful enemies? Have you seen any

evidence that your career in public service is dangerous?

Felten: It depends on what you mean by “dangerous.” If you mean, do people get angry? Yes, I know they do. And a few of them hold a grudge, but mostly, they don’t. I think if people are convinced that you’re calling it as you see it and that it’s not about a vendetta against anyone in particular, and if they believe what you say is really driven by the technical facts on the ground, then I think they will, over time, come to accept that it’s annoying at times, but it’s not spiteful.

McGraw: Who had to move the farthest in their position to understand the objective reality that you were trying to present?

Felten: I don’t know. I think in some cases, the emphasis on the issue that there was disagreement about simply passed. In the case of Java, for example, Java security was a huge deal at the time, and Sun had really enormous aspirations for Java. Now I think their aspirations are narrower, and the uses to which Java is put equate to different kinds of security problems than the ones we were looking at back then. So, the issue about which there was disagreement just isn’t as big a deal anymore. And sometimes it’s sort of procedural. I worked on the Microsoft antitrust case with the Department of Justice, and that case, of course, was eventually settled. Right now, Microsoft and the DOJ are basically getting along under the terms of the settlement, so it’s not an area in which there’s continuing serious dispute.

McGraw: One area in which there does seem to be a continuous dispute going on would be with digital protections and the RIAA.

Felten: That’s right, yes. There’s still a fight over digital protection or dig-

ital rights management [DRM] technology. It involves a lot of different players: not only the record companies and the movie studios, but a lot of technology companies are building business strategies around this stuff. Apple is a very prominent example of something that has accumulated a lot of market power by clever use of digital rights management technology.

In fact, that’s the mean effect that Apple’s DRM has had: not preventing copying but giving Apple market power, helping it shape and control what happens with online music.

McGraw: One of the things that you’ve had to do because of your involvement with these high-profile situations is become media savvy. It seems like you know how to get attention and keep it with a clever hook. Where did that skill come from?

Felten: It’s probably practice—seeing what happens when you say something or act in a particular way and then seeing how it ends up in the media. One of the things I learned early on was that if you’re reporting a security flaw in something, the media wants to portray it as a “this person says X, that person says not X” kind of story. That story doesn’t really inform anybody.

It’s much more productive to try to find a way to tell the story in a way that the vendor can actually agree with. And that has to do, partly, with how you present the story initially to the public, and it also has to do with

talking to the vendor in the right way beforehand, so you don’t get a lot of people contradicting each other in the media. Instead, you can agree on what’s true and what’s not.

McGraw: Have you found that the analogies and metaphors you’re using have shifted over the years as you’ve done more public discourse? I’m thinking about the early days, in the mid-90s, when we were releasing things to the media, but it was mostly the tech media. Now, when you’re testifying in front of Congress, you have lawmakers who might not be computer people.

Felten: Yes. You obviously have to use an analogy that is closer to what they’re used to. I’ve found a lot of value in using analogies to older technologies like the telephone system, transportation, cars, airplanes, and so on. Or making analogies, especially in security cases, to situations where people are used to seeing security technology, like an automatic teller machine. There’s a whole set of security mechanisms around that: the receipt, the camera, the way the records are kept, the encryption of the connection back to the bank and—

McGraw: The limited amount of money in the machine itself.

Felten: Yes, the limited amount of money in the machine itself, limitations of how much you can take out at any one time, the whole problem

About Ed Felten

Edward Felten is a professor of computer science at Princeton University and director of the Center for Information Technology Policy. He has a BS in physics from The California Institute of Technology (Caltech), and an MS and a PhD in computer science and engineering from the University of Washington.

Felten has advised the US Federal Trade Commission on spam, the Transportation Security Administration on airport security and privacy, and the Department of Defense on data mining, privacy, and information technology research priorities. In 2003, *Scientific American* named him to its list of 50 visionaries in research, science, and technology.

of counterfeit machines. You can get through a lot of interesting security problems by using analogies like that. And choosing the right analogy is incredibly important.

McGraw: What's the most powerful analogy that you've come up with along those lines?

Felten: Consider DRM technology and the way it actually works technically. It's about control, and what devices can be compatible with what other devices. You can take a lot of ground in this area by abstracting it to other cases, even low-tech cases in which compatibility is important: compatibility of tires with the wheels of a car, compatibility of compact discs with CD players, compatibility of stereo speakers with the equipment that drives them, even the compatibility of antenna broadcasting television with the antenna and TVs that are receiving it. When you talk about people designing technology that is deliberately incompatible and then talk about the government actually passing laws to foster this deliberate incompatibility, I think it brings home to people the fundamental strangeness of digital rights management.

McGraw: You spent your last sabbatical with Larry Lessig at Stanford Law School. One question that computer scientists want to know is, why is public policy in the law so important for a computer scientist to be working on?

Felten: It used to be that the stuff we, as computer scientists, did was not all that interesting to most of the people in the world. I mean, yes, high-tech was cool, people had seen computers, but nowadays, so much of what happens in everyday life is mediated by computer technology.

Policy makers have figured out that regulating the technology is a way that they can try to pull the levers and control the way the world

develops and the way people behave. Sometimes they think it's easier to control the technology than to control the behavior that the technology enables. Then they get in and start messing around with the technology. It used to be that you could go months without having any hearings on Capitol Hill related to computer technology. Now, there are multiple hearings every week, and all kinds of different congressional committees are talking about doing all kinds of different stuff. They worry about gambling, so that's now considered a technology problem. They worry about child molesters and child stalkers, so that's viewed as a technology problem.

McGraw: Is that because of the newness of the technology? Similar to how people would say "telephone involved in murder" back at the turn of the century?

Felten: Exactly. Nowadays, if a telephone is involved or an automobile is involved, it's just normal. So it's partly the hype, but it's also partly that computers and the Internet are used in lots of everyday activities, and I think to the people who don't understand them, it seems easy to regulate and control the way they work in order to change behavior.

McGraw: You and I agree that having technological tools to deeply probe security is important for cutting through snake oil and to expose those things that don't work. Some of these tools—decompilers and rootkits, in particular—are now being used by the good guys, and of course, some are standard tools for the bad guys. I think there's an important lesson here that technology is agnostic.

Felten: For the most part, yes. I think there's a real tendency of policy makers who don't understand technology to try to outlaw broad categories of technology, not realizing how

much the good guys make use of the very same tools that the bad guys use. Again, this is a case where analogies are really valuable. You can talk about something like a kitchen knife or a crowbar that can be used to cause all kinds of harm, but you certainly wouldn't want to outlaw kitchen knives, nor would you want to try to have regulations micromanaging the design of kitchen knives to make them less dangerous.

McGraw: Here's sort of a philosophy question for you, then. Is there any sort of technology that deserves to be outlawed *prima facie*?

Felten: I think a very few technologies are so inherently dangerous that just having them around is dangerous, but I'm thinking more of biological and nuclear agents, for example.

But when you talk about security technology, no, I think it depends on how it's being used and how it's being protected and so on. I think it's very dangerous to say that there are certain things that are offlimits, even for the good guys doing good things. This is really just a road to not understanding, to giving the bad guys the advantage of knowing more about how their bad technology works than we do.

McGraw: I, for one, believe that we have to do all that we can to really understand what security attacks are like because if we don't, we're just going to be building pretend solutions.

Felten: Right, and it's easier to build and sell pretend solutions if there's nobody out there talking about whether they're really effective and what the bad guys actually do. There's a dangerous syndrome we can get into where we try to keep ourselves from understanding how our systems can fail rather than keeping them from failing. You see this all over the place. You see it in security and a lot in e-voting, where it seems like sometimes the goal of some

people is to prevent finding out about problems rather than to prevent problems.

McGraw: One last question. What is the biggest challenge with raising an 11-year-old girl?

Felten: I think the biggest challenge—I don't know if this is true about kids in general, but I think probably it's true about mine—is just trying to keep them engaged in the world and keep them believing that they can do great things if they work at it. Kids naturally, I think, have a lot of curiosity and really want to get involved in things, so just keeping that alive while they learn more and become more capable is the most important thing.

McGraw: So they can become little tinkerers.

Felten: Little tinkerers, that's the goal, whether it's writing or whatever, getting them creating stuff and trying things out.

The *Silver Bullet Security Podcast with Gary McGraw* is a series of in-depth interviews with prominent security experts. A complete audio version of this Silver Bullet interview, as well as others, is available in podcast form at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/ and through iTunes. □

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 coauthor of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), *Java Security* (John Wiley & Sons, 1996), and four other books. His latest book is *Software Security: Building Security In* (Addison-Wesley, 2006). 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.

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% off the regular price!

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