PCWorld.com - Three Minutes With Security Expert Bruce Schneier

Three Minutes With Security Expert Bruce Schneier

Security expert pushes full disclosure, forcing vendors to admit and fix bugs quickly.

Kim Zetter, PCWorld.com

Friday, September 28, 2001

Bruce Schneier is founder and chief technology officer of Internet security firm Counterpane. He has written two books on cryptography and computer security, *Secrets and Lies* and *Applied Cryptography*, and is an outspoken critic of Microsoft and other software vendors that produce products that contain dangerous security holes. We spoke with him about who is responsible for software security flaws and what consumers can do about the growing problem.

PCW: Are there more security holes in software, or are we just getting better at finding them?

Schneier: Both. There are thousands and thousands of security holes in software. We are better at finding them, but there are many that we don't find. The problem is getting consistently worse. The basic reason is complexity. Complexity is the enemy of security. As systems get more complex, they get less secure.

PCW: Why don't software vendors devote more time to testing products to find and fix security holes before delivering programs to market?

Schneier: Because the marketplace doesn't reward security. A company

like Microsoft could spend an extra year developing the next version of Windows--throw an extra 200 or 500 people at the program, testing it for security problems--but then the software would be a year late getting to market.

PCW: Microsoft says it did this with Windows 2000. According to Scott Culp, program manager for Microsoft's Security Response Center, the company held back the operating system for so long in order to fix security bugs.

Schneier: They said [Windows 2000] would be more secure than any other version to date. But there are more security holes in it than any other version of Windows.

PCW: Why is it that hackers and security pros find security holes that Microsoft doesn't seem to be able to find?

Schneier: It doesn't just happen to Microsoft. There are thousands of people looking for security bugs, so they're bound to stumble upon them. It might take days, weeks, months--there are just so many holes to find. I'm sure the software companies do some testing and find some holes, but they're not doing a lot. They'll tell you they'll do a lot, but they're not.

There has to be a market incentive to provide security. Either you lose sales, or you get sued. But there is no such product liability in software. If Microsoft produces an insecure product and your data gets stolen, they are not liable.

I think consumers should be livid about this. We would never stand for this in a stepladder or an automobile or an aircraft, yet we stand for this in software all the time.

PCW: Yes, but no one's going to get killed by...

Schneier: But people do get killed by software. It doesn't happen often,

but there have been deaths from software bugs in medical devices. But usually you just read about Windows. Usually you just lose a lot of money. There's been an enormous amount of money lost because computers have failed. Where are the class-action suits against [companies like] Microsoft?

PCW: But you've said that the more complex software gets, the more it will have flaws.

Schneier: But there's a balance. The automobile manufacturers have managed to strike this balance. We get new cars every year, new features every year, yet there is liability. They're not going to give you a feature that they know isn't safe, even though it would be fun to have. So there is a balance, and that balance is struck over years through litigation, through laws and policies. The problem with software is that you just get one side--you just get features; you don't get reliability or safety or security.

PCW: You talked about the fact that there is no forward learning in software; the same problems seem to be creeping up over and over again.

Schneier: Buffer overflows are the poster child of why problems aren't getting better. They were discovered in the 1960s and were first used to attack computers in the 1970s. The Morris worm in 1989 was a very public use of an overflow, which at the time knocked out 10 percent of the Internet--6000 computers. Here we are 40 years later, and buffer overflows are the most common security problem. And that's an easy problem to fix. If you are a software vendor, there is zero excuse for buffer overflows.

PCW: Is Microsoft good about fixing problems once they're discovered in its products?

Schneier: They actually spend a lot more time paying lip service to security and not doing security. When a security bug is [found in a

Microsoft products], they will deny it until it's made clear that it's true.

PCW: Are you saying the Microsoft Security Response Center is not responsive?

Schneier: If it's an easy fix, they'll fix it quickly and announce how good they are. If it's a hard fix, they'll tell you it's not a problem. That is, until they fix it, and then they'll tell you how good they are. Unfortunately, Microsoft treats security problems as public relations problems, and they'll do whatever they can do to get the most PR.

PCW: Is full disclosure beneficial or harmful to security?

Schneier: The full-disclosure movement appeared because companies were ignoring the problems with security holes or lying about them. Security professionals and amateurs would find a security flaw, alert the company, and the company would threaten them with a lawsuit and not fix the problem. Or they would send the vulnerability to an organization like CERT [the Computer Emergency Response Team at Carnegie Mellon University], which would sit on it for five months.

So the full-disclosure movement was formed out of frustration. And by God it works. If you told Microsoft there was a problem a bunch of years ago, they would have told you to shut up. Nowadays they know they better fix it fast because it's going to be in the newspaper next week.

In some ways full disclosure helps the bad guys, but it also helps the good guys. So it's double-edged. I think if we said we're no longer going to do full disclosure, the companies would go back to paying lip service and not care about it. So you need it to keep the pressure on. Right now what the community has settled on is alert the company, give them reasonable notice, and then announce the vulnerability. And that seems to be working.

PCW: Many bug finders provide exploit code with their vulnerability announcement. Why give a warning to users about a hole and at the same time give hackers a tool to exploit it?

Schneier: Because, unfortunately, many companies say, Well, that's a theoretical vulnerability but it doesn't actually work.

PCW: You could just send Microsoft the exploit to prove the hole is not theoretical and not post it publicly where everyone can get it.

Schneier: But then [the vendor] will lie. They'll say they never received it or they tested it and it didn't work. You're assuming that the companies are being honorable, and they're not.

I don't like the fact that vulnerabilities get in the hands of script kiddies who exploit them. I would prefer if we could announce the vulnerability, we wouldn't explain the details, the company would fix it, and all would be good. But that's not always the way it happens.