

Interview

Silver Bullet Talks with Ross Anderson

Ross Anderson is a professor of security engineering at Cambridge University, where he leads the computer laboratory security group (www.cl.cam.ac.uk). Anderson founded the Foundation for Information Policy Research (www.fipr.org), an organization exploring the interplay between computing and the law, as well as IT's social effects.

Featured here is an excerpt adapted from the full interview between Anderson and Silver Bullet host Gary McGraw. Their conversation ranged widely, from project management to the economics of security to man-in-the-middle attacks. You can listen to the podcast in its entirety at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet, and you can subscribe to the series on iTunes.

Gary McGraw: You recently placed your book, *Security Engineering* [Wiley, 2001; www.cl.cam.ac.uk/~rja14/book.html], online for free. What's the response been like?

Ross Anderson: The response has been great. The last royalty check I got from Wiley was satisfactorily up, and I proved to my satisfaction and my publisher's that the online book doesn't compete with the print edition.

It took me a couple of years to convince them, but what was very helpful was that Cambridge University Press put my colleague David

MacKay's book on coding theory online three years ago, and it greatly helped his sales. What seems to happen is you put your book online, people find it easily, refer to it, and say, "Hey, this is good. I want this on my shelf." Then they go to Amazon and buy it.

McGraw: Regarding security engineering and, in particular, software security, do you think we've been making progress in those fields over the past decade?

Anderson: There's been a little bit of progress in that there are no longer quite as many stack-overflow vulnerabilities as there used to be, but there are plenty of others. I believe that as software gets more complex, you're going to see an equilibrium which is determined more or less by sociocultural and economic factors rather than by the kind of tools that people have for vulnerability finding.

As we give people better tools, they'll just make more complex software. As we give them higher assurance systems, they'll take more risks with them. We're likely to end up in a world where there's a constant stream of vulnerabilities, and managing them becomes a very important process.

McGraw: Does that suggest there's some kind of equilibrium point that we've already reached, even though we're changing some factors?

Anderson: Yes. Take an example from the world of dependability and software project management: for about the past 30 years, people who study large software projects have reckoned that about 30 percent of them fail and don't work at all, or they go wildly over budget and over time, and so on and so forth.

Now, since the 1970s, we—the computer science community—have made available to developers much better tools in that we no longer program in Fortran and Cobol. We've got all sorts of mechanisms for managing large complex projects, and so what do people do? They build bigger and better disasters, right? But the 30-percent failure figure—and in fact, it's a slightly higher failure figure in government—reflects underlying institutional realities.

McGraw: The economics and security subfield that you've helped found has really become quite a hot topic. Where do you think things currently stand in that area?

Anderson: We've got over a hundred active researchers, and we've got two annual conferences now: the Economics of Securing the Information Infrastructure that Stuart Schecter started on the East Coast in November of last year, and WEIS, the Workshop on Economics and Information Security, is still the main event.

McGraw: What's the most interesting, nonobvious result from that work?

Anderson: There have been many interesting and nonobvious results. The fundamental insight is that most systems fail not because of technical problems but because incentives are wrong. I think the best paper at WEIS last year was by Ben Edelman in which he pointed out that Web sites bearing the TRUSTe certification mark were twice as likely as random, similar Web sites to be malicious.

McGraw: Not surprising, really.

Anderson: This is an effect of adverse selection. Good operators—people with an established corporate brand don't bother with things like TRUSTe—whereas all the shysters and hucksters and fly-by-night companies, go and get that mark because it gives them some respectability they think they need.

What's enormously important to the online economy nowadays is another result that Ben puts in the same paper. Namely, if you look at the top-rated free-search items on Google and compare them with the top-rated advertisement slot, the Web site in the top-rated advertisement slot is more than twice as likely to be a scamster site as the top-rated free search site. Ben's conclusion was, "Don't click on ads."

If everybody in the online world read this paper and thought about it carefully, then Google would be in bankruptcy tomorrow. These results are important for business as a whole as well as, of course, for security engineers and software developers.

McGraw: You've pointed out many times the imbalance between victims—those, say, who have to use Microsoft Office and fall prey to malicious code attacks—and those who build things and could mitigate the problem, such as Microsoft. What's a

About Ross Anderson



Ross Anderson is a professor of security engineering at Cambridge University. His research interests include security economics, filtering systems, and cryptology. He and Eli Biham designed Tiger, a cryptographic hash function. In 1998, Anderson helped set up the Foundation for Information Policy Research (FIPR; www.fipr.org), which promotes research and seeks to educate the public in areas such as computing and the law. Anderson has a PhD in computer science from Cambridge University.

good way to address that imbalance? Are there economic tools?

Anderson: If you look at the theory of tort, a risk should lie with the party that's best able to mitigate it. That means that it should be Microsoft's job to see to it that their software ships in as close to an unhackable form as they can get it.

McGraw: To some extent, you might say that the invisible hand of the market—pulling an Adam Smith metaphor—has caused Microsoft to at least change their behavior in some ways.

Anderson: There has been a significant amount of pressure on them, but Microsoft's pretty well a monopoly because of the network effects that you get with platforms. It's all very well for guys like me to escape their clutches—I use a Linux box in the lab, and I've got a Mac that I carry around with me. But for the average person, there isn't a practical alternative to using Windows, and this means that they just basically have to put up with what Redmond [Microsoft's headquarters in Washington state] ships to them.

It happens not just as an issue in technology platform markets but also in financial markets. For example, European customers have poorer protection against online banking scams of every kind, from cloned ATM cards to phishing scams, than in the US. It's interesting to see that many of the new e-money providers—the nonbank

payment services companies—are operating essentially under European rules rather than under American rules. At present, PayPal is very scrupulous at repaying every one of their customers who is the victim of a scam, but their terms and conditions do rather appoint them as the judge and jury and go as far as they can to ruling out any independent regulation. In that respect, they're falling inside the European camp, and I predict that there's going to be some serious tension that will involve not just computer security, per se, but regulators, the anti-money-laundering crowd, the FBI [US Federal Bureau of Investigation], comparable agencies here, and so forth because phishing is one of the biggest growing threats on the Internet, and technical mechanisms alone aren't going to fix it.

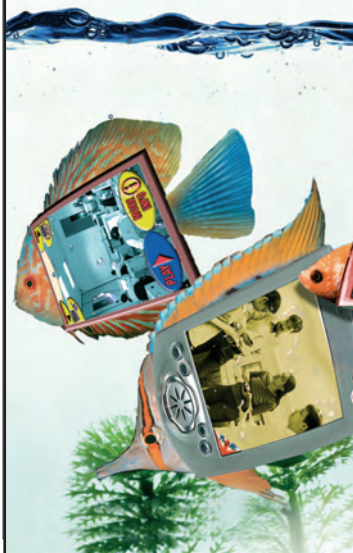
McGraw: One of the things that I love about your work is your nonsense approach to telling it like it is when it comes to attacks. Presumably, you find the act of describing attacks and security failures essential to good engineering.

Anderson: Absolutely. Civil engineers learn far more from the bridges that fall down than from the much greater number of bridges that stay up. Similarly, if somebody's going to call themselves a security engineer, then they really have to study how things fail. That means that you have to read the press, the mailing lists, comp.risks, and plug into all the various sources of infor-

Tried any new gadgets lately?

Any products your peers should know about? Write a review for *IEEE Pervasive Computing*, and tell us why you were impressed. Our New Products department features reviews of the latest components, devices, tools, and other ubiquitous computing gadgets on the market.

Send your reviews and recommendations to pvcproducts@computer.org today!



www.computer.org/pervasive

mation about the bad things that are going on in the world.

McGraw: This notion of gag orders to stifle discussion of security apparatus—I find that misguided and unethical, and I know that you do, too.

Anderson: I was a victim of this a few years ago when a certain large bank put an order against me in the high courts in London when I was appearing as an expert witness in a case over some disputed ATM withdrawals from one of their accounts.

McGraw: That was Citibank, right?

Anderson: Indeed. There's currently an application [petitioning] a judge in Berlin to ask the judge [in London] to order Citibank to raise the gag order so that I can testify in a Citibank case in Berlin. So this has all sorts of unpleasant spillover effects.

On a larger scale, we're seeing a tendency in a number of countries, including, unfortunately, Britain, to pass laws criminalizing the manufacture, possession, or use of hacking tools. This is now causing problems for some people in the UK who are running computer security courses; it's creating sufficient legal uncertainty that university lawyers are saying, "No, you can't have your students doing key search or WiFi hacking or whatever" experiments.

McGraw: We'll end up with a bunch of dumb people who are supposed to defend against these attacks.

Anderson: Indeed. In fact, the law's not particularly well drafted, and the Home Office says that they didn't mean it to stop research, but the mere fact of it being obscure and the fact that corporate bureaucracies and universities are risk averse is beginning to cause a problem in some places.

McGraw: Do you think that what was done to adjust the US Digital Millennium Copyright Act—

which has other problems other than the one we're speaking of—to let security researchers look at security apparatus is sufficient?

Anderson: I don't know because I don't work in the US. I haven't followed that particularly closely. It was something out of the corner of my eye, no more than that. But certainly, we need the space to do our jobs.

Another problem that's coming up in the UK and Europe is an attempt to license security personnel. We had a law introduced in Britain a few years ago that enables the government by regulation to license security people. This was brought in initially to stop organized criminals supplying bouncers for pubs and clubs. But once the law is there, the officials took it into empire-building mode, and there's currently some mutterings about compulsory registration for security consultants.

McGraw: Wow, interesting. That's not been seen over on this side of the pond.

Anderson: Security consultants are such an enormously broad church—ranging from system administrators at one end to specialists like the people who sweep 10 Downing Street for bugs on the other end—and there are dozens of different communities, each with their own cultures. The sys admin culture is generally, like much of the computer culture, relatively libertarian and west-coast based, whereas security specialists who have come out of an Army background think that regulation is just fine because it helps to keep down the competition.

It's a very inappropriate measure that's trying to force an awful lot of little specialized subindustries into one straightjacket, and it's something that you should fight as hard as you possibly can if some misguided congressman tries to introduce it on your side of the pond.

McGraw: Switching gears, why do you suppose that the same old attacks keep on applying over and over again? In particular, I'm thinking of your man-in-the-middle work on RFID systems. How can we teach builders to know about these attacks and their patterns?

Anderson: I don't really think that you can, unfortunately. Man-in-the-middle attacks have been around since at least the time when [Sir Francis] Walsingham doctored a letter from Mary Queen of Scots to her supporters—which was the 16th century. He added a few extra cipher groups that basically instructed her supporters to send her an enciphered list of [the conspiracy's] supporters, basically disclosing the whole conspiracy to the hangman's noose.

Knowledge of this is becoming widespread, I think, thanks to phishing. But people tend to think, "It doesn't apply to me," and you've got the unfortunate deployment of a whole lot of applications on RFID just at the same time that the mobile phone industry is working hard to put 500 million attack platforms out there in people's pockets—I'm referring to mobile phones with NFC [near-field communication] capability. An NFC phone, with appropriate software, can act as an RFID tag and also as a reader; it can be a pseudo-server to one client and pseudo-client to another server, and the two can communicate by GPRS [General Packet Radio Service].

Now, you could not have engineered a better platform for middle-person attacks if you had set out to do it, and the fact that they've made it into a huge business model is just amazing. A lot of people who rely on RFID for low-value payments, road-toll tags, prisoner tagging, keeping hooligans out of football grounds, and so on are going to find that their systems are spoofed. We've had some fun

thinking of all the applications that people can get up to.

McGraw: I bet you wrote it down, too.

Anderson: If you look at my Web site [www.cl.cam.ac.uk/~rja14/], you'll see that there's a paper which is a summary of the talk that I gave at Financial Crypto last month.

For example, bad people who at present go through subway trains mugging people won't have to carry knives in the future. They'll just carry an NFC phone, and as they walk past everybody, just go ching, ching, ching, ching, and take 9.99 pounds out of their electronic purses.

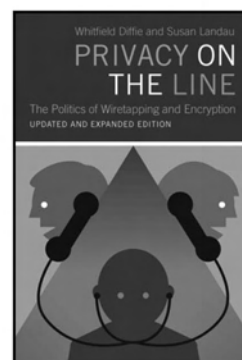
If the ruler of Korea wanted to do a denial-of-service attack against the French—for example, if he decided he didn't like the Parisians—he could just get one of his satellites to collect 9.95 euros from every Frenchman by sending the appropriate signals from orbit.

The potential for mischief is quite mind-blowing. What this means in practice is that a whole lot of systems are going to have to be re-engineered. That's going to cost a lot of money.

You can find additional podcasts in the series, including those featuring Peter Neumann and Annie Antón, at www.computer.org/security/podcasts or www.cigital.com/silverbullet. □

Gary McGraw is *Cigital's* chief technology officer. His real-world experience is grounded in years of consulting with major corporation and software producers. McGraw is the author of *Exploiting Online Games* (Addison-Wesley, 2007), *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.

New from The MIT Press



Privacy on the Line

**The Politics of Wiretapping
and Encryption**
Updated and Expanded Edition

Whitfield Diffie and Susan Landau

"This authoritative treatise helps unveil some of the mystery and puts contemporary freedom, privacy, and security issues in perspective."
— *Publishers Weekly*

400 pp. \$27.95 cloth



Wired Shut

**Copyright and the Shape
of Digital Culture**

Tarleton Gillespie

"Gillespie has boldly attempted a broad and deep analysis of copyright that integrates cultural, historical, legal, social, political, and technological perspectives—and he succeeds. This is an unusual, excellent, vitally important, and urgently needed book."

— Kirsten Foot, University of Washington

420 pp. \$29.95 cloth

To order call **800-405-1619**.

<http://mitpress.mit.edu>



\$29

New Lower Subscription Price!

IEEE
SECURITY & PRIVACY

Subscribe to our
magazine today
for only \$29—
our lowest price ever!

You'll receive 6 issues of today's
leading-edge, peer-reviewed
software development information.

Ask us how
you can get this great deal on
IEEE Security & Privacy magazine!

S&P is the premier magazine
for security professionals.
Every issue is packed with
tutorials, best practices, and
expert commentary on:

- attack trends
- cybercrime
- security policies
- mobile and wireless issues
- digital rights management
- and much more.

Subscribe at www.computer.org/services/nonmem/spbnr