

# Interview

## Silver Bullet Speaks with Dan Geer

By GARY MCGRAW  
*Cigital*

**D**an Geer is chief scientist at Verdasys. Long ago, he ran the development arm of the Massachusetts Institute of Technology's (MIT's) Project Athena, where his staff pioneered Kerberos, the X Window System, and much of what we take for granted in distributed computing.

Featured here is an excerpt adapted from the full interview between Geer and Silver Bullet host Gary McGraw. Their conversation ranged widely, from Dan's work in Project Athena and his thoughts on data security all the way to hog raising. 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 subscribe to the series on iTunes.

**Gary McGraw:** Your paper, "Cyber Insecurity: The Cost of Monopoly" [[www.ccianet.org/papers/cyberinsecurity.pdf](http://www.ccianet.org/papers/cyberinsecurity.pdf)], caused a seemingly well-orchestrated splash. Did you accomplish what you wanted to with that paper?

**Dan Geer:** I think it's fair to say there is acceptance across the board that having everything just alike is a dangerous trade-off. On the one hand, everything just alike gives you the maximum ability to manage things because everything is alike. On the

other hand, having everything just alike is the highest level of danger. I believe that there's a common acceptance that that's true.

What isn't accepted all around is how you should negotiate the trade-off. To have everything alike on the grounds that it's easy to manage allows you to harden systems. But my personal belief is that the word "harden" in this case means "harden" as in brittle. Versus harden in the sense of tough, which I think you get from diversity. In the academic world, there are people who look at how to manufacture artificial diversity out of what is otherwise, shall we say, a field of cloned computers.

**McGraw:** Do you think that market pressures tend to enforce or erode diversity?

**Geer:** I think they tend to erode diversity when we're talking about a commodity. How many companies

are there that make PVC pipe, for example? The answer is a very small number. On the other hand, when what we're talking about is not a commodity, I don't think the market actually enforces monoculture. I think it's the other way around. So one could say, to pick on Microsoft, that their great trick was somehow or other to make their operating system appreciated as a commodity and at the same time, escape the commodity pricing pressures that ordinarily go with that.

**McGraw:** Do you think that the open-source movement is in some sense correcting the market? Is such correction an emergent phenomenon that is destined to occur?

**Geer:** Yes, I think that it's destined to occur, and it's not going away. If anything, the pressure on interoperability, in particular, supports the open-source and open standard side. For those of us present at the start of

### More about the Silver Bullet Security Podcast series



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 at [www.computer.org/security/podcasts/](http://www.computer.org/security/podcasts/) or [www.cigital.com/silverbullet/](http://www.cigital.com/silverbullet/).

the Internet and at the beginning of the Internet Engineering Task Force [IETF], the only thing we ever really wanted was interoperability.

Ultimately, that very pressure—the “do the things at least talk to each other?” pressure—counteracts the monoculture pressure quite a lot. If we were to standardize—in the sort of physical, operational sense, not in the sense of the formal written standards—how things talk to each other, it doesn't matter what's at the other end. Furthermore, there are lots of suppliers who are much better off in a standardized situation than if the only way you can get two things to talk to each other is to buy them both from the same guy.

**McGraw:** Since we've already hopped into the way-back machine, I want to ask you about Project Athena [the MIT project referred to earlier]. How did that work influence your thinking about computer security?

**Geer:** Well, the wonderful thing about having been on Project Athena—besides the fact we were early enough that we could have all sorts of problems without someone else overtaking us from behind just because we were having them—was, because it was at MIT (our student body being what it was), if I wanted to test something, I could merely announce that it was impregnable, and testers would come out of the woodwork whether I wanted or not. People would show up—

**McGraw:** That happened to Larry [Ellison, Oracle's cofounder], too, when he said Oracle was unbreakable.

**Geer:** I don't think he was planning it as much as we were. We were doing it cold-heartedly.

**McGraw:** See, you did it first!

**Geer:** Yes, we did it first. But what it

did was to influence me on the idea that obscurity doesn't help. For example, we literally published the root password to all of our desktops to discourage people from thinking it was a challenge to break into them.

The password was worthless—“Mr. Root.” And it was roughly like if you've ever bought a small piece of consumer electronics, like a hairdryer, and it says right next to the Phillips head screws, “No user serviceable parts inside.” That's all we were trying to do, “Yeah, you can break this thing open. It won't do you any good, because you can just type the password. Help yourself.”

Instead, we put effort into recovery from whatever people did to the machines. There's a bank in New York—I can't name them, unfortunately, but I suspect they're not alone because the banks all copy each other—and they have decided that, from this point forward, none of their investment security will be around

2006  
**ISSE**  
INFORMATION SECURITY SOLUTIONS EUROPE

Rome, Italy 10 – 12 October 2006

The Independent European ICT Security Conference and Exhibition

## A thousand threats. Many Solutions. One Conference.

ISSE 2006 is the essential conference for anyone in the IT security arena, bringing together Europe's top ICT security experts, suppliers and implementers. We provide you with all the latest research, case studies and technologies to ensure you have security covered. What's more, our conference is totally independent, so you get the facts - **not a sales pitch.**

In three days you can choose from over 70 presentation sessions on all the hot topics in ICT security, including:

- Identity Management
  - Emerging Technologies
  - Trusted Computing
  - Security Management
  - Privacy and Data Protection...
- ...and many more.

### Programme Highlights



**Bruce Schneier**, Founder & CTO, Counterpane Internet Security Inc

Bruce is an internationally renowned security technologist and author. In his keynote he will explore why, fundamentally, security is all about economics and how changing economic incentives could do more to improve security than technology.



**Bart Preneel**, Professor, Katholieke University Leuven

Bart is a respected professor, consultant and expert in cryptography and information security. In the closing plenary he will look at recent developments in cryptography, how advanced cryptographic techniques can address trust, privacy and intelligence issues, and the impact of quantum cryptography and computing.

Organised by



Owned developed and run by



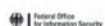
Programme compiled by



Hosted by



Supported by



To register for ISSE 2006 or for information: ● Visit: [www.eema.org/isse](http://www.eema.org/isse) ● Call: +44 1386 793 028 ● Email: [isse@eema.org](mailto:isse@eema.org)

## About Dan Geer



In addition to his duties at Verdasys, Dan Geer is also principal of Geer Risk Services. In past positions as a consultant and an officer in several startups, he has provided industry leaders with high-level strategies in all matters of digital security and in promising areas of security research. He is a widely noted author in scientific journals and the technology press, and has coauthored several books on risk management and information security. Geer has testified before the US Congress on multiple occasions and has served in formal advisory roles for the Federal Trade Commission, the National Research Council, and the National Institute of Justice.

Geer has an ScD in biostatistics from Harvard and an SB in electrical engineering from Massachusetts Institute of Technology (MIT). He holds several security patents and serves both fiduciary and nonfiduciary roles for several promising startups. He is also past president of the Usenix Association.

making failure less likely. All of it, instead, will be around making failure less meaningful. They, in other words, are going for mean time to repair equals zero rather than mean time between failure equals infinity.

**McGraw:** That reminds me of how we approach bank robbery today. Instead of trying to stop people from robbing the bank, we want to make sure that we catch them as soon as they do.

**Geer:** Sure, you give them a dye pack.

**McGraw:** Which is an interesting tactic. I suppose that it works somewhat.

**Geer:** You give them a dye pack, you record some serial numbers before they go out the door, you have a special bag of money for when the robber comes [...] something like that. That idea of suppressing mean time to failure and mean time between failure is important. But at some point, it becomes more cost effective to decrease mean time to repair. Availability is time between failures divided by the sum of time between failures and time to repair. You can get availability to one either by making the time between failures infinite or making the time to repair zero. Either way works.

**McGraw:** And we should be looking at both.

**Geer:** If you only handle one of them, you're missing the point. You're spending more money or you're underprotecting. Those are your choices.

**McGraw:** Recently, you've turned your attention to data security. I wanted to know why you think that's the next big thing.

**Geer:** Well, I can't be certain it's the next best thing, but like anybody else, I make bets from time to time. The bet here is based on two things: one, I think that corporate information is becoming more valuable, relatively speaking, than other things. Grace Hopper, for heaven's sakes—now we're talking 35 years ago, 40 years ago—said, "Someday, corporate balance sheets will list information because it is more valuable than the machines that contain it." I think that "someday" is now. If I steal a laptop out of your car, there is no company in the country that will be harmed by the cost of a stolen laptop. But there are an awful lot of companies, and you can read this in the newspaper everyday, that are harmed by the—"hmm, now, what was on that laptop again?" problem.

**McGraw:** Right, the example *du jour* is the VA [Veterans Administration], which lost millions of identities when a laptop was stolen in May 2006.

**Geer:** There's no shortage of proof that the value of information is rising faster than the value of the things wrapped around it—whether it's computers or companies or whatever.

**McGraw:** I think you once mentioned some striking figure about the growth of data over time.

**Geer:** That was the other thing I was going to say, actually. Don't get me wrong about this—this is a back-of-the-envelope rough estimation—but if you look at Moore's law, information has been doubling every 18 months. And horsepower per dollar, some say it's slowing down and some say it's not, but let's suppose it stays constant. That's an 18-month doubling in what you get for a dollar. Storage prices are doubling for what you get for a dollar faster than that—like every 12 months. And bandwidth prices, in the laboratory—not necessarily what you can buy from Verizon, but laboratory, anyway—are doubling every nine months or so.

If you get 18, 12, and 9 for doubling times, and you carry it 8, 10 years in advance, you do get two orders of magnitude for CPU power. But you get three for storage, and you get four for bandwidth. This tells me that there's no doubt the future is more data rich in terms of volume, and yet, despite that volume growth, these data are more in motion.

**McGraw:** That worries me a little bit because we already have trouble describing policy for data just sitting around. We're producing more and more in that sort of awful grid of access control stuff—our good old Bell and LaPadula model from 1973 just isn't going to work.

**Geer:** Look at the wonderful Web site that Hal Varian put together called, “How much Information 2003” [www2.sims.berkeley.edu/research/projects/how-much-info-2003/]. It hasn’t been updated in three years because Hal is now, I think, chief economist for Google. But, in any case, at that point, the estimate was total information produced per person on the planet—and we’re, of course, including a great number of people who live on a dollar a day—is 800 megabytes. If I’m right about doubling times, it’s way above that now. That’s an awful lot of information.

If I wanted to do something mean, if my job were to go cause some havoc, well, I’d write a little something or other that took Excel spreadsheets and fiddled a small number of the numbers in them by a little bit, all the time, forever, and passed it along to the next guy. Just a little bit here and there. Bit rot, if you want to call it that.

**McGraw:** Right.

**Geer:** Now, you tell me how long before, instead of 5,000 copies of the budget, you have 5,000 things—each of which is an approximation of an original file you no longer have—what will that do to you?

**McGraw:** Ouch.

**Geer:** I think, in other words, back to the point about why I am working on data security. I’m betting that the other problems (which are by no means solved) pale in comparison to the theft, misappropriation, poisoning, whatever term you want to use, around data, because our acquisition, retention, and processing of data continue to rise in amazing ways. When you really think about it historically, what other products doubled in their price performance every 18 months, much less 12 or nine? Nothing except computing. So let’s

assume for the moment that all of that value is now just as much at risk tomorrow as it is today. Just multiply this risk factor by the volume alone.

**McGraw:** One last question. You and I are probably the only two computer security guys who raise hogs. How many do you have going now?

**Geer:** At this very moment, none, because the smokehouse is full. □

*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.*

# 15 Years of BREAKING the rules... Now we're Finally MAKING the Rules!

Register by July 14 to save up to \$500  
Enter priority code D0118

**Join LinuxWorld** as we celebrate the 15th anniversary of Linux, and dive into the open technologies that have already evolved from a kernel to industrial-strength corporate applications—and are still transforming IT all these years later.

## Go Deep in 100+ Sessions on Key Linux and Open Source Topics

Discover the Full Power of Today's Linux Get the Skills, Solutions, and Insight Your Business Needs

- Iron-Clad Security for Open Environments
- Managing Mixed Environments
- Virtualization
- Scalable Open Source Applications
- Desktop and Mobile Linux
- Web Services and SOA
- VoIP
- And More

## Brainstorm with Top Open Source Experts including

- Alan Boda
- Fabrizio Capobianco
- Chris DiBona
- Scott Handy
- Greg Kroah-Hartman
- Eben Moglen
- Bernard Traversat

## KEYNOTE SPEAKERS

**Guru Vasudeva**  
**Lawrence Lessig**  
**Peter Levine**

**Greg Besio**  
**Richard Wirt**

Get complete details at [www.LinuxWorldExpo.com](http://www.LinuxWorldExpo.com)  
Register by July 14 with priority code D0118 and save up to \$500.



**Don't Miss the Biggest Linux Event Ever!**  
Hundreds of products, services, and training sessions all under one roof!

## OPEN. For Business.

### Check out the latest products and services from hundreds of key exhibitors

- AMD
- CA
- Dell
- EMC
- HP
- IBM
- Intel
- Novell
- Oracle
- Unisys
- VMware and more!

**Feed Your Mind** in Visionary Keynotes by Lawrence Lessig and other Linux and open source luminaries

**Feel the Energy** of a full slate of 15th Anniversary Events



Conference: August 14 – 17, 2006  
Expo: August 15 – 17, 2006  
Moscone Center, San Francisco

LinuxWorld is open to business professionals only. No one under 18 years of age will be admitted.

ORACLE NOVELL PLATINUM SPONSOR HP PLATINUM SPONSOR IBM PLATINUM SPONSOR PALMSOURCE An ACSIS Company PLATINUM SPONSOR COVERITY SILVER SPONSOR WYSE SILVER SPONSOR SAP SILVER SPONSOR SECURITY & PRIVACY MEDIA SPONSOR IDG WORLD EXPO

© 2006 IDG World Expo Corp. All rights reserved. LinuxWorld Conference & Expo, LinuxWorld and OpenSolutions World are trademarks of International Data Group, Inc. All other trademarks are property of their respective owners.

D0118



**\$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](http://www.computer.org/services/nonmem/spbnr)