

Interview

Silver Bullet Talks with Eugene Spafford

GARY MCGRAW
Cigital

Eugene Spafford is a professor of computer science at Purdue and the executive director of Purdue's Center for Education and Research in Information Assurance and Security (Cerias). Spafford's also an IEEE Fellow and has received several awards for his work, including the IEEE Computer Society Technical Achievement Award. He works to inject security reality into the commercial space, most notably through his work with Tripwire, the first free intrusion detection system distributed on the Internet, and his books, *Practical Unix and Internet Security* (O'Reilly & Associates, 2003) and *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats* (ITAA, 1989).

Featured here is an excerpt adapted from the full interview between Spafford and Silver Bullet host Gary McGraw. Their conversation ranged widely, from software testing to ethical hacking. 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 full series on iTunes.

Gary McGraw: Some of your really early academic work was on software testing. Then you moved into the security field,

which now seems to be catching on to testing. What role do you think software testing plays in computer security?

Eugene Spafford: I think it plays an important role, especially if you look at testing as a very broad concept—more than simply just testing the code but also testing its performance interrelated to other artifacts, testing user interface perceptions, and so on.

We use a lot of software that isn't developed carefully, and the tools and techniques and languages aren't necessarily the best for producing high-quality, robust software. Testing is a way for us to attempt to reduce some of the problems that may occur with it. It's a mechanism that's fairly well understood by people.

I don't think testing is going to go away any time soon. I think it does play an important role, especially when we start talking about porting software to new environments or new user populations.

McGraw: Testing, when considered from the software reliability or quality perspective, has a lot to teach security about how you might build an assurance case and what kind of testing is actually effective. Do you think that the security field is beginning to understand that there's a real academic underpinning for testing at all?

Spafford: There's not really a simple answer to that, unfortunately, because we have such a broad scope of development activity. We have people, for instance, who really do understand security and who use more formal development methods with well-designed specifications and tools, particularly if they're building embedded software or they're building for some, but not all, specially dedicated security applications or defense applications. On the other end of the spectrum, we have code that's put together by people who don't have much training in security, or in software engineering for that matter, in which they throw things together. It evolves over time. It has lots of patches. They're still somewhat blissfully unaware of good techniques to use.

The challenge with testing is in building testing software that can work on artifacts that might not have well-stated specifications and be used by people who might not have a lot of familiarity with good testing technologies.

The testing community has also traditionally developed testing against specifications to make sure that programs do what they're designed to do. In the security realm, what we want to test is making sure that a program doesn't do anything beyond what it's designed to do. That's a new area where much of the testing that goes on now has

About Eugene Spafford



Eugene Spafford is a professor of computer science at Purdue University, where he has served on the faculty since 1987. Spafford's current research interests are primarily in the areas of information security, computer crime investigation, and information ethics. He is also the executive director of Purdue's Center for Education and Research in Information Assurance and Security (Cerias).

He is also involved in several professional societies and activities, including serving on the Computing Research Association's board of directors and as chair of the ACM's US Public Policy Committee. From 2003 to 2005, Spafford was a member of the President's Information Technology Advisory Committee (PITAC), and he continues to serve as an advisor to

more than a dozen federal agencies and major corporations, including the United States' Federal Bureau of Investigation, Government Accountability Office, National Security Agency, and Air Force.

Spafford is a fellow and lifetime member of the ACM, a fellow of the American Association for the Advancement of Science (AAAS), a fellow of the IEEE, a life member of Sigma Xi, and a lifetime member of the Information Systems Security Association (ISSA), as well as a member of its Hall of Fame.

Spafford received a BA with a double major in mathematics and computer science from the State University College at Brockport in New York. He received his MS and PhD in information and computer science from the George Institute of Technology, where he was one of the original members of the Clouds distributed operating system design team.

ad hoc tests for—buffer overflows, for instance—

McGraw: Or maybe just fuzz testing.

Spafford: Yes, simple fuzz testing to see if a program gets an unexpected behavior for input that wasn't part of the specification, and that really is very immature technology overall. I think we have a long way to go both on testing and on development.

McGraw: I believe software security is, to some extent, a sexy subset of software behavior. Do you think that we're making progress on the software behavior front?

Spafford: Some. I actually think that security has more to it than that because we also have to look at human behavior and setting policy aspects. There are also issues of after-the-fact investigation, and privacy. That's part of the issue—we really don't have a good definition for boundaries. It's not clear that we need boundaries, although for those of us who are doing research, developing the tools, and teaching the practitioners, it's helpful to know how much we should be including. The field is still developing, and we're still learning.

McGraw: Computer security is a lot more commercial than it used to be. As an academic, what role do you think commercial certifications have in computer security, and do those certifications replace or obviate academic training?

Spafford: This again goes to the issue of what the scope of the field is. If we look at some of the certifications that are out there, there are two broad categories: the training certifications and the educational certifications—if you will, the professional certifications.

The training certifications are the ones that are offered by vendors and some of the specialized security training institutes, even by law enforcement agencies for those who are doing forensic investigation. Basically, those training certificates say that those individuals have been exposed to certain tools and technologies and know how to apply them to a given situation. We know of cases, certainly, where 110 percent of everybody who pays the fee gets the certificate.

There are other kinds of certifications. I would say that some academic degrees fall into this category as well, where hopefully the content is structured so that someone who gets through and

masters it can be said to actually understand some of the deeper relationships of the concepts and be able to apply them in new situations—take the abstractions and apply them to new tools and new problem sets.

There aren't a lot of those out there, but there are some, and some of the more advanced security management and auditing certifications seem to cover some of that territory. Again, as a really fast-evolving field, it's difficult to say what's fundamental and what isn't that people should be trained on. At one point, talking about programming flaws in Fortran and Cobol may have been central, and now not really quite so much.

McGraw: Right. It seems that there are two major clumps of security people in the world. There are practitioners who are focused on operations, such as the people who administer and set up and run all of the security apparatus including firewalls and antivirus, and then there are security engineers. It's not clear that they should really have the same sorts of certifications or background, frankly.

Spafford: That's correct. I don't know whether under operational

personnel you're also including the people who perform the audits for compliance and who do the investigations?

that they can't put all the funding and effort in at the backend when a problem occurs and fix it quickly. For instance, when the PITAC

McGraw: Do you think that the recent information warfare stories about the Russian script kiddies, Estonia, and the Chinese hackers getting into the Pentagon network will help?

In today's world—and this is perhaps why we don't see some urgency in some officials—the idea of an all-out world war ... is just inconceivable because our economies are so interlinked.

McGraw: That's a really good question, actually. Where do those people fall, in your opinion?

Spafford: I sort of actually see that as a third area of emerging specialization, that those individuals need to understand how the systems are constructed and interact, but don't necessarily need to have all the skills to build the systems themselves. They need to understand how those systems are supposed to be configured and behave, but don't necessarily need to know everything involved in running them.

In addition, however, when you have people who are doing compliance auditing and investigations for law enforcement or defense purposes, they need to have additional information about motives, laws, regulations, and so on. That really does seem to me to be an area that has emerged and is continuing to evolve as a third area.

McGraw: You've participated in several blue-ribbon panels. What happens with those reports once they're done?

Spafford: That's an issue that is frustrating for some of us who are in those groups. We're trying to come up with agendas that people can rally behind to make a difference, and it's very difficult because policymakers and people who control budgets don't seem to fully grasp both the magnitude of the problem that is building and the fact

[President's Information Technology Advisory Committee] report came out, it was presented to the Executive Office of the President. Members of the committee then went out and briefed officials associated with Congress—for instance, some executive agencies, some press, and so on—trying to build a certain level of awareness and concern that might translate into the development of some programs.

Unfortunately, it didn't. It generated some interest from a few places, but nobody in a position to actually affect policy really seemed to get it, and I don't know whether that's because they just didn't see it as a serious enough problem or maybe they thought it wasn't as pressing as other problems.

McGraw: Certainly, the US federal government has had a hard time getting its arms around cybersecurity and taking it seriously.

Spafford: It certainly has not been handled well, and if you look at some of the issues that are involved, there are almost two dozen agencies across government that have some role to play in this arena. They can't agree where the lines of demarcation are between them or who should be coordinating the efforts, or even who should be making the investments. Of course, that hinders our development of defenses, and as more systems get put into play, they're being put into play with weaknesses inherent in them.

Spafford: I have mixed feelings on this, in part because we don't know exactly the magnitude of what's really going on underneath the surface and therefore, what kind of threat picture this really poses for our various leaders. I think the trend, however, that is emerging should be raising some warning bells in government.

And that's because those [break-ins] are more economically motivated. We are familiar with the kinds of break-ins now that are occurring a lot on commercial systems—phishing, credit-card fraud, identity theft, and so on for consumers. Those are all obvious identity frauds.

But we're also seeing financial fraud—more organized crime attacking financial systems, for instance. Committing fraud on a large scale—some of the targets that I'm thinking of are attacks on inter-bank transfers, for instance, or large-scale counterfeiting or theft, draining of accounts. Money laundering is another big problem in support of other kinds of criminal activities such as narcotics trafficking or illegal gambling and moving the money from place to place.

McGraw: Online games, which I've been working on lately, are great ways to launder money.

Spafford: Yes. Those provide an amazing way for somebody who wants to transfer [money]. There's a third category, and you mentioned some of the stories that are appearing about the nation-state kind of activities. If you look at those, they have a very significant economic component. The Esto-

nia incidents shut down the banks and the commerce in the country for, in some cases, weeks—a huge financial hit on the country.

Those are some of the other things that we're seeing—nation-states being accused of espionage. It used to be, 20 years ago, that they were simply after military information. In today's world—and this is perhaps why we don't see some urgency in some officials—the idea of an all-out world war against some of these countries is just inconceivable because our economies are so interlinked.

From a nation-state perspective, coming in and stealing trade secret information, stealing competitive advantage, or sabotaging competitors for national industries amounts to huge differences for state-owned industries or large-scale companies that have a national interest. That appears to be one of the motives emerging from

the stories for why some of this is occurring. We know some countries have publicly declared that their state intelligence services are devoted to providing economic advantage to national industries.

McGraw: That changes the threat profile pretty significantly.

Spafford: It does. It's something that instead of being a military problem is still a national security problem, but it's also a huge economic problem that we're all facing.

McGraw: I want to change gears just a little bit. I wonder about the critical role that real exploit discussion plays in security. If designers and developers need to deeply understand exploits to avoid building broken systems, and people who do this illegally are considered criminals we don't want to talk to, how do we bal-

ance out these opposing views, or are they not really opposing?

Spafford: I don't think they're really opposing, and I believe that a lot of what's talked about in ethical hacking is a little bit overdone, in part because we failed to build the systems properly in the first place. How many times do you actually have to do a buffer overflow to understand how it works?

Certainly there's no reason for somebody to make their career to have to continually build toolkits and exploit buffer overflows. The fact that we haven't gone back and fixed the basic processes that cause these to occur is really the problem itself.

As long as we're faced with some of these badly constructed artifacts, then maybe it's a form of self-defense to make sure that some of the common problems aren't present. But I think too much weight

Workshop on Usable IT Security Management (USM) July 23, 2008 Carnegie Mellon University, Pittsburgh

Part of the Symposium on Usable Privacy and Security (SOUPS), USM '08 solicits research and position papers from academia and industry about *usability aspects of IT security management*. Building on the success of USM '07, the workshop will provide this time another opportunity for interdisciplinary researchers and practitioners to discuss this fascinating and important topic.

Those interested in presenting at the workshop should submit a research or position paper of up to six pages, along with a cover letter describing their research interests, experience, and background in the area of usable IT security management. Workshop papers will be posted on the SOUPS website and distributed to attendees on the SOUPS 2008 CD. However, workshop papers will not be formally published, and therefore may include work the authors plan to publish elsewhere.

Submissions are due April 13

<http://cups.cs.cmu.edu/soups/2008/usm.html>

is given to it as a matter of how are we going to understand security? Because understanding how to break something doesn't necessarily show you how to fix it.

McGraw: If you break something through blind, crazy, black-box testing or obvious testing, then you know that it's bad. If you don't break it through the same sort of obvious black-box testing, that doesn't mean that it's good.

Spafford: Exactly—well, it's also the case that if you break it, that doesn't provide a fix, necessarily. One of the problems that I have seen recently in some of the work I've been doing with large businesses and government agencies, is that they are simply getting hammered by the people who are publishing the exploits to the problems they find without really giving thought to the consequences.

Well, most aren't [careful] because most of the people who publish the exploits—you've got

two or three people working in a back room—their total experience is with a couple of PCs running Linux or Windows on a desktop. But when you're looking at an agency, like a large bank or the US Air Force, they're running tens of thousands of machines using legacy applications in critical day-to-day environments. They can't roll out a patch even as fast as what a vendor puts in place. They're stuck. And so what's happening is they're being endangered on a regular basis by these people who are supposedly showing all of us where the problems are and how to fix them. And so this whole idea of breaking systems as a way of protecting them really has a number of flaws to it, and those are just a couple of them.

McGraw: Nevertheless, we do really need to talk about exploits and how they really work—not necessarily to “out” vendors or to get people in operational trouble, but just to understand the nature of real exploits.

Spafford: Exactly, and we do need to do that. We do need to document. But more than simply then publishing exploits or particular patches—and this is where the research aspect comes in and the responsible part—is stepping back and saying, “Well, where did the processes go wrong so another buffer overflow got into place? What's a generic construct that we can use to avoid these in the future? Such as, for instance, getting away from the C-language family and using something else.”

I actually believe that part of this has to do with the nature of how we think about our field; in general, how we talk about computer science and engineering. We have many people who view it as a scientific pursuit where there is a correct approach. In fact, many are trained to have the attitude that if

they go in and use the mechanisms they've been taught, what they'll produce is a correct artifact.

In fact, it is an engineering approach where because of factors that we don't think about, because of flaws in some of the tools we use and mistakes of the people involved, there are going to be flaws, and we haven't built the artifacts with that assumption in mind.

McGraw: We've got to revisit those basic assumptions.

Spafford: We really do, I think, have to revisit our whole attitude of how we build systems, to build compensating correction and detection into them as we go along.

McGraw: Do you think that modern social networks like MySpace and Facebook in any way replace the early Usenet newsgroups?

Spafford: I think they're manifestations of the same basic idea, which is to share things that we find interesting with like-minded individuals, whether they're mailing lists, newsgroups, or going way back, things like MUDs [multi-user dungeon, domain or dimension computer games] and BBS [bulletin board system]. You know, instead of MUDs now, we've got Second Life.

McGraw: Actually, instead of MUDs, now we have World of Warcraft.

Spafford: Yes, and who knows what we'll have next, but I don't see those being significantly different from each other.

McGraw: One last question, which is completely off topic, but who has influenced your career the most?

Spafford: I don't think I could either pin the blame or the credit on

www.computer.org/security/podcasts

The Silver
Bullet
Security
Podcast
with Gary McGraw



Check out a free series of interviews with host Gary McGraw, featuring in-depth interviews with security gurus, including Avi Rubin of Johns Hopkins & Bruce Schneier of Counterpane Internet Security!

Sponsored by *Cigital* and
IEEE Security & Privacy

Stream it online
or download
to your iPod...

any individual because there are so many. My interests really, looking back and even looking forward, don't fit in any one particular niche that somebody has had.

Recently, I was talking with a couple of friends of mine. My father passed away this summer, and I was thinking one of the things that he and my mother both greatly impressed on me was that whatever I did with science and technology, I should keep in mind that people were at the other end, and that the one thing that I couldn't create for myself, that other people had to bestow, is respect and trust—well, that's two things that they have to bestow—those are not things you can manufacture.

So those have guided me a lot in some of the things I've done, generically. If you look at the technology, I've picked up bits and pieces in software engineer-

ing from a variety of people, in security from a variety of people. I think of three people that have set examples for me. Peter Neumann, both in security and in reliability.

McGraw: A past Silver Bullet victim [www.computer.org/security/podcasts; www.cigital.com/silverbullet/show-014/].

Spafford: A great interview and just a wonderful thinker. He's done so much for the field. Another in security from the business side who has impressed a lot of thinking about the business processes, William Hugh Murray, and I don't know how many people in the academic side are familiar with his work. And Peter Denning. Many of the things that he wrote and did in talking about the nature of the profession have had a big influence on me.

You can find additional podcasts in the series, including those featuring Mikko Hypponen and Markus Jakobsson, 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 corporations 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.

14th New Security Paradigms Workshop



September 22-25, 2008

Lake Tahoe, California

NSPW welcomes papers that present a significant shift in thinking about difficult security issues, build on such a recent shift, offer a contrarian view of accepted practice or policy, or address non-technological aspects of security. Our program committee particularly looks for new approaches to information security, early thinking on new topics, innovative solutions to long-time problems, and controversial issues that might not be accepted at other conferences but merit a hearing. We discourage papers that represent completed or established works, or offer incremental improvements to well-established models. NSPW expects a high level of scholarship from contributors.

NSPW is unique in format and highly interactive in nature. Each paper is typically the focus of one hour of presentation and discussion. The resulting intensive brainstorming has proven to be an excellent medium for furthering the development of the paper ideas. The proceedings, which are published after the workshop, have consistently benefited from the inclusion of workshop feedback.

Important Dates

Submissions: April 11

Notifications: June 3

for more information

www.nspw.org



\$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