

Interview

Silver Bullet Talks with Gary McGraw

JAMES MCGOVERN

The Hartford Financial Services Group

James McGovern, an enterprise architect at The Hartford Financial Services Group, turns the tables and interviews Silver Bullet host Gary McGraw in this third-anniversary issue. The full interview is available at www.computer.org/security/podcasts or www.cigital.com/silverbullet.

James McGovern: Cigital and Fortify have partnered to release the Building Security and Maturity Model [www.bsi-mm.com], which outlines the practices and approaches of enterprises that actually have a clue in making their security posture better. Could you describe some of the human aspects that the leaders of these organizations have, such as their backgrounds, business verticals, their personalities—those types of characteristics?

Gary McGraw: One of the interesting things about this work was, it struck us to study real software security initiatives that are under way and have been for awhile. As you might imagine, many of the people running some of these initiatives are friends of mine because we all work in the same discipline.

Of the 35 programs that we're

aware of, we picked what we considered the top nine and called the people running them and said, "Hey, you guys want to do some science?" We all laughed about it being like anthropology, and everyone agreed to help.

The backgrounds of these guys vary pretty widely. Steve Lipner has been doing computer security for almost as long as I've been alive. He worked in the early days on firewalls and network security and helped to stand up Microsoft's vulnerability response center. Then he moved into software security from there and has been instrumental in getting the Trustworthy Computing Initiative at Microsoft to be useful.

On the other hand, Brad Arkin, who is running the program at Adobe, was one of my guys. In 1997, he helped form the Software Security Group with me at Cigital. I have a really different relationship with both of those guys. They're both very committed professionals and really interested in causing software security to occur.

Jim Routh, whom you might know from The Depository Trust and Clearing Corporation (DTCC), is sort of a quintessential New York executive. He's very savvy politically and understands how to position software security as a money thing. He is very good at publicity and not only that, runs one heck of a software security program.

These guys all have fairly diverse backgrounds, and the cool thing is, they're all willing to talk about what they're doing. That was the most exciting part of this project. We weren't sure what we were getting into when everybody agreed to do the interviews. Everyone was forthcoming, and building the model was exciting because we had all this real data to work on.

McGovern: Sometimes in large enterprises, working on security agendas is somewhat of a thankless job in that there's always a desire for people to leave and start consulting because it's a little bit more lucrative. What are these guys doing to keep top talent on staff so they can sustain their software security programs?

McGraw: Two things about software security that's naturally appealing is it's an intellectual challenge and it's an awful lot of fun. It's not a domain that's stagnating or is boring or where you end up doing the same thing every day, all day. Instead, trying to figure out how to teach, say, tens of thousands of developers in some situations, or maybe hundreds in smaller initiatives, is something that's really fun.

It takes a combination of skills. You have to have the right kinds of technical skills to be able to pull

About Gary McGraw and James McGovern

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.

James McGovern is an enterprise architect for The Hartford Financial Services Group. He is coauthor of *Java Web Services Architecture* (Morgan Kaufmann, 2003), *A Practical Guide to Enterprise Architecture* (Prentice Hall, 2003), and *J2EE Bible* (Wiley, 2003). McGovern is a member of the Java Community Process, and is currently working on Performance Metric Instrumentation (JSR 138) specification. He is also a member of the Worldwide Institute of Software Architects, and holds industry certifications from Microsoft, Cisco, and Sun.

off code review in various different languages. You have to have the capability to talk to, understand, and work with enterprise architects, which can be a real challenge. You have to have the capability to move up the food chain and justify what you do. And the natural coolness factor of software security might be one of the things that these guys use to help them retain their top talent.

I'm a consultant, and I have the same issue. Frankly, over the years, I've mentored and trained a whole slew of people, many of whom ran out and started their own companies. That was fine with me because it's kind of like seeding the world with this software security idea. If you understand that the world is a small place and people are going to have their own career paths and they're going to follow their own way, and you understand that that's good and you work with that, it can actually turn out to be a benefit in the long run.

McGovern: Many enterprises are now outsourcing or offshoring software development. What are the challenges in terms of having a software security practice?

McGraw: One of the challenges is that many of the people who decided to offshore to India couldn't even outsource to downstairs before they got started. They just added a 2,000-mile problem to their inability to set clear require-

ments and acceptance criteria.

Those two factors are very helpful. But really, I think outsourcing and looking at outsourcing in particular as its own thing is almost xenophobic. The real problem is "other people's code." If you consume COTS [commercial off-the-shelf] code or you buy software from vendors or you cause other people to write software for you, you have the same problem: How do I know I can trust it? What sorts of testing should I do before I accept it? How should I bind it from a legal perspective?

We touch on some of these activities in the BSIMM, and there are some leaders in the space. Jim Routh, whom I mentioned before, is a guy who I would certainly turn to to talk about how he's controlling his vendors because I think he's kind of a bellwether for things to come.

McGovern: Many organizations no longer budget for developer tools. We get tools like Eclipse and those types of things for free. Do you think static analysis will fail because no one's funding developer tools?

McGraw: Well, so far, there's been no evidence of that from the market. In tracking the software security space, I can tell you that the 2008 numbers show roughly a 40 percent growth in source code analysis tools, and roughly a 30 or 32 percent growth in black-box

testing tools, which are mostly around the Web.

This means that the intuition that there's no budget must not apply to everybody because somebody's paying for these tools. We're talking about a market in the source code analysis space that easily accounted for maybe \$200 million of the \$500 million software security space. I think that it's continuing to grow.

Now, you did mention Eclipse, and that's worth pursuing a little bit. They give away IDEs [integrated development environments] for free, and it's very clear to me, John Steven [Cigital], and others that many of the techniques and scanning attempts that these source code analysis tools do could in fact be encapsulated by the IDE. The editor should notice when you're typing a stupid function and tell you why not to do that.

What it won't be able to do is multipass compilation, dataflow analysis type stuff, which these tools are beginning to do a little bit better. Some of the really easy stuff is going to be just taken over by the IDE. We will know that source code analysis has arrived as soon as the big players get serious about it. (By big players I mean IBM and HP.)

McGovern: Many CIOs and business executives like the concept of metrics. What metrics should people be thinking about related to software security?

McGraw: We have an unfortunate result to describe to the world coming out of the BSIMM study and that is that everybody agrees metrics are important and not only that, all of the nine that we studied use metrics. They all have their own great metrics, and they think the metrics are a key part of their program.

The problem is that all of the metrics are directly tied to the culture of the organization that's using them. So it's very hard to take an idea for a measurement in one organization and transplant it to another. I kind of liken it to organ transplant: chances of rejection by the host are high.

This means that it's more of a challenge than, say, people who participate in the security metrics list or even Andrew Jaquith [*Security Metrics*, 2007, Addison Wesley] himself might have thought in the beginning. What we've come to in the BSIMM is, "Hey, let's just look at activities and let's do some measurement of activities and not try to measure the resulting software to see whether or not it's secure." Now, that's a problem with our science because we can say these organizations that appear to be building better software are doing the following activities, but we can't say for certain that it is in fact resulting in more secure software in any objective fashion because there just simply aren't any metrics.

The silly metrics that we all talk about such as defect density per Kloc (1,000 lines of code) and stuff like that are not very useful at measuring actual software secu-

urity. They're just sort of indicators. It'd be like figuring out how your car's doing by looking only at the temperature gauge.

We have that challenge to face. We think that the notion of publishing a BSIMM yardstick and having people apply it all over the place is going to be very helpful from a metrics perspective, and we hold out great hope that that will actually happen.

McGovern: In today's current economic climate, budgets are under pressure. If you had to focus on software security with all things being important, how would you determine what's more important between buying a static analysis tool, doing log management, federated identity, entitlements management? How would you guide an IT executive to make that trade-off?

McGraw: Well, the answer is always going to be dependent on the organization. I hate to be slippery, and I don't mean to be slippery, but I think that's the real answer.

For example, among the nine, one of the cultures that we studied is very much code-driven. It's a bunch of Unix hackers who are C kernel guys and amazingly great coders. If you want to approach software security with them, it had better be about the code.

On the other hand, there are organizations that have regulatory compliance issues, and they need to think about other aspects of software security, so a code-centric approach might not work as well in their culture.

You have to look at the situation and figure out what is going to benefit you the most. That's why consultants like us get paid money to do that sort of thing because it turns out that there isn't really an obvious answer for everyone.

McGovern: To become a competent software security professional, what do you think the ideal career path looks like? For example, give us the three lines that we need to tell our enterprise HR departments.

McGraw: Must be a coder.

That's the only line, really. Then we can teach them everything else. I think the notion of starting with people who are very steeped in software development is the only way to go. There are some people like me who have been coding since they were 15 and maybe don't code every day now, but we're software guys. Those people, in my experience, make the best software security people if they also have kind of a twisted, evil mind and can think like a bad guy. You need to look for that, too.

If I had to choose one over the other, I would certainly choose software smarts over malicious mental capabilities.

You can find additional podcasts in this series, including those featuring Daniel Suarez, Bill Brenner, and Laurie Williams, at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/. For a full transcript of this particular podcast, see <http://www2.computer.org/cms/Computer.org/dl/mags/sp/2009/03/extras/msp2009030008s.pdf>. □

James McGovern is an enterprise architect for The Hartford Financial Services Group. Contact him at james.mcgovern@thehartford.com.

IEEE Computer Society Members

SAVE 25%

on all conferences sponsored by
the IEEE Computer Society

www.computer.org/join

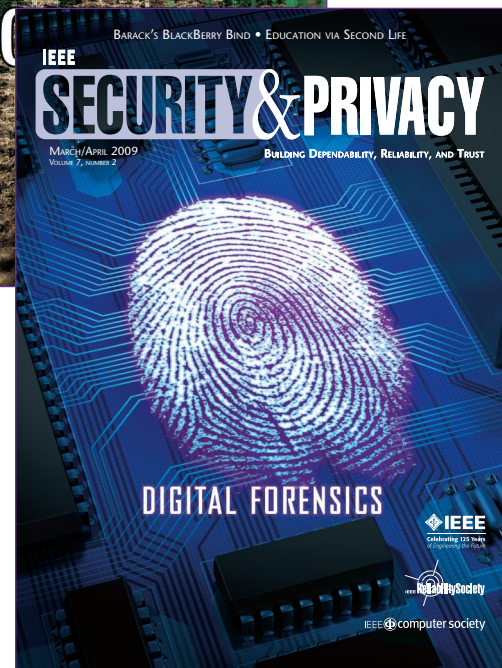
Nonmember rate of \$32 for *S&P* magazine!

IEEE Security & Privacy is
THE premier magazine
for security professionals.

Top security professionals
in the field share information
on which you can rely:

- Silver Bullet podcasts and interviews
- Intellectual Property Protection & Piracy
- Designing for Infrastructure Security
- Privacy Issues
- Legal Issues & Cybercrime
- Digital Rights Management
- The Security Profession

Visit our Web site
at www.computer.org/security/



Subscribe now!

www.computer.org/services/nonmem/spbnr