

Interview

Silver Bullet Talks with Gunnar Peterson

GARY MCGRAW
Cigital

Gunnar Peterson is a software security expert and a managing principal at Arctec Group, a Minneapolis-based consulting firm. His work centers around service-oriented architecture (SOA), Web 2.0, and other distributed systems. Peterson's blog, <http://1raindrop.typepad.com>, is devoted to topics in software security. He also edits *IEEE Security & Privacy* magazine's Building Security In column with John Steven and Deborah Frincke.

Gary McGraw: We'll start with a deceptively easy question: What is security?

Gunnar Peterson: That is a deceptively easy question. From a technical perspective, I guess we've all been trained by Dan Geer to say that security is really risk management—we want to enable businesses to do what they want to do, but we don't want to spend \$11.00 to protect something that's worth \$10.00. Although we don't want to spend too much on security, we want to make sure we're spending security dollars in the right place. I would say that security—like Dan said in his famous speech 10 years ago—is about risk management, and that perfect security, especially in enterprise security, is never go-

ing to exist, but we can certainly strive toward making systems more robust and resilient.

McGraw: A lot of people in your particular subdomain—SOA and Web 2.0—think of security as a set of features or functions or a thing. What is wrong with approaching security that way?

Peterson: Well, what's wrong with that is that security isn't something that is done in a point scenario. It's something that's at a system-level property, typically. You have customer data that's in a bunch of databases and mainframes and ERP [enterprise resource planning] systems, but you have to protect it from an end-to-end standpoint—all the different places it traverses because it leaves any individual given policy domain pretty quickly, especially in the world of SOA, where the whole goal is to integrate across silos.

The problem with approaching security as a set of features is that you miss that end-to-end context, and if you have a red security domain and a blue security domain, you very quickly have something that becomes purple at runtime, and that's a bad thing.

McGraw: We all know purple is bad.

Peterson: Yes, the anti-purple security model. When you pack-

age everything up and engineer it down to the point where it's ready to be deployed, it may look like a feature that you want to build into the system from a developer viewpoint. But the thinking—the logical design thinking—has to extend beyond just a feature-by-feature standpoint; you have to look at it from a system view.

McGraw: You've been working for many years with Web-based systems, and you've developed your brand around SOA and Web 2.0. How are things going in the Web 2.0 security space?

Peterson: I tend to see them as different spaces, although that might be because I'm too close to it to think of them as the same thing from a larger industry standpoint.

The SOA folks tend to be more of the enterprise folks—more the Fortune 500 people who probably think that a combination of things they can buy from vendors like IBM, Oracle, and Microsoft can solve their problems. I'm not throwing those companies under the bus; I'm just saying that it's more of an enterprise mindset. Something you buy or consulting services you buy to solve your problem would be sort of how I'd characterize the SOA space. Not that there aren't lots of individuals at these big companies doing really

About Gunnar Peterson



Gunnar Peterson is a founder and managing principal at Arctec Group, which supports clients in strategic technology decision-making and architecture. His work focuses on distributed systems security architecture, design, process, and delivery.

impressive things.

Web 2.0 is more of a bottom-up, grassroots movement. In that case, I think people are more into writing the code. Certainly, I don't think people assume going in that they're going to buy a Web 2.0 solution from IBM, whereas you can go to IBM and buy three different enterprise service buses to build out your SOA. I think it's a different starting point.

McGraw: Explain what's going on in each of those places with security.

Peterson: I think—and maybe this is where your question is leading—a lot of the problems you end up having to solve are pretty much the same—even though the starting points are different. A lot of the tough problems to solve revolve around wanting to integrate data. In a SOA world, we're going to put stuff on SOAP Web services and into XML documents, we're going to route them around on an enterprise service bus, and hook SAP, Siebel, and PeopleSoft and all these wonderful back-end systems together. In the Web 2.0 world, we're going to have mashups—data coming from all kinds of different places—and we're going to mash them up in a nice little Ajax screen inside of a browser, which will all work together at runtime.

McGraw: It sounds like lots of data exposure no matter which way you slice it.

Peterson: Yes, but I think the subtle differences are that in the Web 2.0 world, the mashup is really governed by what users want. So, "How do I want my Google Finance page to look?" or something like that. Whereas in a SOA case, we may have a SOA behind our Web 2.0, but the SOA case is really driven by business process. Company A bought Company B, and they really need their claims systems or mortgage processing systems to work together. The unifying construct there is probably more like a business document or business process. But at the end of the day, you've got different policy domains, different data owners, and different technologies, so there's sort of this missing security construct, which is how do we do security at a message/document level through XML security or something like that.

McGraw: In the early days of SOA, the idea was to use the WS GLOB-* functionality, which harkens back to my earlier question. Is security a thing? Because that seems to be implicitly saying yes.

Peterson: I tend to think of security as a set of services, and that set of services is some kind of mix of what Butler Lampson calls the gold standard of information security: authentication, authorization, and auditing. It's called the gold standard because they all start with "A-u." Little periodic table of elements humor there for you.

McGraw: We're all groaning over that one.

Peterson: You're sort of delivering something along those lines or something along the lines of confidentiality, integrity, and availability—the classic CIA view of the world.

The idea would be that the message that's traversing those

policy domains would give you the primitives [so] that you could make an authentication and an authorization decision, that it would have some level of confidentiality and integrity to protect it when it traverses those policy domains. The key thing that we think about in these domains and with these technologies that's different from the classic role-based access control world is in a classic role-based access control world, we would assume we have control of the subject, the object, and the session, and so we really own both ends of the pipe. We own the session; we know the role of the person or the organization that's playing.

In a SOA especially, and also in the Web 2.0 world, we probably know almost none of those things, and yet we still have to make these security decisions. What WS-Star*, WS-security, and SAML [Security Assertion Markup Language], which is another spec, do is they don't make decisions like that; they give you primitives to help you make those decisions, and they package them up in something called a claim. A claim is a way to attach a token to a message, and then that claim actually has to be evaluated on the endpoint.

It's not this Newtonian universe of role-based access control, where I have this one concept of time, and time is always going to be set to X. It's much more of an Einstein universe view of the world, where I'm going to make a claim about a message, and then you are going to have to evaluate it locally and decide what you want to do with it.

McGraw: Security people whine that we haven't even secured Web 1.0 applications yet, and now we're moving on to Web 3.0. Do you think we're doing anything right? Are we moving forward?

Peterson: That's a good question. I

would be in the group that whines that we haven't solved the Web 1.0 problems whatsoever. Look at the OWASP [Open Web Application Security Project] guide (around 300 pages) and see how much of that is actually being implemented in the real world, and it tells you all you need to know about the gaps in Web 1.0. The problems we've been describing here become much worse when you mix the red policy domain with the blue policy domain.

McGraw: Ugh, there's that purple again.

Peterson: The one thing that WS-Star[★] and SAML have given us is a set of security mechanisms and standards that work at the data level. From that standpoint—capability-wise—we're beyond where we were. It still needs to be baked into the infrastructure, so really good support for WS-Security and a lot of the standards build on top of that. In WebSphere—if you want to look at IBM as the bellwether of the industry, which probably is about as good a fulcrum as we have—that really came with this WebSphere 6.1.1 Web services feature pack, which isn't that old; I think it's a year old or even less. This stuff still has to get baked into the infrastructure, developers need to be trained, and architects need to think about things beyond just saying, “You know, we're inside the firewall, so we're cool,” for it all really to work.

There's this notion of a race against whatever the attacker community keeps coming up with, but the ability to apply security at a data level is going to be fundamental to solving any of these problems.

McGraw: Part of the answer there is federated identity.

Peterson: Federated identity would be another building block, and in the simplest way, being able to port

identity assertions from the red domain to the blue domain without it ever becoming purple would be the goal there.

McGraw: We're slamming purple today!

Peterson: Since we have no visual aids, I thought I'd use as many colors as possible.

McGraw: Explain very briefly what the idea behind federated identity is and why it matters.

Peterson: The biggest single reason why it matters is it's a technical solution that maps directly to the way almost every single business actually does business in the real world. As opposed to a 100-page policy on authentication and authorization that leads you down a rabbit hole that says you need to own the subject, object, and session, the federated identity approach says that it's the relationship between an identity provider and a service provider. We have a way—through message-level security—to sign and encrypt our credentials, pass them across a potentially untrusted system, and do business together. That's how your mortgage gets processed, that's why you can use an ATM machine in the Bahamas or in Norway, and your bank knows how much to take out.

There has to be a way for all of these pieces to work together, and there has to be some level of confidence in the system, and the best thing about it is that it gets us out of this business of having people randomly go into Web browsers and type the username and password into something that's going to traverse an untrusted system.

McGraw: Who's leading in terms of vendors or technology stacks?

Peterson: From a big company standpoint, Microsoft, through

Kim Cameron's work with the IdentityBlog. The Laws of Identity [www.identityblog.com/?p=352/#lawsofiden_topic3], and defining the identity metasystem, clearly has been the leader. When I picked up the *Linux Journal* about two years ago and saw the face of Microsoft's chief architect for identity on the cover, I almost fell over. It was a real watershed moment in terms of standard support openly embracing Java and PHP and implementations of these identity technologies, and recognizing that the only way federation will work is if all of these parties are able to interoperate.

From a small company standpoint, Ping Identity is another company that I've worked with a number of times that's really leading the charge in terms of innovation: ways to really push these technologies, make them simpler and easier to use, and be able to deploy this stuff really quickly, which I would not underestimate, in any of these new technologies, some of the engineering work that needs to go into them.

McGraw: What worries me is that it's all built on top of the Bell-LaPadula concept of a matrix. The matrix is so big that even if you federate it with everybody, it just gets bigger. Is there an alternative?

Peterson: The really valuable thing that they've done is they've separated the authentication logic from the authorization logic, and while this could easily manifest itself in very complex matrices, it buys you a lot of architectural benefits, not the least of which is being able to authenticate locally, say, on a laptop, and then do your authorization somewhere closer to the mainframe or the resource side.

The other thing that it buys you is it doesn't necessarily require that you use any specific model—although people frequently do—

but in the simplest case, it can be just agreeing on a simple attribute—name-value pair. That allows you quite a lot of flexibility to invent or use whatever access control model; if you like [the] Clark-Wilson [model] better, then here are your attributes to do that on the authorization side, and have a nice day.

McGraw: You've been applying these ideas in the field with large enterprises for many years. What kind of advice do you have for technical software security types who want to become consultants?

Peterson: It's always easier if you understand where you're starting from, so if you're starting from the software side, you need to learn a lot about security; if you're starting from the security side, you have to learn a mountain of stuff about software. In fact, it's easier to come from the software side, which is where I came from, and learn what you need to know about security.

The single best consulting book I've ever read is Gerald Weinberg's *Secrets of Consulting: A Guide to Giving and Getting Advice Successfully* (1986, Dorset House). It's a lot of very homespun wisdom, and it just comes down to listening to your clients and really putting yourself in their shoes. The people I learn the most from are the people in the trenches that are the ones holding the flaming bag.

McGraw: That doesn't sound like a good thing to hold.

Peterson: Well, it's not. Let's say you're an architect at a big company. You've been working there 10 years, you've got a good reputation, you've deployed a lot of stuff, and then one day someone says, "You own the software security problem. Go fix this. Here are 5,000 applications." The first thing I'd do is have them read Ross Anderson's book, read your books, and go

from there. At the same time, they have to craft some kind of message to the thousands of developers, and it better work, and it better not cost the company an arm and a leg, and so on. It's a daunting challenge, and I always try as a consultant to put myself in the shoes of the person who has to carry out these things. The one-word answer to your question is, "Try to find some solution that's cost-effective."

McGraw: That was a lot of words for one word.

Peterson: That's a one-word answer. That's why I'm a consultant.

McGraw: You're going to Metricon again. I was just at SIFMA [Securities Industry and Financial Markets Association] in New York and talked to Phil Venables [CISO at Goldman Sachs] and Robert Vitali [CISO at Morgan Stanley] about metrics. They've given up on financial measures outside of high/medium/low risk and are more focused on measuring controls. Have you seen any evidence of that in the Metricon group?

Peterson: It's a pretty big area, so any evidence is pretty large, but I can't think of one that comes leaping to mind. There was a big study just done at Verizon, which actually is much more in the pro-control space, although against patching, and it's quite an interesting study to read. I use metrics in a couple of different ways. In general, I like to put a number on anything I can; that turns out to be hard to do in a lot of areas.

McGraw: If you put one very large number, it takes care of all the possible information. Just put pi on there, and it's all good.

Peterson: Usually when you start down the road of software security, a lot of companies are either in

phase 1 or phase 2 of doing a lot of these things. Especially outside of the financial services world, they're not necessarily at phase 7 or 8 of the software security road to nirvana.

A lot of the questions are, "Where do we start?" Pete Lindstrom [Spire Security] told me a long time ago that an asset is worth no less than what you pay to own, operate, and maintain it. I like those numbers to break down the big projects in the company, and it may be fairly simplistic, but to understand where the IT budget is going—forgetting about security—and trying to align your security money spent with where IT is spending its money, and where the business is investing.

Granted, an asset is hopefully worth more than what you spend on it, if you're a business and you like making profits, but at least it gives you a floor value that says it's worth no less than this. It's quite interesting to break down the budgets of what companies spend on their network—writing checks to Cisco and so on—what they spend on their host, what they spend on applications, and what they spend on data. They typically spend the most on applications, but if you look at the security budget, they typically spend the most on network security and among the least on application security.

McGraw: That seems upside down.

Peterson: The conclusion is that the people in the People's Republic of IT Security are possibly way smarter than the business, or the other possible conclusion is that IT security is just totally out of whack and strategically misaligned with where the business is going. I don't necessarily say that you should spend a dollar-for-dollar level of prioritization to what the business does, but in terms of risk management and focusing security around assets, you want to

be aligned/prioritized the same way as the business so that you're spending most of your money on software security.

McGraw: The financial sector has really come around to that thinking already, but many of them are on step 7, and so we have some more evangelism to do in the rest of the community.

Peterson: Yes, and the paths diverge at a certain point. I'm out here in Minneapolis, and we have a couple of big banks here, but I spend a lot of time with insurance companies, manufacturers, and nonfinancial services companies, and at a certain point, they can learn a lot from what the financial services people are doing. But at a certain point, the paths to software security nirvana diverge because in financial services, you find very hard edges around certain parts of their businesses, particularly around transactional systems and so on.

McGraw: Because they're regulated.

Peterson: And because the business hasn't changed for a long time. Then you go to something like insurance, and the entire business is exception processing, and all of the boundaries are blurred. That's partially why you might see role-based access-control-type thinking more prevalent in financial services and probably why it won't work as well outside of financial services. For the 450 out of the Fortune 500 that are not in financial services, what kind of architectures will they drive?

I have had this conversation with a number of software security vendors in the space, saying, "You know, what got you to this point in maturity of the industry isn't going to get you there." You can't take the exact same model that a big bank uses and plunk it down at a big insurance company. Yes,

they're both US\$70 billion companies, but they're set up differently.

McGraw: An off-the-wall question: as a fly fisherman, how do you feel about wormers?

Peterson: I like fly fishing. I'm not going to throw stones against the wormer people as long as they don't make big splashes and scare all the trout away and things like that.

McGraw: How about those of us who prefer to fish with explosives?

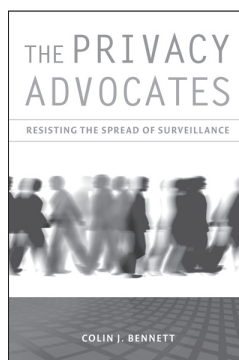
Peterson: That I would have a problem with. The availability of my fishing resource starts to dwindle pretty quickly.

McGraw: Yes, but instant gratification is a good thing! One boom, many bodies.

Peterson: Well, I think the quote I like is, "Calling fly fishing a hobby is like calling brain surgery a day job."

You can find additional podcasts in the series, including those featuring Jeremiah Grossman, Laurie Williams, and Bill Brenner, 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. Contact him at gem@cigital.com.

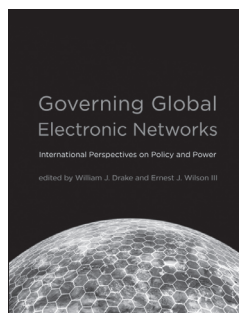


The Privacy Advocates

Resisting the Spread of Surveillance
Colin J. Bennett

"A thoroughly researched, well structured, and highly readable account of the persons and groups behind the 'privacy movements,' their motivations, strategies, and the conflicts they encounter—this book completes the highly acclaimed, groundbreaking work on the political analysis of regulating privacy."
—Herbert Burkert, University of St.Gallen, Switzerland

296 pp., 11 illus., \$28 cloth



Governing Global Electronic Networks

International Perspectives
on Policy and Power

edited by William J. Drake
and Ernest J. Wilson III

Experts analyze the global governance of electronic networks, emphasizing international power dynamics and the concerns of nondominant actors.

Information Revolution and Global Politics series
720 pp., 10 illus., \$50 cloth



The MIT Press Computer
and Information Science Library
<http://cisnet.mit.edu>

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

