

Interview

Silver Bullet Talks with Christofer Hoff

GARY MCGRAW
Cigital

Christofer Hoff is the director of cloud and virtualizations solutions at Cisco. He has also been a chief security architect at Unisys, a chief architect, a CSO, and a CTO. Hoff has a well-trafficked blog at www.rational survivability.com/blog.

Gary McGraw: At RSA 2009, the number one buzz word was “cloud” and “cloud security.” Pinning down cloud computing and cloud security by attending that show is kind of like trying to nail fog. So, what is cloud computing anyway?

Christofer Hoff: Well, there’s fog and then there’s my favorite analogy of the “goat rodeo,” but I think they’re both relatively accurate. It’s very interesting that this question comes up so many times, and I’ve rehearsed the answer depending on the audience. What I’ve kind of arrived at is that there are two very interesting perspectives to take when answering that question: one from the providers’ perspective—the vendor community, those that offer cloud services—and then one from the consumers’ perspective.

From the perspective of a consumer, anything—any service, any company, any vendor, any technology that would otherwise al-

low them to take their content and their data and place it in the stewardship of somebody else—these days is called “cloud.” So, from the consumers’ perspective, that’s Mobile Me, it’s iTunes, it could even be the Sidekick data storage story that we saw a week ago (in terms of failure).

McGraw: Isn’t it data “loss-age” that they’re doing?

Hoff: Data loss-age, yes.

McGraw: We’ll lose your data forever! <laughs>

Hoff: That’s right—guaranteed for only \$20 a month.

But the point is, from [the consumers’] perspective, anything you ultimately connect to—usually using the Internet—is “cloud based.”

On the vendors’ side, we apply all sorts of rules and logic that says, ‘Well, that’s really not cloud because it doesn’t satisfy certain basic tenants—for example, it doesn’t have elasticity, it doesn’t have self-service, there’s no dynamism ...’

So, there’s the technical answer and there’s the non-technical answer. I think they’re both right in terms of qualification. But to me, cloud is an operational model. It’s a way of more efficiently and more effectively using computing resources managed by you or managed by somebody else. Essentially

it stems from the ability to utilize our computing resources more efficiently and, in some cases, use a pay-for-use model to do so. It’s also a fantastic set of fodder for blogs, quite honestly. <laughs>

McGraw: There’s been an awful lot of hype around cloud stuff, including cloud security. I guess that’s one of the problems. Because there’s so much hype, it’s hard to tell what’s real and what’s just baloney. In your opinion, what are the worst pieces of hype that need to be overcome?

Hoff: Not that I want to dwell on the Sidekick data loss-age story again, but I think [we need to overcome] the notion that clouds are impervious to failure, that somehow ultimately we have invented or introduced new technology or capabilities that solve a set of problems that we have been dealing with for quite some time in some “automagical” way.

A lot of interesting expectations are being set. This is classically illustrated by Larry Ellison’s rants on the topic of cloud, which are both humorous and, in some cases, realistic. This is the argument that there’s nothing new, and we’ll be doing [the same thing] for years, versus the notion that maybe technological advances aren’t that different, but how we plan to use [them] and how

[they're] being operationalized is the difference.

From the perspective of the hype machine and how consumers look at cloud, a year or two ago we didn't even have the word in our vocabulary. The branding elements and the marketing associated with what cloud is going to deliver versus what it delivers today as part of a normal evolutionary step forward, and the way in which we enjoy computing has—in the vendor scramble associated with making sure that you're included in the magic quadrant or whatever that might be—really just fueled the fire in terms of making things very confusing.

But back to your question, 'What is cloud and what can it deliver?' Clearly, we have great illustrations of what cloud computing is and the potential it can offer: Amazon Web Services, services like Google and Salesforce.com. There are also very interesting things that are going on with the development of people and corporations using private cloud capabilities, the extension of Web 2.0, and mashups. I think in the long term that the hype gets outweighed by use cases and the realities of how people are using the technology and the operations. Ultimately, it'll settle down like it always does.

McGraw: Let's turn to security. I really love your presentation entitled, 'The Frogs Who Desired a King,' which can be found on the Rational Survivability blog. In that presentation, you discussed three varieties of cloud computing. What are those three levels? Then let's talk about security in all three.

Hoff: The three classical service models that relate to cloud—these weren't defined by me; these have kind of come to the forefront in discussions and certainly have been made a little bit more concrete by

About Christofer Hoff



Christofer Hoff has more than 19 years of experience in high-profile global roles in network and information security architecture, engineering, operations, and management. Currently, he is the director of cloud and virtualizations solutions at Cisco. He specializes in information/operational risk management, network security, engineering, and architecture, with a focus on emerging technologies and disruptive innovation such as virtualization and cloud computing. Prior to his current position, Hoff served as Unisys' chief security architect and Crossbeam Systems' chief security strategist. He was the CISO for a US\$25 billion financial services company, was founder/CTO of a national security consultancy, and led the security engineering team for one of the first global managed network security service providers. He is a prolific blogger and can be found at www.rationalsurvivability.com/blog.

the folks at NIST with the publication of their documents. People are using the vocabulary, known as the "SPI" model: software as a service [SaaS], platform as a service, infrastructure as a service.

Those three models are ways of describing—especially as it relates to security—how you define groups and draw lines in the sand where the providers' responsibilities end in terms of security, management, operations, etcetera. It's a very useful way of applying some definition to how people are offering services and how they are ultimately consumed.

McGraw: I think of them as virtual hardware, virtual operating system, and virtual apps.

But here's the problem. We're not so bad at protecting hardware—not virtual hardware, but just plain, old hardware. We're pretty bad at protecting virtual operating systems, and we're particularly bad at protecting virtual applications.

So, it strikes me that security maps really differently into these three levels.

Hoff: It certainly can. In between the time I wrote the 'Frogs,' presentation and my latest one, I wanted to weigh in, relating the SPI model from a security or a technician's perspective (as some-

body who's been involved in networking or application security) to a set of models that they would identify with.

I'm very visual, so I like to [use] pictures a lot. I came up with a way of mapping some of the complexity of the model (which I built with a community effort) saying, 'If you look at infrastructure as a service, when you map that to something you are familiar with, you'll see that it is facilities, hardware, a layer of abstraction, and core conductivity instead of API's.' That's kind of infrastructure as a service. Then you put your stuff on top of that. It could be virtualized. It doesn't have to be, but you put your stuff on top of that if you're a consumer.

Platform as a service is essentially infrastructure as a service with a layer of integration and middleware that allows people to develop and build applications, usually hooked to a particular development environment or programming language on top of the infrastructure-as-a-service layer. Software as a service is all of that, plus applications, data, content, metadata, and the way it's presented and managed.

The interesting point about the SPI model when you map it to security and the comments you were making about the relative levels of security they're in is that the lower down the stack you go—from

software as a service to platform to infrastructure as a service—the more responsible you are as a consumer for the security and management of the resources that are running in that service.

McGraw: Because you're putting more stuff on top of the service.

Hoff: That's right. More specifically, the provider draws their line kind of lower and lower as it goes. So, you take an infrastructure-as-a-service provider like Amazon Web Services, which does a fantastic job of offering what ends up being all the moving bits—a hypervisor—and then they provide you a shell (an AMI within which you can put your content, operating systems, and data). But where they draw the line from a security perspective is from the hypervisor on up. They ensure that the operations of that environment work as advertised, and they're as secure as they can be to provide you a certain service.

McGraw: Then they have the advantage of being a kind of grid underneath their hardware solution. So you get scalability and all sorts of other stuff that may or may not be associated with cloud.

Hoff: That's exactly right. I wrote a blog post about that the other day, where ultimately, there's not a lot of variability in workload [when] what you're offering in that regard are fixed compute and memory configurations.

You can get variability of the content within the AMI in the packaging, but if I know what my fixed workload looks like based on small and medium and large instances of compute, then essentially as an operator I'm providing one task—a grid-like task of offering compute and storage services. What you do with it is your business.

So [providers'] security from that perspective is quite well defined.

Now, if you go to the other end of the spectrum with software as a service, [providers] own the entire thing soup to nuts. With infrastructure as a service, you're building in security. With software as a service, you're essentially RFP'ing [request for proposal] or contracting security in because what SaaS [provides] you from a security perspective is what the provider builds into it.

Somewhere in the middle is this very interesting—I don't want to say, 'no man's land,' but platform as a service. Platform as a service, especially as it relates to security, gets a little interesting because the development environment, and the hooks that you have in the programming languages that enable you to develop your apps, are tightly coupled in one instance to the platform. Since you are writing the applications and you own the data, maintaining and managing security as it relates to that model is kind of stuck in between this shared/co-operative approach, which is very interesting when you're trying to balance that out.

When I look at talking about security and cloud, I try to abstract things. I separate them out into three classes of cloud "anatomy," as I call it. There's one block that I classify as infrastructure, which everyone is familiar with. It's kind of the cogs, the moving parts, the router, switches ...

McGraw: I always think of it as kind of a big pile of discs, just because that's easy to conceive.

Hoff: Yep. But it could be processor, memory—it's anything we use to compute/network/storage. That's the foundational layer. At the very top is "infostructure," which is apps, data, metadata, service deliveries, service definition.

It's all of the things that you would imagine—the content and services—that would be delivered. And stuck in the middle between infrastructure and the infostructure is something I call 'meta-structure,' which is actually the glue and guts that holds those two things [together] and/or allows them to be abstracted from one another. So, that's anything from BGP [Border Gateway Protocol], DNS [Domain Name System], PKI [public-key infrastructure], identity access management, IP and address management, things that essentially glue those two stacks together, whether that's in the monolithic environment, traditional non-cloud environment, or a cloud environment.

Sorting those things out, mapping them back to the SPI model, and understanding what our options are from the perspective of securing those various blocks is the challenge, especially when you look at the fact that if cloud is not technology but really an operational model, then you have to look at what that does to how you operationalize security. That's the part where things start to get a little, well, cloudy. □

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.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.



■ Subscribe Now!

IEEE *Security & Privacy* magazine is the premier magazine for security professionals. Each issue is packed with information about cybercrime, security & policy, privacy and legal issues, and intellectual property protection.

Watch for these special issues! ■

Mobile Device Security ■ Sharing Sensitive Information ■ S&P of Cloud Computing
Reliability of Embedded and Cyberphysical Systems ■ Engineering Secure Systems

www.computer.org/security