

# Interview

## Silver Bullet Speaks with Marcus Ranum

By GARY MCGRAW  
Cigital

**M**arcus Ranum is chief of security for Tenable Security, where he's responsible for research in open source logging tools and product training. He serves as a technology advisor to several start-ups and venture capital groups. Ranum is the inventor of the proxy firewall, an excellent photographer, and a good marksman.

Featured here is an excerpt adapted from the full interview between Ranum and Silver Bullet host Gary McGraw. Their conversation ranged widely, from Marcus's work on proxy firewalls and his thoughts on hackers all the way to power tools. 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). You can also subscribe to the free podcast at iTunes.

**Gary McGraw:** You're known for inventing the firewall. And it's certainly in widespread use. Is that good?

**Marcus Ranum:** Well, first off, I didn't exactly invent the firewall. Sorry about that. I took a lot of ideas that people smarter than me already had, rationalized and realigned them, fused them together, and brought the first commercial firewall to market.

Are firewalls a good idea? Firewalls are a great solution for the prob-

lems that they were designed to solve. The problem is that the Internet has become more complicated than the problems that firewalls can solve. So we have these customers who buy firewalls and say, "I'm protected," and don't realize that they're only somewhat protected. They're dealing with pretty complicated application mixes that they really can't understand, and the designers of the firewalls can't understand them either. And if you can't understand something, there's no way you can secure it.

**McGraw:** If you treat it as a one-size-fits-all solution to security, you're in trouble.

**Ranum:** Anybody who comes along and tells you, "I've got a one-size-fits-all solution for pretty much everything," is either ignorant or lying.

**McGraw:** Sometimes it's hard not to become cynical when faced with so-called progress in the field. Do you think we're making forward progress?

**Ranum:** I don't think we're making progress. I think the situation is getting worse. If you look at the size of the computer security industry, its growth over time, and then look at the rate at which systems are being penetrated, those curves are not correctly aligned with the demographics of computing. So the progress is getting worse, in spite of how much we keep spending.

I don't think there's necessarily a correlation between how much we spend and how much we get. Because if there were a correlation between how much we spend and what we get, you could say it's negative, right? We should stop spending

### About Marcus Ranum



**M**arcus Ranum is a world-renowned expert on security system design and implementation. He is recognized as the inventor of the proxy firewall and the implementor of the first commercial firewall product. Since the late 1980s, he has designed several groundbreaking security products, including the Digital Equipment Corp. Secure External Access Link (DEC Seal), the Trusted Information Systems (TIS) firewall toolkit, the Gauntlet firewall, and the Network Flight Recorder (NFR) intrusion detection system.

Ranum has served as a consultant to many Fortune 500 firms and national governments, as well as serving as a guest lecturer and instructor at numerous high-tech conferences. He was awarded The Internet Security Conference (TISC) Clue award in 2001 for service to the security community in 2001, and the Information Systems Security Association (ISSA) Lifetime Achievement Award in 2000.

money on computer security so the problem will stop getting worse. The situation doesn't look very good right now.

curity" [[www.ranum.com/security/computer\\_security/editorials/dumb/](http://www.ranum.com/security/computer_security/editorials/dumb/)], is one of my favorite pieces of writing in computer security. Why is it

## I think the stupidest idea that I've seen in computer security is the whole notion of penetration testing.

**McGraw:** What's the silliest stuff you've seen out there?

**Ranum:** I think the stupidest idea that I've seen in computer security is the whole notion of penetration testing. There are lots and lots of people who make tons of money on it. And lots and lots of people spend lots of money on it. But the basic premise of penetration testing is that you've got something that you don't understand and you're trying to achieve an understanding of it by having some outsider—who also doesn't understand it—attack it, simulating someone who doesn't understand it, trying to figure it out. Now if that's not the dumbest thing you've ever heard of, I don't know what is.

If you want to understand whether a piece of engineering construction is going to do the job, you have to go back and look at the statement of the problem you're trying to solve. And then you have to look at your design to see if the solution matches the design, which matches the scope and required strength of what you're trying to build.

The problem is, of course, that it's too late to go back and look at all the networks that have been built in the industry, and say, "What's wrong with them? How do we fix them?" Everybody basically wants to say, "Well let's throw more Band-Aids at it. And let's get some professionals in to come tell us where to stick the Band-Aids."

**McGraw:** Your treatise, "The Six Dumbest Things in Computer Se-

curity" [www.ranum.com/security/computer\_security/editorials/dumb/], is one of my favorite pieces of writing in computer security. Why is it that people do these silly things? Why don't they just do the most obvious commonsense stuff?

**Ranum:** There's two things going on. First, computer security, even though it seems like it's been around for a while, is a fairly new field. And there's only a small handful of people who are actually trying to figure out what the laws of physics of computer security are. In a science like physics, the underlying rules have been well enunciated for quite some time—at least a good understanding of the underlying rules—so if someone comes along and says, "I have a perpetual motion machine," people laugh at them, and put that statement to a series of questions. But because computer security is so new, and the underlying rules really haven't been internalized by people, if someone comes along and says, "I have this one-stop doodad that sits on your network and fixes security," a lot of people say, "Oh, that's great. I'll take five."

And the other problem is just human nature. We want the simple solution. The best analogy that I keep coming up with for computer security is the multibillion-dollar diet industry in the United States. Everybody wants to be thin. Everybody knows that if you eat less and burn more calories, the second law of thermodynamics is going to take care of it and make you smaller. This is just a fact of physics. But instead, there's this huge multizillion-dollar industry that's based on the predicate that you can eat a gallon of Ben &

Jerry's [ice cream] a day and all you have to do is take one little pill, and you won't have to actually work out or eat less, which is fundamentally stupid. That's what's so amazing to me. It's like there are people who will try anything to lose weight except diet and exercise.

And there are people who will try anything to secure their networks, except design them correctly, control the access levels within them, segment their networks, understand their traffic, and monitor things closely.

**McGraw:** It seems so straightforward when you put it that way.

**Ranum:** Yes, it does. And that's one of the reasons why people like me—the very few of us industry curmudgeons—go around and say, "Hey, this is all stupid." You've got a problem that people treat like it's rocket science, but there's actually kindergarten solutions just sitting there in front of everybody—you wonder what's wrong with people.

**McGraw:** Lately you've been harping on the importance of software security and building things properly. I know you've always been a proponent of solid engineering. Do you think we're making any forward progress on that end of the equation?

**Ranum:** It's slow. People are starting to get it. But it's like pushing a huge rock uphill. When I talk to senior managers now, I tell them, "You know that you're spending a gigantic amount of resources on patching busted software?" And they say, "Yeah, well that's a drag. We've got all these FTEs [full-time equivalent employees] that are doing nothing except patching. We've got these patching products"—all this kind of nonsense. Then I nail them with the simple question, "Have you ever done any kind of an analysis on how much it would cost to do it right and

forget about it?” They say, “Is that even possible?” I say, “Well it’s not that difficult. But it’s not easy.”

This reminds me of a Web site that a friend of mine and I built back in 1996 for a friend who had some peculiar security requirements. We just custom-coded this very small thing that was very simple and reviewed it. We nailed the thing down as tight as we possibly could. It was running on an old operating system that was minimized and stuff like that. That site is running absolutely untouched, unpatched, unmodified. We basically completely forgot about it. I don’t think we even have the source code for it anymore. When you do it right, the cost of maintenance is zero. Whereas if you buy something that’s awful, and you try to patch it—

**McGraw:** Especially if it’s being changed every second because it’s so problematic to begin with.

**Ranum:** Right. And that’s the other part that I really don’t understand. Because when I first started off as a systems and network administrator, I worked next to the mainframe guys from hospitals. And the mainframe guys understand this, the rules of production systems. You make it work. You don’t touch it. And if it breaks, you fix it. But if it’s not broken, you don’t fix it. You sit in your office and drink coffee.

**McGraw:** That was one of the problems Microsoft was trying to address with their Patch Tuesday—the notion that these patches came out arbitrarily and often, and maybe they could just push them all out once a month. Do you think that’s a good thing or a bad thing? What’s happened?

**Ranum:** I think it’s insane. Microsoft has a difficult problem. They have addicted their customer base to a constant stream of features. And, unfortunately, they’ve addicted

their customer base to a constant stream of unreliability that comes along with that stream of features. Whereas the other way of looking at it would be following my favorite philosopher of science, Richard Feynman, who would basically say, “You know, if the design of your system doesn’t say that it needs to be

patched every Tuesday, and it needs to be patched every Tuesday, there’s something fundamentally wrong with it. You need to go back and look at it and ask yourself, “What am I doing that’s stupid?””

The fact that the most important operating system in the world is under such a high level of attack,

## BUILDING SECURITY IN...



### SOFTWARE SECURITY: Building Security In

GARY MCGRAW

READ CHAPTER 5:

Architectural Risk Analysis ONLINE.

ISBN: 0-321-35670-5



PUT  
SOFTWARE  
SECURITY  
INTO PRACTICE  
TODAY  
WITH THESE  
BOOKS!

### SOFTWARE SECURITY LIBRARY


GARY MCGRAW, JOHN VIEGA,  
and GREG HOGLUND

Avoid risks and build security into your software with these three field-defining books: *Building Secure Software*, *Exploiting Software*, and *Software Security*.

ISBN: 0-321-41870-0

FOR A SNEAK PEEK, DOWNLOAD SAMPLE CHAPTERS ONLINE AT  
[www.awprofessional.com/security](http://www.awprofessional.com/security)

Available wherever technical books are sold.

  
Addison  
Wesley

and appears to have so many chinks in its armor that it needs to have a formal mechanism that rolls together all these bugs on a single

without burglars, we wouldn't need any locks. Think how much money we could save if we didn't have to buy any locks.

## But without hackers, without people probing and penetrating, and releasing vulnerability information about our systems, we wouldn't need a computer security industry.

day—doesn't that seem kind of brain damaged to you?

**McGraw:** It certainly makes it an easy target if they put all of the holes into one patch.

You give no quarter to hackers at all. Why not? Isn't talking honestly about attacks essential to getting past pretend security?

**Ranum:** Talking honestly about attacks is essential, sure. I mean, you want to talk about paradigms for attack and defense. The US Army and most other nations that take warfare seriously have war colleges in which they examine both sides of attack and defense. It's part of the engineering discipline of understanding your problem before you go after it in the first place.

The problem with the hacking scene, and the whole way that the scene is being played, is they're uninvited into the scene, right? So essentially what they're really doing is victimizing us. This is another area—when I float this—where people's heads just explode, because the industry is so accustomed to not thinking about it this way. But without hackers, without people probing and penetrating, and releasing vulnerability information about our systems, we wouldn't need a computer security industry.

I know that sounds silly. But it's a truism. And it is absolutely true, in the same sense as saying that

**McGraw:** It's removal of the adversary.

**Ranum:** Yes. But the part that people don't seem to want to accept is that there is a moral dimension to this. In a very real sense, by requiring me to protect myself and my systems, they're victimizing me twice. First, they're making me spend all this money and time farting around with computer security when I'd rather be doing photography, or playing with my dogs. So they victimize me once there. And then the second place they victimize me is if I don't do a good enough job defending against them; they get me anyway. So the whole computing world is being doubly victimized by hackers.

**McGraw:** Do you think they're helping to get us past pretend security? Could we do that with science alone?

**Ranum:** Again, if they weren't there at all, we wouldn't need security, right? We wouldn't need pretend security. We wouldn't even need real security.

**McGraw:** If we didn't have oxygen on this planet, we wouldn't need any fire control mechanisms.

**Ranum:** Right. Basically what you're saying is the evolutionary argument. Being an evolved human being that walks upright—I apologize if any of your listeners are Cre-

ationists—but being an evolved human being who walks upright, I can thank my evolved state on all of the predators that tried to eat my ancestors and failed, and on all of the viruses that tried to kill them and failed. Well, you could thank the hackers in the same sense that we could thank the predators.

**McGraw:** Just co-evolution.

**Ranum:** Yes, it's co-evolution. But you know what? I don't think that there were a lot of cavemen who looked at that saber-tooth tiger and said, "Thanks for making me better." And the hackers are asking us to do that. I'm sorry. You're not welcome.

**McGraw:** One last question. What's your favorite power tool for use in home repair and improvement?

**Ranum:** My favorite power tool? Well the simple answer, of course, would be a cordless screwdriver. Although there's probably cooler tools, that's just such a humble tool, you know? □

**T**he *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 in podcast form at [www.computer.org/security/podcasts/](http://www.computer.org/security/podcasts/) or [www.cigital.com/silverbullet](http://www.cigital.com/silverbullet).

**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](mailto:gem@cigital.com).



**\$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)