Interview

Silver Bullet Talks with John Savage

GARY MCGRAW
Cigital

John Savage is the An Wang Professor of Computer Science at Brown University and served as a Jefferson Science Fellow in the US Department of State during the 2009–2010 academic year. In his lengthy career, he has held many positions and received several honors for his work in theoretical computer science and computational nanotechnology. His latest book is *Models of Computation: Exploring the Power of Computing* (www.cs.brown.edu/~jes/book).

Hear the full podcast at www.computer.org/silverbullet or www.cigital.com/silverbullet.

Gary McGraw: As a studied computer scientist and theoretician, what is your frank assessment of the state of cybersecurity as a discipline?

John Savage: Although it's 25 or 30 years old, it's still in its early stages. The first course on computer security was taught at Brown just a couple of years ago, so I would say we have a long way to go. The problems are very hard and intellectually challenging, and have a great practical importance.

McGraw: What issues are top of mind at the State Department when it comes to cybersecurity and other cyber issues?

Savage: The State Department's role, as you know, is not to solve the problems of cybersecurity. Its role is to represent the interests of the United States abroad, through its embassies and by working with international bodies. In particular, it works with other agencies of the federal government and the cybersecurity coordinator's office to formulate policy. This process has been underway for some time, but it picked up steam in 2009.

McGraw: What do you think about the technical background knowledge that policymakers bring to this question? Do they seem to understand what it is they're supposed to set policy about, or is it some sort of magic to them?

Savage: It's not magic. The people I dealt with in the cyber affairs office are very intelligent people who are quick studies and have been able to come to grips with cybersecurity issues from a sufficient depth of knowledge. Admittedly, the policy issues that they've addressed so far have not been profound, such as the BGP [Border Gateway Protocol] trust issue. It's very important, but hadn't come to their attention during my tenure.

When I was a Jefferson Science Fellow, I was invited to give a lecture in the State Department before a very large audience. One of the points I made then—which I still profoundly believe in—is that you need to have technologists and policymakers at the table at the same time. There are technological solutions unknown to policymakers, that if they understood them, might result in a different set of policies being established. Second, as policymakers confront challenging issues, they can turn to technologists, ask for advice, and try to encourage them to find solutions. Solutions don't come quickly, of course, but I think both can benefit. We can be much more effective working together.

McGraw: Do you think it makes sense to form military units in cyberspace as a reaction to our worrisome dependency and systematic vulnerability?

Savage: The short answer is yes. You're talking about CYBERCOM [US Cyber Command]?

McGraw: CYBERCOM and the notion of defending this broken thing that we've built.

Savage: I think it's unavoidable. At least 20 nations are preparing for cyber conflict, so everybody has to sharpen their offensive and

 1540-7993/11/$26.00 © 2011 IEEE COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES

About John Savage

John Savage is the An Wang Professor of Computer Science at Brown University and was a Jefferson Science Fellow in the US Department of State from 2009 to 2010. His research interests extend into theoretical computer science and computational nanotechnology. In 1979, he cofounded Brown's Department of Computer Science, which he chaired from 1985 to 1991. Savage has a PhD in electrical engineering from MIT. He's a fellow of the ACM, an IEEE life fellow, and a Guggenheim fellow. Savage has received a Fulbright Hayes Research Award and has written three books, the latest being *Models of Computation*. He lives in Providence, Rhode Island. Contact him via www.cs.brown.edu/people/faculty/jes.html.

defensive weapons. But the thing that disturbs me about this is that there's a rush to militarize cyberspace, when, in fact, cyberspace should be treated the way the radio spectrum and telecommunications in general have been treated.

McGraw: As a common, so to speak.

Savage: Yes, as a common. Tony Rutkowski, who used to be at the FCC [US Federal Communications Commission], wrote a piece on the first cyber war, which he describes as the conflict that emerged early in the 20th century about disputes over the use of the radio spectrum and wireless communication standards after the *Titanic* went down. Nations around the world decided, "Let's not fight over this space. Let's partition it. Let's agree on standards." This was done through an organization that eventually became the International Telecommunications Union. I don't think we can ever demilitarize cyberspace, but I do think that we should invest very large efforts to reduce risks, to reduce tension, and if we can, to try to demilitarize it, but I think it may be beyond that now.

McGraw: I like the idea of talking about cyberpeace instead of cyberwar. It doesn't have the same sex appeal, though.

Savage: As you've said, you wrote two books, and the one on hacking has had a lot more sales than the one on cybersecurity.

McGraw: I call it the Nascar effect.

Savage: People do like to see a crash. Crashes are exciting.

McGraw: That's why there's no Volvo car safety channel.

Savage: But the public has to understand that these problems are real and serious, and can have a tremendous impact overnight on our economy. It's really the economy that's at risk here, more than anything else.

McGraw: There are very important tensions between modern systems for attribution based on cryptography and individual liberty in an open society. What are your thoughts about that?

Savage: In cyberspace, you need both secure authentication methods and anonymity. You also need a form of e-cash. I have a colleague here, Anna Lysyanskaya, who has done research with a colleague at IBM and obtained patents in the area of anonymized commerce. I think it's important to have anonymity, but if you're going to deal with corporate or government secrets, you need to be able to authenticate yourself over insecure networks. So it's a mixture of both, I think.

McGraw: You know, of course, some people want to push attribution so far as to completely get rid of the possibility of anonymity. We have to keep that in mind as well.

Savage: It's never gonna happen. The public would object to that.

McGraw: In your view, is WikiLeaks part of the press, meaning it should be protected by the First Amendment, is it some sort of a new beast, or is it, in fact, a terrorist organization, as some politicians have said?

Savage: I would be cautious about declaring it a terrorist organization, because if you did that, then you'd have to accuse *The New York Times* among other respectable outlets as having trafficked with terrorists.

McGraw: I think some people would like to do that, actually.

Savage: Two things interest me about it. One is that PFC [Private First Class] Bradley Manning is the primary culprit here, and two, were adequate controls put on the databases that he used to access the documents he was able to exfiltrate?

McGraw: Exactly. Was nobody paying attention that everything from SIPRnet was being stuck on a USB drive?

Savage: To me, this is such an obvious mistake, to allow someone to do this without being monitored. There should have been controls on the volume and the number of items per day a person could download.

McGraw: We seem to either be in danger of a cyber arms race or of

destroying our glass house with a cyber rock. Why do you think that the cyberwarriors in the Defense Department [DoD] and the intel community especially, who are separate and distinct from the people in the State Department and in the executive branch, focus all of their attention on offensive weaponry these days?

Savage: Well, you're making an assertion here that the intelligence community is focusing on offensive weapons. Is that correct?

McGraw: I think the intelligence community is focusing on offensive weapons for espionage, and the DoD is focusing on offensive weapons for warfare.

Savage: I would agree with that. I've spent only one year in government, so I'm not an expert on what I'm about to say, but I do have the impression that the role of the military, its sanctioned role, which we want it to play, is to protect the nation. [The military] tends to bring the best and brightest minds to play in that task. They work hard at it. They're proactive. And if you're proactive, you're going to get access to the best minds to confront a brand-new challenge. You're going to prepare for the possibility of attack, and you certainly also are going to prepare for defense.

McGraw: I've seen much more preparing for offense than defense, just from my own chair, in my discussions with the guys who are running these things, and that worries me, because I agree that you need to focus on both.

Savage: Let me say this, if they're doing superbly in defense, they won't tell you. If they understand how to defend against intrusions, they won't tell you. They'll keep it a secret.

McGraw: I'm not thinking about operational defense of the sort that we over-focus on. I think policymakers are paying a lot of attention to reactive threat-reduction centers and certs and the things that you talk about in some of your writings, rather than building things properly and security engineering, and I think that that's a rather fundamental mistake.

Savage: It is, and it's partially because they don't understand the technology or what options exist at the technology level. Thus, the conversation is reduced to lecturing to the public on the need to follow best practices and keep software up to date.

McGraw: Which is a little hard to do.

Savage: Right. But what's missing in this picture is that we as users of software systems cannot repair them. We can't even tell if they're broken. We can't tell if they've been penetrated, so who should be responsible? It seems to me it has to be the people who sell us these products. But, unfortunately, the common practice, as we both know, is that when you acquire a piece of software or hardware, you sign a license that says the vendor is not responsible for any of it, and that has to change. Not overnight, but it has to change.

McGraw: Let's assume that Stuxnet was a product of a nation-state. It's a pretty big assumption, but let's just assume it was. Do you think that the use of such a cyber weapon is morally justified?

Savage: Yes, I do. It's as morally justified as an attempt to sabotage a piece of physical equipment.

McGraw: What implications does nanotechnology, especially computational nanotechnology, have for cybersecurity?

Savage: On the surface, I would say none, except for the fact that as we make our components smaller, we put more components on a chip, which gives us some scope to change the way in which we write code and implement chips. For example, in the past, field-programmable gate arrays would have been seen as very expensive, so vendors wouldn't use them. They would use ASICs [application-specific integrated circuits] or do their own design using CAD tools. In the future, they'll have more real estate available, and as they do, I think, for security reasons, they should start changing the way in which they write code. They should put some monitoring on their chips so that they can find intrusions and identify unusual activity.

Today, we incorporate drivers into our operating systems, so a company like Microsoft will produce an operating system and run a whole battery of tests to make sure that it has no buffer-overflow attacks, heap-overflow attacks, or other things through managed memory. I have a son who works at Microsoft, and he tells me that he's able to not only write code much faster, but it's much more secure. As we know from published reports, the number of major updates that Microsoft has had to do has gone down relative to its competition.

McGraw: I agree with you that Microsoft has made some progress, but do you think some of that will find its way into hardware?

Savage: Well, it could, but it still incorporates drivers developed by others. Why? For efficiency reasons. These drivers can be put in a user space, so why aren't they? [Microsoft] has implemented address space layout randomization and data execution protection. Those are important steps, but they can be subverted, as we know.

McGraw: Yes, and sometimes they get skipped in various applications, which was a subject of a conversation I had with Ivan Arce in an earlier episode.

Security is not free. Coming back to the nano point: because you have more components in a chip, you have more latitude to exploit a variety of techniques to make software and systems more robust.

Savage: Yes, I recall reading that. So fix the code. Rewrite the code. My point is, as we both know, security is not free. Coming back to the nano point: because you have more components in a chip, you have more latitude to exploit a variety of techniques to make software and systems more robust.

McGraw: I think it's kind of ironic that we spend a lot of effort to come up with a universal computational device, a universal Turing machine, so to speak, and then we get all upset when it does some of the things that of course it is allowed to do by theory. Why don't we just have special-purpose machines that can't do everything? That would seem to help from a security perspective.

Savage: A good programming practice, as I'm sure you know, is if you can write a piece of code that implements a finite-state machine, do it.

McGraw: It's part of the principle of least privilege, sort of an axiom to that.

Savage: Right, so yes, you should, but, also we need expressiveness. Almost any good programming language is Turing complete. So the power of Turing machines there is unavoidable, unfortunately. And it's not that the Turing machine was invented so that it would create the problems. It's just a reflection of the Church-Turing thesis that this is the most general model of computation that we've invented.

McGraw: Once you turn it to 11, it's hard to step it back down to 5.

Switching gears again, what's the best piece of fiction that you've read recently?

Savage: My reading tends to be technical, more policy-related these days. I've been doing a tremendous amount of reading for my spring course. Oh, I did read *The Girl with the Dragon Tattoo*, the first book in the series. I understand that she's quite a geek, and the later books are supposed to be interesting, so I decided I should read them, but I haven't read them all yet.

McGraw: What's the most interesting nonfiction text that you've read lately?

Savage: The one nonfiction idea that I think is most interesting and potentially, although not yet, exciting, is the new solution to the crypto computing problem due to Craig Gentry, which is fully homomorphic encryption. Do you know about this?

McGraw: I don't.

Savage: What Craig Gentry has shown in a STOC [Symposium on Theory of Computing] paper in 2009 is that it's possible to encode data so that when you compute on the data, it remains encrypted. And you never have to decrypt until you bring the results home. His technique for doing it looks challenging, but it's actually very fascinating. While still extraordinarily inefficient, his techniques have the potential to eventually extend cryptography to computation. The reason it doesn't normally extend is because it's difficult to do both addition and multiplication on encrypted data. In other words, provide a way to encrypt so that when you do either addition or multiplication—think of addition as "or" and think of multiplication as "and"—you can produce an output that can be put back into the same code that was used to encode the data before you did the operations.

McGraw: That would do a lot for digital rights management, among other things.

Savage: Yes, it would. But right now, it's impractical to use.

McGraw: Thanks very much. This has been great.

Savage: It's been a pleasure for me as well, Gary.

Show links, notes, and an online discussion can be found on the Silver Bullet webpage at www.computer.org/silverbullet. □

Gary McGraw *is Cigital's chief technology officer. He's the author of* Exploiting Online Games *(Addison-Wesley, 2007),* Software Security: Building Security In *(Addison-Wesley, 2006), and seven 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.*