Silver Bullet Talks with Jamie Butler

Gary McGraw | Cigital

Hear the full podcast at www.computer.org/silverbullet. Show links, notes, and an online discussion can be found at www.cigital.com/silverbullet.

Jamie Butler is chief technology officer (CTO) and chief scientist at Endgame, a leading provider of cybersecurity solutions to detect, block, and evict advanced threats at the earliest phase of the kill chain. At Endgame, Butler leads research on advanced threats, vulnerabilities, and attack patterns. He has directed vulnerability research teams at several prominent companies including FireEye, where he was chief architect, and Mandiant, where he was chief researcher. Butler also served as a computer scientist at the National Security Agency (NSA) and coauthored Rootkits: Subverting the Windows Kernel.

What are your responsibilities as Endgame’s CTO and chief scientist?
Since starting in March 2015, my primary focus has been building the research team. I’ve hired incredibly talented researchers and data scientists, including a director from the NSA who leads our malware research and threat intelligence. For me, the chief scientist role is about internal research and building detection into our product suite, whereas the CTO part is more about talking to investors and the press.

I’m a coder at heart so I can never get rid of my coding job. I like to take it with me wherever I go. Recently, I told Endgame’s CEO that I was writing some code for a product. He said, “I’m not sure you should be doing that,” and I said, “I’m not sure I should be either, but it keeps me happy.”

In its first iteration, Endgame was all about offense and helped introduce active defense to the private sector. Has this changed?
I haven’t been here that long, but it did start with an offensive mentality to help the government in areas like exploit research.

There were a few start-ups that were talking up a big game in terms of attacking back. What are your thoughts about this as a philosophy? Do you think the private sector should be allowed to do this?
It’s really difficult. If you don’t get the attribution right, you’re actually victimizing potentially innocent bystanders in the process. So I don’t espouse the hack-back, and our CEO is pretty firm on that as well.

Have we made progress in adopting ideas from the attacker community to inform our engineering?
At Endgame, we take an offensive-based approach—how attackers think and work—and use this against attackers. I’ve hired a cross-disciplinary team of academics, data scientists, and civil servants from the Department of Defense and intelligence community, so I believe we’re uniquely positioned to deliver this capability to the marketplace.

If you want to get data off an endpoint, there are products out there that will do it, but they don’t have any intelligence built into them. So you need an expert to make those tools useful. It’s important to consider attackers’ patterns and motivations and then design the product to detect these things. That’s what we’re building at Endgame.
I wrote *Exploiting Software* a million years ago with Greg Hoglund, who is coauthor of your *Rootkits* book. We first wrote about rootkits in *Exploiting Software*, and we figured we’d get a lot of flak for it, but we got less than we expected. I think many people understand that you need to know the attacker perspective to defend effectively.

Hoglund and I submitted a sample chapter, the introduction, and the outline to the publisher, Addison-Wesley, who shopped it around to other experts in the field. Some of them said, “Why in the world would you want to publish a book like this?” It was tough at first to get the contract because some people think you’re helping the enemy. I come from the world where you have to do proof of concept to get vendors to change their security.

Tell us about OS security. Things have changed a lot since you started your rootkit work—I think for the better. Do you agree?

I think Windows has advanced the most. I’m not a Linux expert by any means, but you can still do some of the old tricks from Windows on a lot of the Linux boxes. I’m really impressed by the amount of research and investment Microsoft has put into its OS. Microsoft has hired some great people in the security industry.

You started your career at the NSA before moving on to Mandiant, HBGary, and FireEye. Can you compare and contrast those worlds?

I was brand new to computer security when I was hired at the NSA. The NSA had a great program called SERIP at the time, which was an incentive, because it was great training experience and the NSA paid for your master’s degree. This is when I went to UMBC [University of Maryland, Baltimore County] and got my MS in computer science. IAD, the Information Assurance Directorate, was responsible for securing the government’s computers. The hard part was that IAD really didn’t have authority over any of the government institutions it was asked to help. So staff couldn’t evaluate NASA or even Department of Defense systems unless they were invited. And even if they were, they couldn’t mandate patches or remove software because of its vulnerabilities.

During my last three years at the NSA, I was in signals intelligence. I worked with some brilliant people, always learning new things. I was still fairly new to the industry and I felt more of a sense of purpose because I was trying to actually fight terrorism and spies. But after five years, I decided I needed to try something in the commercial sector.

When high school or college students approach me and ask about careers in the NSA, I always encourage them to go there. If they aren’t specialists yet and don’t know exactly what they want to do, the NSA is a great training ground. It invests a lot in its people, or at least it did when I was there. It’s not a bad road to go down.

And then you worked for Mandiant for seven years, before FireEye bought it.

My wife’s former employee introduced me to Mandiant. He invited me to dinner with Kevin Mandia, CEO, and Dave Merkel, the VP of engineering. At dinner, they gave me a David and Goliath story. They were a small start-up trying to take on the incumbent, which really drew me to the company. They wanted a Windows endpoint and I said, “Yeah, I know a few things about that,” so I started there.

There were about 26 or 27 people when I joined, and our revenue the first year was under $5 million. It was really small. We were about 500 people when we were acquired. We had just taken on $70 million of funding from a few venture capitalists, so the company exploded.

As a Black Hat committee member, do you think a security engineering track would be useful at its conferences?

I think it would. We have a software engineering track that covers security issues and coding, but not many people submit to it. We have so many new people coming into the field every day. Some incubators out there take someone who has never written code before, and after three months they’re actually extremely hirable. We’ve done that at Endgame. I’m not sure about the previous places I’ve worked, but Endgame invests a lot into a broad
spectrum of skills and backgrounds. One of the things that has always drawn me to computer security is that you can be a huge success regardless of your training or education. It’s you against the machine or the attacker, but we need to learn from those that have gone before us and established things like secure coding practices.

One last thing from left field. I know you’re into humanitarian causes. What are you most interested in right now?

I support Hackers for Charity. Founder Johnny Long moved his family to Africa and is trying to help the local people, train them so they can be self-sufficient and do computer-type work. I look at this as an incredible example. That’s pretty amazing and selfless of him. I also support a local charity called International Justice Mission, which fights human slavery and sex trafficking all over the world.

The Silver Bullet Podcast with Gary McGraw is cosponsored by Cigital and this magazine and is syndicated by SearchSecurity. McGraw is Cigital’s chief technology officer. He’s the author of *Software Security: Building Security In* (Addison-Wesley 2006) and eight other books. McGraw received a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him via http://garymcgraw.com.