

Interview

Silver Bullet Talks with Mikko Hyppönen

GARY MCGRAW
Cigital

Mikko Hyppönen is the chief research officer for F-Secure, where he has worked since 1991 as an active malicious code researcher. Hyppönen and his team have done prominent work against the Sobig.F, Sasser, and Zotob worms. He's also been active in the discovery of malicious code used for "good," such as Sony's infamous digital rights management rootkit.

Featured here is an excerpt adapted from the full interview between Hyppönen and Silver Bullet host Gary McGraw. Their conversation ranged widely, from mobile phone security to Finnish hip-hop. You can listen to the podcast in its entirety at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/, and you can subscribe to the full series on iTunes.

Gary McGraw: What are the good and bad things about running a high-tech company in Helsinki, Finland?

Mikko Hyppönen: There are a lot of things that work to your advantage, and there are things that don't really help. You have a whole market in which Europeans like to buy from European companies. That's an advantage. Of course, the big

markets are run by the big brands, and it's really hard to build a strong brand when you're coming from a smaller country.

The other advantage is time zones. We are seven hours ahead of the East Coast. When big things start to happen—a virus outbreak—we typically get to analyze it for several hours before our competitors in the US wake up, which is a nice thing for us. It works both ways.

McGraw: You became well-known for your work on worms, such as Sobig and Sasser. Why are worms no longer making the news?

Hyppönen: Because worms aren't really the right tool to use if you want to become rich by writing malware. Worms are worms because they spread on their own. They have their own mind, which means they get out of hand. If you think about the big Windows worm outbreaks, things like the Sasser and I-Love-You worms, they became such big news because they got out of control and infected way too many machines to stay unnoticed.

In fact, we can argue that the motive of the hobbyists who wrote these early worms was to become famous and get on the front page of *The New York Times*. But today, malware authors have changed almost totally from good old

hobbyists and teenage kids to professionals who do this for money.

McGraw: Are the professionals using the same techniques, but in a much stealthier and smarter manner?

Hyppönen: Actually, I'd say in a more controlled manner. The techniques are very similar; they're the same ideas like email-spreading mechanisms that we've seen since around 1998–1999 when the Windows email worms started spreading.

The difference is that a traditional email worm infects your PC and sends a gazillion copies of itself to every single email address listed in your address book. Modern bots and Trojans infect your PC and then wait for instructions, spreading further from your machine only when told to, and they're only told to in a nicely controlled fashion.

The guys who orchestrate the botnets (herders) only infect a handful—a few thousand—of PCs a day, and that stays under the horizon—nobody pays attention, it doesn't make big headlines, but they still get what they want.

McGraw: Some people have complained that your work on mobile phone security hypes up a problem that doesn't exist. Yet, real malicious code like the Cabir worm

does exist. Do you think that this is because the US is behind on cell technology and adoption?

Hyppönen: Yes. There are often surprised faces and more questions about mobile threats and mobile security when I speak about these things in the US—much more than in Europe or in Asia, where many people have seen these threats for themselves and smart phones have been commonplace for much longer.

Pretty much the only smart phones you could actually see in the US before the iPhone were BlackBerries, which are quite different from the kind of smart phones and communicators people have been using for many years in Asia, and to some extent, over here in Europe. As an example, I've received—genuinely received to my own personal mobile phone—four viruses so far.

McGraw: Which worm was it?

Hyppönen: Once in London, once in Sweden, and twice here in Finland—all variations of the Cabir or the CodeWarrior worms. Of course, I have antivirus on my phone and my smart phone, so nothing ever happened. And I keep my Bluetooth on and visible so I can keep monitoring what's going on out there.

But I wasn't inviting anything. One of these things was beamed to my phone from a passing car. I was standing next to a car at a red light, and that car apparently had an infected phone somewhere inside, and it beamed a virus to my phone. So the problem does exist.

We have been following it since we found the very first mobile phone virus in the summer of 2004. Right now, the total count of all mobile phone malware, which by the way, includes malware for BlackBerries, is getting closer to 400. It's still far from the total of

About Mikko Hyppönen



Mikko Hyppönen is the chief research officer for F-Secure. He led the team that took down the worldwide network used by Sobig.F in 2003, was the first to warn about the Sasser outbreak in 2004, and the first to stop the Zotob worm in 2005. In 2007, *PC World* selected Hyppönen as one of the 50 most important people on the Web.

Hyppönen has addressed the most important security-related conferences worldwide. He is also an inventor and holds several patents, including US patent 6,577,920 for "computer virus screening." He has been the subject of dozens of interviews in global TV and print media.

Apart from computer security issues, Hyppönen enjoys collecting and restoring classic arcade video games and pinball machines. He lives with his family, and a small deer community, on an island near Helsinki.

all PC malware, which is around a thousand times more—400,000.

McGraw: What can we expect when it comes to malicious code on mobile devices? Are there any interesting things that people need to be aware of?

Hyppönen: Absolutely. One thing, which is an obvious difference between infecting computers and infecting phones, is that computers don't have a built-in billing mechanism that exists on every single device. But phones do. If you make a phone call, that's a transaction. That moves money. If you call a premium rate number like a 1-900-number—that's a transaction that costs more money, and money is moved between individuals. For example, if your iPhone gets infected by a Trojan that can control the device, it can make phone calls or send text messages to premium rate numbers and move money from your account to somebody else's account.

We have seen some documented cases where this has actually happened. Last May, we found a Trojan that was distributed on a mobile phone freeware/shareware download site, where people can download applications for their phones. One of those applications claimed to be a tool that would speed up Web surfing on your

phone for Symbian-based devices—phones made by Nokia or Sony Ericsson. Of course, it didn't do that at all. Instead, it started sending these premium rate text messages, and it would send a US\$5.00 message every five minutes, or something along those lines. It does add up.

McGraw: When's the first zombie network built of all cell phones going to happen?

Hyppönen: That's something we've been thinking about. I think the reason why we will be seeing the first mobile phone botnet is mobile phone spam, which isn't a big problem right now. Mobile phone spam is a problem in some parts of Asia—Malaysia, Indonesia, and the Philippines—where people complain about mobile phone ads being delivered via text messages or Bluetooth beaming on mass scale.

But otherwise, pretty much globally, it really isn't a big issue. The reason is that email is totally free. You pay nothing, especially if you hijack somebody else's machine to send the emails for you, you don't even pay for the electricity. It's totally free. You can send as much as you want, billions. No problem. Text messages are cheap, but you still have to pay something, so you can't send them out in un-

limited quantities unless you use somebody else's phone to do it.

McGraw: I remember back in the

McGraw: It's just a matter of time.

Hyppönen: Exactly when, I can't guess. It's been really hard to esti-

The likelihood of some sort of malware or some sort of self-replicating code appearing on the iPhone device—I think that's quite likely. I'd say there's a 90 percent chance we'll see it sooner or later. —Hyppönen

early days of SMS [short message service], my brother used to have to pay \$0.50 every time he got a message, so I would send him a message that said, "This message cost you \$0.50." And then he would call me up and yell at me.

Hyppönen: That's the stupidest idea ever, to charge for receiving a message.

McGraw: It didn't last very long, did it?

Hyppönen: Exactly. This could lead to a situation where somebody distributes a cool game that all the kids download and install on their phone. The game has a hidden functionality that could later connect all those phones—let's say 10,000 or 100,000—to a central Web site where they get instructions. Now they [the game distributors] could start, in the middle of the night, to go through the address books of the phones, sending anonymous Viagra ads to everyone in those address books, which would nicely move the charges away from the real spammer to the innocent bystanders who are infected. Second, they could hide the real party behind the ads. Third, it would nicely give them the target address list; they would know who to send the spam to because they could look in the address books or the contact lists of all the infected phones. Could happen.

mate the development so far. Before we saw the very first mobile phone viruses, we had these brainstorming sessions and thought about what they would look like—we were pretty wrong. We thought that the first mobile phone viruses would be simple ports of existing Win32 viruses, but we haven't seen that at all.

McGraw: Even with the advent of Windows Mobile, you haven't seen that?

Hyppönen: Well, we have seen some cases of Windows Mobile malware, but they've been unique, written from scratch. Nobody's taken the existing source code of some common Windows XP email worm and ported it to Windows Mobile, which is frankly surprising.

McGraw: The iPhone has to be one of the most intensely studied closed systems. iPhone hacks are really hot right now. Do you think it's a bad idea to have a closed system like that?

Hyppönen: I can see why they did it, and they're free to do it. But it's not going to last for long. It will change because there's been so much hype, and we have seen just how much interest there is in the device. Because it's closed in the sense that you can't just pick your operator, there's going to be massive motivation for hackers to break the thing.

While they're doing that, they'll uncover all sorts of other nasty things. We have to remember, this is one to zero, this is the first attempt from Apple at this thing. Do you think it's bug-free? Do you think it's perfect? I don't think so. There will be issues—there have been issues already.

The likelihood of some sort of malware or some sort of self-replicating code appearing on the iPhone device—I think that's quite likely. I'd say there's a 90 percent chance we'll see it sooner or later.

McGraw: One of the important lessons that I learned when I was working on *Exploiting Online Games* was the risk posed by fat clients, clients that control lots of state in a distributed system that operate outside of trust boundaries. I think the cell phone is beginning to look an awful lot like that these days.

Hyppönen: Yes, tell me about it. My cell phone is an E-90 Communicator, which has a 300-MHz processor. It has 8 Gbytes of storage space. I have Doom, Doom 2, and Quake ported on this thing—they all run at 20 frames a second. It has 800 by almost 400 pixel resolution.

This is very close to a laptop you could buy perhaps four years ago. It has all the Office applications—everything that you think a normal computer would have, so it's definitely a very fat application and the amount of attack vectors, because there's so many different ways of moving data to and from this device, is just mind-boggling; so absolutely, all that applies.

McGraw: I also think that people are beginning to write applications in a way where they crack a piece of the application off and hand it over to the client to execute. So if you think about service-oriented architecture or Web 2.0 stuff, then

you can see that we're building systems that are going to have really interesting new problems.

Hypönen: Absolutely, plus all these different scripting platforms are built into different systems that are basically just another facet of the same thing.

McGraw: How did you get started in computer security?

Hypönen: I suppose it really starts from the Commodore 64 because I used to write programs for it. I even sold my programs as a teenager—disk turbo loaders and different kinds of applications. To get any kind of performance out of those 1 MHz machines, you had to write in Assembly, so I spent quite a bit of time writing large programs in Assembly.

Many years later, I went to this company and I started writing database applications and different sorts of high-end development. The company turned out to be Data Fellows, which is the same company I'm still working for today. We later renamed ourselves F-Secure because in the early days, we did lots of things.

Really, I was writing database applications for some sort of factory development systems when I started, but we started to move more of our attention into data security and into viruses, which at the time were spreading on floppy disks instead of the Internet.

To analyze those viruses, which were written in Assembly, you had to be able to read Assembly, and I was pretty much the only guy in the company who had those skills when we started getting the very first virus samples. So of course, they were handed to me.

As you know, Assembly language 8-bit and the 16-bit Assembly language of DOS that we were working with are quite different, but then again not that different. I moved from one Assembly language to another and started cracking viruses. Back then—1991 or early 1992—I'm looking at these long interrupt lists printed on paper and different reference books for memory maps of MS-DOS 3.3 and trying to figure out how these huge viruses would work. And "huge" would be like a 700-byte virus.

McGraw: Isn't that funny? Switching gears, you also have a band called the FSMCs or I guess you call it the Management Consoles?

Hypönen: That's correct. FSMCs in da house!

McGraw: You produce inscrutable Finnish hip-hop.

Hypönen: Surprisingly, Finnish is a language perfectly suited for hip-hop.

McGraw: Because it's so inscrutable. Are there more CDs in the works from your band?

Hypönen: Of course, but we're not about to quit our day jobs.

You can find additional podcasts in the series, including those featuring Greg Hoglund and Peter Neumann 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. He is a member of the IEEE Computer Society Board of Governors. Contact him at gem@cigital.com.

COMPUTER, COMMUNICATIONS AND INFORMATION SECURITY



**Join Our Best
Researchers and Developers
in Securing the Future**

Lincoln Laboratory is looking for new colleagues who will: Analyze network topology using passive & active techniques and explore network security analysis & visualizations. Candidates will instrument binaries to dynamically track information flow, develop prototypes of new, efficient cryptography protocols and design and develop security evaluation testbeds for wired and wireless networks.

Education/Skill Requirements:

PhD or MS in Applied Mathematics, Computer Engineering, Electrical Engineering or Computer Science. Must have experience in computer networking protocols, distributed networking and graph theory. Required track record in some combination of software development and mathematical modeling, computer security research and development, and pattern classification techniques. Knowledge of C or C++ (for protocol implementation), Java (for interface design and visualization) and a scripting language (for testbed design) a plus. Strong communication skills with sponsors and other research sites are essential.

For detailed position and application information, see www.ll.mit.edu/careers/careers.html.

US Citizenship required. EOE.



LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY



\$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