

Chris Young, Intel Security exec, on fighting cybercrime

October 16 2015, by Pete Carey, San Jose Mercury News

When Intel bought McAfee five years ago, it was a surprising move by a giant chip company with a core computer hardware mission into the complex software business of protecting computers from hackers and crooks.

Now it looks like it was a smart move. Cybercrime has become a thriving industry and the emerging Internet of Things will have billions of smart devices powered by the kind of electronics Intel makes. Without security measures, those devices could become a hacker's playground and a consumer's nightmare.

But applying security to silicon is just getting started.

Intel's Chris Young, [senior vice president](#) and general manager of the Intel Security Group, spoke with the San Jose Mercury News about new security challenges and recent reports that rocked the automotive business with demonstrations of how a connected car can be taken over by hackers.

Q: Five years ago, some analysts were scratching their heads and wondering why a hardware company like Intel would buy a security software company like McAfee.

A: Well, why not? If you think about it, every big player is in security. I can't find one that's not - Cisco, HP, Microsoft - every major player is either in security with products and services that are dedicated to

security or they're doing a lot of work to build more secure experiences, build more security into their platforms and products. I think there was good foresight from Intel to say cybersecurity is going to be a big issue and we want to build up our skill set and get out in front of that curve.

Q: Let's talk about the security of computerized automotive controls. Is there any security?

A: There is. There have been some hacks that were highly publicized, but there have actually been a lot of best practices that have shown themselves as well.

Q: The hackers who took over the computer of a 2015 Jeep Cherokee in July and controlled the car exploited the fact that the car could be controlled wirelessly. Isn't that a big worry?

A: The reality is a car is a complex system. A car isn't just one computing device, it's more like having many PCs or smartphones all in one system that's riding around on four wheels. The system has to work together so there's some complexity there, and we've connected many of those vehicles to the Internet to provide good navigation experiences. The things we're getting over the next five-10 years will make it better for us users, but there's a security element that needs to be thought through.

Q: But the new applications seem to be outpacing the security.

A: This is all happening in a very short period of time, because of all the new services available, and what smartphones have been able to bring to our ability to do navigation, and new services like Uber. All of that is really blurring the lines between automotive and what's online. They're the same now.

Q: So we're driving around in a bunch of computers?

A: Pretty much, with a lot of software.

Q: Should we be wary of buying a connected car?

A: Well, anytime you can access a system certainly the wrong person can - it's like a lock on your door. You can get in, but if somebody gets the key they can get in too. You want to have doors. I would say that being able to update software in cars net-net is a good thing, just like we need to do on PCs or servers or on our smartphones. When you find vulnerabilities or things that are wrong, the sooner you can respond and update your software on the device, the better the overall protections there are. That's come out as a best practice.

Q: Tesla updates its software wirelessly doesn't it?

A: Tesla updates their software frequently. They have a very agile ability to provide new features and security updates. I own one. I've been using the product for two and half years and I love it, and I'm a security guy and it makes me feel it's a better situation.

Q: Cars are just one part of a growing Internet of Things where computing power is sprinkled on all kinds of devices. Does that change the security industry's approach to defending against hackers?

A: We see a couple of things. One is that when it comes to connected devices that consumers use, what the Internet of Things is really going to mean is more personalization of computing. We won't go to a computing device to compute. We will just be computing all the time. We're going to be computing without thinking about it, as opposed to thinking about computing.

I think that's a profound change in how technology is advancing. We have to be thinking more about personal information. Our role at Intel Security is to make sure the users, owners and custodians of that information can do the best job of protecting it so that it doesn't fall in the hands of people that have not been designated to receive it. That's the mission we're on.

Five things you didn't know about Chris Young

1. His first job as a golf caddy taught him the value of hard work.
 2. His first car was a stereo-less Toyota Camry, which he purchased from his aunt and drove for seven years.
 3. He hails from Ohio and loves the Ohio State Buckeyes and the Cleveland Cavaliers' LeBron James.
 4. He would pick Will Smith to play him if a movie was made about his life.
 5. His greatest hero is his mother, who once told him: "If you don't know what to do, do something."
-

Chris Young

Age: 43

Career: Currently senior [vice president](#) and general manager, Intel Security Group, 2014-present; senior vice president for Cisco's Security

Business Group, 2011-2014; senior vice president and general manager at VMware, 2010-2011; senior vice president of products for RSA, the [security](#) division of EMC, 2004-2010.

Education: Bachelor's degree, cum laude, Princeton University; MBA with distinction, Harvard Business School

Family: Married, two children

©2015 San Jose Mercury News (San Jose, Calif.)
Distributed by Tribune Content Agency, LLC.

Citation: Chris Young, Intel Security exec, on fighting cybercrime (2015, October 16) retrieved 23 April 2024 from <https://phys.org/news/2015-10-chris-young-intel-exec-cybercrime.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.