SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode Helps Intel Product Security

Intel needs no introduction. The $60 billion technology giant has been at the forefront of information technology since it introduced the world's first commercial microprocessor chip in 1971. In an industry that has seen companies come and go with each succeeding wave of computing, Intel has managed to maintain its leadership position. Today, its business has become so broad – spanning everything from virtual reality to the Internet of Things – that Intel describes itself, simply as a company that *"expands the boundaries of technology to make the most amazing experiences possible."* While not known primarily for its software, Intel relies heavily on software development to enable its innovation.

For the past 14 years, David Doughty has served as Intel's Senior Director of Product Security Engineering. The holder of a Bachelor of Science degrees in Computer Engineering, Doughty started his career as a software developer and has been involved in the security side of engineering since the mid-1990s. Today, he manages a corporate level team of security professionals.

"About 13 years ago, Intel instituted a program to drive security assurance on our products," Doughty recalled. *"It started in the hardware space, but it grew very rapidly out of hardware into the software domain. We saw that more people were attacking at the higher levels of the stack, in the software. But we have seen, year after year, a growing amount of activity to try to target places lower in the stack. And so, our program has always been one that has encompassed both software and hardware."*

Doughty is in charge of Intel's corporate security assurance program for all the company's products.

"It breaks down into three buckets," he said. *"The first bucket is preventive activities – for example, our security development lifecycle, those processes that you should follow to try to provide good security. Then you complement that with the second bucket, detection. Before we ship anything, we essentially hack our own products. The third bucket is response. You put the product out into the marketplace, and when something is found, you need to have good mechanisms in place to be able to respond to those issues with fixes and get those fixes deployed to the people who are affected by them."*

For David Doughty, ensuring secure software at Intel begins early with new-hire education. When new people join Intel they get introduced to security issues and the resources that are available to help them solve security problems.

Once that awareness has been developed, Intel begins the process of improving product security using automation.

"We have found it very effective to make use of automation tools whenever possible," said Doughty. *"For example, there are a number of products out in the marketplace that perform static analysis of code, in order to try to identify some common programming errors that lead to vulnerabilities like a buffer overflow. We bring those tools into the environment and run them on a consistent basis."*

As cybersecurity threats have expanded and multiplied, Intel has adopted a strategy that breaks every product down according to the risks it presents.

"We call it our Risk-Based Approach," said Doughty. *"Every product is unique. You cannot just look at them and say you need to do exactly the same thing without analyzing it. And so we have a process by which we try to understand, what are the real risks and threats that this product experiences? That includes both what is inherent in the product, and also the environment that the product is going to be delivered in. Is that product going to be put on a client's PC? Enterprise setting? The threats are different. So, we assess those threats, establish what the risks are, and then perform the activities required to manage those risks."*

Participating in SAFECode is key to the effort. Doughty was immediately drawn to joining SAFECode when he saw the other companies involved in the organization.

"At Intel, we have always benefited from engaging the community outside the company," he said. *"We saw that SAFECode included companies that have developed a lot of experience over the years. We wanted to be a part of that community, actively sharing with them, learning from each other what is working and what is not."*

Doughty was also committed to SAFECode's mission of increasing security assurance across all companies and products and improving overall security, industry-wide. Participating in SAFECode has helped Intel to develop more effective processes.

"Intel has embraced agile as a software development approach for quite some time," Doughty said. *"But there is an art to figuring out, as you are working these very short development cycles, how to apply a security development lifecycle to it. You cannot use the traditional lifecycle, which has many steps and may span six months to a year. Instead, you're working in a two-week sprint. One of the things that has really been beneficial for us from working with the folks at SAFECode, like Microsoft, Adobe, and others, is to further refine how we take and apply these steps and security practices in an agile environment."*

Looking ahead for Intel, David Doughty sees the need for secure software development practices to only increase.

"One trend that gets a lot of attention is the Internet of Things," he noted. *"So many devices – whether it be a camera, a watch, a drone – are becoming part of the Internet of Things. We're finding computing now in places where we never found it before. And so we need to take into account some very different environments. Take autonomous driving, for example, we're seeing an intersection between safety and security. That is something we have to be very cognizant of, and stay ahead of, to ensure that our products are going to meet all requirements. I think that is an area where we will see a SAFECode kind of approach to manage the relationship between the two domains of functional safety and security."*

As Intel's technologies bring more intelligence into devices in all facets of life, it makes the job a bit more challenging, but it's a good challenge.

About SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe Systems Incorporated, CA Technologies, Dell EMC, Intel Corporation, Microsoft Corp., Siemens AG and Symantec Corp. For more information, please visit www.safecode.org.