Security
April 20, 2009 4:00 AM PDT

Secure software? Experts say it's no longer a pipedream

by Elinor Mills

With the **Conficker worm** still hot and Microsoft patching multiple software vulnerabilities **last week,** it might be reasonable to assume the bad guys are winning the battle to get control over Internet-connected computers.

That's not necessarily the case. Developers are increasingly equipped with tools to shore up their products and vendors are collaborating in unprecedented ways to not only close holes in software, but also make sure they aren't in there in the first place, according to security experts.

"I think the industry as a whole is definitely getting better, but the spread between the best and the worst is widening," said Dan Geer, a risk management specialist and chief information security officer for In-Q-Tel, a nonprofit venture capital firm that invests in security technology.

"Conficker did far less damage in 2009 than it would have done in 2003," said Dan Kaminsky, director of penetration testing at IOActive. "Windows used to be a lot easier to blow up."

But on the eve of RSA, **the world's largest security conference**, which starts on Monday, experts say the hunt is on for the elusive Holy Grail of computer security-vulnerability-free software.

At RSA shows in years past, Microsoft was roundly criticized for releasing software full of security holes. **In**

2002, the company launched its Trustworthy Computing initiative, vowing to make security a top priority. Seven years later, the move is bearing fruit. The company reports that there are far fewer security holes in newer versions of its products and weaknesses in its operating system overall have dropped. Web applications have become the security bad boys of software.

In the second half of 2008, the proportion of Microsoft vulnerabilities on Vista-based machines accounted for just 5.5 percent of the total, Microsoft says. Machines running Vista were found to have 60 percent fewer infections than those running Windows XP, the company said in **a recent report**.

Microsoft went from being the vendor responsible for the greatest proportion of vulnerabilities to being third, with 2.5 percent share, according to research last year from IBM's X-Force. The lion's share of the vulnerabilities come from start-ups racing to be the next Facebook, and 70 percent of them are doing the security testing and review after they release the product, Microsoft says.

"Security is an inherently hard problem. It's difficult to get to perfection for any company," said Steve Lipner, senior director of security engineering strategy in Microsoft's Trustworthy Computing Group. "What we are seeing is the percentage of vulnerabilities coming out of major software organizations is dropping as a percentage of the total of vulnerabilities reported."

Better tools, fewer mistakes

The company has turned its Security Development Lifecycle (SDL) process into a pseudo-religion for other companies to follow. **Last year**, Microsoft began offering free SDL tools so outside developers can assess their practices and analyze their software designs to look for security weaknesses.

The tools for writing secure code are getting better, so developers are less likely to make mistakes, said Johannes Ullrich, chief security researcher at the SANS Institute security organization.

Microsoft isn't alone in providing help to the developer community. **HP is offering** a free tool that helps find holes in Flash applications, and **last week** announced tools that nonsecurity professionals can use to do security testing. **IBM sells a tool** for Flash and

Ajax developers, and **last week** the CERT Coordination Center at Carnegie Mellon released an open-source tool for testing ActiveX code.

In particular, Microsoft's recent release of an open-source tool called "!exploitable Crash Analyzer," which simplifies the process of identifying exploitable vulnerabilities during application development, is a "game changer," said Kaminsky.

"I don't think it's ever been quite so easy for non-security developers to recognize when they have vulnerabilities, when they have a flaw that could be used by a bad guy," he said.

Despite the recession, the software security market is growing significantly, accounting for more than $450 million in revenue in the U.S., Gary McGraw, chief technology officer at software security consulting firm Cigital, wrote **in an article last week**.

The challenge for developers

McGraw recently got a peek at the secure development processes at Microsoft, Google, Adobe, Wells Fargo, The Depository Trust & Clearing Corp., and four other leading companies, and released a report card of sorts (although grades are confidential) that other companies can use to gauge their level of progress. The **Building Security in Maturity Model** is "an objective yardstick" for development of products that are secure, McGraw said.

"In my view, software security is getting more and more important every single day," he said. "The good news is we are actually making some progress." The tools are out there, but the problem is developers often aren't trained, experts said.

A **Forrester survey commissioned by Veracode** and released last week found that only 34 percent of companies have a comprehensive software development lifecycle process that integrates application security and 57 percent of organizations don't have systematic application security training programs for developers.

Ullrich advocates a concept he called "software security street fighting"--where developers avoid complex techniques in which holes are more easily created.

"Developers, to some extent, can't really win," Ullrich said. "They have to be right

every single time, while an attacker only has to be right once." Meanwhile, companies are increasingly cooperating to fight off threats, such as **Conficker** and **attacks on a major flaw in the Domain Name System** (DNS) that threatened to create chaos on the Internet. Microsoft, IBM, Intel, Cisco, and Juniper Networks also have formed the **Industry Consortium for the Advancement of Security on the Internet**.

"In my mind a massive theme going on is that security is now larger than any individual company. It's larger than Microsoft, it's larger than the U.S. government," said Kaminsky, who first discovered the DNS hole. "This is something we're all going to need to work together on and have been to great effect."

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Vulnerabilities & attacks**

Tags: **Microsoft**, **security**, **development**, **SDL**, **RSA 2009**

Share: Digg Del.icio.us Reddit Yahoo! Buzz

Related

From CNET

Windows 7 security enhancements

Secure software? Experts say it's no longer a pipedream

Microsoft to patch Excel hole, seven others

From around the web

Secure software? Experts say it's no lon... CNN - Tech

Conficker Removal Reminders
Washington Post Blogs - Faster...

More related posts powered by Sphere