Editor: Scott L. Andresen, sandresen@computer.org
Briefs editor: David Ladd, daveladd@microsoft.com

News

Addressing The Monoculture

By Greg Goth

A new term has bubbled out of the specialized arena of academic nomenclature and into the mainstream, from daily newspaper columns to transcripts of Congressional hearings. That term is "monoculture."

According to some of the leading computer-security experts in the US, the dominance of Microsoft's Windows operating system has created an unsafe monoculture, in which critical networks and applications are tied together by one OS, and as such are all vulnerable to the same attacks. In a spate of activities regarding Windows' place in critical operating environments, elected officials, engineers, advocates, as well as Microsoft defenders and detractors have begun debating anew how—or if—stakeholders should hold Microsoft accountable for security flaws in its software.

In July 2003, the Department of Homeland Security announced it had awarded a US$90 million contract to Microsoft to supply desktop and server software. Within days, the Computer and Communications Industry Association (CCIA), a Washington D.C.-based industry organization that advocates networking technology diversity, requested that DHS Secretary Tom Ridge reconsider the contract.

In September 2003, seven leading security experts issued *CyberInsecurity: The Cost of Monopoly* (www.ccianet.org/papers/cyberinsecurity.pdf), a report claiming that Microsoft's business and software design practices pose a threat to the security of critical government and commercial networks. Distributed by the CCIA, the report advocates that no single OS be installed in more than 50 percent of the critical infrastructure. The CCIA did not pay the authors or contribute to its writing. Following the report's release, lead author Dan Geer was fired from his position as CTO of security firm @stake (they did not comment for this article). Geer's exit might have focused more attention on the report than it would have received otherwise.

In October 2003, Microsoft CEO Steve Ballmer addressed security concerns and procedures at length at the Microsoft developers' conference (https://s.microsoft.com/presspass/exec/steve/2003/10-09wwpc.asp). A day prior to Ballmer's speech, the US House Government Reform Committee's technology subcommittee—alluding to, without specifically naming Microsoft—asked DHS CIO Steven Cooper if monoculture should be a concern.

However, whether the new discussion will lead to any significant change in network-security or government-purchasing policy is unknown. While the introduction to the report calls it the "wake-up call that government and industry need to hear," it might also be perceived as a shot across the stern of a ship that's already sailed.

Market reliance

In the US, the political realities surrounding the Microsoft antitrust case have grown progressively less favorable for advocates of a policy deemphasizing use of Microsoft products, and neither commercial competition nor the much-ballyhooed attempt to provide an open-source desktop have managed to dent Windows' dominance.

"It's true, we have missed a golden opportunity," says CCIA president and CEO Ed Black. "I'm not convinced we don't have additional opportunities coming up that might not be perfect. They might only help ameliorate the problem. But by no means should everybody throw their hands up and say 'There's nothing we can do.' "

However, Geneva-based developer John Carroll, CEO of Turtleneck Software and a columnist for zdnet.com (www.turtlenecksoftware.com/default.aspx?section=8), believes the report to be a reprise of an unwarranted attack on Microsoft.

"I consider the CCIA report to be an attempt to open another front in the antitrust war against Microsoft," Carroll says. "The settlement between the [US Department of Justice] and Microsoft closes the book on attempts to reduce Microsoft's dominance of software markets, at least for now. That doesn't mean that

they can't try to link the issue to the war on terrorism. In this case, the CCIA replaces arguments related to economics with arguments related to national security. Both serve the same purpose, which is to encourage government to regulate downwards Microsoft's market power."

One veteran security expert, however, says the arguments about market equilibrium and the relative power markets and government should hold are beside the point in evaluating the danger of relying on Windows for critical applications. Peter G. Neumann, principal scientist at SRI Computer Science Laboratory, says monocultures by their very nature are unstable, and that Windows is simply not a securely designed product.

"The situation is inherently unstable, where you have a system in which the pieces are not only not modular, but also not relatively encapsulated, which means if something goes wrong in one module, it doesn't affect other modules," Neumann says. "One of the biggest problems with Microsoft's architecture is that there's no architecture."

Neumann cited an example, to which he has referred in testimony before the US House of Representatives, about a US Navy cruiser that shut down for more than two hours due to a failure in a Windows application.

"That shouldn't happen in a well-designed system. The application should not be able to shut down the operating system," Neumann says. "The fundamental problem is that unless you have a very strong architecture that is inherently capable of being made secure, and you have a strong sense of software engineering, which means you're practicing abstraction and modularity and encapsulation, and information hiding, and separation of duties, and principles of main privilege and all that—unless you have that—there's no hope for trying to secure a product that is supposedly backwards-compatible in some sense with all the bad software you've been developing the past 10 years. Now, given the fact the thing was never designed to be networked, the problem is even more difficult."

Counterpane Internet Security cofounder Bruce Schneier, one of the authors of the CCIA report, says the issue must be held in perspective.

"In some ways, this has nothing to do with Microsoft in particular," Schneier writes in his *Crypto-Gram* newsletter (www.schneier.com/crypto-gram.html). "Our concerns would be no different if everybody ran Macintosh OS X or Linux. Security researchers sounded the same alarm in 1988, when the Morris Worm infected about 5 percent of the UNIX systems on the Internet. Today the monoculture is more pervasive."

On the other hand, he says, it is about Microsoft, in that the company has used security as a justification to hide file formats from competitors and prospective partners, and to develop more applications and platforms that will be so tightly coupled into the Windows environment that interoperability with other products will be difficult at best.

"In economics, this is called lock-in," he says, "actions by a company to ensure its customers can't switch. It's bad for society and it's also bad for security."

Monoculture revisited

The dominance of Windows isn't the first computer monoculture to confront policymakers and consumers. In the 1960s and 1970s, the US DOJ and IBM contested a protracted antitrust case that resulted in immense changes in the market. While some aspects of the two dominant players of their respective eras are comparable, the extent of the network makes the Microsoft dominance much more dangerous for security, CCIA's Black asserts.

In 1969, IBM, which had, up to that time, sold its computers as complete hardware–software systems, agreed to debundle hardware and software.

"IBM acted fairly responsibly—not without reluctance—but fairly responsibly, to make sure software and hardware were separate products," Black says. "They debundled hardware and software the same way people want Microsoft to debundle Windows and other products, with the same impact, because many of these products could become platforms, sparking a tremendous amount of innovation and competition."

"With IBM, you were dealing with people who were very sophisticated, you had a lot of stuff custom-rigged. When you moved into a broad-based networked world, which is where we are, that's where you need a whole different approach. I think most people in Silicon Valley with any memory would agree the modern software industry was largely created because of the IBM ruling," Black says.

The dominance of Windows isn't the first computer monoculture to confront policymakers and consumers.

However, Carroll says Microsoft's critics are wildly overstating the benefits of a diverse operating environment.

"I didn't argue that monoculture doesn't have negative aspects. Rather, I argued that (a) platform diversity is not as secure as its proponents claim it is, given the difficulties of properly managing a diverse platform and application environment, and (b) you sacrifice economics of scale and add to development complexity by forcing platform diversity," he says. "Corporations and regular consumers need to properly understand the risks involved with using popular operating systems and applications. That doesn't mean, however, that the risks outweigh the cost-saving benefits of standardization on one platform, nor that platform diversity is automatically more secure than platform consistency.

"Even a casual reading of software history shows that it tends to be dominated by one company. Today, Microsoft dominates, though, before them, IBM ruled the software and hardware landscape. The root cause of this is the need for standards in a product that lacks natural compatibility, because standards, even of the de facto sort, lower costs for consumers and developers that target the market.

"It is good that consumers factor monoculture costs into their calculations when choosing a particular platform. It is not good to treat those costs as more important than any others."

Real-world synthesis

While the debate continues, the short-term effect of the CCIA report and the attendant discussion is, at the very least, a raising of awareness that goes to the very top of Microsoft.

In his October speech, Ballmer put the current security crisis in the pantheon of the company's moments of epiphany, equating it with the "call of the Internet in 1995, and this notion that we were being left behind," and the antitrust case.

"I think this issue, this crisis right now, that our customers and our partners are highlighting for us of security is that kind of defining moment," Ballmer said.

CCIA's Black says the report might have been just the most visible tip of a surge of discontent, and that Ballmer's speech was a reaction to that groundswell.

"We criticized the DHS for announcing a contract that was all Microsoft," Black says. "We've had meetings with the DHS people, and they indicated to us that they got it. They realized there was real danger in going the way they were going, and said they were going to be in touch with Microsoft to express how concerned they were. So I think Microsoft has been getting a lot of comments from a lot of people. Ours was a bit more out front and got publicity, but, in truth, I think they had such a bad problem they were getting hit by government and corporate CIOs, a lot of people were beating up on them."

However, Schneier says he is not convinced any significant improvement in Windows security is pending. Ballmer's speech, he says, was not a reaction to the CCIA report, but rather to the attention it received.

"It was a reaction to the press reaction to the report, a very important difference," he says. "As soon as the press started reporting it, he had to respond. In this case, it had the great spin of @stake firing Dan."

Schneier reiterated his long-standing belief that Microsoft will continue to give cursory attention to security until the company is held liable for bad software. As long as Windows dominates the desktop, and as long as economic losses caused by worms and viruses don't impact Microsoft's bottom line significantly, he sees no real resolution.

"It would have to be something where Microsoft feels the business pain. Right now they feel the PR pain," Schneier says. "So what do they do? We issue a report; they have a guy make a speech. A speech has never secured a computer."

When I asked a Microsoft representative whether the company would respond directly in writing to the report, she said, "The widespread use of Microsoft products around the world means we are constantly working to be responsive when vulnerabilities occur. That means sharing what we know with government, our industry counterparts, and the general public. Clear channels of communication are essential to addressing security threats." Then she clarified herself by saying "No."

For more information on the monoculture issue, see page 14.

***Greg Goth** is a freelance writer based in Connecticut.*