COMPUTERWORLD

by **Paul Roberts**

Black Hat: NAC solutions vulnerable to attack

News
Aug 03, 2006 • 3 mins

Cisco Systems Endpoint Protection Microsoft

They're not as secure as widely believed, says security expert Ofir Arkin

Network access control (NAC) technology has been promoted as the savior of beleaguered enterprise networks, but IT managers who hang their hats on client health screening should think again, according to Ofir Arkin, a security expert at Insightix.

In a presentation at this year's Black Hat Briefings conference in Las Vegas, Arkin raised questions about the efficacy of NAC technologies from vendors such as Cisco Systems Inc., Microsoft Corp. and Symantec Corp.. He said the current generation of NAC products is riddled with holes that make it easy for hackers to circumvent the technology's protections.

A Cisco executive acknowledged that NAC technology has a ways to go before it provides comprehensive protection.

In a wide-ranging presentation that mostly avoided dissections of specific products, Ofir said that across-the-board NAC solutions have holes or vulnerabilities in their protections that could be used by malicious hackers to gain entry to NAC-protected networks.

For example, NAC products that use Dynamic Host Configuration Protocol proxy servers to enforce security policy do nothing to stop machines that obtain static IP addresses for their network connections rather than using DHCP. That makes significant portions of enterprise networks invisible to the NAC products, Arkin said.

NAC solutions that enforce access through network switches, such as Cisco's Network Admission Control, also have weaknesses, Arkin said.

For example, Cisco's NAC technology is specific to the company's switches and routers. But enterprises often use a mixture of switching and routing gear, and hackers can find their way into an enterprise network simply by finding and connecting through an unmanaged switch, Arkin said.

Hackers can also spoof media access control and IP addresses for "known" systems that are allowed access, he said.

NAC products that rely on the 802.1x protocol to enforce access policies before systems are assigned an IP address provide tighter control, but they don't cover devices that don't support the 802.1x protocol, such as legacy hardware, printers and other devices, Arkin said.

Other security experts at Black Hat also expressed doubts about the NAC paradigm. Marc Maiffret, of eEye Digital Security, whose vulnerability scanning tools work with Cisco's NAC and other solutions, said that NAC systems that rely on antivirus software to report on the "health" of a system are suspect at a time when critical security holes are being reported in products from Symantec, McAfee Inc. and other vendors.

Computerworld Smart Answers Learn more

Explore related questions

Ask a question

ASK

Malicious hackers could use exploits of antivirus software, Web browsers or other desktop software to make infected clients appear to be adequately patched and have up-to-date

antivirus definitions, he said.

Asked about Arkin's presentation, Cisco Chief Security Officer John Stewart acknowledged that NAC technology is in its infancy and has a ways to go before it will provide comprehensive security.

"The technology's immature. But [NAC] will increase my capability to keep my network in good condition," he said. "Can it be maneuvered to have false data? Yes. Would it be completely the case that every device on my network will provide false data? Unlikely."

Stewart added, "It's inherently going to be found that there are weaknesses. But I think that's the wrong thing to focus on. We want to address the weaknesses but focus on the benefits."

Sponsored Links

Empower your cybersecurity team with expert insights from Palo Alto Networks.

Accelerate impactful results with Elastic on Microsoft Azure. Seamlessly access Elastic Search, Observability, and Security within the Azure portal to quickly derive and act on data insights.

Secure AI by Design: Unleash the power of AI and keep applications, usage and data secure.

Copyright © 2025 IDG Communications, Inc.