The dangers of too much Java

January 31 2013

Assistant Professor of Computer Science and Engineering Justin Cappos.

Justin Cappos, an assistant professor of computer science and engineering at the Polytechnic Institute of NYU-Poly, has long been wary of the security risks inherent in Java, the programming language developed by Sun Microsystems in the 1990s. Referring to the libraries of algorithms, data structures, and commands that are part of every computing language, he said, "In Java, the standard libraries are huge; they involve about a million lines of code. A small problem in any one of those lines can leave Java vulnerable to attack."

Lately, those security issues have been receiving increasing attention in the press. On January 13 of this year, for example, Oracle released Java 7, Update 11, and within a day, as journalists worriedly reported, hackers had begun exploiting glitches within the update. Cappos explained one of the major dangers of such exploits, warning, "A hacker taking advantage of bugs in Oracle's program could conceivably make your computer part of a botnet, a collection of machines whose security has been breached and which are now under the control of that party." Because botnets have been used to send viruses or worms, commit fraud, and collect personal information via spyware, among other malicious activity, the social and financial ramifications are enormous. As Oracle admits on its Web site, "Successful exploits can impact the availability, integrity, and confidentiality of the user's system."

While the company continually develops "patches" to try to correct the problems, Cappos is not confident that any lasting solutions will be found. "There's no end in sight," he said. "As fast as Oracle can fix one bug, another is discovered." He strongly suggests that users disable Java on their machines. "Other computer-security experts agree, and we're not being alarmists here. Even the Department of Homeland Security is making the same recommendation." He stresses that disabling Java will not affect a computer's performance or utility. "The program once made the browsing experience more powerful and responsive and allowed for wonderful, complex websites," he recalled.

"But Java is now totally unnecessary for most end-users, and developers of Internet Explorer and Chrome have worked to make disabling it a simple process anyone can complete. Firefox and Safari now disable Java by default." Cappos cautions that many people confuse Java and JavaScript, although the two are vastly different products whose similar names are merely the result of a poor marketing decision. "I once heard an apt description that Java is to JavaScript as car is to carpet," he quipped. "JavaScript is unequivocally not part of the Java platform and

does not pose similar dangers."

Years ago, Cappos approached the software giant about its security risk of having a large amount of security critical code in Java. He draws on practical experience with a secure execution environment for the Seattle TestBed, a free, community-driven, open-source system that operates on laptops, servers and phones. The global distribution of the Seattle network provides the ability to use it in cloud computing, peer-to-peer networking, ubiquitous/mobile computing, and distributed systems, among other application. It boasts thousands of users around the world, including major universities and research facilities and is open for anyone to participate in.

Because Seattle's sandbox employs only about 8,000 lines of trusted code, it runs in a safe and contained manner, with minimal impact on system security and performance. "We're always working to see how far we can push. We want to make it even smaller," Cappos said. "A million lines is obviously just too much."

Provided by Polytechnich Institute of New York City

Citation: The dangers of too much Java (2013, January 31) retrieved 23 June 2024 from https://phys.org/news/2013-01-dangers-java.html