

New Program by Computer Scientist Prevents Crashes and Hacker Attacks

December 26 2006

Today's computers have more than 2,000 times as much memory as the machines of yesteryear, yet programmers are still writing code as if memory is in short supply. Not only does this make programs crash annoyingly, but it also can make users vulnerable to hacker attacks, says computer scientist Emery Berger from the University of Massachusetts Amherst.

With such problems in mind, Berger created a new program that prevents crashing and makes users safer, he says. Dubbed DieHard, there are versions for programs that run in Windows or Linux. DieHard is available free for non-commercial users at www.diehard-software.org.

Almost everything done on a computer uses some amount of memory—each graphic on an open Web page, for example—and when a program is running, it is constantly requesting small or medium chunks of memory space to hold each item, explains Berger. He likens the memory landscape to a row of houses, each with only enough square footage for a certain number of bytes. The problem, says Berger, is that sometimes when memory real estate is requested, programs can unwittingly rent out houses that are already occupied. They also might request a certain amount of square footage when they actually need more, so an item can spill over into another “house.” These mistakes can make programs suddenly crash, or worse.

“Ironically, crashing is the best thing that can happen,” says Berger. “An overflow also can make your computer exploitable by hackers.”

One way that the computer becomes more vulnerable results from the fact that “addresses” that are designated for a password, for example, will be on the same lot on the same street in every version of the program. So if a hacker overwrites a password, he or she can easily locate the password address on any of the umpteen versions of the program that are out there.

DieHard presents several remedies to such problems. First, it takes a compact row of memory buildings and spreads them around in the landscape. It also randomly assigns addresses—a password that has a downtown address in one session may be in the suburbs next time around. And in some versions of the program, DieHard will secretly launch two additional versions of the program the user is running—if a program starts to crash, that buggy version gets shut down and one of the other two is selected to remain open. DieHard can also tell a user the likelihood that they’ll have been affected by a particular bug.

These problems wouldn’t arise if programmers were a little less focused on speed and efficiency, which is rarely a problem these days, and more attentive to security issues, says Berger.

“Today we have way more memory and more computer power than we need,” he says. “We want to use that to make systems more reliable and safer, without compromising speed.”

Berger developed DieHard together with Microsoft researcher Ben Zorn. Berger has received a \$30,000 grant from Microsoft, a \$30,000 grant from Intel, and a \$300,000 grant from the National Science Foundation for his work on DieHard.

Source: University of Massachusetts Amherst

Citation: New Program by Computer Scientist Prevents Crashes and Hacker Attacks (2006, December 26) retrieved 19 April 2024 from <https://phys.org/news/2006-12-scientist-hacker.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.