

Software industry's 'patch culture' attack

An attack from the security chief of software giant Oracle on the so-called culture of patching and bug-ridden products in the software industry has drawn fire from industry observers, citing the comments as hypocritical and naive.

Chief Security officer Mary Ann Davidson was speaking at the recent WWW2006 conference in Edinburgh, Scotland, when she commented on how the software industry was allegedly packed with bug-filled products, saying that "you wouldn't get on a plane built by software developers." CDNet reported on the speech in which Davidson described the industry as one in which most software developers weren't trained to "think in terms of safety, security and reliability" but instead being attached to a culture of "patch, patch, patch." This "patch culture" was costing businesses \$59 billion, she said.

Software patches are small pieces of software that are designed to either fix or update computer programs and are more common in large-scale projects. Although designed to smooth out problems, increase usability and get rid of pesky bugs, patches can sometimes introduce new problems, too. While being criticized as being inefficient and wasteful, it can also be a necessity when insecure software is built.

Davidson drew comparisons between software engineers and civil engineers, saying "What would happen if civil engineers built bridges the way developers write code? What would happen is that you would get the blue bridge of death appearing on your highway in the morning." She claimed that while civil engineers were trained to think in terms of safety, security and reliability, software engineers were not.

These problems were part of a broader picture that touched on national security and potential regulation of the software industry. Davidson said that she had taken a straw poll of the chief security officers on the CSO, a professional organization for security officers, and that many of them thought that the industry should be regulated. If regulation was brought in, the industry would only have itself to blame: "Industries don't want to be regulated, but if you don't want to be regulated, the burden is on you to do a better job."

The Oracle manager's comments were jumped on by industry observers and hackers and slated as being hypocritical. Discussants at the Slashdot technical online forum revealed that Oracle itself had a five-year turnaround between when it received reports on the bugs in its own software and when it actually got around to fixing them. Comments made on the forum reflected the mood that Oracle ought to remove the beam in their own software before criticizing the speck in others.

Davidson's analogy between civil and software engineers was also roundly mocked and criticized as being extremely naive. If bridges were indeed built to the same demands and deadlines as software products they would be expected to be built in any location, able to cope with any conceivable vehicle that could be driven over it, and resistant to terrorist attacks -- all while being built at low costs. Software is expected to be cheap, released quickly and able to run on multiple platforms, and bug-ridden programs are the inevitable outcome of working to these tight and frugal demands. The secure bug-free software that security officers desire can certainly be built, but only after a lengthier, more expensive development process -- and its this, industry observers say, is where the problem lies. "Bean-counting" managers will still aim for the bottom line of saving money and getting products to market quickly, at the cost of security and function.

Observers believe the call for regulation may have been missing the point somewhat, with suspicion that the target of regulatory activities wouldn't be the buggy products being released but the hackers who draw attention to the bugs.

One aspect of Davidson's speech that seemed to escape criticism was the comment that the British were better at hacking due to their skill, disrespect for authority and "just a touch of criminal behavior."

Copyright 2006 by United Press International

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