

Researchers discover new way to patch holes in the 'cloud'

November 29 2010, By Matt Shipman

Researchers from North Carolina State University and IBM have invented a way to update computer systems packaged in virtual machines in a computer “cloud” – even when those programs are offline.

The new cloud computing patch tool developed by NC State and IBM is called Nuwa and protects [virtual machines](#) (VMs) from cyber-attacks by ensuring that they always receive important [security](#) upgrades. In addition, the researchers have determined that offline application of security patches is more than four times faster than online patch application. The tool is named after a Chinese goddess who patched a hole in the sky.

A paper describing the research, “*Always Up-to-date – Scalable Offline Patching of VM Images in a Compute Cloud*,” will be presented Dec. 10 at the Annual Computer Security Applications Conference in Austin, Texas.

“We’ve designed a way to patch these virtual machines while they are offline, so that they are kept up to date in terms of security protection,” says Dr. Peng Ning, professor of computer science at NC State and co-author of a paper describing the research. “Current patching systems are designed for computers that are online and they don’t work for dormant computers or virtual machines. The tool we developed automatically analyzes the ‘script’ that dictates how a security patch is installed, and then automatically re-writes the script to make it compatible with an offline system.”

Nuwa leverages a collection of techniques developed by IBM, called Mirage, that is used for performing efficient offline introspection and manipulation of a large collection of VM images, to allow cloud administrators to patch multiple VMs simultaneously. A program already exists that allows cloud computing systems to operate more efficiently by saving one version of a computer file that is used by multiple VMs – rather than saving the same file repeatedly for each individual VM. Nuwa takes advantage of this technology and, by patching one file, can ultimately protect all of the VMs that use that file.

NC State and IBM have successfully tested and evaluated Nuwa on the IBM Research Compute Cloud, a compute cloud that is used by IBM researchers worldwide.

Cloud computing enables users to create many VMs on one large computing platform, with each VM being able to perform various computer functions. It is so easy to create these VMs, that businesses and individuals will often create them to perform very specific tasks on a periodic basis. Because many of these VMs are used infrequently, they are often left dormant for extended periods of time, so that they are not consuming energy and computer resources when not in use.

These dormant periods pose a significant security problem, because VMs that are offline do not receive security upgrades, known as patches. This leaves the VMs vulnerable to cyber-attacks when they are brought back online. The VMs are particularly vulnerable if they have been left dormant for months, and missed significant patches.

More information: *“Always Up-to-date – Scalable Offline Patching of VM Images in a Compute Cloud”* by Wu Zhou, et al. IBM T. J. Watson Research Center. Presented: Dec. 10, 2010, at the Annual Computer Security Applications Conference, Austin, Texas.

Provided by North Carolina State University

Citation: Researchers discover new way to patch holes in the 'cloud' (2010, November 29)
retrieved 23 April 2024 from <https://phys.org/news/2010-11-patch-holes-cloud.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.