NAIST® Research Highlights

Nara Institute of Science and Technology | **Internet Engineering Laboratory** www.naist.jp/en

Cloud computing offers many benefits, but it can comprise security.

Cloud computing

Security vulnerabilities detected

A security analysis highlights the vulnerabilities of popular cloud management software, OpenStack

An analysis of the most widely used open-source cloud management software, OpenStack, by NAIST researchers confirm concerns about its security. In particular, it exposes OpenStack's susceptibility to security problems propagating between different parts (or 'trees') of its system[1].

Cloud computing offers individuals and companies many benefits, including convenient access to data and the ability for team members in different locations to simultaneously work on the same projects. But accompanying its rapid rise in popularity are concerns regarding security. In particular, software that provides free tools for constructing and managing cloud computing platforms for both public and private clouds — known as open-source cloud management software — has come under scrutiny.

The most popular open-source cloud management software platform is OpenStack. In addition to having a reputation for being easy to use, it is backed by some of the biggest names in information technology, including Dell, NEC, Hewlett-Packard and IBM. Furthermore, it is supported by an enthusiastic global community of volunteers. However, its security vulnerabilities have scored highly on the National Vulnerability Database, a publicly accessible database for computer-related vulnerabilities managed by the U.S. government.

To evaluate these concerns, Takeshi Okuda and colleagues at NAIST's Internet Engineering Laboratory performed a security analysis of OpenStack. They did these by performing a fault tree analysis, to evaluate the vulnerabilities of the cloud management software. A fault tree is a helpful tool for quantitatively analysing a system, as it generates a graphical representation of an undesirable event in a system based on Boolean logic.

Using this approach, the researchers were able to generate high-level vulnerability trees, which can be used by organizations wanting to quantify their own OpenStack cloud infrastructure. They found that the high degree of interconnectedness of OpenStack's architecture means that security problems in one tree can propagate to other trees.

However, the team was not able to evaluate OpenStack's security as completely as they had hoped, because the currently used naming system for vulnerabilities fails to account for subcomponents of main components.

The results were not a complete surprise to the researchers as they had "expected to find some sort of vulnerability propagation between the different components," explains Fall Doudou, a doctoral student from Senegal. "But the fact that the security quantification could not be more accurate came as a surprise."

The researchers are now planning to come up with a new naming system that takes into account all the details of the components of OpenStack while conforming with the current standards in the community.

Reference

1. Fall, D., Okuda, T., Kadobayashi, Y. & Yamaguchi, S. Towards a vulnerability tree security evaluation of OpenStack's logical architecture. *Lecture Notes in Computer Science* **8564,** 127–142 (2014).

More information about the group's research can be found at the Internet Engineering Laboratory webpage:
http://isw3.naist.jp/Contents/Research/cs-07-en.html