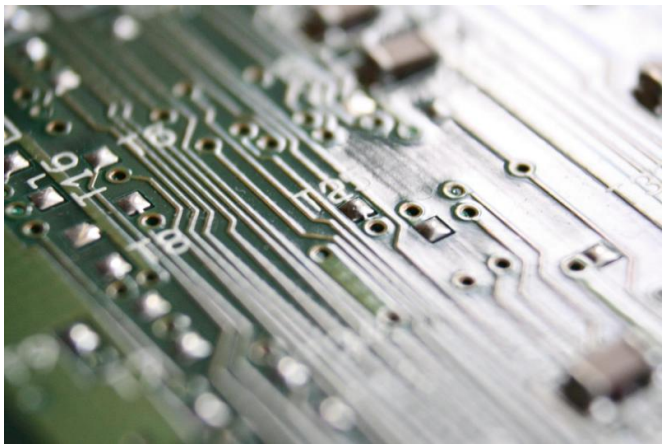
# New hacking technique imperceptibly changes memory virtual servers

11 August 2016



Credit: Public Domain

For the first time ever a team of Dutch hacking experts, led by cyber security professor Herbert Bos at Vrije Universiteit Amsterdam, managed to alter the memory of virtual machines in the cloud without a software bug, using a new attack technique.

With this technique an attacker can crack the keys of secured virtual machines or install malware without it being noticed. It's a new deduplication-based attack in which data can not only be viewed and leaked, but also modified using a hardware glitch. By doing so the attacker can order the server to install malicious and unwanted software or allow logins by unauthorized persons.

**Deduplication and Rowhammer bug**

With the new attack technique Flip Feng Shui (FSS), an attacker rents a virtual machine on the same host as the victim. This can be done by renting many virtual machines until one of them lands next to the victim. A virtual machine in the cloud is often used to run applications, test new software, or run a website. There are public (for everyone), community (for a select group) and private (for one organization accessible) clouds. The attacker writes a memory page that he knows exists in the victim on the vulnerable memory location and lets it deduplicate. As a result, the identical pages will be merged into one in order to save space (the information is, after all, the same). That page is stored in the same part of the memory of the physical computer. The attacker can now modify the information in the general memory of the computer. This can be done by triggering a hardware bug dubbed Rowhammer, which causes flip bits from 0 to 1 or vice versa, to seek out the vulnerable memory cells and change them.

**Cracking OpenSSH**

The researchers of the Vrije Universiteit Amsterdam, who worked together with a researcher from the Catholic University of Leuven, describe in their research two attacks on the operating systems Debian and Ubuntu. The first FFS attack gained access to the virtual machines through weakening OpenSSH public keys. The attacker did this by changing the victim's public key with one bit. In the second attack, the settings of the software management application apt were adjusted by making minor changes to the URL from where apt downloads software. The server could then install malware that presents itself as a software update. The integrity check could be circumvented by making a small change to the public key that verifies the integrity of the apt-get software packages.

**Advise NSCS**

Debian, Ubuntu, OpenSSH and other companies included in the research were notified before the publication and all have responded. The National Cyber Security Centre (NSCS) of the Dutch government has issued a fact sheet containing information and advice on FFS.

**'Hack-Oscar'**

The researchers presented their findings this week during the UNESIX Security Symposium 2016 in the United States. Recently they won the Oscar of hacking: the Pwnie for another attack technique that allows attackers to take over state-of-the-art software (such as the new Edge browser on Microsoft Windows) with all defences up, even if the software has no bugs. Moreover, they can do this from JavaScript in the browser.

**More information:**
www.cs.vu.nl/~kaveh/pubs/pdf/ffs-usenixsec16.pdf

Provided by University of Amsterdam