National Cyber Security Centre
Ministry of Security and Justice

Use virtualisation wisely

Ensure you know the neighbours of your sensitive virtual systems

Factsheet FS-2016-05 | version 1.0 | 10 August 2016

Virtualisation of ICT services ensures more efficient and flexible use of hardware. This factsheet is about specific risks that arise when you use virtual servers to outsource ICT services. Your virtual server has an unknown number of virtual neighbours on the host. By using the newly discovered Flip Feng Shui attack method, an attacker can penetrate a virtual neighbour or have it install malware. To date, an attacker could only eavesdrop on the activity of virtual neighbours. The success probability of such an attack was much lower. The NCSC advises to establish, in rules on information security, which types of systems in your organisation may be virtualised. Additionally, establish in which types of cloud these types of systems may be accommodated.

Background

Virtualisation of ICT services ensures more efficient and flexible use of hardware. Most ICT systems hardly ever make full use of the available processing power, memory, disk space and bandwidth. By having multiple ICT systems share the hardware of a single physical computer, this hardware is used for a larger share of the time. This practice is called (hardware) virtualisation.

A well-known example of virtualisation is using a 'virtual private server' (VPS), for example by renting it. Vendors range from small ICT companies to global players such as Amazon EC2 and Microsoft Azure.

Target audience

Information security professionals, administrators and architects of organisations that purchase or internally use virtualised services (such as cloud servers).

This factsheet was written in collaboration with:

Team High-Tech Crime
Onderzoeksteam 'Flip Feng Shui'[1]
Belastingdienst
Atos

[1] Kaveh Razavi, Ben Gras and Erik Bosman, Vrije Universiteit Amsterdam; Bart Preneel, Katholieke Universiteit Leuven; Cristiano Giuffrida and Herbert Bos, Vrije Universiteit Amsterdam.

A virtual server is accommodated on a ***host***. That is the physical system upon which the virtual server runs. The host is administered by the vendor that provides you with the virtual server. Your virtual server usually has anunknown number of virtual neighbours on the host. These are virtual servers of other clients of the vendor. Vendors accommodate the virtual servers on a group of hosts, a so-called cloud. There are multiple types of clouds, which differ in the extent to which virtual servers of different clients are accommodated on the same host. Refer to the box 'Clouds: public, community and private' for more details.

The ***hypervisor*** is the software on the host that provides the different virtual servers with access to the shared hardware of the host. Well-known hypervisors on servers are, for example, KVM, VMware ESXi and Xen.

Virtualisation is also used on client systems. Well-known hypervisors on client systems are, for example, Oracle VirtualBox and VMware Workstation. The technical observations in this factsheet are equally applicable there. The perspective for action, however, is focussed on server applications.

Clouds: public, community and private

An attacker can only perform attacks with Flip Feng Shui or side channels if his virtual server runs on the same host as his victim. The easier it is to acquire a virtual server on the host of your virtual server, the easier an attacker can attempt to penetrate.

In the NCSC whitepaper Cloud Computing, several types of clouds are discussed. These differ in the ease with which an outsider can acquire a virtual server on one of the hosts.

A ***public cloud*** is accessible for everyone. Everyone who is willing to pay can have a virtual server on one of the hosts.

A ***community cloud*** is accessible for a limited group. The selection mechanism differs between vendors. An example is a vendor that employs a client acceptance procedure.

A ***private cloud*** is only accessible for one organisation. This organisation can host the cloud themselves or outsource this hosting to an external provider.

This factsheet is about specific risks that arise when you use virtual servers to outsource ICT services. Additionally, every use of cloud services implies more general risks. If you use virtual servers, these risks apply as well. These risks are discussed in the NCSC whitepaper 'Cloud Computing'.[2] This factsheet forms an addition to the advice in the whitepaper.

What is the matter?

Attackers are capable of adjusting data of servers that are their virtual neighbours. This allows them to penetrate these servers or have them install malware.

The Flip Feng Shui attack method (see box) is the first example of an attack technique that allows the attacker to perform changes in the memory of another virtual server. In this way, he can attack the virtual server directly.

Flip Feng Shui is not just a theoretical vulnerability. An attacker can use Flip Feng Shui in a practical setting, on a host with tens of virtual servers. However, a targeted attack is more difficult. It is not easy to obtain a virtual server that runs on the same host as a given virtual server. The probability of success of Flip Feng Shui therefore largely depends on the type of cloud on which the virtual machine is accommodated.

Academics and other researchers have been finding ways for a virtual server to eavesdrop on his virtual neighbours for years. A way to eavesdrop on virtual neighbours is called a ***side channel***,[3] because it is an unintended channel of communication.

When an attacker is able to eavesdrop upon his virtual neighbours, he can acquire confidential information that is processed on the other servers. Most side channels only leak a limited amount of information. The most attention is therefore given to eavesdropping on cryptographic keys. These are, after all, small pieces of information that are nevertheless crucial for information security. With an eavesdropped cryptographic key, an attacker can decrypt encrypted data storage or intercepted network traffic.

Side channels are not easy to abuse in practice. Most known side channels have only been applied successfully in a laboratory setting. In practice, hosts contain tens of virtual servers. An attacker can hardly discern the signals of his target from those of other servers. Also, it is not easy for most attackers to enforce that their virtual server runs on the same host as their victim.

[2] See https://www.ncsc.nl/actueel/whitepapers/whitepaper-cloudcomputing.html.
[3] Side channels occur in more places than just between virtual servers. For example, side channels can exist between two processes on the same system.

The Flip Feng Shui attack method: question and answer

How does the Flip Feng Shui attack method work in essence?	An attacker rents a virtual server on the same host as your virtual server. Next, the attacker ensures that the hypervisor deduplicates a certain part of the memory that both virtual servers share. That means that both systems store certain information that they both process, in the same part of the physical memory. By employing the so-called rowhammer technique[4], the attacker is able to change the information in this memory without the hypervisor or your virtual server noticing. In this way, he is able to convince your virtual server to install malware or allow logins by unauthorised persons.
Which systems are vulnerable?	All virtual servers that are accommodated on hosts that apply memory deduplication.
I am the owner of a virtual server: how do I mitigate the vulnerability?	You cannot mitigate the vulnerability yourself. Urge your vendor to disable memory deduplication on the host on which your virtual server is accommodated.
How likely is it that I will encounter the attack method?	The researchers have not published the code that they wrote to perform the attack method. For an attacker with limited knowledge and means, the attack method is therefore hard to perform. For an attacker with ample knowledge and means, the information in the research report is enough to perform the attack. A criminal organisation or foreign intelligence service is probably capable of doing this. However, this does require them to adjust their code for the specific operating system that you run on your virtual server.
How is the attacker able to penetrate the virtual server?	In the research report, the authors describe two attacks on Debian and Ubuntu, as an example. With the first of these two attacks, an attacker is able to penetrate a server. The attacker aims to change a setting of OpenSSH. He slightly changes a public key that is authorised to login to the server. He is easily able to break this modified key. In this way, he is able to access the server.
How is the attacker able to have the virtual server install malware?	In the research report, the authors describe two attacks on Debian and Ubuntu, as an example. With the second of these two attacks, an attacker is able to have the server install malware. The attacker aims to change the settings of software package manager apt. He slightly changes the URL from which apt downloads software. He thus ensures that the server installs malware that masquerades as a software update. He circumvents the integrity check by also slightly changing the public PGP key with which apt checks the software.
What makes this attack method different from similar techniques?	Previously discovered attack methods, so-called side channels, aim to eavesdrop on a virtual server on the same host, and gain access to confidential information. This is the first attack method that enables an attacker to change the contents of the memory of another virtual server. In this way, he can directly attack the virtual server.
Why is the attack method called Flip Feng Shui?	The name of the attack method consists of two parts. 'Flip' refers to the bit flips that the attacker is able to achieve on your virtual server. 'Feng Shui' is a Chinese philosophy about bringing things in harmony with their environment. The way in which virtual servers adopt the changes from their neighbours in this attack is highly reminiscent of this philosophy.
Where can I find more information about the attack method?	The researchers have presented their findings on the USENIX Security Symposium 2016. Their slides and research report are available on https://www.vusec.net/projects/flip-feng-shui/.
I have a different question.	A more extensive variant of this 'question and answer', including perspective for action for owners of hosts, is available on https://www.ncsc.nl/english/current-topics/factsheets/flip-feng-shui-attack-method-question-and-answer.html.

[4] See for example https://en.wikipedia.org/wiki/Row_hammer.

Perspective for action

1. Perform a risk analysis to determine for each type of ICT system of your organisation whether it should be virtualised. Establish in which type of cloud these types of systems may be accommodated. You can determine this by considering the sensitivity of the processes of which the systems are part.
2. Ask your vendor in which types of cloud he can accommodate your virtual servers. Ask which admission criteria they apply to their private and community cloud offerings.
3. Establish your choice in rules about information security, including the supporting considerations.
4. Migrate virtual ICT systems that do not run in the appropriate type of cloud to a private or community cloud or a non-virtualised environment.

What could happen?

If you use a virtual server, a virtual neighbour can change data in the memory of your server. In this way, he can break into your virtual server. He can do this with the Flip Feng Shui attack method (see box). It is to be expected that more similar attack methods will be found in the future. Flip Feng Shui can also be used when the host contains many other virtual servers, as well. However, the attacker has to enforce that his virtual server runs on the same host as his target. This, of course, does not apply in an untargeted attack.

Aside from Flip Feng Shui, attack methods with which virtual servers can attack their neighbours have been known for some time. However, the probability of success of such an attack is much lower. Aside from the task of running a virtual server on the same host as the target, it is not easy to eavesdrop on one virtual server amidst tens of others. The probability of such an attack is therefore small. For most virtual servers general cloud risks are much more relevant, such as the risk that your vendor or a third party is able to access your data via the hypervisor.

Each attack in this category is only possible as long as the owner of the host has not yet performed the right update or set the correct setting. In general, vendors of hypervisors publish updates or instructions to prevent newly discovered attack methods. As a customer, you cannot easily determine whether your vendor has already applied such measures.

What does the NCSC recommend?

The NCSC recommends to establish which types of systems in your organisation may be virtualised in rules about information security. Establish in which type of cloud these types of systems may be accommodated. These rules should be applied when purchasing or securing ICT systems. You determine which types of systems to consider by performing a risk analysis. You may, for example, decide that you accept the risk of attack methods such as Flip Feng Shui and side channels in a public cloud for certain categories of systems. This conclusion is justified, for example, when these systems rarely process sensitive information.

Only if an attacker is able to become your virtual neighbour, can he perform attacks via side channels or Flip Feng Shui. These attacks therefore do not work if the attacker does not have access to virtual servers on the same host. You can enforce this by ensuring that only your organisation may accommodate virtual servers on this host, and that the attacker is not able to penetrate the other servers. Ask your vendor which admission criteria they apply when admitting virtual servers on the hosts on which your virtual servers are accommodated.

Apply your modified rules for virtualisation of ICT systems to existing virtual servers as well. Migrate ICT systems to cloud environments of the right type. Migrate to non-virtual servers if your rules about information security state that these systems may not be virtualised.

Finally

Flip Feng Shui presents a significant change to the risk profile of virtual servers. Side channel attacks were a mostly theoretical risk. That does not apply to Flip Feng Shui. Vendors can take measures to prevent the attack method. It is to be expected that researchers will discover similar attack methods in the coming years. It is therefore important that your vendor is up-to-date with the latest developments.

Publication
Nationaal Cyber Security Centrum (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2016-05 | version 1.0 | 10 August 2016