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[1], 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 host: how do I mitigate the vulnerability?	Disable memory deduplication in the configuration of your hypervisor. In old versions of some hypervisors, memory deduplication is enabled by default.
Memory deduplication provides me with a large efficiency advantage. Can I mitigate the vulnerability in some other way?	The article of the researchers describes several alternative measures. Zero-page deduplication is a less drastic form of memory deduplication. If you use this, Flip Feng Shui can no longer be performed on your host. This form of memory deduplication yields less efficiency advantage than full memory deduplication. Another case in which Flip Feng Shui cannot be performed, is if the internal memory of your host is resistant to known rowhammer techniques. However, there is no easy way to determine if the internal memory of your server is resistant to known rowhammer techniques. Also, new rowhammer techniques are discovered regularly. The internal memory of your server may prove to be vulnerable to one of these new techniques.
I use ECC memory in my host. Can the attack method still be performed on my host?	The use of ECC memory makes it harder to perform the attack method. The host will notice single bit flips and is able to correct them. An attack then costs twice as many bit flips and is correspondingly more difficult. The researchers have observed that multi-bit flips occur as well. The use of ECC memory therefore does not fully prevent the attack method.
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.
Can this attack method also be applied against other virtual machines than servers, such as on a workstation?	Yes. The attack method does not use specific properties of servers, so an attacker can also use the attack method on other virtual machines. However, he needs to already have access to another virtual machine on the same host. The probability of this is much higher on a host that runs servers with many different administrators.
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	The name of the attack method consists of two parts. 'Flip' refers to the bit flips that the attacker is

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

Flip Feng Shui?	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/.