Flip Feng Shui
(Rowhammering the VM's Isolation)

Kaveh Razavi*‡, Ben Gras*‡, Erik Bosman‡,
Bart Preneel◊, Cristiano Giuffrida‡, Herbert Bos‡

*** Joined First Authorship**
‡ Vrije Universiteit Amsterdam
◊ Katholieke Universiteit Leuven

Flip Feng Shui (FFS) is a new exploitation vector that allows an attacker virtual machine (VM) to flip a bit in a memory page of a victim VM that runs on the same host as the attacker VM. FFS relies on a hardware vulnerability for flipping a bit and a physical memory massaging primitive to land a victim page on vulnerable physical memory location.

While the requirements for FFS may seem unrealistic, our work shows that it is possible to implement FFS reliably today in the cloud using Rowhammer, a wide-spread DRAM glitch, and memory deduplication, a popular memory management feature that reduces physical memory footprint of VMs by merging memory pages with the same content.

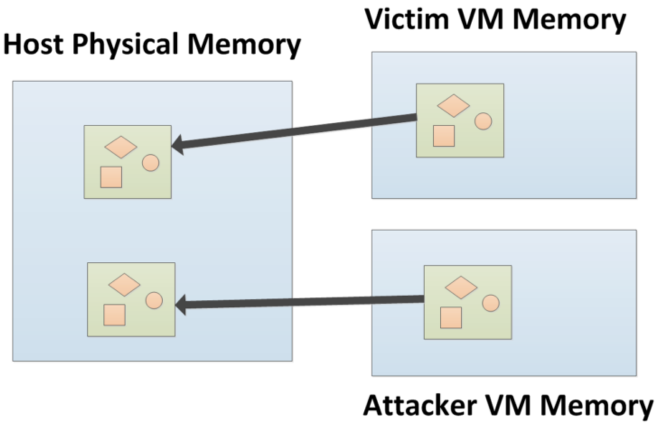
For a simple and slightly humorous explanation of FFS, please watch the following teaser video: https://youtu.be/ViIrZYpOyWQ

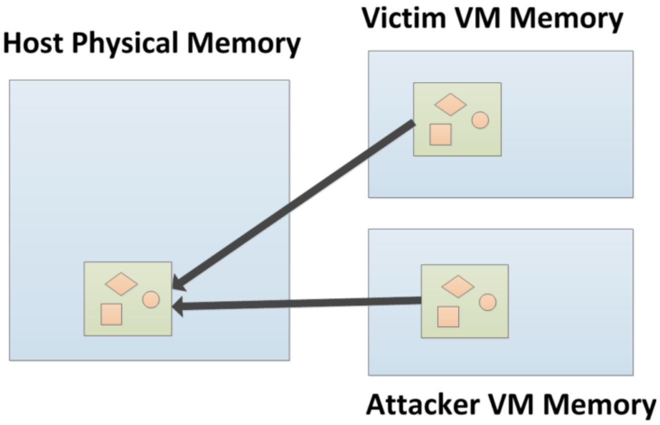
Flip Feng Shui: The Mechanics

Our FFS attack runs in three phases:

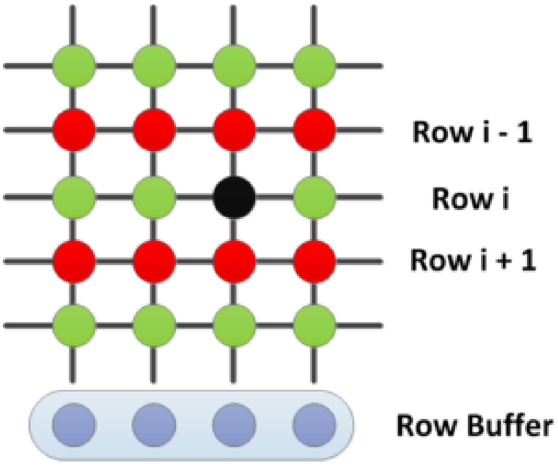
1. The attacker VM first profiles its memory to find memory cells vulnerable to Rowhammer. The data stored in these memory cells can change without writing to them by triggering Rowhammer.

2. Once a suitable bit flip has been found (i.e., one at the right offset within a memory page), the attacker writes a memory page that she knows exists in the victim on the vulnerable memory location. Memory deduplication engine then merges the victim's page with the attacker's page like shown in the figure below.





3. If the attacker VM’s physical memory is chosen to back both pages (refer to our USENIX paper to see how this can be done), the attacker can then trigger Rowhammer to modify the memory of the victim. As shown in the figure below, DRAM is organized in rows, and repeated activation of two rows (e.g., row i-1 and i+1) can trigger a flip in another row (e.g., row i).



Note that simply writing to the deduplicated page from the attacker triggers a copy-on-write event to preserve the correct memory isolation semantics, but with Rowhammer, since the bit flip happens directly on the DRAM, there will be no copy-on-write, compromising the VM’s memory isolation even under full memory virtualization provided by recent processors.

So what can an attacker do with FFS? We demonstrate two attacks: breaking OpenSSH’s public key authentication and fully compromising apt-get.

Compromising OpenSSH

Our first attack flips a bit in the page cache of a victim VM storing the authorized_keys file of OpenSSH. authorized_keys files stores the (often) RSA public key. A user with the RSA private key associated with that public can then login to the SSH server.

The security of this scheme depends heavily on the fact that the private key cannot be easily derived from the (known) public key by factorization. We perform a FFS attack on the public key to flip one of its bits. A bit flipped public key becomes much easier to factorize. Once we have all the factors, we can generate a new private key corresponding to the bit flipped public key and SSH with an unmodified OpenSSH client.

You can find a demo on our local testbed showing a cross-VM SSH compromise with FFS here: https://youtu.be/TqWmP2owbdo

Compromising apt-get

In our apt-get attack, we chain two FFS attacks to trick apt to install a tampered software packaged from a malicious repository without any suspicious warning.

We first flip a bit in the page cache storing apt-get’s sources.list file to change one of its domain names, for example, we change ubuntu.com to ubunvu.com. At this point, the victim’s apt-get requests will redirect to our repository, but no malicious package can be installed since the packages should be signed to be trusted by apt. We now flip a bit in the page cache storing the trusted.gpg effectively corrupting one of the two Ubuntu Archive Signing Keys. We have pre-computed factors for a number of these corruptions (i.e., bit flips) and as soon as we find one, we can sign any package that we want for apt-get to install. A demo of this attack can be find here: https://youtu.be/cs7xDkBG7_4

We redirect the victim’s apt-get from ubuntu.com to ubunvu.com and make her install a backdoored version of coreutils.

We have registered all possible domains that are one bit flip away from ubuntu.com and debian.org. We would like to hand these domains over to the correct authority. Please get in touch if you think you are one.

Reception

- The disclosure effort is led by the National Cyber Security Centre (NCSC) in the Netherlands. Their advisory/factsheet about FFS can be found here.
- They have disclosed the issue to many parties including OpenSSH, GnuPG, VM monitor vendors (Oracle, Redhat, Xen, VMware), and Debian and Ubuntu, all before the paper was public. All these parties have responded.
- Most specifically, GnuPG strenghened their key signature checks to protect against the FFS attack. Commit here.
- There has been quite some media attention. Please follow this link about the media attention: https://www.vusec.net/2016/08/flip-feng-shui-news/

Hammertime simulator

We developed Hammertime, an open-source Rowhammer simulator – available on github – to foster further research on the Rowhammer bug. The simulator allows researchers and practitioners to simulate hardware bit flips in software, using bit-flip patterns (or fliptables) from a large set of DRAM chips. We plan to integrate more features and bit-flip patterns in the near future.

Papers

K. Razavi, B. Gras, E. Bosman, B. Preneel, C. Giuffrida, H. Bos, Flip Feng Shui: Hammering a Needle in the Software Stack, in: USENIX Security, 2016

Frequently Asked Questions

- **Why the name Flip Feng Shui?**
  Feng Shui is the Chinese philosophy of harmonizing with the environment. The term Heap Feng Shui has been previously used by hackers to describe the arrangement of the heap in a certain way that allows for a successful control-flow hijack. Flip Feng Shui is the art of arranging physical memory in a certain way so that a hardware flip results in a successful compromise.

- **How different is this from Dedup Est Machina?**
  Very different. Dedup Est Machina primarily targets browser exploitation. Both use a combination of memory deduplication and Rowhammer, but Dedup Est Machina uses deduplication to leak memory addresses randomized by ASLR while Flip Feng Shui uses deduplication to surgically place sensitive data on vulnerable physical memory locations.

- **How wide-spread is Rowhammer? How can I check whether my DRAM is vulnerable?**
  According to the original Rowhammer paper more than 85% of DDR3 modules are vulnerable to Rowhammer. You can try our highly optimized profiling tool released as part of the Hammertime simulator.

- **I have DRAM with Error Correcting Code (ECC). Am I safe against FFS attacks?**
  Triggering Rowhammer over DRAM with ECC is harder than normal DRAM. There are, however, DRAM modules with multiple bit flips per ECC domain that ECC cannot correct. At this point, it is still unclear whether these DRAMs can be reliably exploited.

- **I use a public cloud provider. Am I at risk?**
  It is difficult to say. NCSC is in contact with major cloud providers and VM monitor vendors to ensure that the issue is resolved for most cloud users.

- **I am a public cloud provider. How can I protect my customers?**
  Disable memory deduplication. It comes under different names: Kernel Same-page Merging, Transparent Page Sharing, Content-based Deduplication, etc.

- **How can I follow Flip Feng Shui related news?**
  We maintain a page about Flip Feng Shui related items found here: https://www.vusec.net/projects/flip-feng-shui/