Flip Feng Shui:
Hammering a Needle in the Software Stack

Kaveh Razavi  Ben Gras  Erik Bosman
Bart Preneel\textsuperscript{1}  Cristiano Giuffrida  Herbert Bos

August 10, 2016
Teaser

- OpenSSH compromise
- apt-get compromise by GPG signature forgery
- No software bug
- Weak assumptions
- Demo!
Contribution

Flip Feng Shui is a novel exploitation structure
  ▶ Hardware glitch
  ▶ Memory massaging primitive
Makes the glitch
  ▶ Easy to target precisely
  ▶ Reliable
We demonstrate FFS = Rowhammer + Memory Deduplication
Outline

Flip Feng Shui At Work
Outline

Flip Feng Shui At Work

Flip Feng Shui Mechanics
Outline

Flip Feng Shui At Work

Flip Feng Shui Mechanics

OpenSSH Attack
Outline

Flip Feng Shui At Work

Flip Feng Shui Mechanics

OpenSSH Attack

GPG/APT Updates Attack Demo
Outline

Flip Feng Shui At Work

Flip Feng Shui Mechanics

OpenSSH Attack

GPG/APT Updates Attack Demo

Notification, Conclusion & Further Resources
Section 1

Flip Feng Shui At Work
Flip Feng Shui

- Flip one bit per page in a co-hosted victim VM

- Whenever you know its contents

- Organised bitflip

- DRAM glitch

- Breaks CPU virtualization isolation
Section 2

Flip Feng Shui Mechanics
Flip Feng Shui Mechanics

- Co-hosted VMs
- Memory deduplication
- Rowhammer
- RSA
Memory deduplication

Virtualization Host

Victim

Attacker

Backing memory
Memory deduplication

Virtualization Host

Victim

Attacker

Backing memory
Memory deduplication

Virtualization Host

Victim

Attacker

Backing memory
Memory deduplication

Virtualization Host

Victim

Attacker

Backing memory
Memory deduplication

Virtualization Host

Victim

Attacker

Backing memory
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips

Row Buffer

Row i

Row i - 1

Row i + 1
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips

![Diagram showing rowhammer effect with green circles representing memory cells and red circles highlighting flipped bits. The row buffer is also depicted.]
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips
Rowhammer

- Causes charge to leak in DRAM
- DRAM row activations cause flips

![Diagram showing Rowhammer mechanism](image-url)
Memory deduplication + Rowhammer = FFS
Memory deduplication + Rowhammer = FFS

Virtualization Host

Victim

Attacker

Backing memory
Memory deduplication + Rowhammer = FFS
Memory deduplication + Rowhammer = FFS

▶ FFS breaks COW
RSA

- Public key cryptosystem
- Two keys: public and private
- Compute secret private from factorization
FFS - What now?

Break weakened RSA.
Section 3

OpenSSH Attack
authorized_keys file

Looks like this:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDX
y7MdVToVAvKB0/Xven/kqBzfRZm+GITl6sB0u+Aa
3/UTC3x+eKjB2jf+48kTP7AvsdbSwg9Q5upN77xX
3mNGwwj1RUQpOPPc99XH09M84iCydE+9smYseySf
bJQnrov5Ricz2Z18Neuy5ZUH/Ldrf1NSwWoo5NZL
6tj0E9JvZurMPPk2EqEyHltEFC60etJwEfaPq9k0
glmzFtBWLHR4dF1796JeVkJFwcmMaykAoN+jR2n
MlayP1UxdWR0JwxZ2cJ9la/QLXvv8x0ts0RGp9ZG
5BWq0cD781evuSS3i9BNg60s17mlxo6Mc3oUbew
/7ddV08WjdRBn7iQF9WN beng@mymachine
```
OpenSSH FFS attack

Virtualization Host

Victim

Attacker

Backing memory
OpenSSH FFS attack

Virtualization Host

Victim

Attacker

Backing memory
OpenSSH FFS attack

Virtualization Host

Victim

Attacker

Backing memory
OpenSSH FFS attack
OpenSSH Attack

- Could retry
Section 4

GPG/APT Updates Attack Demo
GPG/APT Updates

- With FFS we flip /etc/apt/sources.list
- With FFS we flip /etc/apt/trusted.gpg
- Use computed private key
- Long term RSA Ubuntu signing keys
Section 5

Notification, Conclusion & Further Resources
Notification

- Notified: Red Hat, Oracle, Xen, VMware, Debian, Ubuntu, OpenSSH, GnuPG, some hosting companies

- Thank you NCSC

- GnuPG commit
Conclusion

- Flip Feng Shui breaks isolation
- Co-hosting VMs is risky
- Disable memory dedup

https://www.vusec.net/projects/flip-feng-shui