# AMD’s EPYC server encryption is the latest security system to fall

Chris Lam

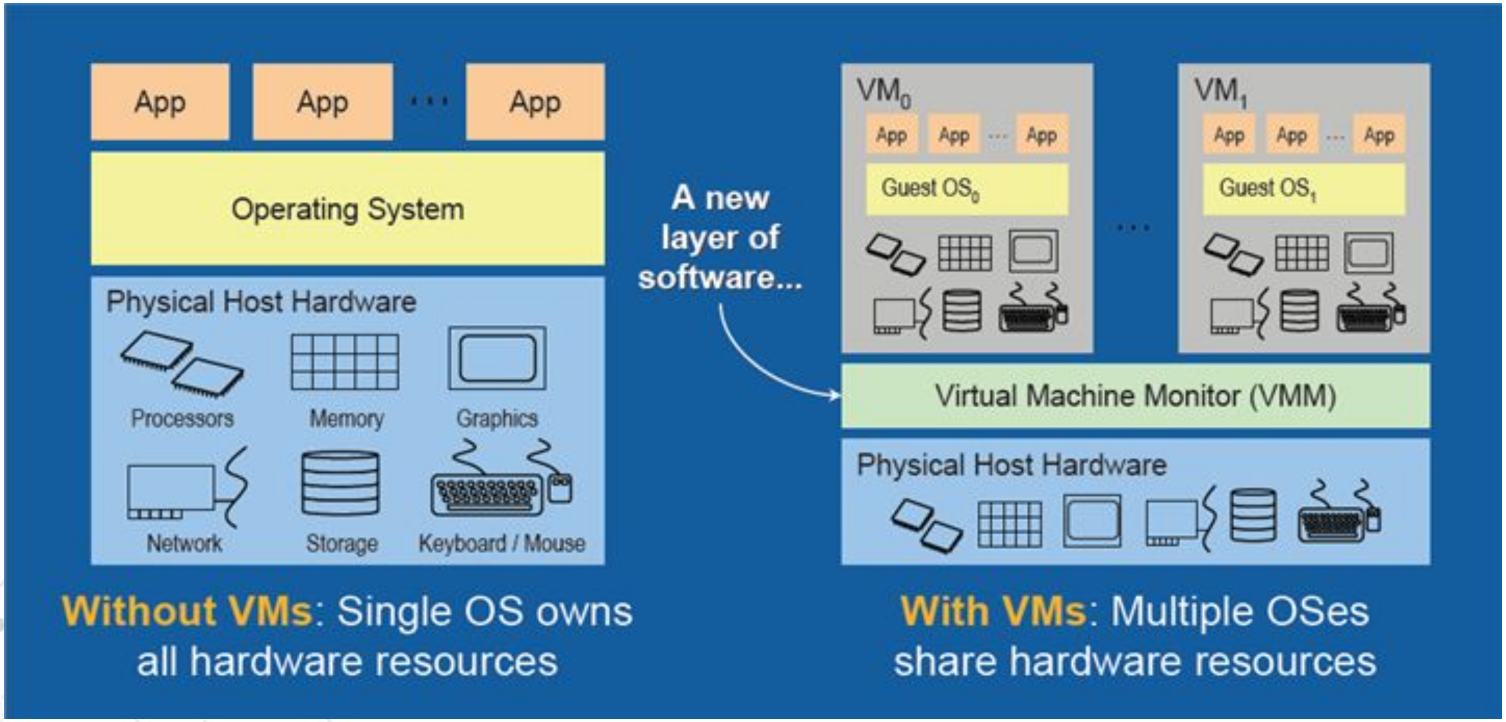
## Main Idea

“Researchers… in Germany have published a paper detailing how to compromise a virtual machine encrypted by AMD's Secure Encrypted Virtualization (SEV).”

- Virtual Machine/SEV
- Meltdown/Spectre
- Security/Implications

# Virtual Machine

- Virtual Machine - emulation of a computer system
  - Handled by a hypervisor/virtual machine monitor
- Host PA → Guest PA → Guest VA



Without VMs: Single OS owns all hardware resources

With VMs: Multiple OSes share hardware resources

# Pros and cons of virtualization

## PROS

1 physical system (cheaper & efficient)

Multiple OS’s

## CONS

Upfront costs

Complexity

Compatibility

Security

# AMD Secure Encrypted Virtualization (SEV)

“Guest owners wish to protect the confidentiality of the data running within their guests. While they trust the platform owner to provide the infrastructure to run their guest, they benefit from reducing their risk exposure to vulnerabilities within that infrastructure. The SEV feature encrypts the contents of the memory of the guest and provides assurances that it was encrypted properly. The encryption of memory places an additional burden on attackers within the operational environment who may have already obtained some illicit access to the guest’s memory through a vulnerability in the hypervisor or other supporting enterprise software. “

# AMD Secure Encrypted Virtualization (SEV)

## The Issue

SEV tries to address attacks that gain control of the hypervisor.

The most recent security attack, entitled “SEVered” by German researchers, “ trick a service in the VM, such as a web server, into returning arbitrary pages of the VM in plaintext upon the request of a resource from outside.”

Takes advantage of lack of integrity protection in memory encryption: HV is responsible for Second-Level Address Translation

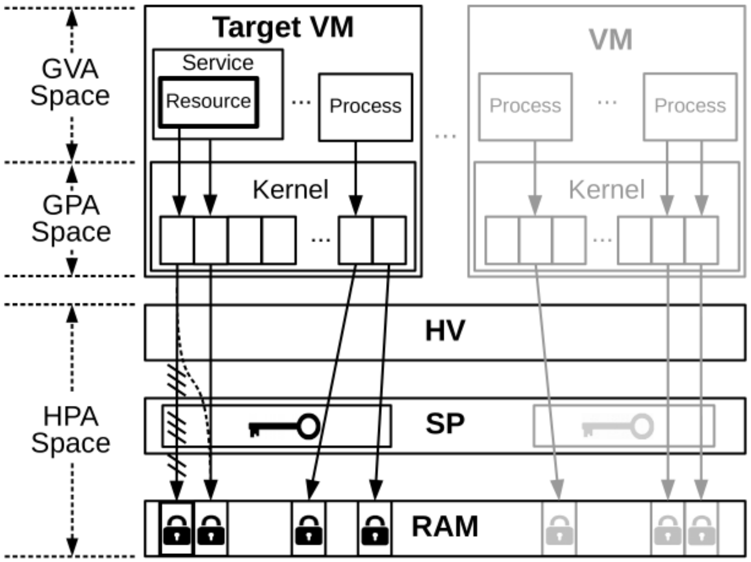
# Recent computer vulnerabilities

## Meltdown/Spectre

Exploits speculative execution

## SEVered

Exploits lack of integrity protection in encryption



# Implications

Proof-of-concepts: future-proofing

Can trust ever be eliminated (at least in the context of virtualization)?

# Sources

Patrizio, Andy. “AMD's EPYC Server Encryption Is the Latest Security System to Fall.” Network World, Network World, 31 May 2018, www.networkworld.com/article/3278005/data-center/amd-s-epyc-server-encryption-is-the-latest-security-system-to-fall.html.

Du, Zhao-Hui, et al. “Secure Encrypted Virtualization Is Unsecure! .” doi:https://arxiv.org/abs/1712.05090.

“The Advantages of Using Virtualization Technology in the Enterprise.” Intel Software Developer Zone, Intel, 7 June 2017, software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise.

AMD. “AMD EPYC's Secure Encrypted Virtualization (SEV) Feature Demo.” YouTube, YouTube, 20 June 2017, www.youtube.com/watch?time_continue=70&v=qgiUuTmXyGs.

AMD. “Secure Encrypted Virtualization API Version 0.16.” PDF File. 6 June 2018, https://support.amd.com/TechDocs/55766_SEV-KM%20API_Specification.pdf

“Vulnerabilities in Modern Computers Leak Passwords and Sensitive Data.” Meltdown and Spectre, meltdownattack.com/.