AMD DATACENTER SOLUTIONS

AMD EPYC

Helping Secure the Cloud with AMD EPYC™ Secure Encrypted Virtualization

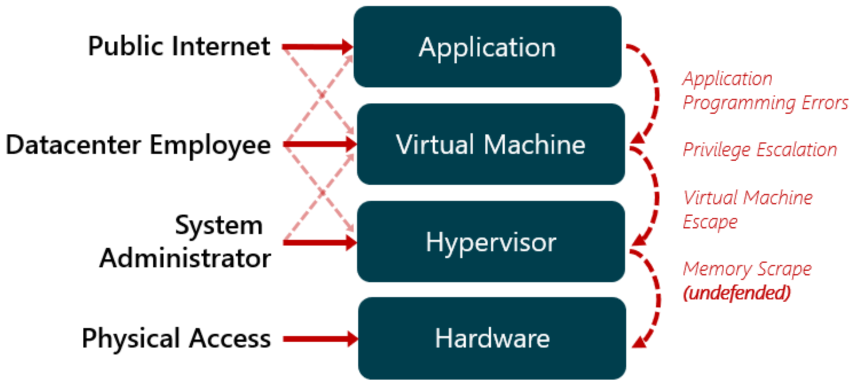
April 2019

The Cloud Needs World-Class Security

Data is money. The bad guys want to steal it.

Enterprises daily migrate tasks to the cloud for ease of management, scalability, and reduced cost. Often, however, they object to moving their most sensitive workloads over concerns about security.

Cloud tenants must trust the host to protect their data. Hosts are incentivized to comply but must in turn trust software to provide isolation – not only between the VM and hypervisor, but from the underlying hardware and every other guest in the system. This can quickly become uncomfortable for the security minded, "just trust me" is not a phrase they like to hear. In a highly networked computer system, anybody with a connection is a potential threat.



For computer systems without adequate hardware security features, when an attacker successfully deploys a virtual machine escape, every process on the box becomes vulnerable. If an insider or attacker has control of the hypervisor, they can read memory at will (note the example at bottom right). No entry appears in a guest log. The tenant is entirely unaware.

The 2015 QEMU VENOM bug provides a concerning example:

> "With Venom, you're able to break out of a virtual machine on a system and get access to other data on that system's network," Geffner says, adding that attackers can use it to "execute whatever code they like" by overwriting critical parts of a machine's memory."
>
> http://fortune.com/2015/05/13/venom-vulnerability

Application Programming Errors

Failures to handle buffer overflows, pathname exploits, SQL injection, and other logic errors allowing an attacker to exploit system resources.

Privilege Escalation

Exploit of an issue that allows a user to gain access that should not be available.

Insider Attack

Through error, coercion, social engineering, or by choice, trusted individuals access or provide access to data inappropriately.

Physical Attack

Data in memory remains readable even when powered off. Lowering the temperature increases the longevity. DIMMS can be frozen then transferred to another machine.

Cold Boot / Platform Reset Attack

Attacker reboots system to USB or other drive. A special operating system dumps system memory.

Virtual Machine Escape

An attacker gains access to hypervisor environment from inside a VM.

Memory scrape

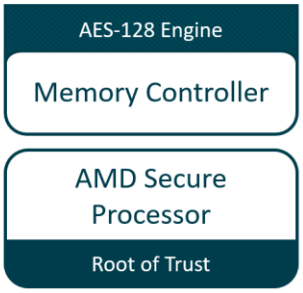
Attacker reads the memory of a running process to steal data.

```
sudo dd
if=/proc/[pid]/mem
of=fifo bs=4096
skip=[#first page]
count=[#pages]
&grep -a -o -b '.\credit-
card.\{16\}' fifo
```

Terminal command to scrape memory **without specialized tools**

AMD EPYC™ Hardware Memory Encryption - defense for data-in-use

To address the cloud trust problem, AMD integrates specialized hardware security components into EPYC™ processors.



AES-128 Engine

Memory Controller

AMD Secure Processor

Root of Trust

AES-128 Encryption Engine embedded in the memory controller. Data in memory is stored encrypted. Keys are not available to the x86 processor.

AMD Secure Processor provides cryptographic functionality for key management.

AMD EPYC™ 7xx1 processors introduced **Secure Memory Encryption (SME)**, and **Secure Encrypted Virtualization (SEV).** Both provide encryption for data-in-use and require no application changes for the end user.

AMD EPYC™ 7xx2 processors (codenamed "Rome") are expected to add additional capabilities including **SEV-Encrypted State (SEV-ES)** and a substantial increase in the number of compute threads and memory encryption keys.

AMD EPYC	Threads	Keys
7xx1 "Naples"	128	16
7xx2 "Rome"	256	511

Secure Memory Encryption (SME)

A single key encrypts system memory. The key is generated by the AMD Secure Processor at boot. SME requires enablement in the system BIOS or operating system. When enabled in the BIOS, memory encryption is transparent and can be run with any operating system.

Secure Encrypted Virtualization (SEV)

One key per virtual machine isolates guests and the hypervisor from one another. The keys are managed by the AMD Secure Processor. SEV requires enablement in the guest operating system and hypervisor. The guest changes allow the VM to indicate which pages in memory should be encrypted. The hypervisor changes use hardware virtualization instructions and communication with the AMD Secure processor to manage the appropriate keys in the memory controller.

SEV-Encrypted State (SEV-ES)

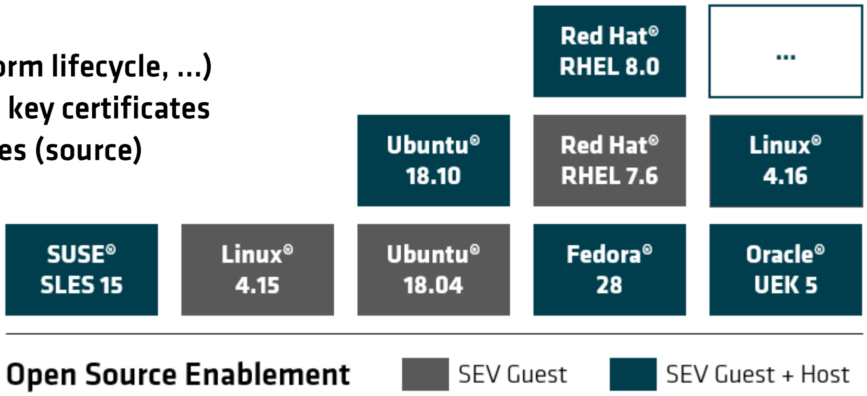
Encrypts CPU register contents when a VM stops running. This helps prevents the leakage of information in CPU registers to components like the hypervisor and can even detect malicious modifications to a CPU register state.

Guest and hypervisor support are available from major Linux® distributors including SUSE®, Canonical®, Oracle®, Red Hat® and Fedora®.

Developers: Help secure your cloud! Get started by visiting the website below.

https://developer.amd.com/sev

- **SEV API (key management, policies, platform lifecycle, ...)**
- **Web tools for obtaining chip endorsement key certificates**
- **SEV-Tool for managing platform certificates (source)**
- **SEV runtime for Kata Containers (source)**
- **AMD public certificates**
- **Documents, videos**
- **And more**



Red Hat® RHEL 8.0

...

Ubuntu® 18.10

Red Hat® RHEL 7.6

Linux® 4.16

SUSE® SLES 15

Linux® 4.15

Ubuntu® 18.04

Fedora® 28

Oracle® UEK 5

Open Source Enablement

▨ SEV Guest ■ SEV Guest + Host

DISCLAIMER

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale.

AMD, the AMD Arrow logo, AMD EPYC and combinations thereof are trademarks of Advanced Micro Devices, Inc. in the United States and/or other jurisdictions. Other names are for informational purposes only, and may be trademarks of their respective owners.