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

Terminal command to scrape memory without specialized tools: 

```
sudo dd if=/proc/[pid]/mem of=fifo bs=4096 skip=[#first page] count=[#pages] 6grep -a -o -b \."credit-card\.\[16\]\" fifo
```
**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 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.

<table>
<thead>
<tr>
<th>AMD EPYC</th>
<th>Threads</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>7xx1 “Naples”</td>
<td>128</td>
<td>16</td>
</tr>
<tr>
<td>7xx2 “Rome”</td>
<td>256</td>
<td>511</td>
</tr>
</tbody>
</table>

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

**Open Source Enablement**

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.

© 2019 Advanced Micro Devices, Inc. All rights reserved

AMD Confidential - NDA Required