Chris Lam

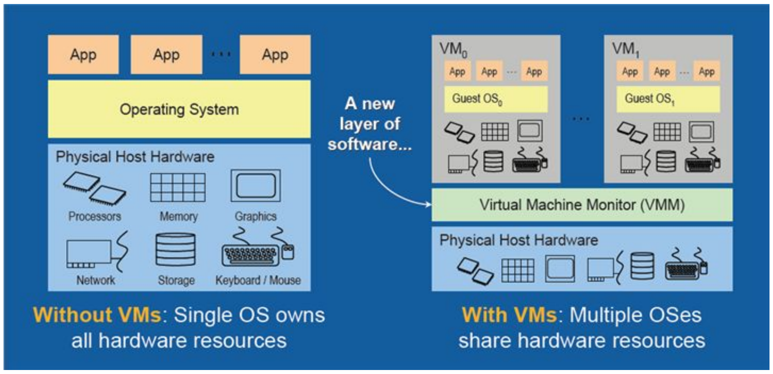
CS 35L

Alan Littlenecker

7 June 2018

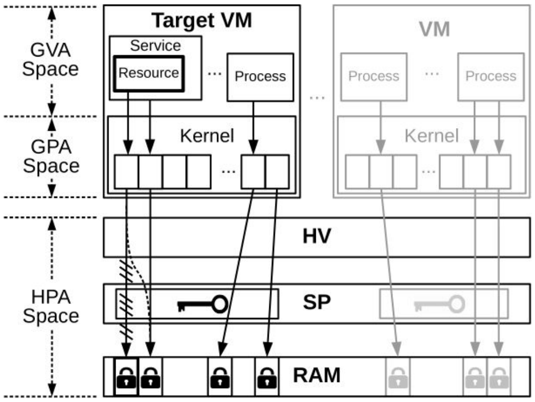
AMD’s EPYC server encryption is the latest security system to fall

The article summarizes the proof-of-concept attack performed on AMD’s new Secure Encrypted Virtualization (SEV) enabled EPYC processors. Andy Patrizio writes of the German researchers’ exploit of an intricacy in AMD’s implementation that allows them to bypass security measures that is supposed to encrypt and protect private data. The article also includes a bit of the relevance of this research finding in the business word, and a statement by AMD regarding their product’s vulnerability.



The new technology revolves around the concept of Virtual Machines (VM), The basis of this groundbreaking innovation is emulating isolated computers within one physical system, such that each virtual machine “believes” they are a system by itself. Due to its efficiency and many other benefits that comes with packing multiple machines in a single, physical computer, virtual machines have become increasingly popular, almost a necessity for businesses. This is an extention or generalization of the concept of virtual memory, which is the illusionary block of memory that an operating system gives to an application; it is illusionary because that block of memory is really just mapped to scattered physical, real memory. By having the host machine (the actual computer that creates the virtual machines) map its physical addresses to the guest virtual machines (each instance of a virtual machine on the host machine), each guest can have the illusion of having an entire set of memory to itself, just like a real physical computer does. An interesting point is that these guest machines themselves often employ virtual memory, mapping the illusionary physical memory given to them by the host machine to its own applications; therefore, a common hierarchy is having Host Physical Addresses (HPA) that Guest Physical Addresses (GPA) map to, which in turn are mapped to by Guest Virtual Addresses (GVA). This 2-level indirection plays an important role in the German researchers' exploit.

AMD's SEV attempts to add another layer of security to these virtual machines. Guest virtual machines are managed by the hypervisor, or virtual machine monitor, on the host machine, and SEV aims to offer real-time memory encryption on each guest machine such that the hypervisor or neighboring guest machines would not be able to access private data. This is done through a Secure Processor, a hardware that handles the encrypting and is separate from the hypervisor. The researchers discovered a method to work around the encryption to gain information it otherwise should not have access to. Specifically, they took advantage of the hypervisor still being " responsible for the Second Level Address Translation (SLAT), meaning that it maintains the VM's GPA to Host Physical Address (HPA) mapping in main memory" (Morbitzer et al., 1). By repeatedly requesting certain resources from a



service running on the VM and remapping the memory, they were cleverly able to put together all of the virtual machine’s memory.

Although it sounds as if the protection that SEV aims to put in place has been completely subverted, this was only a proof-of-concept and had considerable constraints, the main one being the need to have control of the hypervisor to make certain access modifications to allow for the attack to take place. As with Meltdown and Spectre and other vulnerabilities, it is easy to exaggerate the risks they hold; there are not many, if any at all, serious documented reports of hypervisors being hijacked beyond proof-of-concepts. AMD’s SEV is likely geared more toward a marketing scheme, i.e. making their product much more desirable than competitors. In the article, Patrizio states, “This is something cloud providers will like, and it's why Microsoft has signed up as an EPYC customer, because it lets providers assure customers that the memory and the VMs that live on their clouds are completely secured.” While hypervisor hacking may become a bigger threat in the near future, a more interesting question I had for the present is whether we can eliminate trust. That is to say, customers of cloud providers put an enormous amount of trust in putting their data on a machine they do not have physical access to, and AMD seems to be looking to close that gap and profit from it. It seems to be generally accepted that hackers will always find a way and there is no guarantee that a security measure is foolproof, but how much can technology go in protection and privacy?

Works Cited

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/.