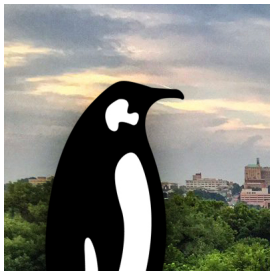

Contribution ID: **155** Type: **not specified**

Linux Virtualization Based Security (LVBS)

Wednesday, 15 November 2023 10:15 (45 minutes)

Linux kernel offers built-in self-protection mechanisms like control-register pinning, module/file authentication and protection restrictions; but a sophisticated kernel-level attacker can still bypass these. To get a much more effective defense, we propose to enforce such protection mechanisms via the hypervisor itself or a hypervisor-backed trusted entity. This also allows us to consider safeguarding and monitoring other critical system assets (passwords, critical kernel data structures) through the same trusted entity. In this talk we want to introduce Linux Virtualization Based Security (LVBS), an umbrella term under which we can offer various hypervisor backed kernel protection solutions.

We want to present a common hypervisor agnostic extendable architecture in Linux kernel that can be used by any hypervisor to implement and extend Linux kernel protections and how different hypervisor frameworks (Hyper-V as an example of type-1 hypervisor and KVM as an example of type-2 hypervisor) can plug into the common layer to harden the Linux kernel. We then will briefly discuss the ongoing work at Microsoft in the Linux kernel to implement the proposed architecture briefly touching upon:

a. Parts of hypervisor-agnostic common layer under development [1]

b. Using Hyper-V's Virtual Secure Mode (VSM) along with the common layer to harden Linux kernel

c. Using KVM along with the common layer to harden Linux kernel [1]

We intend to publish and upstream all the Linux kernel code for this project.

1. https://lore.kernel.org/all/20230505152046.6575-1-mic@digikod.net/
2. https://github.com/heki-linux

Primary author: GOPINATH, Thara (Microsoft)

Co-authors: MORRIS, James; SALAÜN, Mickaël (Microsoft)

Presenters: MORRIS, James; SALAÜN, Mickaël (Microsoft); GOPINATH, Thara (Microsoft)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track