Modern Blue Pills and Red Pills

Asaf Algawi
University of Jyväskylä, Finland

Michael Kiperberg
Holon Institute of Technology, Israel

Roee Shimon Leon
University of Jyväskylä, Finland

Amit Resh
Shenkar College, Israel

Nezer Jacob Zaidenberg
College of Management, Israel

INTRODUCTION

Johanna Rutkowska first introduced the concept of the blue pill and the red pill (Rutkowska 2006). The blue pill is a hypervisor-based rootkit that takes control of a victim host computer. A red pill is a software tool designed to detect a blue pill.

A term that is closely related to trusted computing is the attestation concept (Zaidenberg et al. 2015), where a remote host or local software tries to ensure the integrity of the local machine. This concept was also researched by Kennell et al. (2003) in order to establish genuinity of a remote host. (a physical machine running the correct software as opposed to an emulator or a virtual machine or a physical machine running non-genuine software).

Since the introduction of blue pills, many red pills have been designed for their detection; however, more advanced blue pills have been designed to avoid detection.

Today, modern CPUs (such as Intel core iX processors or ARM8 architecture) feature hardware-supported virtualization. Hardware-supported virtualization provides new capabilities to virtual machine and emulators software. Thus, hardware-supported virtualization makes several "red pill" attempts futile. However, hardware-supported virtualization also provides new forensics opportunities and therefore, many new opportunities to create new red pills.

This chapter describes the red pill and blue pill situation on Intel and AMD virtualizations circa 2018 and the eighth generation of core iX CPUs.

BACKGROUND

Blue pill technology relies on hypervisor technology. This chapter reviews recent advances in x86 virtualization. These new instruction families enable blue pill and red pill technologies.

DOI: 10.4018/978-1-5225-9715-5.ch078

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Hypervisors and Thin Hypervisors

A hypervisor is a type of computer software designed to run multiple operating systems on the same hardware.

As its name implies, a hypervisor has more permission than the operating system (i.e., the supervisor).

Just like the operating system supervises memory and hardware resources for the processes it runs, the hypervisor controls the hardware resources for each operating system.

Hypervisor research started with Popek et al. (1974) who classify hypervisors into two main categories:

1. Type I hypervisors, or boot hypervisors, are hypervisors that the machine starts from the hardware boot. The machine then starts the guest operating system. VMWare ESXi is an example of a modern Type I hypervisor.
2. Type II hypervisors, or hosted hypervisors, are hypervisors that start only after the operating system has started. A modern example for a Type II hypervisor is VMWare Desktop or Oracle Virtual Box.

Regular hypervisors are situated between the hardware and the supervisor (OS), catching interrupts and controlling memory addresses. The hypervisor decides which operating system owns each memory address and which operating system should handle each hardware interrupt.

There is a particular case of hypervisors that do not attempt to run multiple operating systems. Instead, these hypervisors, called "thin hypervisors", supports running only one operating system on the target hardware. Thin hypervisors act as a microkernel that provides specific services. The thin hypervisor passes the handling of all (or almost all) hardware events and interrupts to a single operating system. It also includes very little memory management and relies on the guest OS memory management system and interrupt handling. Microsoft's Deviceguard, TrulyProtect hypervisor for protection against reverse engineering (Averbuch et al. 2013) and Execution Whitelisting (Kiperberg et al. 2017) are examples of thin hypervisors. Virtually all blue pills are thin hypervisors.

x86 Virtualization

The x86 architecture, provide virtualization support by platform-specific instructions. Intel architecture and AMD architecture each provide three3 families of instructions for handling hypervisors. New processor generations optimize these instructions but their structure remains.

The x86 instructions are presented in Table 1.

Table 1. x86 virtualization instructions

	Intel Name	AMD Name	Usages
Virtual-ization instructions	VT-x	AMD-v	Starting a hypervisor
SLAT (second-level address translation)	EPT (Extended page tables)	RVI (Rapid virtualization indexing)	Multiple MMUs for multiple operating systems
IO MMU	VT-d	IOMMU	Assigning IO memory to specific operating systems
VM data structure	VMCS	VMCB	Holding VM information

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/modern-blue-pills-and-red-pills/248110

Related Content

Left-Wing Extremism From the Indian Perspective: An Econometric Interpretation
Sovik Mukherjee (2020). *Encyclopedia of Criminal Activities and the Deep Web (pp. 93-107).*
www.irma-international.org/chapter/left-wing-extremism-from-the-indian-perspective/248034

Beyond the Catholic Church: Child Sexual Abuse in Selected Other Religious Organizations
Dominica Pradere, Theron N. Fordand Blanche J. Glimps (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention (pp. 192-208).*
www.irma-international.org/chapter/beyond-the-catholic-church/301149

Interventions for Sexual Abuse
Prathibha Augustus Kurishinkal (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention (pp. 368-392).*
www.irma-international.org/chapter/interventions-for-sexual-abuse/301160

Regulations for Cybercrimes: The Case of the EU Cybersecurity Act
Delphine Defossez (2021). *Handbook of Research on Theory and Practice of Financial Crimes (pp. 453-476).*
www.irma-international.org/chapter/regulations-for-cybercrimes/275475

Distinctive Slave Mutinies
(2023). *Analyzing Black History From Slavery Through Racial Profiling by Police (pp. 74-94).*
www.irma-international.org/chapter/distinctive-slave-mutinies/321627