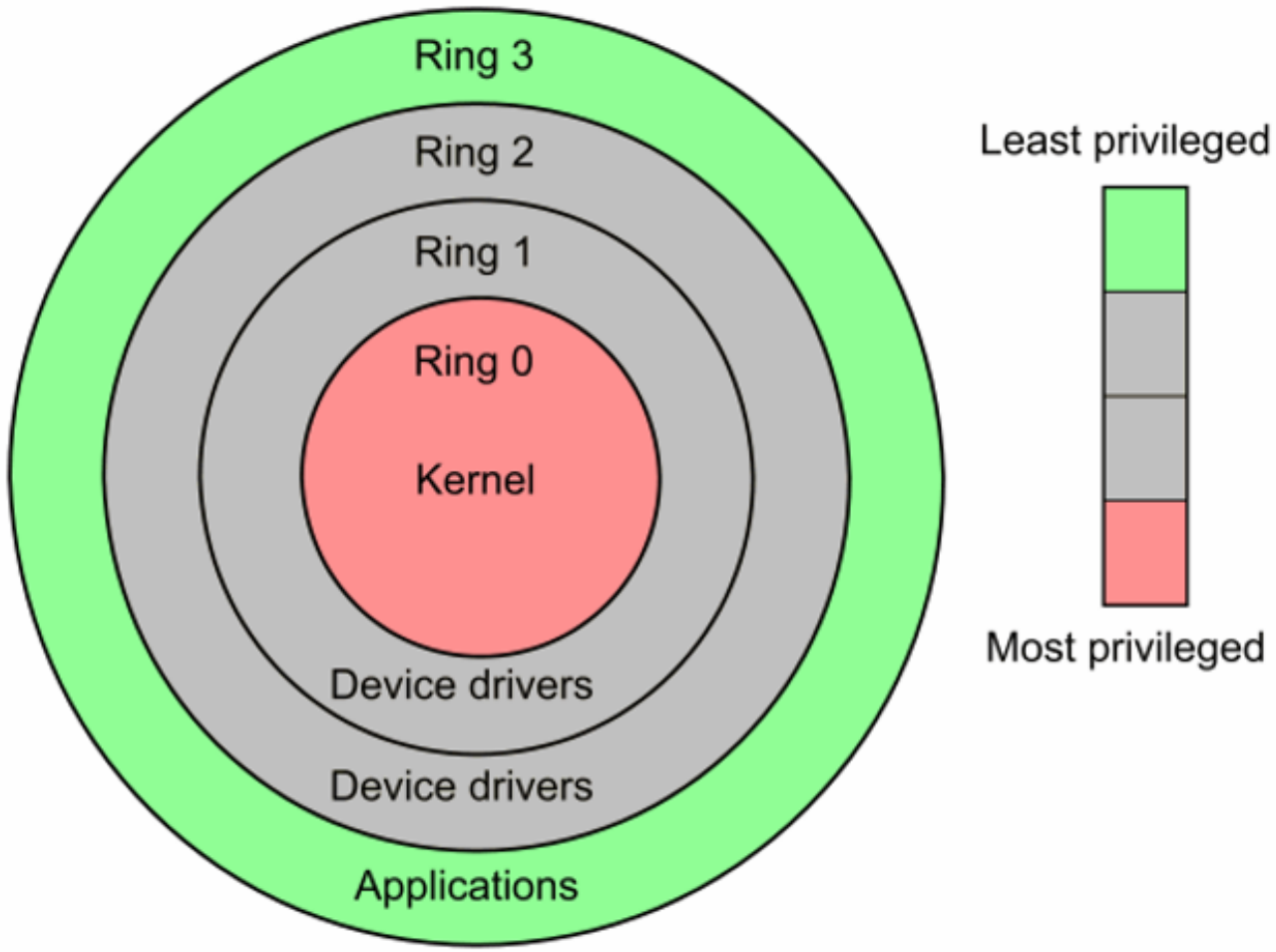
Využitie virtualizácie na zlepšenie detekcie škodlivého software

Martin Ivančík

Školiteľ: RNDr. Jaroslav Janáček PhD.
Konzultant: Mgr. Peter Košinár

Protection Rings



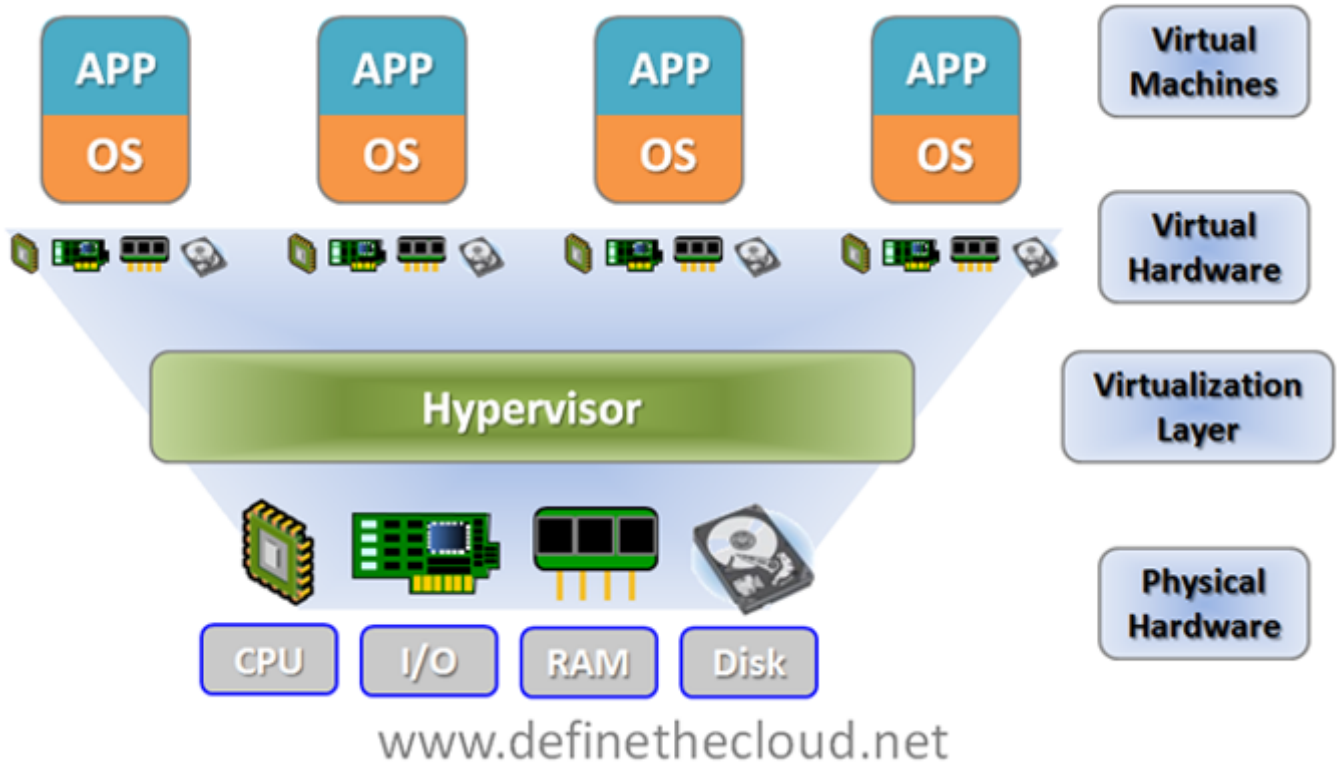
Malvér v jadre OS

- Vyššie privilégiá
- Modifikácia častí OS
- Ovplyvnenie bezpečnostných mechanizmov
- Skrývanie súborov, pamäte, sieťovej komunikácie ...

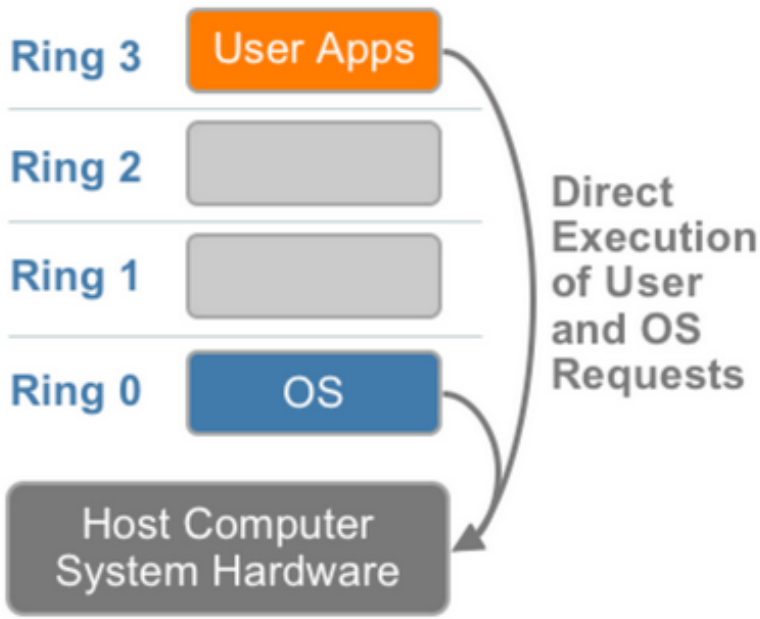
Ochrana systému - rozdelenie privilégií
Vieme sa dostať na nižšiu úroveň ako OS ?

Virtualizácia

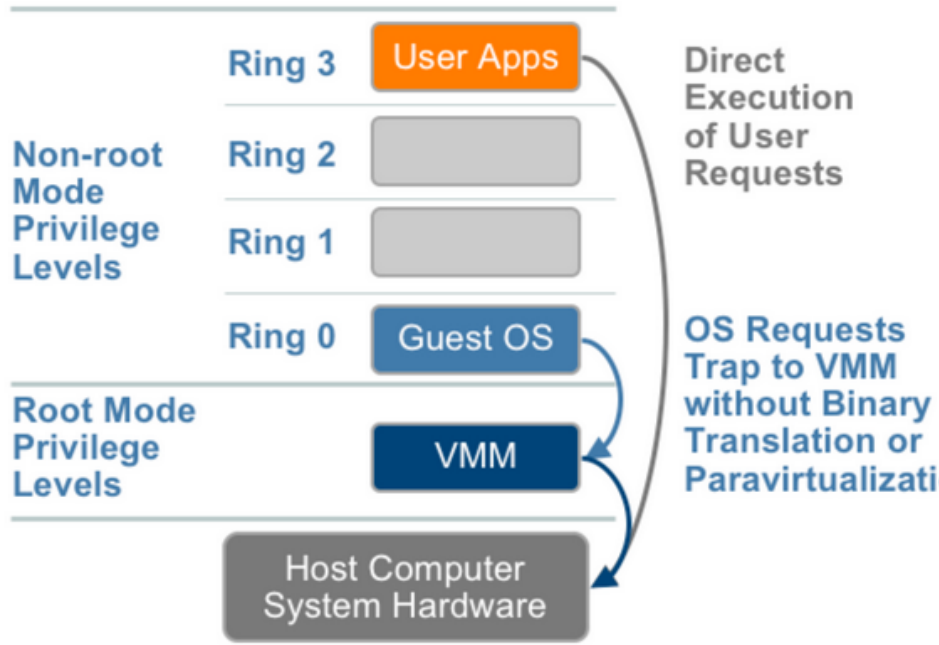
- Simulovať reálne prostriedky
- Spravovať zdroje
- Obmedziť Guest OS
  (prístup k pamäti, privilegovaným inštrukciám, ...)



Hardvérová virtualizácia

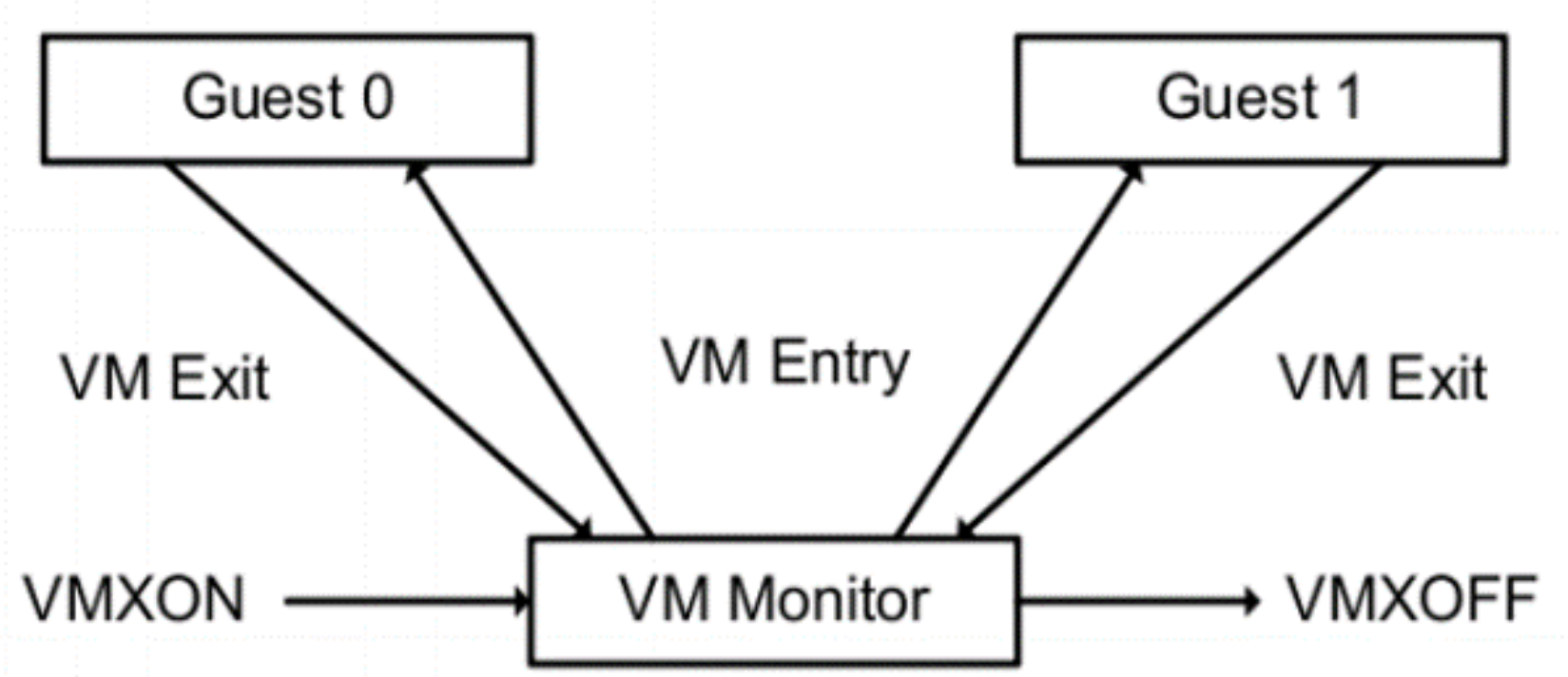


(a) Bez virtualizácie

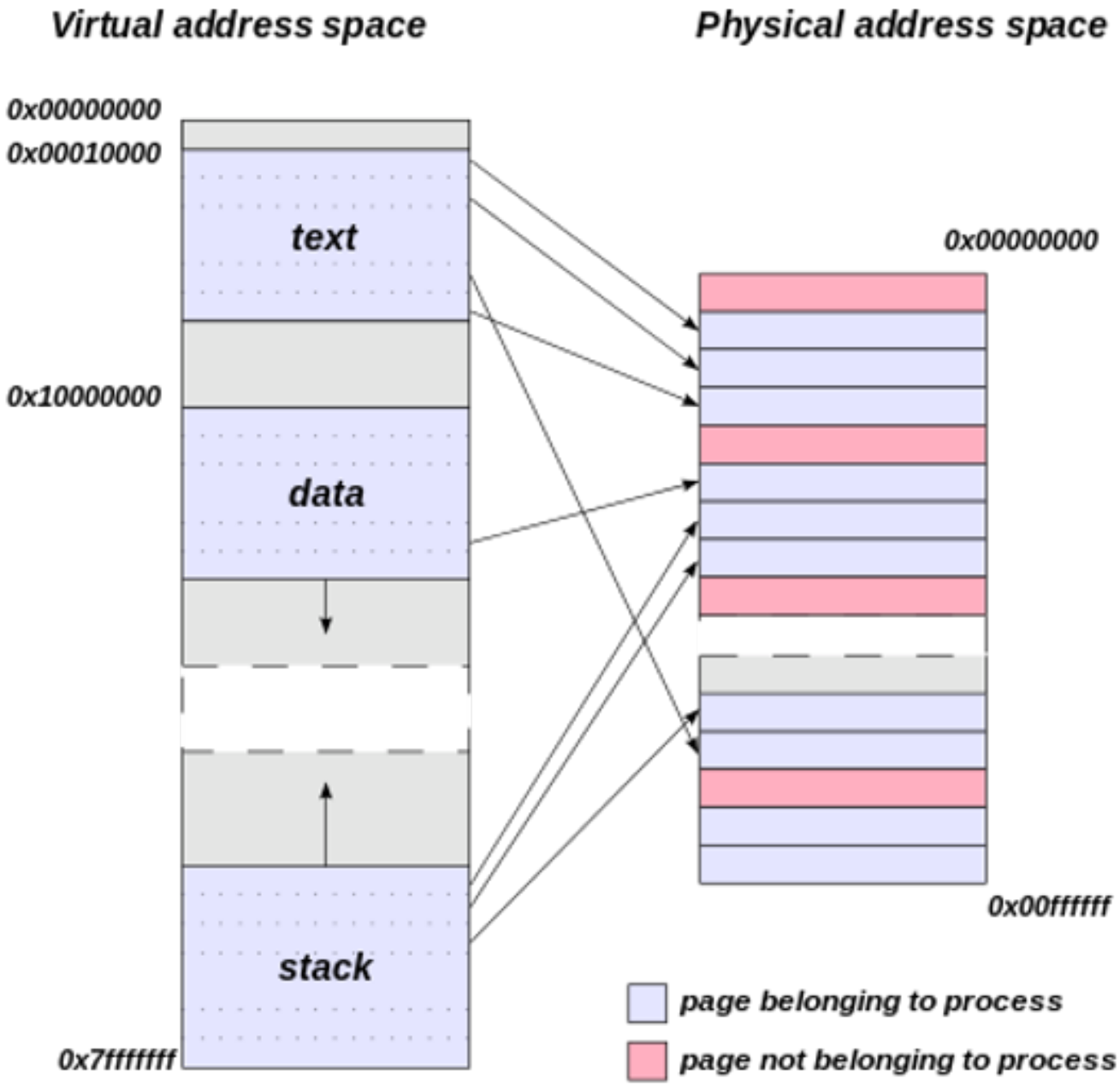


(b) Hardvérová

VMX - Virtual Machine Extension

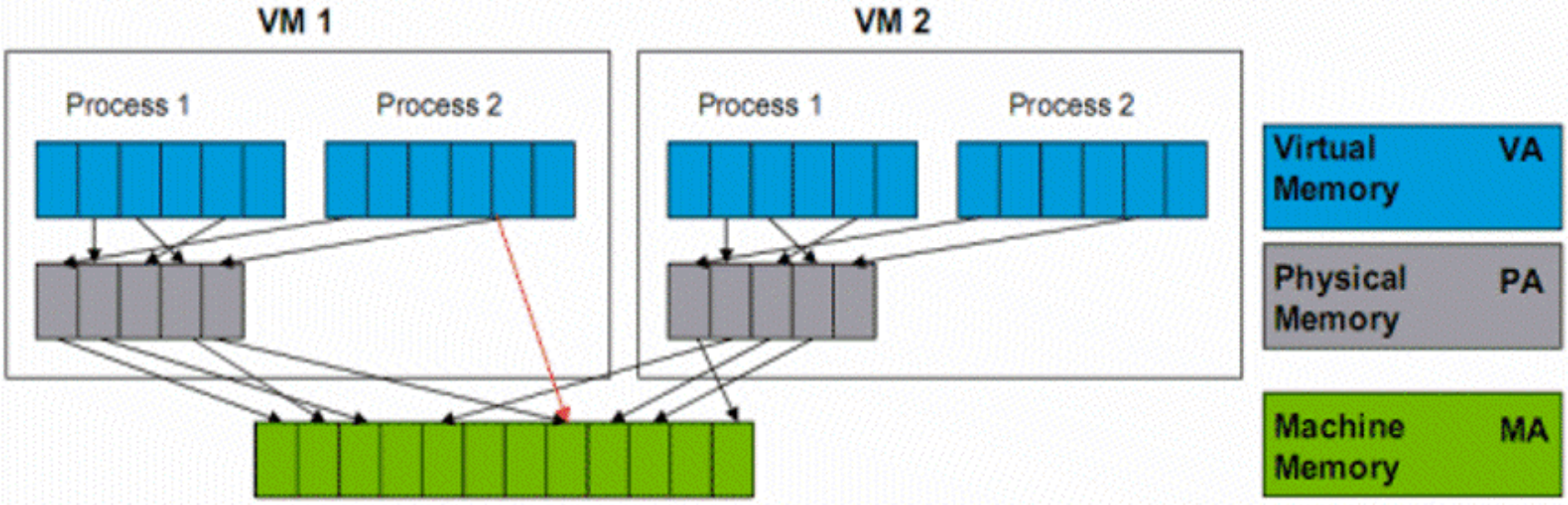


Virtuálna pamäť

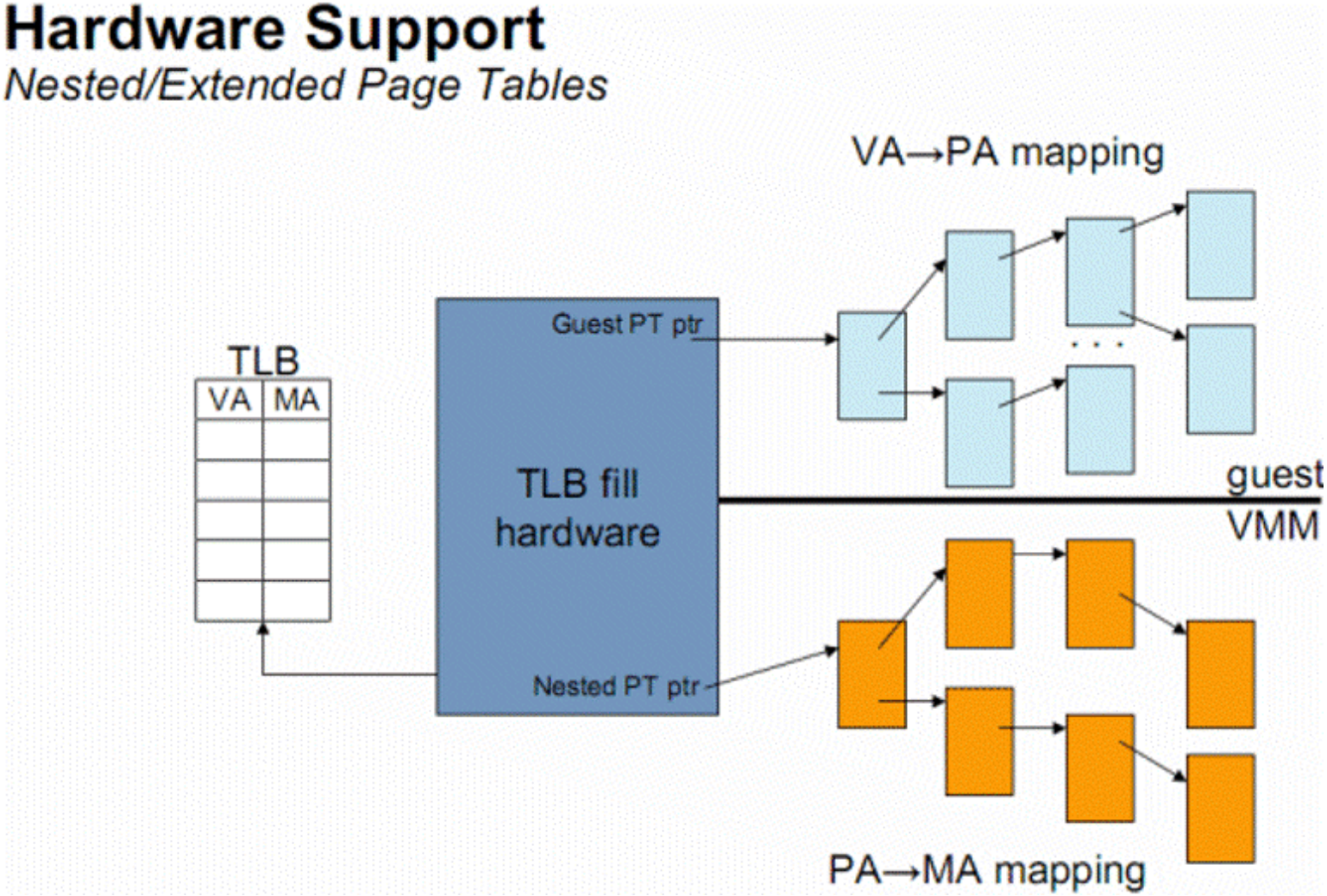


Virtualizing Virtual Memory

Shadow Page Tables



Extended Page Tables



Ciele práce

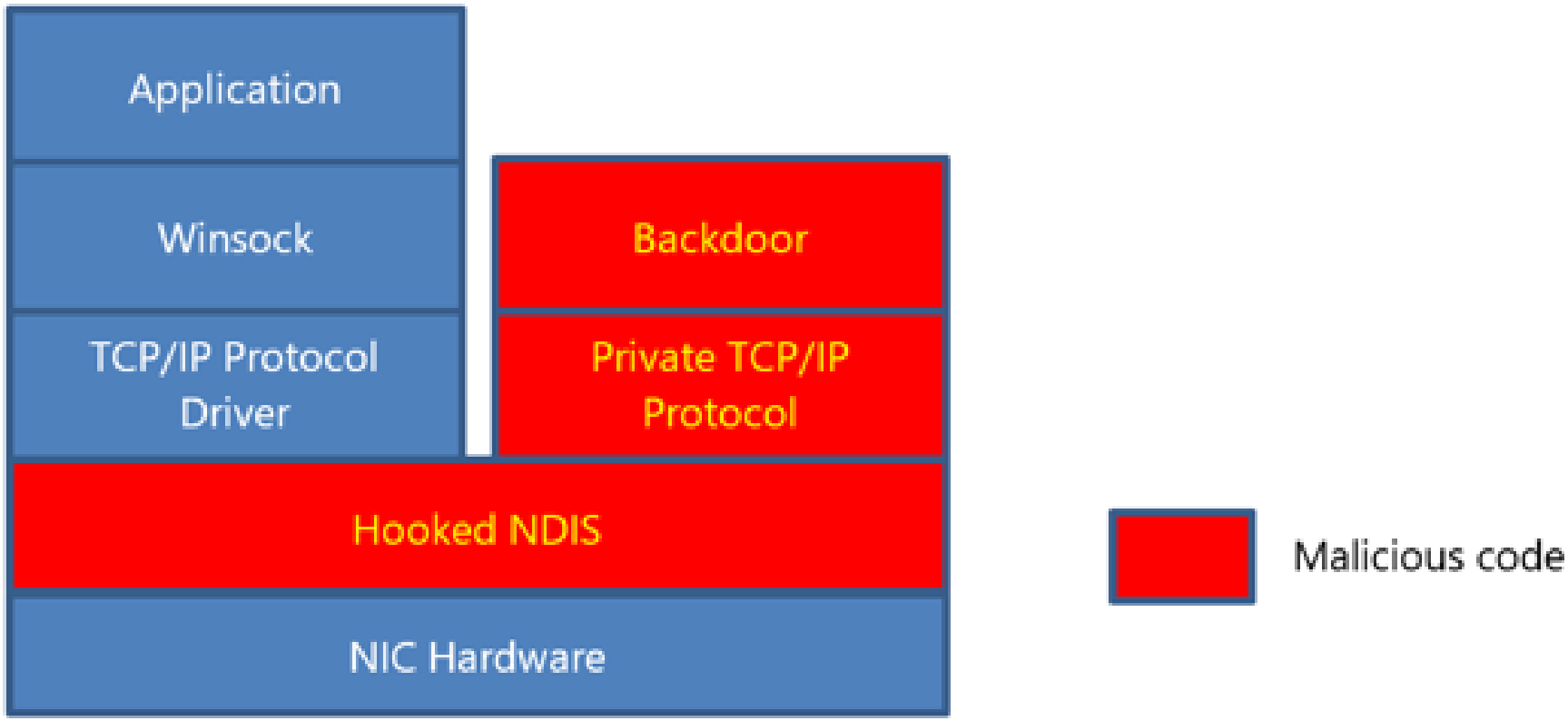
- Preskúmať možnosti využitia virtualizačných technológií na detekciu podozrivého správania softvéru pracujúceho na úrovni jadra OS.
- Implementácia nástroja.

Detekcia skrytej sieťovej komunikácie - TCP spojenia

Inšpirácia pre prácu - Rootkit Pitou

- Zložený z viacero komponentov
- Hlavná funkcionalita implementovaná ovládačom pracujúcim v jadre OS
- Skrytá Komunikácia, odosielanie paketov priamo sieťovej karte
- Rozosielanie spamu

Rootkit Pitou



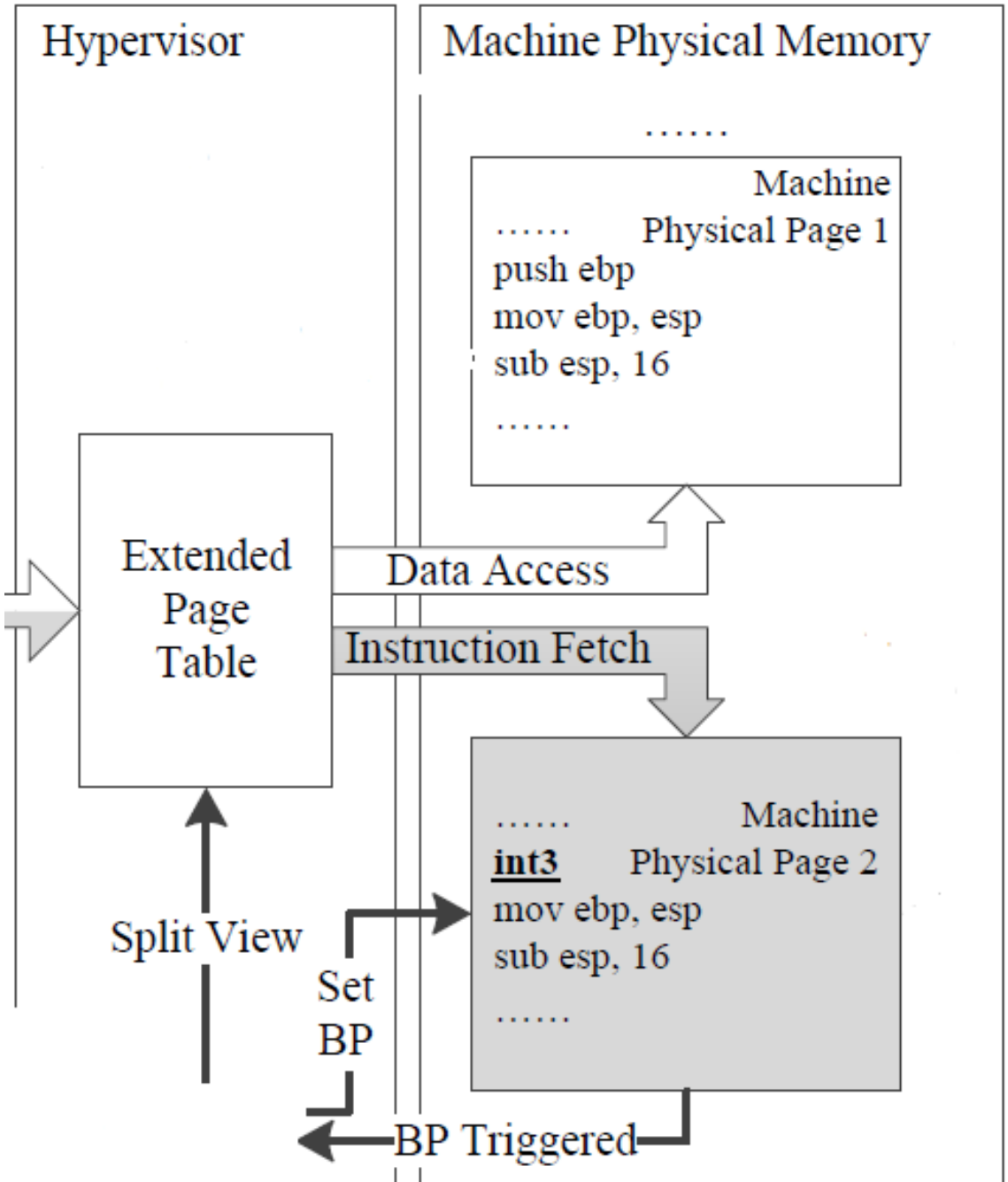
Detekčná metóda

- Slušné aplikácie používajú štandardné metódy a funkcie na komunikáciu po sieti
- Odchytenie odosielaného paketu tesne pred odoslaním zo systému
- Kontrola existencie záznamu o pakete daného spojenia v OS

Odchytenie odosielaného paketu

1. Nájsť SendHandler - funkciu pre odoslanie paketu zo systému
   - Analýza malware - obfuskácia
   - Analýza OS Windows
2. Hooknuť Handler - získať informácie o odosielanom rámci
   - Modifikácia interných štruktúr OS (KPP, viditeľnosť)
   - Využitie virtualizácie na implementáciu neviditeľnej modifikácie funkcií - Existujúca Implementácia Ddimon

Ddimon


Hypervisor
Machine Physical Memory
.....
Machine
..... Physical Page 1
push ebp
mov ebp, esp
sub esp, 16
.....
Extended
Page
Table
Data Access
Instruction Fetch
..... Machine
int3 Physical Page 2
mov ebp, esp
sub esp, 16
.....
Split View
Set
BP
BP Triggered

Kontrola existencie záznamu o odosielanom pakete

- Windows API pre ovládače neexistuje
- Analýza ovládača **tcpip.sys**
- „Ručne“ získať informácie z hashovacej tabuľky

Demo

Záver

- Predstavenie a popísanie druhov virtualizácie a spôsobu ich fungovania
- Analýza malvéru Pitou a vnútorných štruktúr OS Windows
- Návrh detekčnej metódy podozrivej sieťovej komunikácie využitím technológie VT-X
- Implementácia nástroja umožňujúceho detekciu skrytej sieťovej komunikácie
- Úspešné otestovanie implementovaného nástroja

Ďakujem za pozornosť