Ritorno ai fondamenti

(viaggio nei boundaries del sistema operativo Windows)

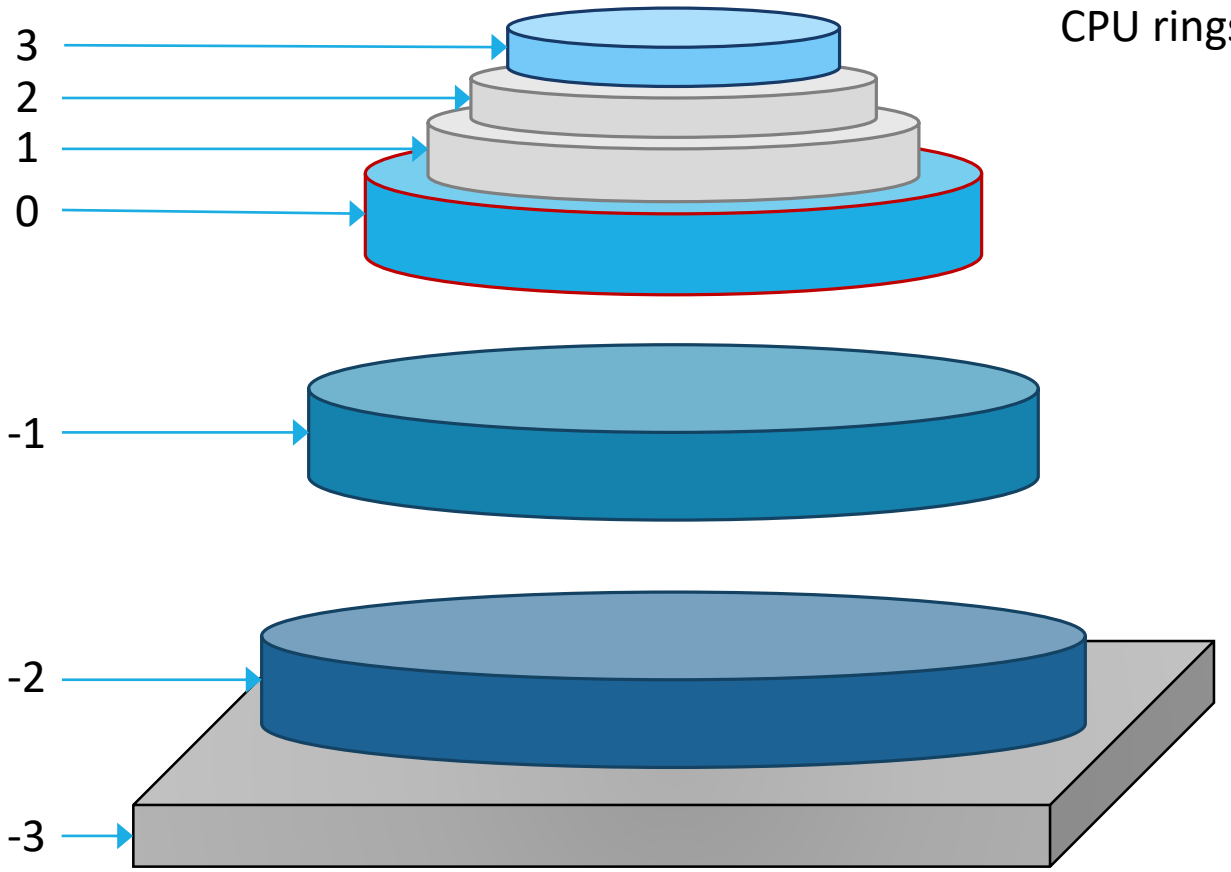
Raffaele Rialdi @raffaeler http://iamraf.net

Senior Software Architect

Presidente DotNetLiguria

CPU Rings

- Applicazioni in ring 3
- Kernel in ring 0
- Hypervisor in ring -1
- System Management Mode in -2
- Una CPU ARC 32 bit in -3
  - Interna alla CPU principale
  - Intel Management Engine



Windows Trust Boundaries in User Mode

Processi

- Un processo è un'istanza di un programma in esecuzione
- Uno o più thread hanno accesso al suo spazio di indirizzamento **virtuale**
  - Da 0 a 2^32 (32bit CPU) o 2^64 (64bit CPU)
- **In altre parole è una sandbox** che isola il codice contenuto
  - Può richiedere l'accesso agli oggetti kernel che saranno usati nel processo
    - Conservati nella Handle Table
    - Chiusi automaticamente ogni volta che il processo viene terminato
- Alla creazione riceve un **access token** associato ad un account Windows
  - È la carta di identità del processo stesso
  - Conserva informazioni di accesso ACL, di auditing (SACL) e l'Integrity Level (IL)

Integrity Levels

- Integrity Levels sono SID molto speciali
  - Assegnabili ai token di processo e ai kernel objects nelle SACL

- Windows usa gli Integrity Levels per proteggere delle risorse in aggiunta alle DACL
- Gli integrity levels sono SID in cui i RID definiscono il livello

Level SID	RID	Token example
Untrusted	S-1-16-0	(0x0000) Chrome worker process
Low	S-1-16-4096	(0x1000) Protected Mode IE7
Medium	S-1-16-8192	(0x2000) Non elevated process
High	S-1-16-12288	(0x3000) Admin process
System	S-1-16-16384	(0x4000) Localsystem and Localservice

Integrity policy

- Integrity policy sono le regole usate da Windows per sapere quando un processo con un livello più basso può accedere ad una risorsa con livello più alto
  - No read up — read vietate
  - No write up — write vietate
  - No execute up — execution vietate (tipicamente creazione di oggetti COM)
- Di default Windows assegna queste policy e IL:
  - No write up + medium integrity level
- I processi sono loro stessi kernel objects ma con "**no-read-up**" e "no-write-up"
  - "no-read-up" evita che un processo possa rubare dati ai processi di livello più alto
- Tutti gli altri kernel object sono solo "no-write-up"
  - Altrimenti potrebbero fare molto poco

Integrity levels associati agli utenti predefiniti

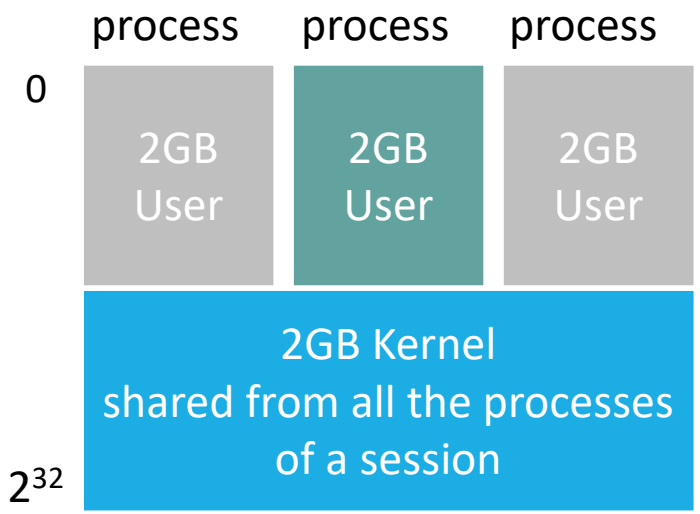
LocalSystem	System
LocalService	System
NetworkService	System
Administrators	High
Backup Operators	High
Network Configuration Operators	High
Cryptographic Operators	High
Authenticated Users	Medium
Everyone (World)	Low
Anonymous	Untrusted

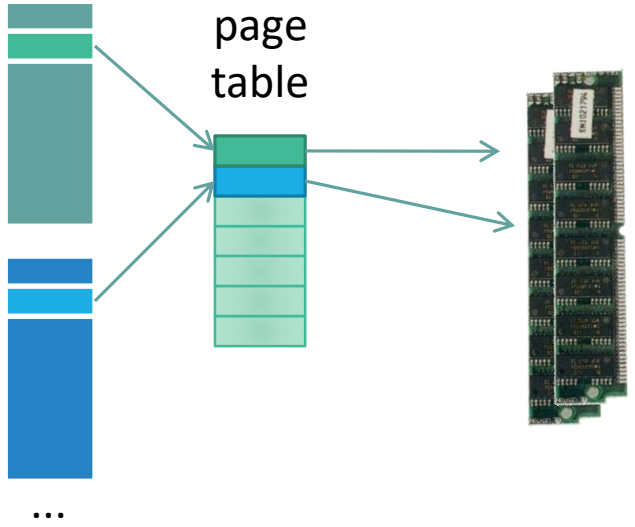
Universal Windows Platform
also known as AppContainers

- Le applicazioni UWP usano la sandbox degli AppContainer
  - Il codice di una App non può "uscire" dalla sandbox
- Ma cos'è una Sandbox? È un set di protezioni applicate al processo
  - Un SID speciale di applicazione
    - Stesso concetto già applicato ai "per-service" SID
  - Integrity Level impostato a "Low"
  - Un flag di "AppContainer" per cui il kernel gli impedisce certe operazioni
    - Per esempio non è possibile eseguire una Listen su HTTP
- Usa "RuntimeBroker" per accedere ai servizi privilegiati
- Il Windows Store previene l'uso delle API potenzialmente pericolose

I confini in memoria di un processo: *spazio di indirizzamento virtuale*

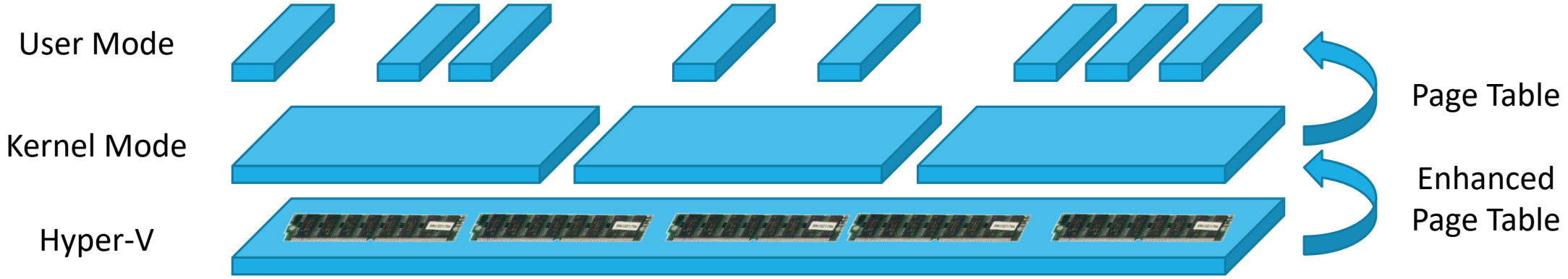
- I 4GB di un processo a 32 bit sono virtuali
- Il kernel mappa la memoria fisica nelle pagine di memoria virtuali
- Le associa ad ogni processo
- Sono condivisibili con più processi se sono in sola lettura





Le basi per la Virtualization Based Security

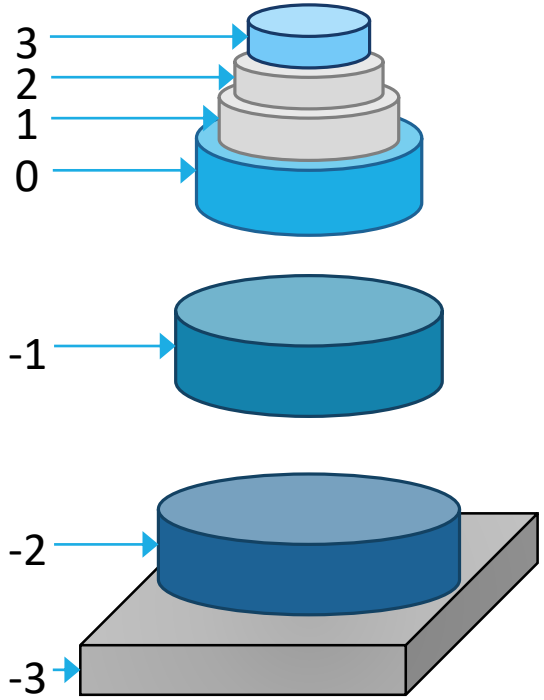
- Hyper-V aggiunge un livello di indirizzamento con una nuova tabella
- La memoria fisica è solo nelle mani di Hyper-V
- Il kernel della VM vede solo la memoria virtuale assgnata da Hyper-V
- Le app vedono pagine di memoria assegnate dal kernel della VM



Windows Trust Boundaries in Kernel Mode

Rings

- Il ring -1 è stato aggiunto per gli Hypervisors
- Il ring -2 esiste fin dal 80386 per il System Management Mode
- Il ring -3 è una CPU separata interna alla CPU principale
  - È attivo anche quando il PC è suspended (**stato S3**)
  - Intel usa Minix (si, proprio quello di Tanenbaum) per gestire il sistema e la CPU
  - Attivo anche da remoto grazie allo stack completo TCP/IP
  - Pùò bypassare tutte le impostazioni (es: Firewall) locali
  - Non è disabilitabile
  - **È bacato** ☺ …. usate Intel-SA-00086 Detection Tool



Windows Trust Boundaries

- Ring -1: Hyper-V
  - È il componente che isola e orchestra le VM e Windows locale
  - Ha potere totale su tutto ciò che gira nei ring >= -1

- Ring 0: Kernel del sistema operativo
  - I driver vivono in kernel mode
  - Il kernel di Windows è chiamato "TCB" (Trusted Computing Base)
  - Ha potere totale sulla propria istanza di OS (VM o locale)

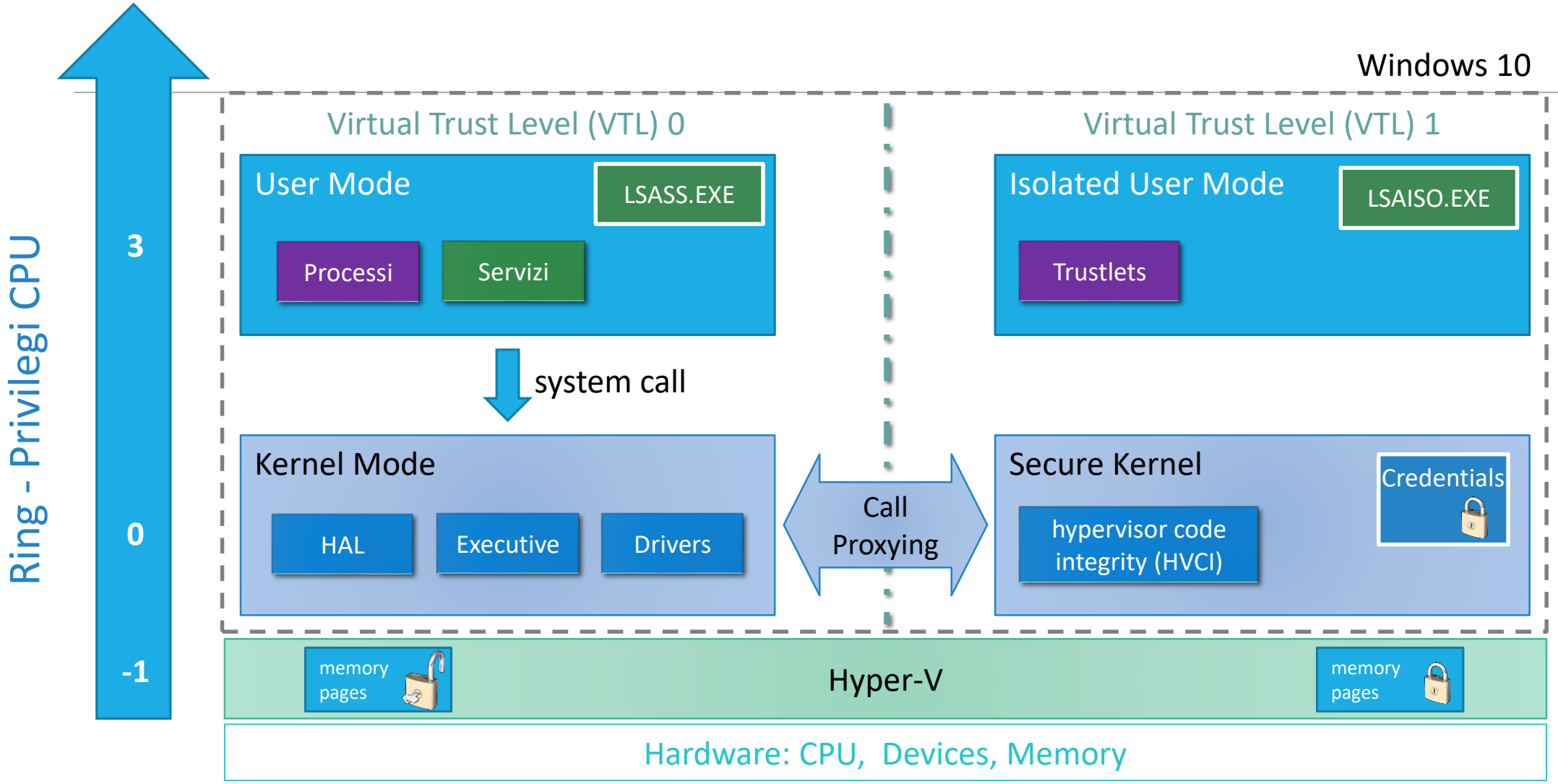
- Ring 3: User Mode del sistema operativo
  - Le applicazioni utente girano qui
  - Può accedere ai «kernel objects» solo se autorizzati

Windows Trust Boundaries in Kernel Mode

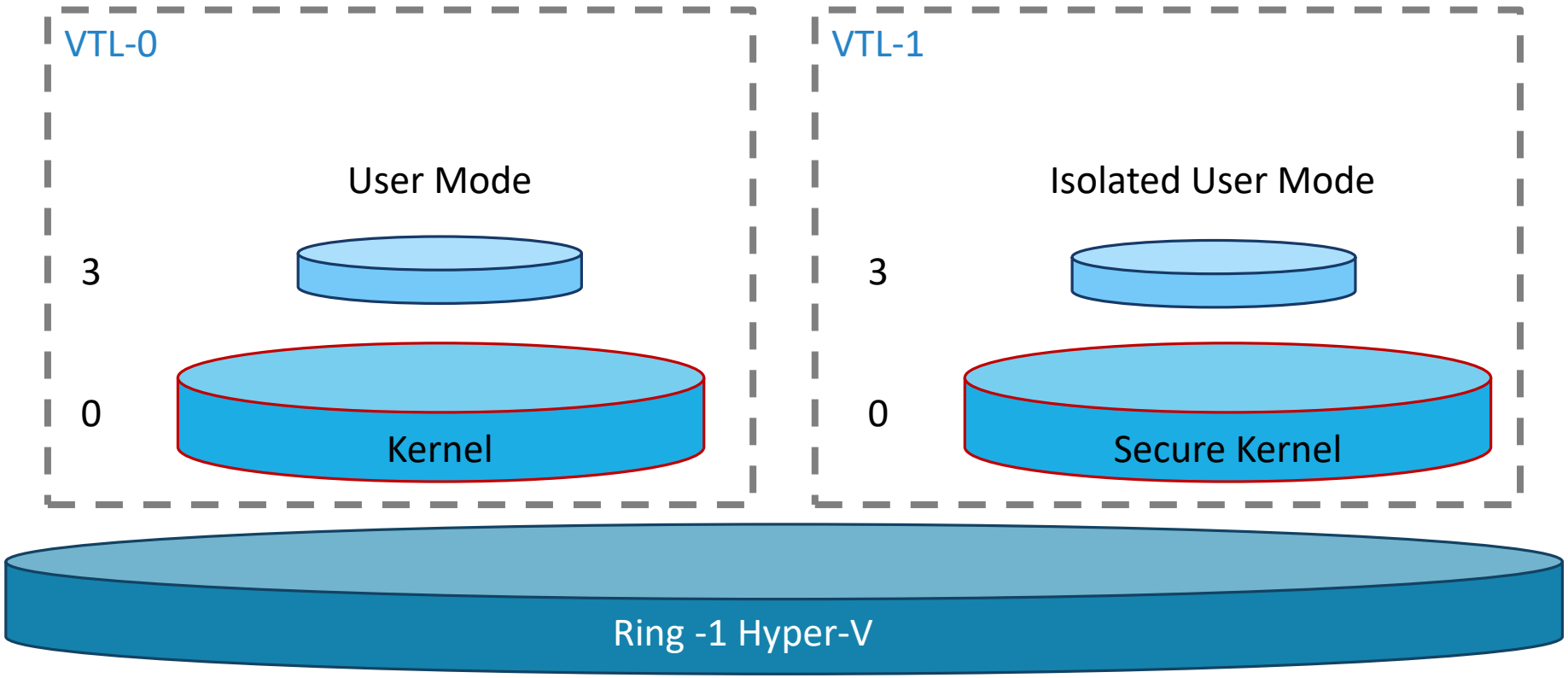
- Dobbiamo assumere che un driver possa aver compromesso il Kernel mode
  - Come posso difendere le credenziali e altre informazioni preziose?
  - Il kernel può fidarsi solo dei ring inferiori … quindi Hyper-V

- Il "**Virtual Secure Mode**" introduce un **secondo Kernel** in Windows
  - Il VSM serve a proteggere pagine di memoria dal kernel primario
  - La priorità tra kernel è stabilita in una scala di "**Virtual Trust Mode**"
  - Il kernel secondario ha un corrispondente "Isolated User Mode"
  - Solo Microsoft può scrivere codice che gira in VSM
  - Abilitato automaticamente insieme ad Hyper-V

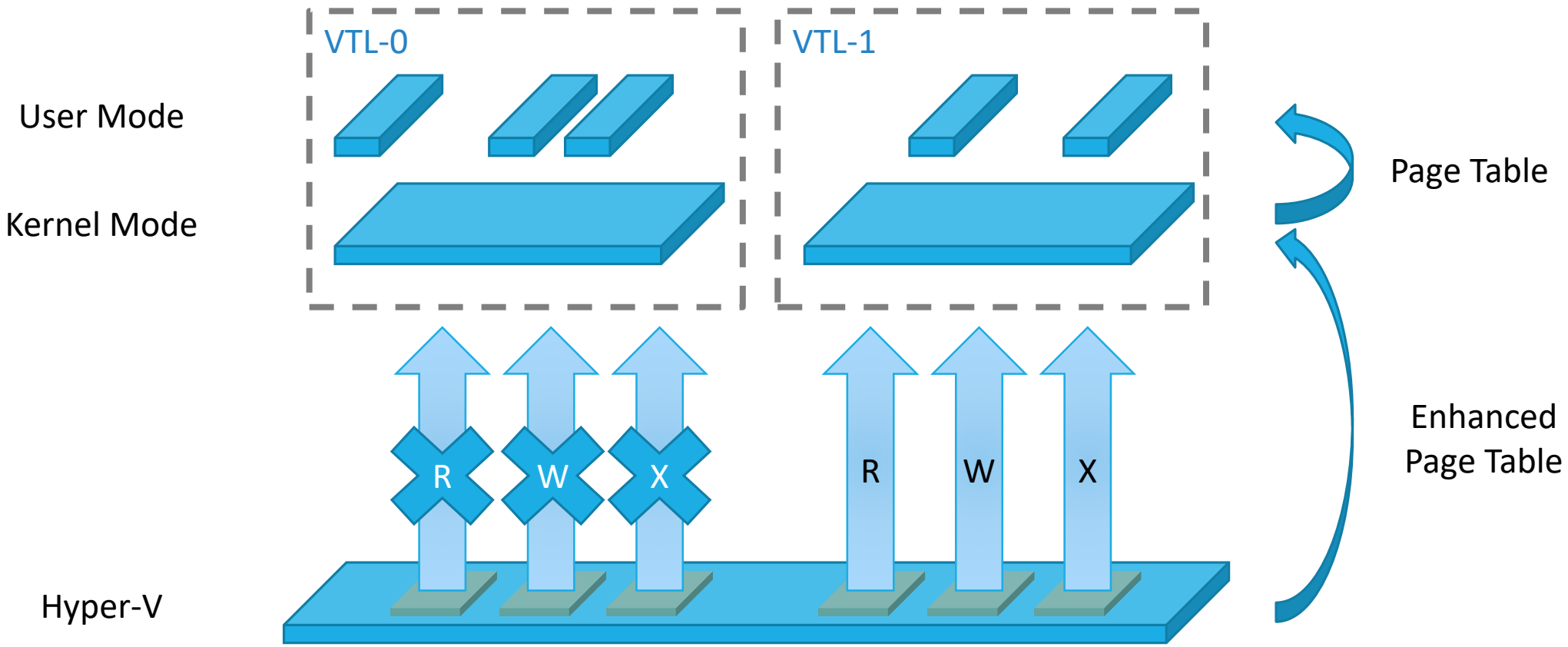
Windows 10 Virtual Secure Mode



CPU Rings e VTL



L'isolamento tra i due User Mode: Processi e Trustlets



Isolated User Mode

- I processi che girano in IUM si chiamano Trustlets
  - Solo Microsoft può scrivere trustlets
  - Il numero di System Call è ridottissimo (no File I/O, registry, network, video, …)
    - Devono chiedere via RPC all'User Mode normale di eseguire le operazioni per loro
    - I trustlets devono creare speciali pagine di memoria e fare marshalling per sanatizzarla
- I trustlets degni di nota:
  - Credential Guard
  - Biometric
  - Virtual TPM (bitlocker, encryption on VM)
  - Kernel Mode Code Integrity (device guard)
  - Windows Defender Application Guard (solo Enterprise Edition)
  - …

Attachi fisici

- Prerequisiti **non** indispensabili all'attivazione di VSM
- Il boot è delicato perché potrebbe compromettere il codice di Hyper-V
  - SecureBoot è preposto a dare queste garanzie
  - Garantisce che alcuni settings iniziali non siano compromessi
- Gli attacchi alla memoria sono possibili tramite DMA
  - Tramite bios, firmware o driver vulnerabili
  - IOMMU / VT-d permette al kernel di impedire che certa memoria sia accessibile via DMA
- Lo store di alcuni secrets può essere compromesso
  - TPM è preposto a fornire questa garanzia

Secure Kernel Code Integrity (HVCI)

- Impedisce al Kernel di creare pagine di memoria eseguibili
  - Le richieste sono sempre supervisionate da Hyper-V
- Le richieste di creare pagine eseguibili vengono redirette al Secure Kernel
  - Il secure kernel rende eseguibile la pagina solo se HVCI lo permette
    - Se sono firmate con un certificato attendibile
    - Se una determinata policy è rispettata
- **Questo permette di creare una policy che permetta l'esecuzione del solo codice firmato con un certificato**
  - Anche per applicazioni in User Mode, scripts, etc.
- **HVCI è al di sopra dei poteri di administrator o dei driver nel sistema!**

Comunicazione tra VTL

- Di norma il kernel comunica solo con un proxy
  - Ogni scrittura verso VTL 1 è negata
  - Può essere fatta solo da codice Microsoft tramite Hyper-V
- **Credential Guard**
  - Usa VSM impedendo le letture verso VTL 1
    - Custodisce in modo sicuro ed isolato i 'secrets'
- **Device Guard**
  - Usa VSM impedendo lettura, scrittura ed esecuzione
    - Powershell scripts, Applicazioni, Drivers, …
- **Guarded Fabric e Virtual TPM**
  - Bitlocker in VM
  - Encryption che permette di rendere inaccessibile una VM dall'host

Domande?


Microsoft Cybercrime Center


Leading the fight
against cybercrime