How to secure your computers with free Microsoft technologies

Charlie Maurice
Social Science Computing Cooperative
charlie.maurice@wisc.edu
Twitter: @charliemaurice

Some Available Microsoft Technologies

- LAPS (Local Administrator Password Solution)
- Bitlocker
- Applocker
- UEFI/Secure Boot
- Credential Guard
- Device Guard

LAPS

- Changes password of Administrator account based on schedule
- Stores password in AD
- EASY

Bitlocker

- At rest encryption of drives
- Can be used on internal disks or USB drives
- Can be set to store backup key to AD or Microsoft Bitlocker Administration and Monitoring (MBAM) (FREE)

Applocker

- Path Rules
- Publisher Rules
- Hash Rules

UEFI/Secure Boot

- Many of the Windows 10 security features require UEFI
- You can now convert a BIOS machine to UEFI without a reinstall
- Secure Boot protects against bootkit/rootkits

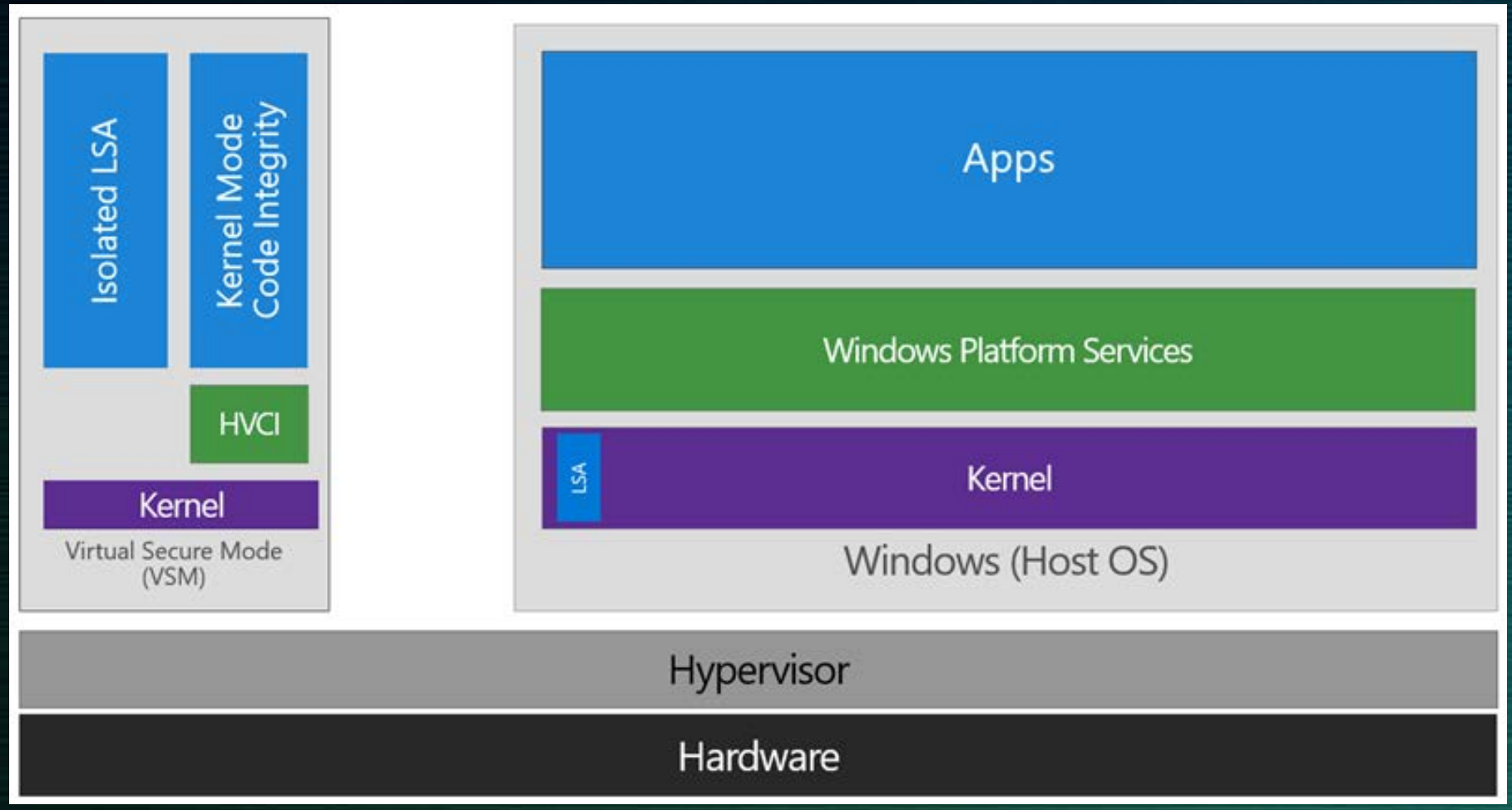
Credential Guard (uses VSM)

- Uses Virtualization to secure the LSA process
- Stored secrets are no longer in memory

Device Guard (uses VSM)

- Hardware based security
- Compliments Applocker
- Provides Code Integrity

Virtual Secure Mode (VSM)



Code Integrity

- Secure Boot
  - Includes Secure Firmware Updates and Platform Secure Boot
- Kernel Mode Code Integrity (KMCI)
- User Mode Code Integrity (UMCI)
- AppLocker