presented by

Microsoft

Hardening the Core:
Enhanced Memory Protection

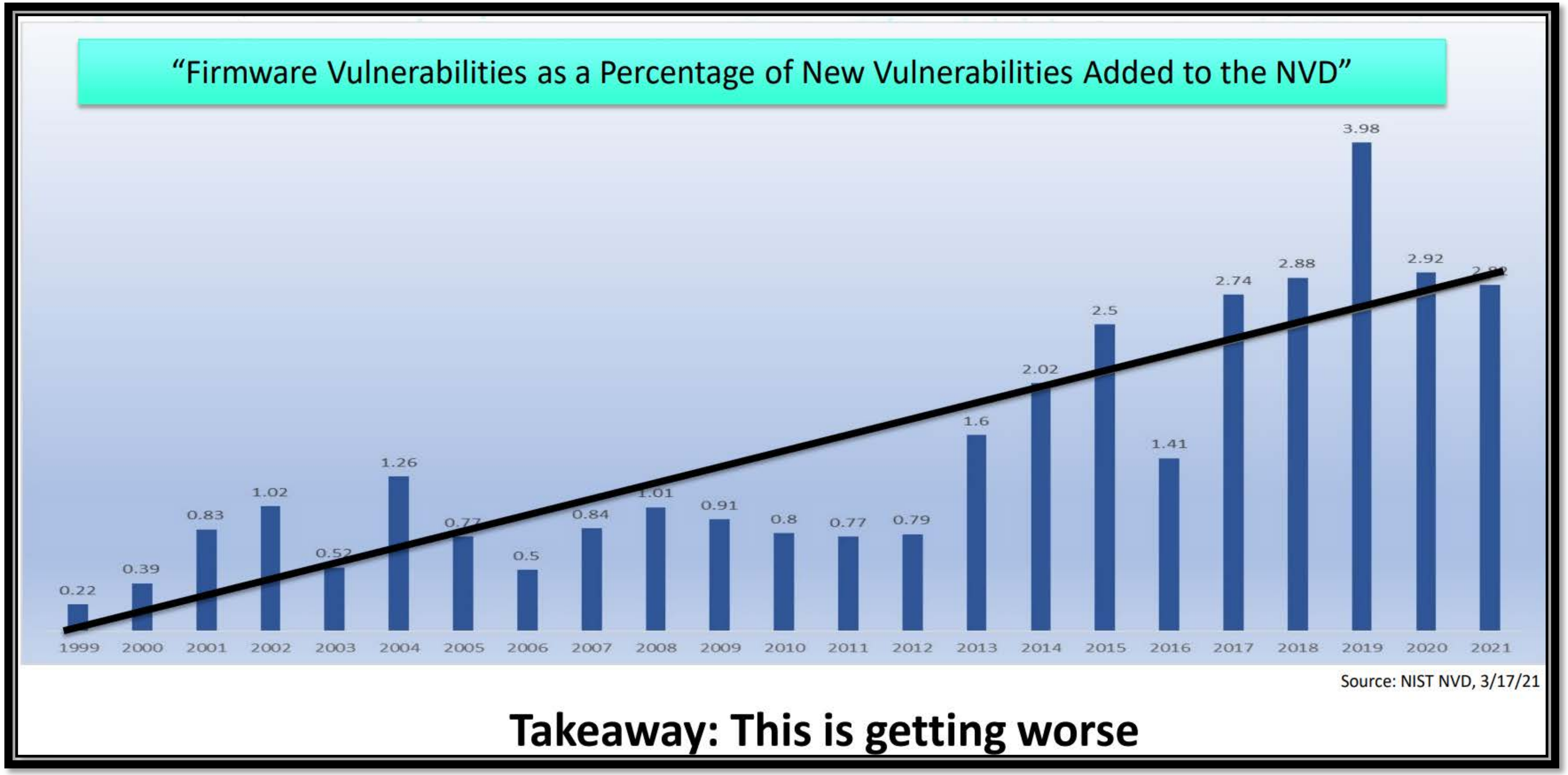
UEFI Fall 2023 Developers Conference & Plugfest
October 9-12, 2023
Presented by: Taylor Beebe (Microsoft)

Agenda

- Current State of UEFI Security
- Enhanced Memory Protection
- Case Study
- Tools & Tests
- Questions

Current State of UEFI Security

Current State



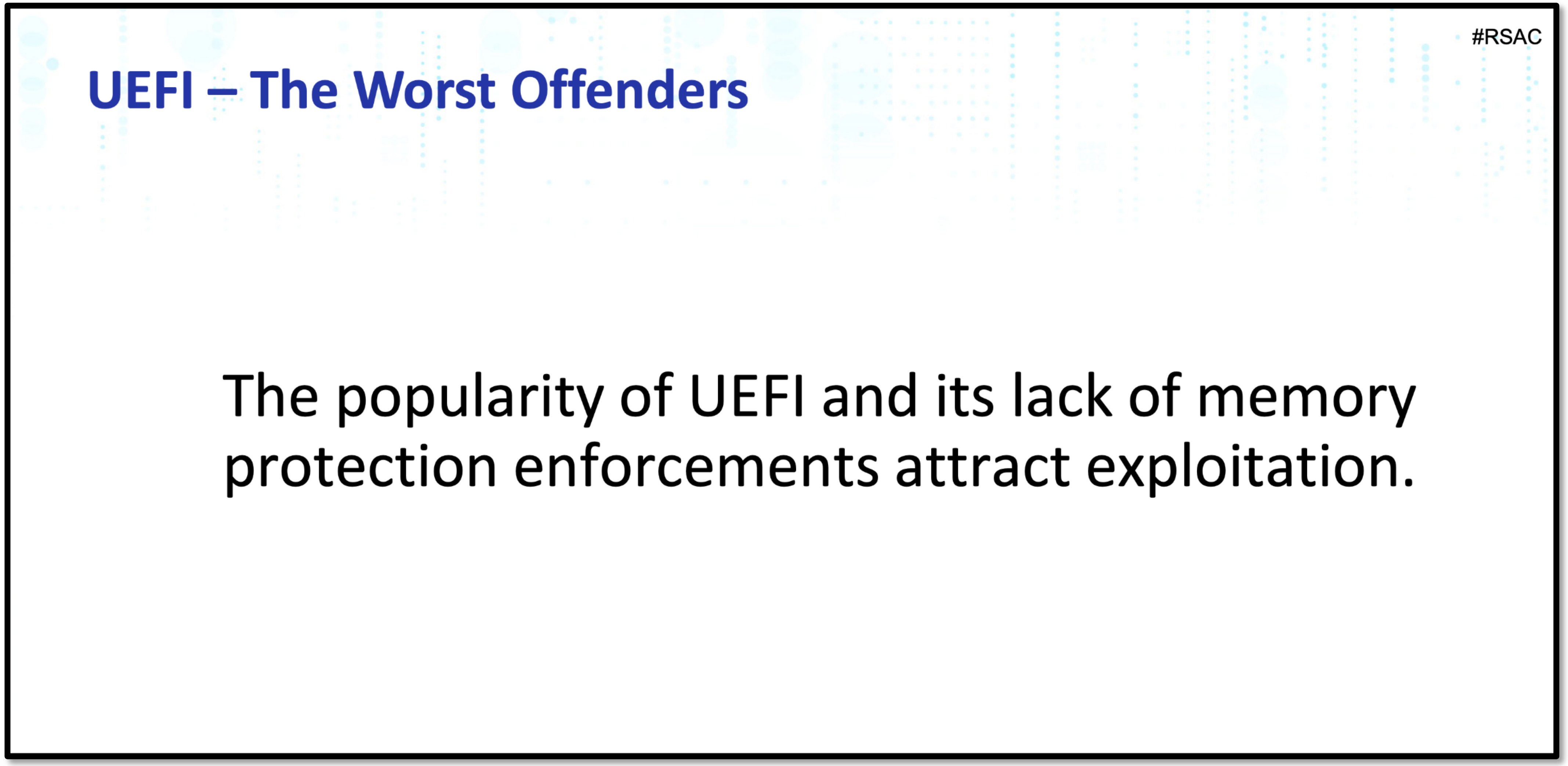
"Firmware Vulnerabilities as a Percentage of New Vulnerabilities Added to the NVD"

Source: NIST NVD, 3/17/21

Takeaway: This is getting worse

Source: DHS CISA Strategy to Fix Vulnerabilities Below the OS Among Worst Offenders

Current State



#RSAC

UEFI – The Worst Offenders

The popularity of UEFI and its lack of memory protection enforcements attract exploitation.

Source: DHS CISA Strategy to Fix Vulnerabilities Below the OS Among Worst Offenders

Current State

- Firmware implementations lack basic memory mitigations present in other system software for decades.
- UEFI implementations vary widely in reliability and security assurance.
- Firmware is foundational to system security – the chain of trust and System Management Mode. Firmware attack vectors threaten to compromise OS security.

Current State

- Known firmware exploits are not being protected against.
- Firmware vulnerabilities are increasing in frequency.

We **must** do better to harden platforms against exploits of common memory-safety vulnerabilities.

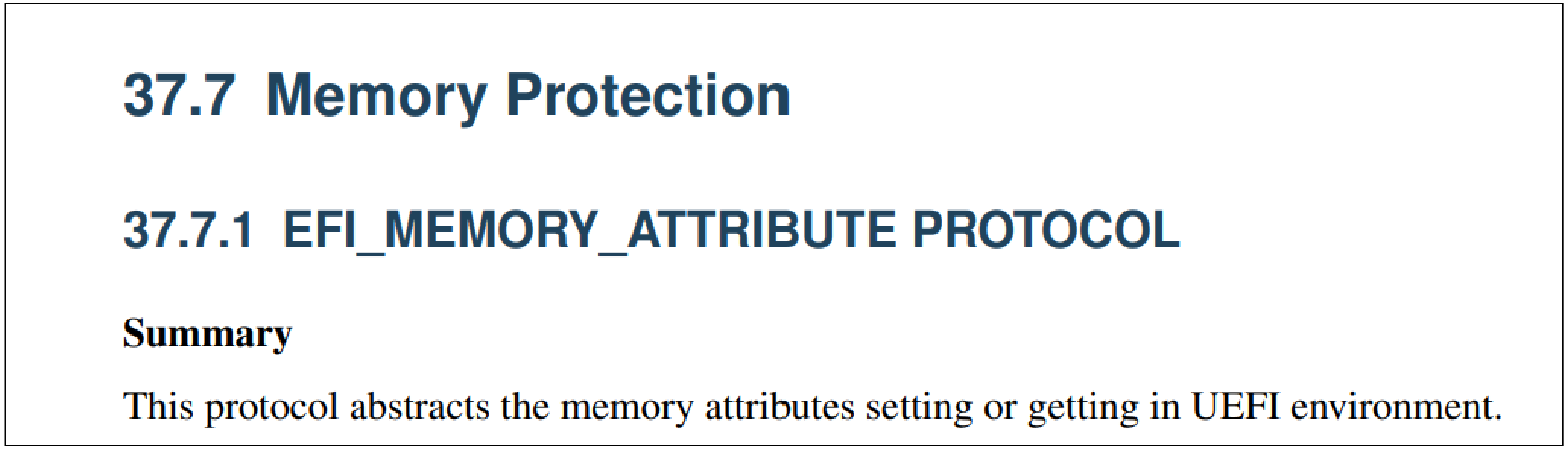
Enhanced Memory Protection

Compatibility Preamble

It will take time and effort for legacy code to be updated to adhere to these new requirements

Enhanced Memory Protection

1. The Memory Attribute Protocol must be present on the platform



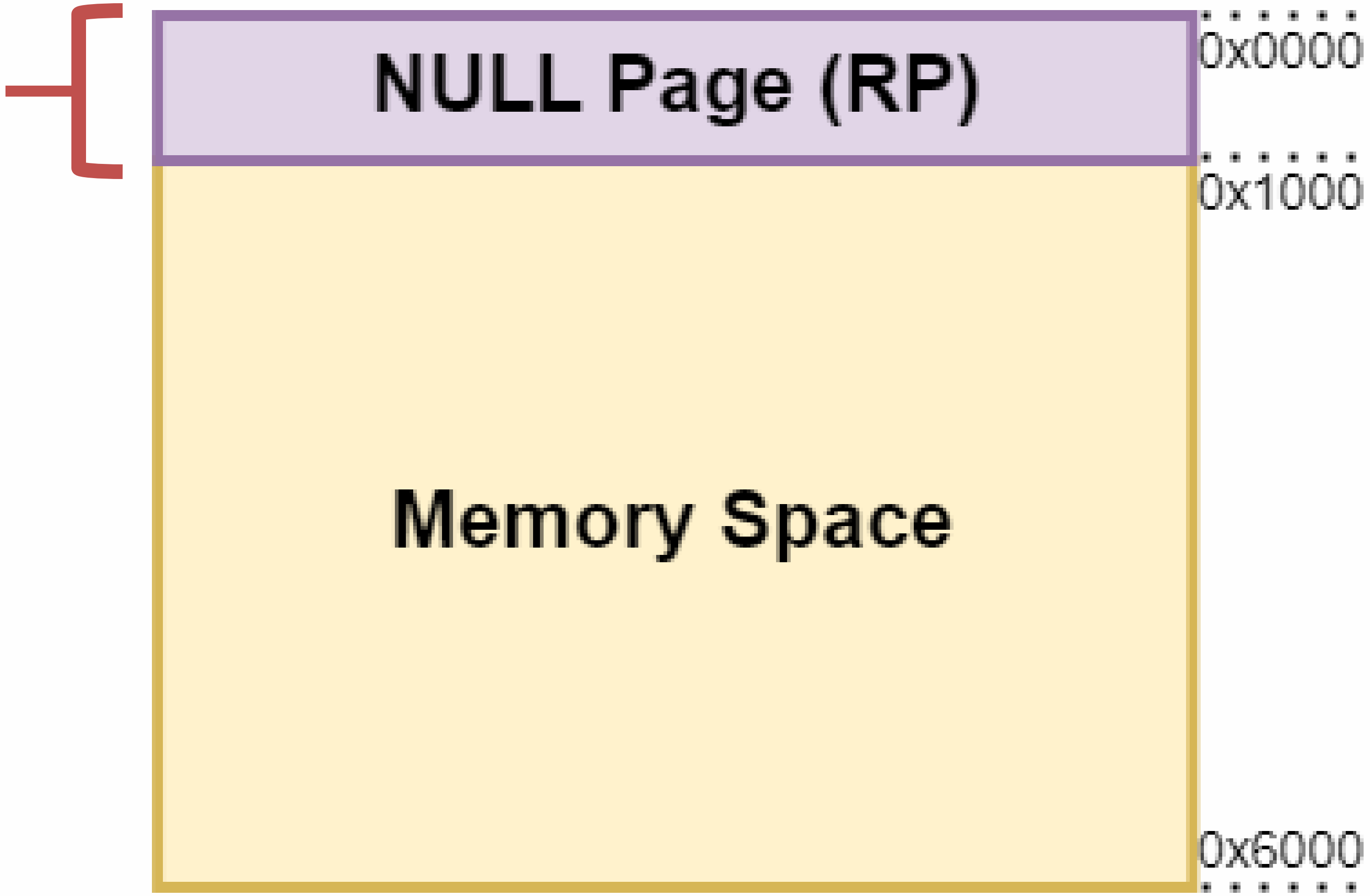
37.7 Memory Protection

37.7.1 EFI_MEMORY_ATTRIBUTE PROTOCOL

Summary

This protocol abstracts the memory attributes setting or getting in UEFI environment.

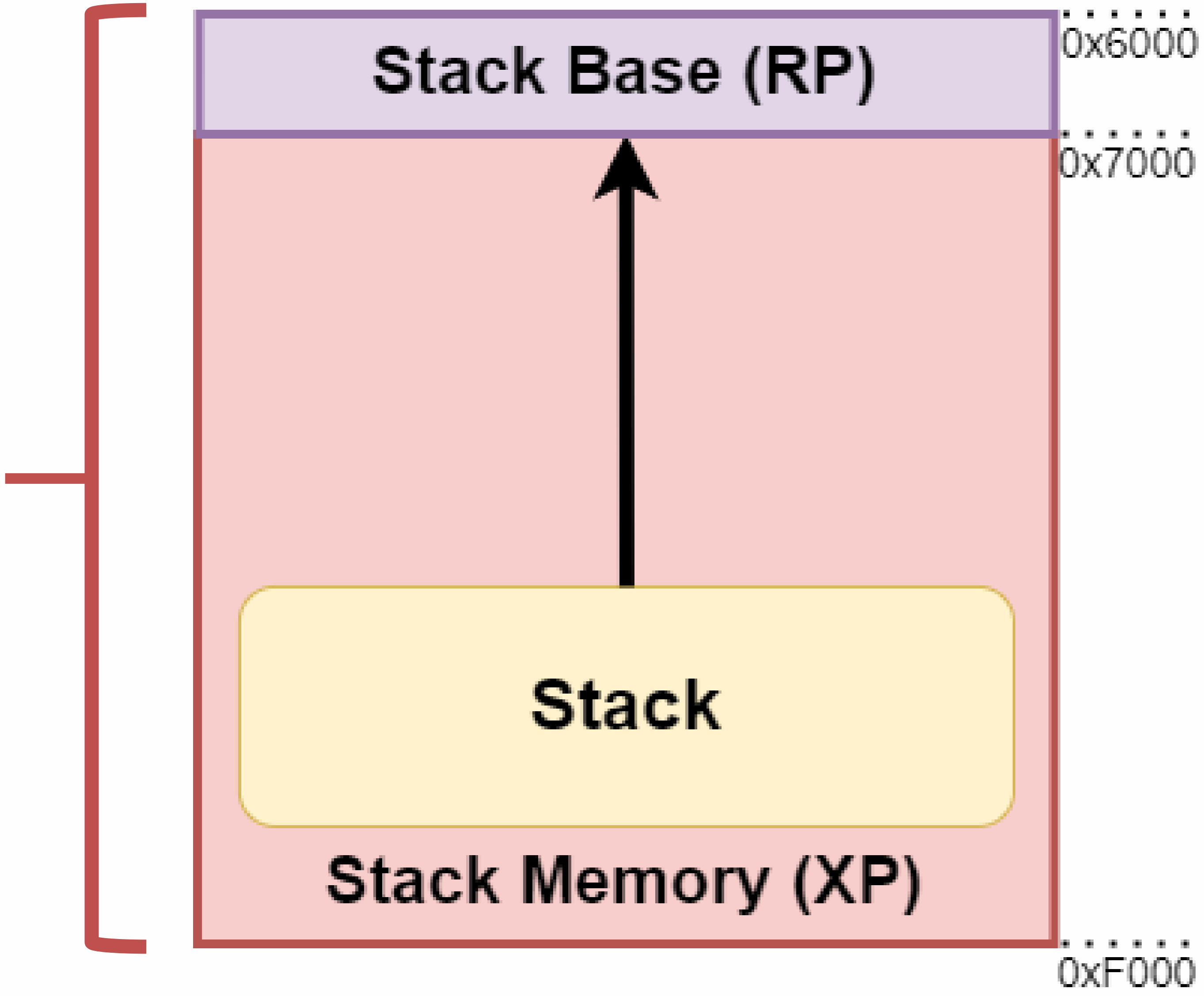
Enhanced Memory Protection



2. Page zero is marked EFI_MEMORY_RP

Enhanced Memory Protection

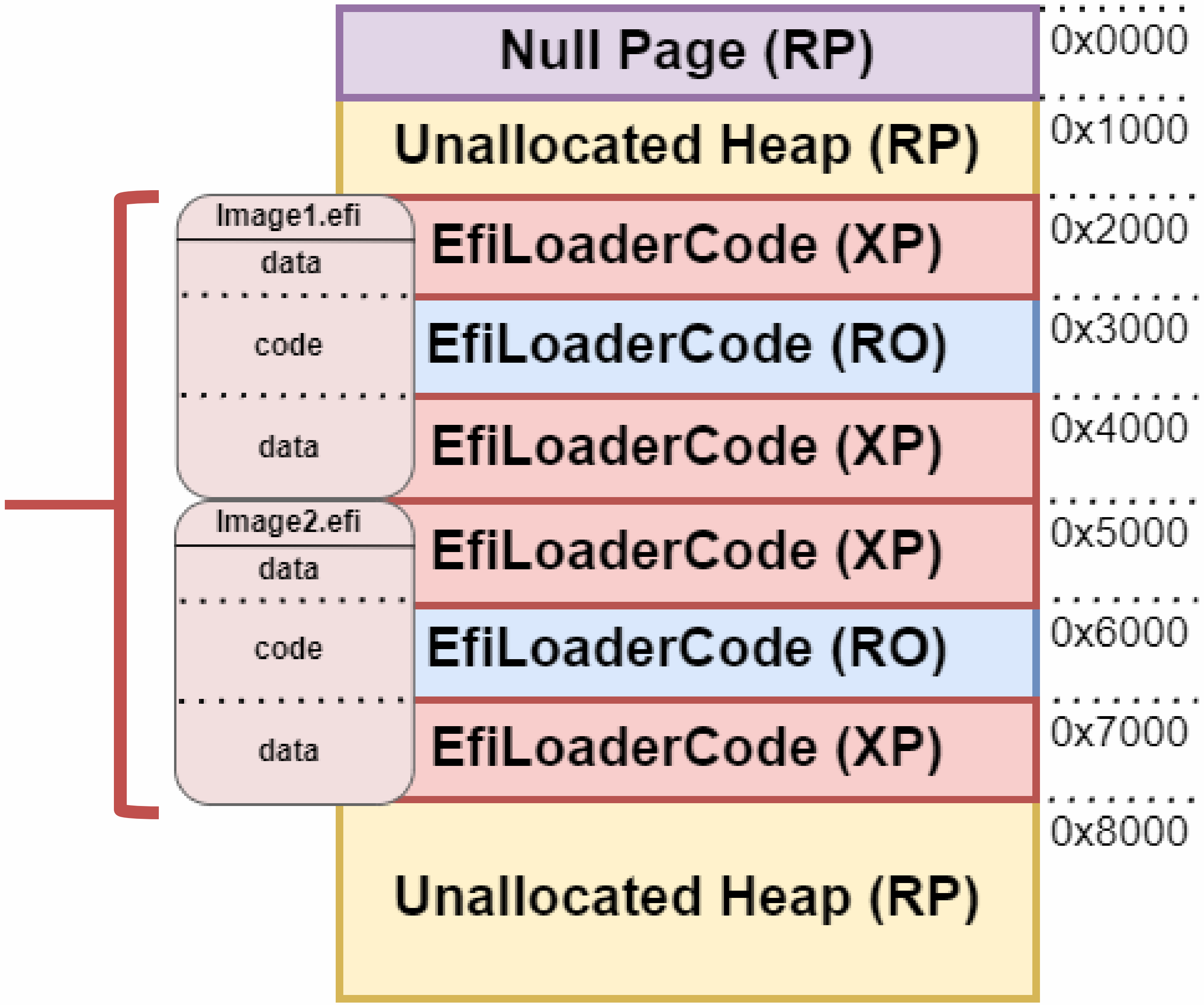
3. AP and BSP stack memory is EFI_MEMORY_XP and the bottom of the stack has a guard an EFI_MEMORY_RP



Enhanced Memory Protection

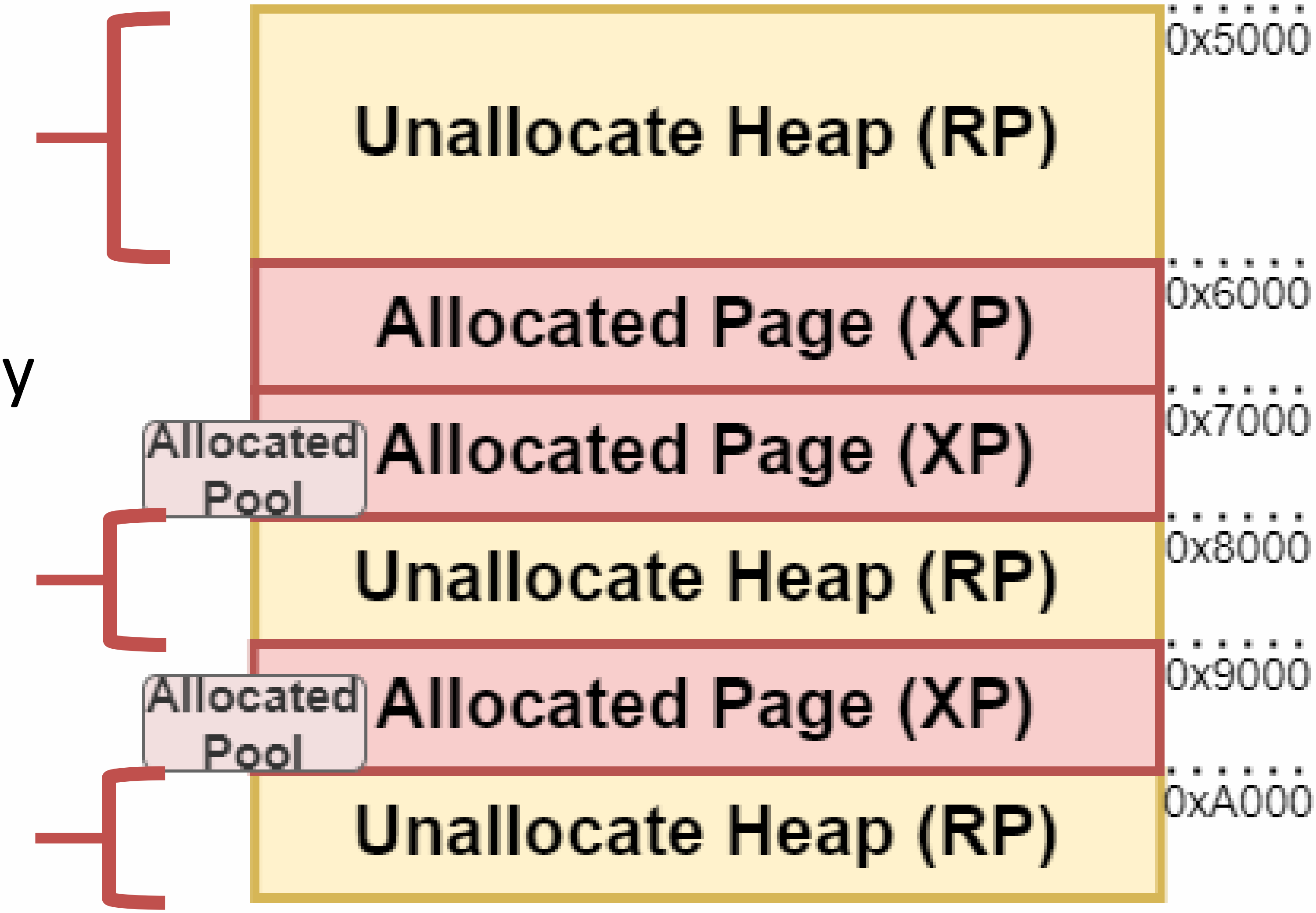
4. EFI_MEMORY_XP applied to data sections

5. EFI_MEMORY_RO applied to code sections



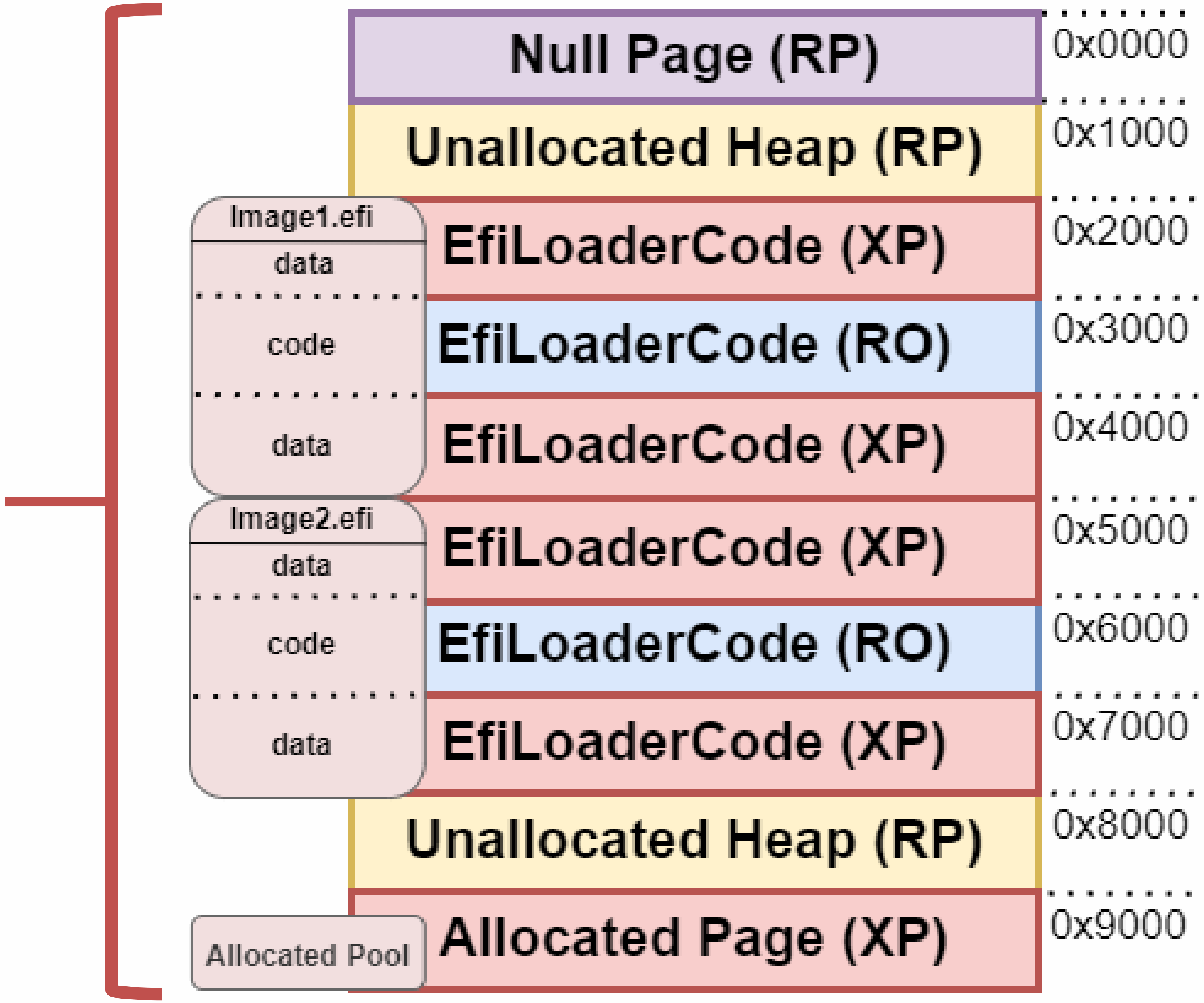
Enhanced Memory Protection

6. Unallocated heap memory is EFI_MEMORY_RP



Enhanced Memory Protection

7. No memory range should be simultaneously readable, writable, and executable.



Enhanced Memory Protection

8. MMIO ranges should be in the EFI memory map and marked EFI_MEMORY_XP

9. Address space not present in the EFI memory map must cause a CPU fault if accessed

Compatibility Mode

1. Allocated buffers will be Readable, writable, and executable.
2. Loaded image buffers no longer have restrictive access attributes.
3. Page zero will be mapped.

Compatibility Mode

- Microsoft is working with partners to add support for enhanced memory protection.
- Compatibility mode may continue be used by legacy bootloaders and OPROMs until their end of life.

Memory Protection: Future

Closing the Gap to Reach a Heightened Security Bar

- Push for enhanced memory protection by default.
- Help our industry partners produce compatible firmware.
- Develop tools to audit and verify memory protection.
- Document how to debug common memory protection violations.

Case Study: Surface Laptop 5

Source: Firmware Attack Surface Reduction (FASR)

Surface Laptop 5

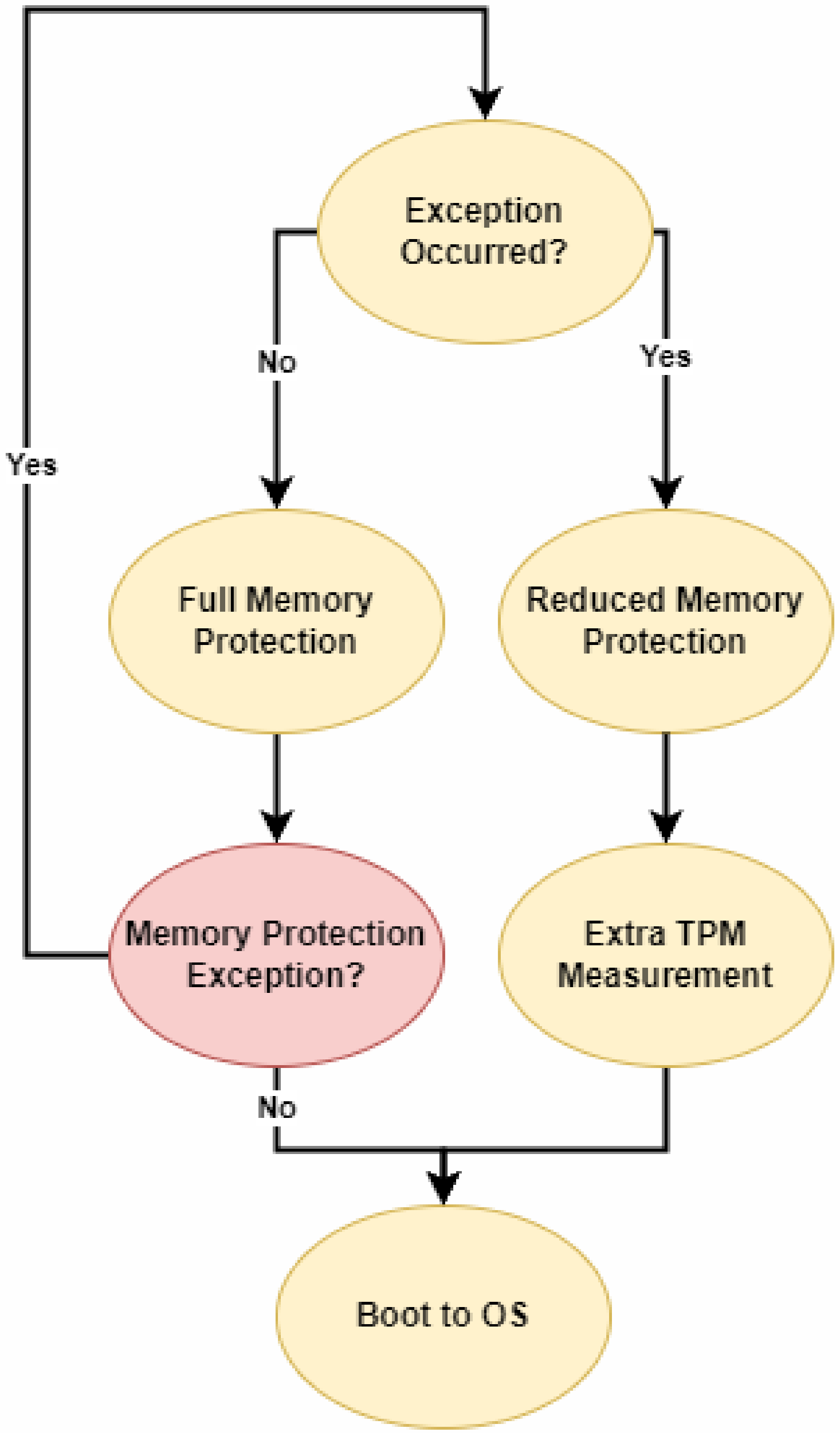
- Surface Laptop 5 runs a fork of EDK2.
- Secured-core compliant firmware solution.
- Enables enhanced memory protection.

Compatibility Concern

Unexpected code paths or unexpected edge cases could occur which result in protection faults in shipped devices.

Exception Handling

- Memory protection related exceptions causes a reboot into a reduced protection state.
- The TPM measurement changes resulting in secured data/secrets to be inaccessible.

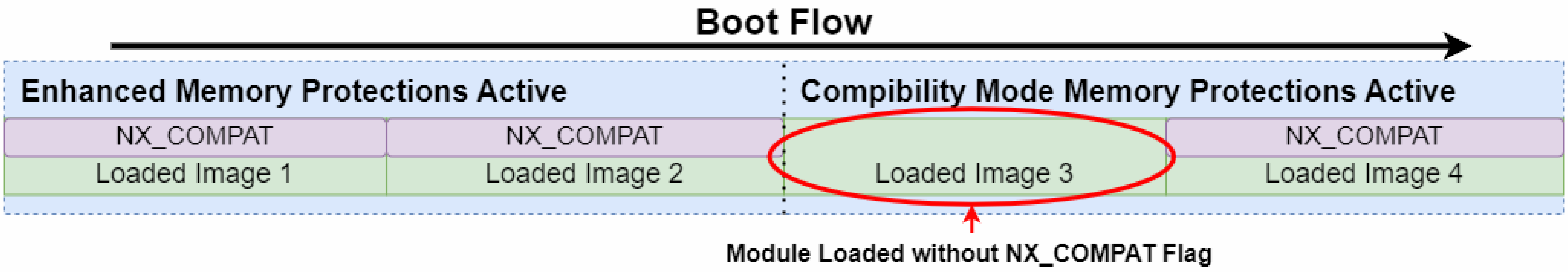


Compatibility Concern

OPROMs may not be compatible with enhanced memory protection.

NX_COMPAT PE/COFF Flag

- Indicates an OPROM or bootloader (like Shim) is compatible with enhanced memory protection.
- If an image is loaded without the flag, the platform enters compatibility mode.



Boot Flow

Enhanced Memory Protections Active

Compibility Mode Memory Protections Active

NX_COMPAT

Loaded Image 1

NX_COMPAT

Loaded Image 2

Loaded Image 3

NX_COMPAT

Loaded Image 4

Module Loaded without NX_COMPAT Flag

UEFI Memory Protection and Windows

Exact details are TBD. Examples:

- Testing: A logo test to check if the system meets the enhanced memory protection criteria
- Transparency: Firmware Security features may be listed out alongside their enablement state in the Windows Security App

Tools and Tests

Tools and Tests

Memory Protection Test App [link]:

- Tests page guards, pool guards, stack guard, NX protection, NULL detection.
- Can be run in 4 ways:
  1. Violating active memory protections and resetting
  2. Building a page table map and inspecting the active protections
  3. Using the memory attribute protocol to inspect active protections

Memory Attribute Protocol Test App [link]:

- Tests the Memory Attribute Protocol functionality.
- Tests for some bugs found as we've added enhanced memory protection compatibility to the Windows Bootloader.

PE/COFF Image Validation [link]:

- Tests PE images against a set of tests and associated requirements.
- This can help confirm that NX_COMPAT is set, sections are aligned, etc.

Tools and Tests

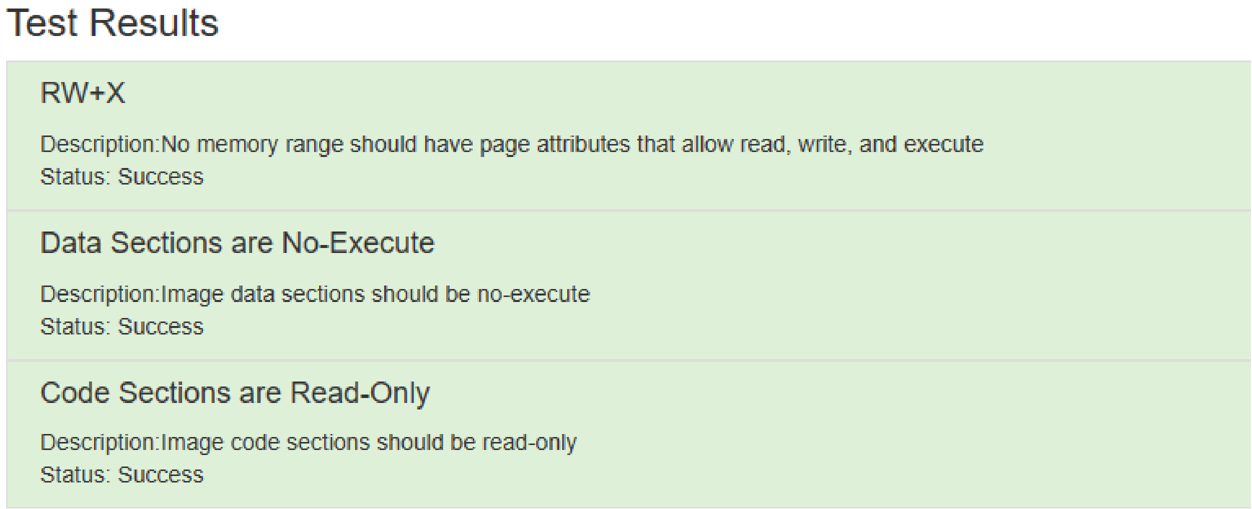
Enhanced Memory Protection Test:

1. UEFI Spec 2.10 Memory Attribute Protocol is present
2. Unallocated memory (EFI Conventional) is EFI_MEMORY_RP
3. Page zero (NULL) is EFI_MEMORY_RP
4. The stack is EFI_MEMORY_XP
5. An EFI_MEMORY_RP guard is at the bottom of the stack
6. New allocations are EFI_MEMORY_XP
7. MMIO ranges are EFI_MEMORY_XP
8. EFI_MEMORY_XP applied to loaded image data regions
9. EFI_MEMORY_RO applied to loaded image code regions
10. No RWX ranges

Tools and Tests

DXE Paging Audit [link]:

- Collects the page table, stack information, EFI and GCD memory maps, loaded images, and processor specific info to generate a human-readable snapshot of memory at the time of the audit.



Test Results

RW+X

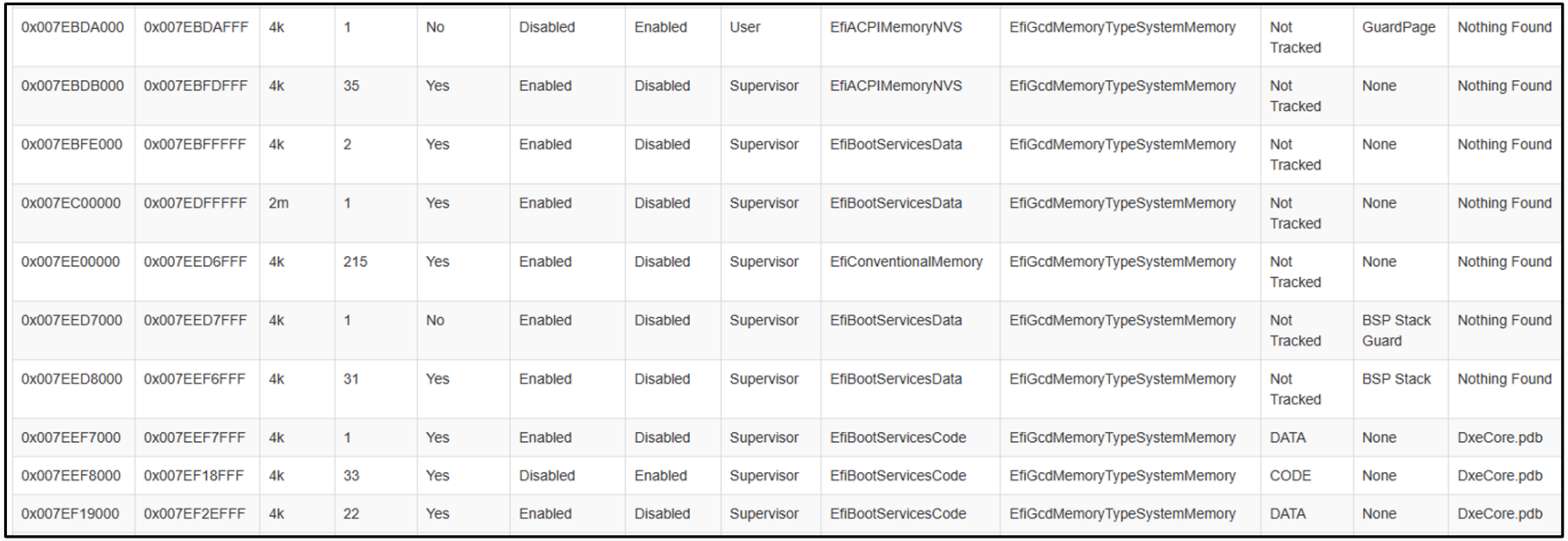
Description:No memory range should have page attributes that allow read, write, and execute
Status: Success

Data Sections are No-Execute

Description:Image data sections should be no-execute
Status: Success

Code Sections are Read-Only

Description:Image code sections should be read-only
Status: Success



0x007EBDA000	0x007EBDAFFF	4k	1	No	Disabled	Enabled	User	EfiACPIMemoryNVS	EfiGcdMemoryTypeSystemMemory	Not Tracked	GuardPage	Nothing Found
0x007EBDB000	0x007EBFDFFF	4k	35	Yes	Enabled	Disabled	Supervisor	EfiACPIMemoryNVS	EfiGcdMemoryTypeSystemMemory	Not Tracked	None	Nothing Found
0x007EBFE000	0x007EBFFFFF	4k	2	Yes	Enabled	Disabled	Supervisor	EfiBootServicesData	EfiGcdMemoryTypeSystemMemory	Not Tracked	None	Nothing Found
0x007EC00000	0x007EDFFFFF	2m	1	Yes	Enabled	Disabled	Supervisor	EfiBootServicesData	EfiGcdMemoryTypeSystemMemory	Not Tracked	None	Nothing Found
0x007EE00000	0x007EED6FFF	4k	215	Yes	Enabled	Disabled	Supervisor	EfiConventionalMemory	EfiGcdMemoryTypeSystemMemory	Not Tracked	None	Nothing Found
0x007EED7000	0x007EED7FFF	4k	1	No	Enabled	Disabled	Supervisor	EfiBootServicesData	EfiGcdMemoryTypeSystemMemory	Not Tracked	BSP Stack Guard	Nothing Found
0x007EED8000	0x007EEF6FFF	4k	31	Yes	Enabled	Disabled	Supervisor	EfiBootServicesData	EfiGcdMemoryTypeSystemMemory	Not Tracked	BSP Stack	Nothing Found
0x007EEF7000	0x007EEF7FFF	4k	1	Yes	Enabled	Disabled	Supervisor	EfiBootServicesCode	EfiGcdMemoryTypeSystemMemory	DATA	None	DxeCore.pdb
0x007EEF8000	0x007EF18FFF	4k	33	Yes	Disabled	Enabled	Supervisor	EfiBootServicesCode	EfiGcdMemoryTypeSystemMemory	CODE	None	DxeCore.pdb
0x007EF19000	0x007EF2EFFF	4k	22	Yes	Enabled	Disabled	Supervisor	EfiBootServicesCode	EfiGcdMemoryTypeSystemMemory	DATA	None	DxeCore.pdb

Thanks for attending the UEFI Fall 2023 Developers Conference & Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

Microsoft