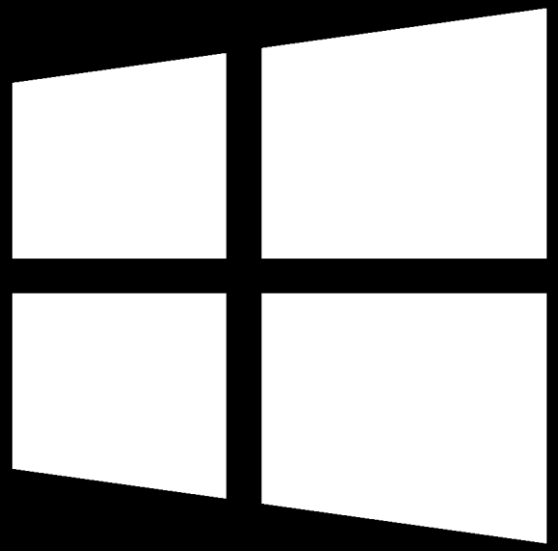


不断增强的 Windows 安全性

Bluehat Shanghai 2019 | David “dwizzzle” Weston | Microsoft OS Security Group Manager


早上好 上海!
震旦

Windows 正在不断进化……

PC 上的 Windows
熟悉的桌面体验
庞大的硬件生态
桌面应用兼容性

Xbox 上的 Windows
Windows 10 界面体验
独特的安全模型
共享的游戏体验

IoT 中的 Windows
基础操作系统
应用和设备平台
运行时和框架

还有更多地方……
适配不同形态设备
界面体验
支持不同设备场景

One Core OS
基础操作系统
应用和设备平台
运行时和框架

所有代码执行均可保证完整性。

用户标识无法被攻陷、嗅探或盗窃。

随意通过物理方式访问的攻击者，无法修改设备上的数据或代码。

恶意代码无法在设备上存留。

违反承诺的举措会被立即发现。

所有应用和系统组件仅具备必须的特权。

增强的安全性

Windows 10 S

1 以管理员身份运行

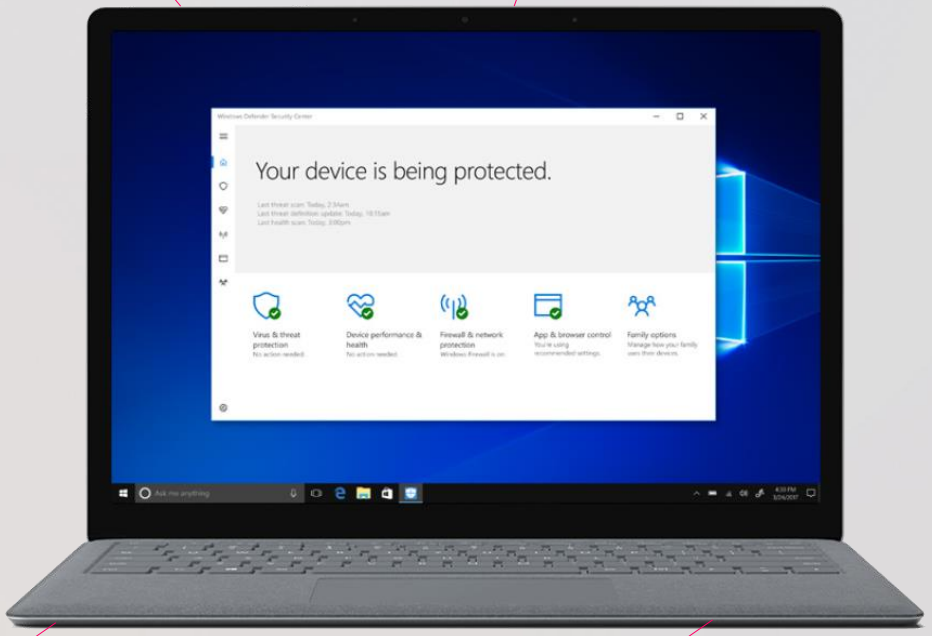
2 执行不带签名的代码

3 使用密码

4 缓解措施并不总能生效

1 强制代码签名

3 阻止来自互联网的脚本和宏



2 无需密码即可登录

4 “Admin Less”用户帐户

10 S：安装数上百万，尚未检测到广泛传播的恶意软件

所有代码执行均可保证完整性。

Windows 10 S

代码完整性的改进

CI 策略移除了大部分“代理的”二进制文件

仅提供带有应用商店签名的应用（UWP 或 Centennial）

支持危险操作的“远程”文件扩展已被阻止

远程 Office 宏默认已被阻止

Windows 10 S

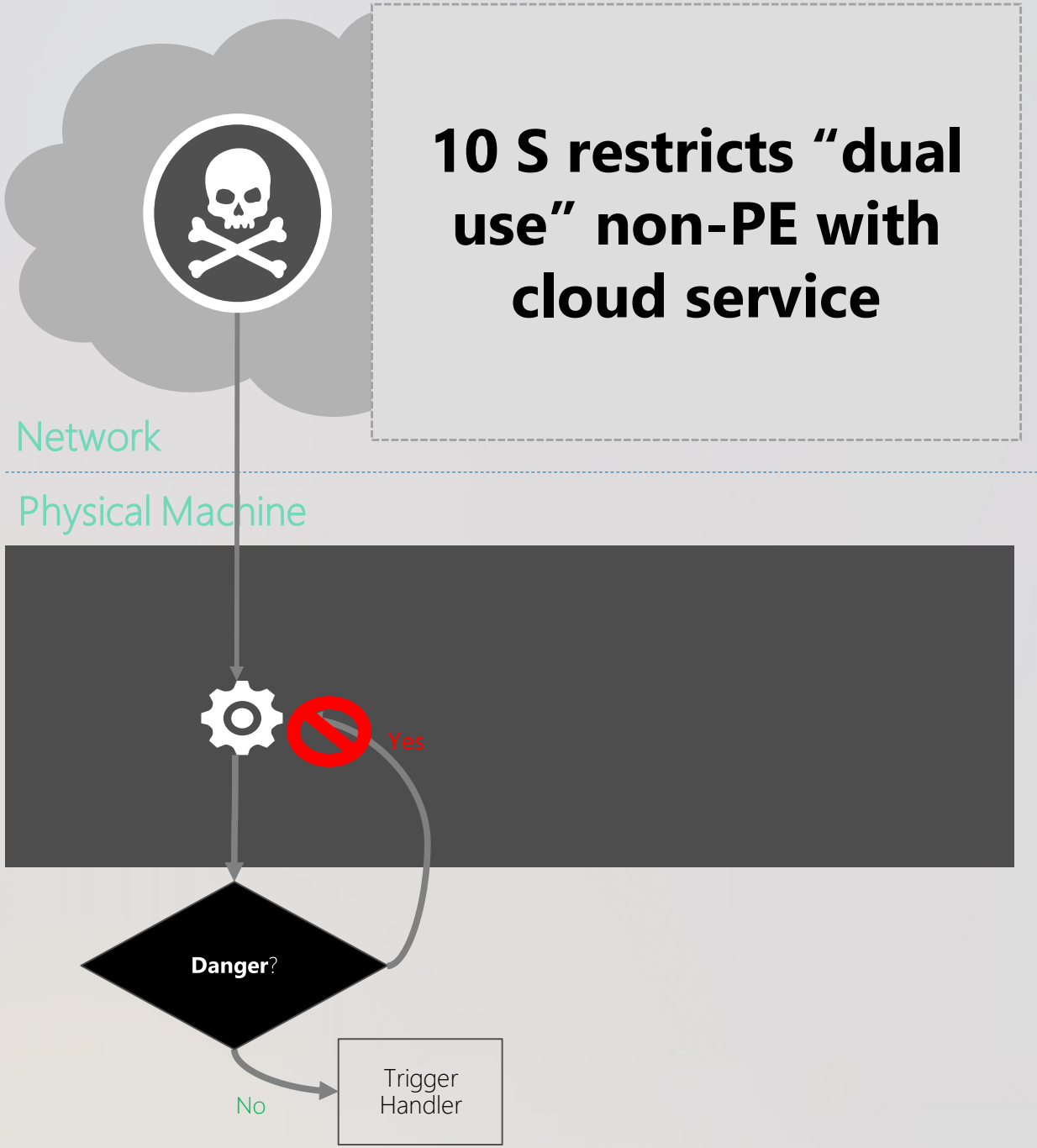
第一重代码完整性保护

“第一重”CI 绕过，使得远程攻击者能够触发未签名代码的初始执行

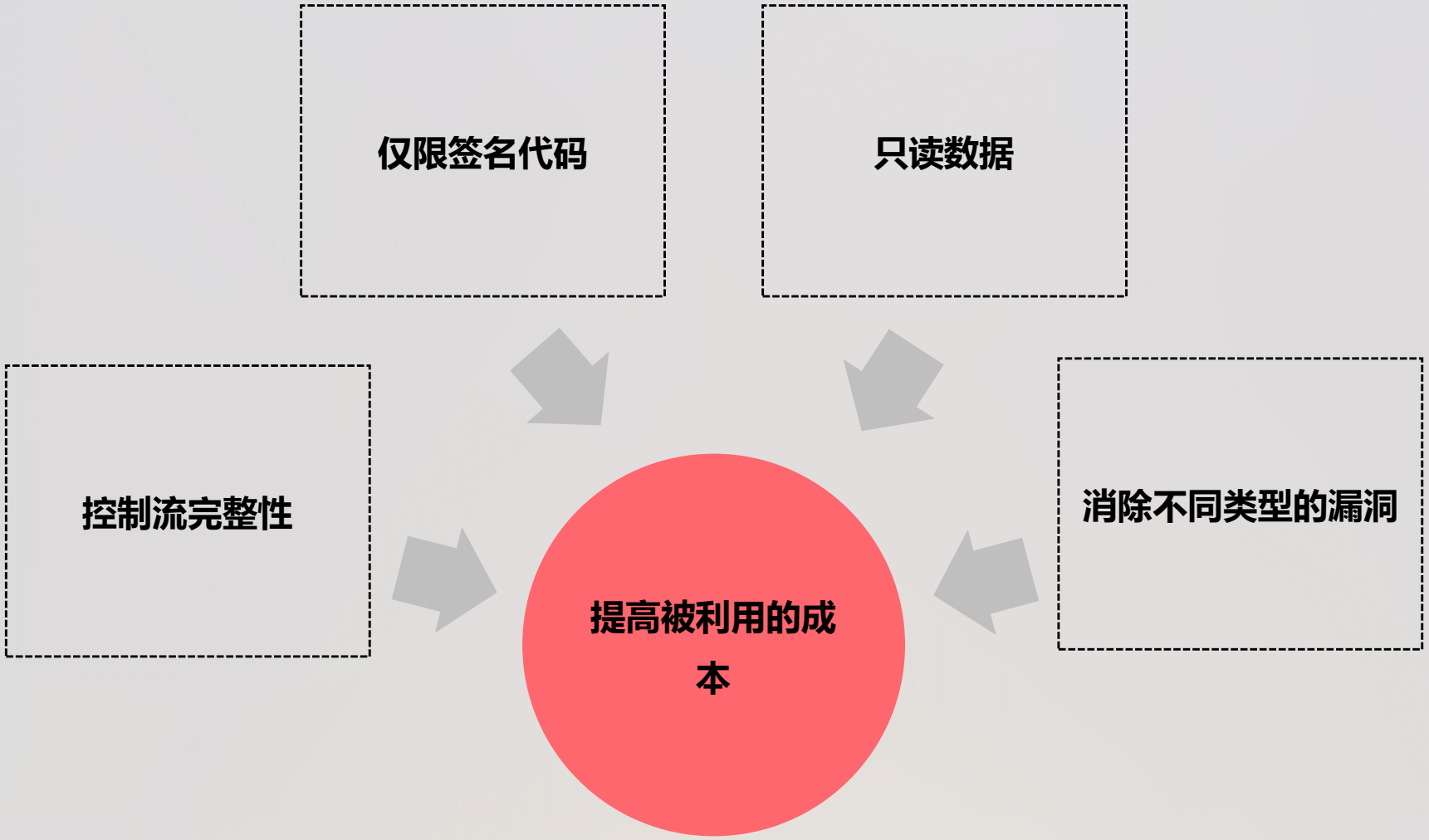
10 S 侧重于防止“第一重”绕过

“第二重”绕过，使得在执行完初始代码 *之后*，可以进一步执行更多未签名代码

10 S 为“第二重”绕过提供了持久的保证



漏洞利用缓解策略



控制流面临的挑战

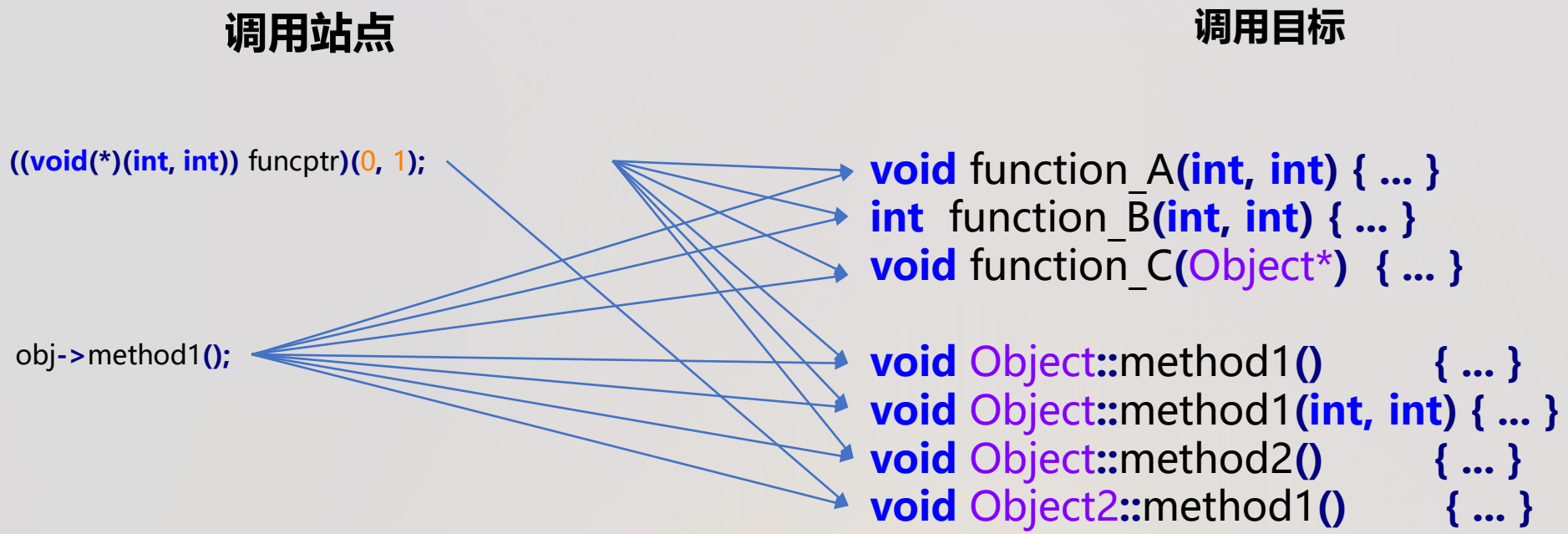
1. 危险的调用目标
2. 不受保护的栈
3. 数据流破坏

改善控制流完整性

CFG

Windows 中的第一代 CFI，出于兼容性和性能方面的考虑，粒度较大

使用“导出限制”减小特定进程（如 Microsoft Edge）中合法调用点的数量



改善控制流完整性

隆重介绍：XFG

目标：通过高效、兼容性高的方式提供更细化的 CFI

概念：通过类型签名检查保证合法的间接跳转

调用站点

```
((void(*)(int, int)) funcptr)(0, 1);
```

```
obj->method1();
```

调用目标

```
void function_A(int, int) { ... }
int  function_B(int, int) { ... }
void function_C(Object*)  { ... }

void Object::method1()          { ... }
void Object::method1(int, int) { ... }
void Object::method2()          { ... }
void Object2::method1()         { ... }
```

XFG 的设计：基础

为每个获取地址的函数分配一个基于类型签名的标志

对于 C 风格的函数，可能为：

hash(type(return_value), type(arg1), type(arg2), ...)

对于 C++ 虚拟方法，可能为：

***hash**(method_name, type(retval), highest_parent_with_method(type(this), method_name), type(arg1), type(arg2), ...)*

在执行每个函数之前紧接着嵌入该标志，使其可通过函数指针访问

为调用点添加标志检查：如果遇到任何标签不匹配的情况则快速退出

CFG 指令：调用站点

```
mov  rax, [rsi+0x98]              ; load target address
call [__guard_dispatch_icall_fptr]
```

目标

```
.align 0x10
function:
        push rbp
        push rbx
        push rsi
        ...
```

xFG 指令：调用站点

```
mov  rax, [rsi+0x98]              ; load target address
mov  r10, 0xdeadbeefdeadbeef      ; load function tag
call [__guard_dispatch_icall_fptr_xfg] ; will check tag
```

目标

```
.align 0x10
dq 0xcccccccccccccccc ; just alignment
dq 0xdeadbeefdeadbeef ; function tag
function:
        push rbp
        push rbx
        push rsi
        ...
```

XFG 的安全性

C 风格的函数指针只能调用具备相同类型签名的地址获取函数

调用点和调用目标具有相同数量的参数，参数与返回值类型相同

C++ 虚拟方法只能调用在自己的类层次结构中具备相同名称和类型的方法

无法调用错误类型的重载方法
无法调用来自其他类层次结构的方法
无法调用同一层次结构中类型相同但名称不同的方法

这已经不仅仅是近似 CFG，而是比它更强大

但是要注意：哈希函数的使用意味着技术上来看，有存在碰撞的可能，但对于大约 55 位哈希来说，可能性微乎其微（从实用性的角度来看尤其如此）

控制流面临的挑战

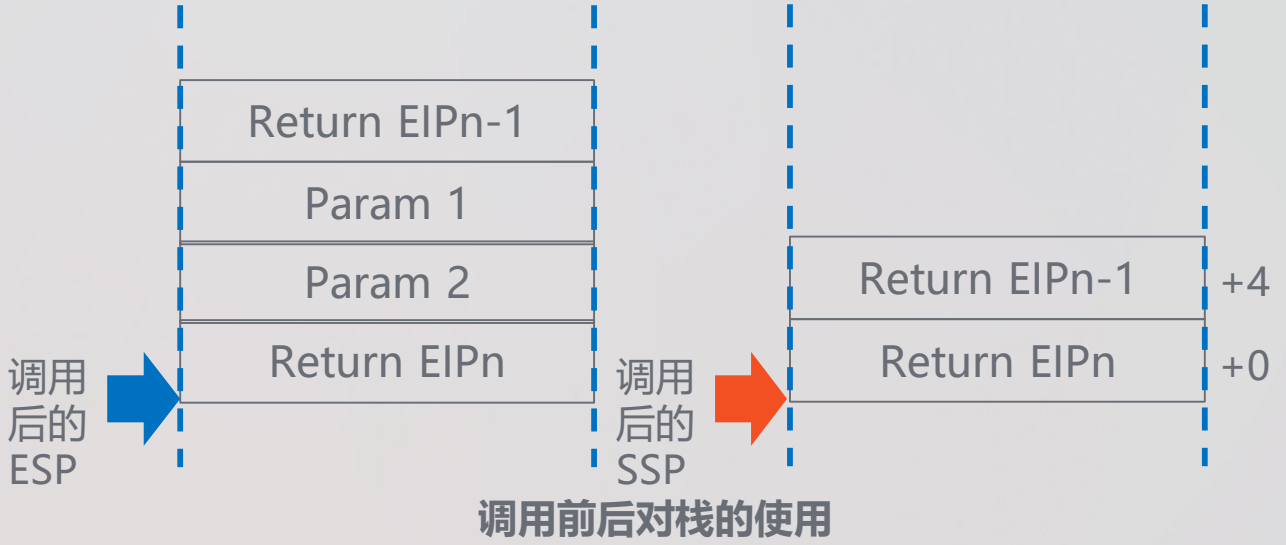
1. 危险的调用目标
2. 不受保护的栈
3. 数据流破坏

反向控制流

影子栈保护

最初曾尝试以软件形式实现栈保护但失败了

OSR 以软件形式设计的影子栈（RFG）未能通过内部的攻击研究



调用前后对栈的使用

控制流实施技术（CET）

可通过影子栈返回地址保护

通过硬件协助缓解控制流劫持和 ROP

在我们的威胁模型中体现出健壮性（在任意地址读写的前提下）

CET 影子栈流程：

函数调用时同时把返回地址压到两个栈里

Ret/ret_imm
同时弹出在两个栈上的返回地址
如果返回地址不匹配则抛出异常

无需为影子栈传递参数

控制流面临的挑战

1. 危险的调用目标
2. 不受保护的栈
3. 数据流破坏

数据损坏保护

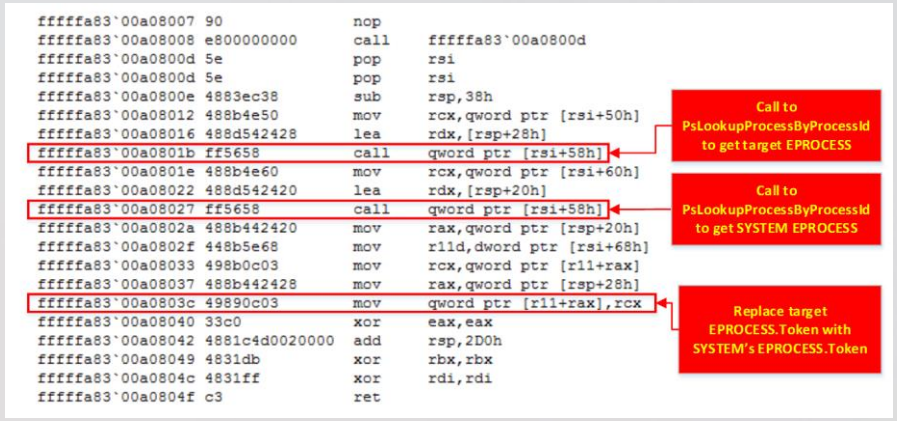
隆重介绍：内核数据保护

问题：对 Windows 内核的利用可通过损坏的数据获得特权提升

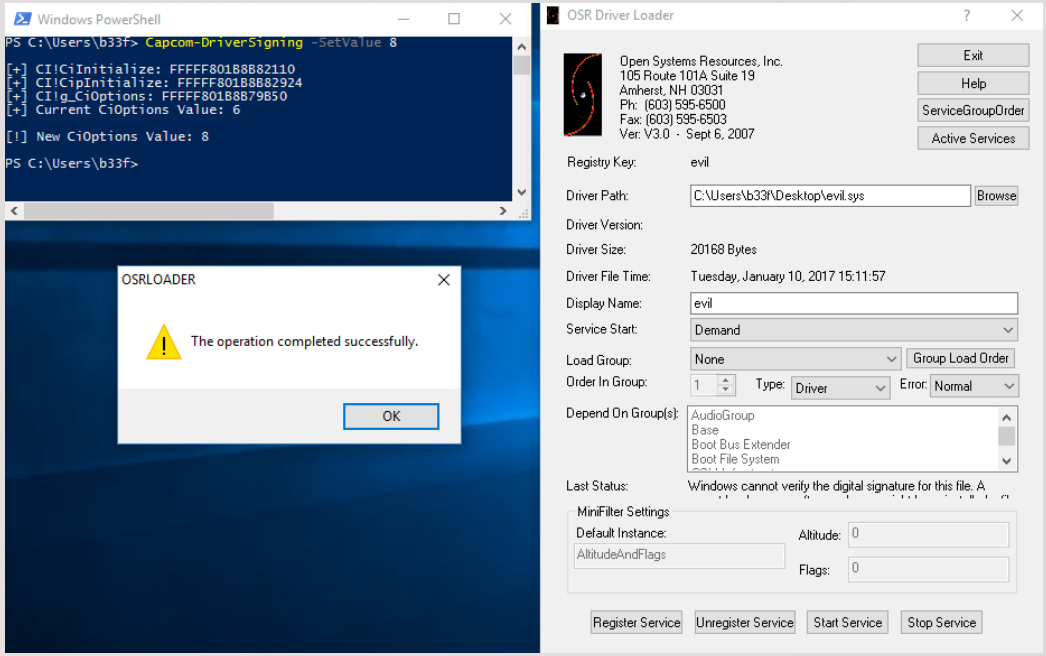
目前状态：基于 Hypervisor 的代码完整性，可防止动态代码注入并强制实施签名策略

仅仅阻止代码还不够，内核还包含了很多敏感数据结构

内核数据保护（KDP）使用安全内核使敏感数据无法被修改

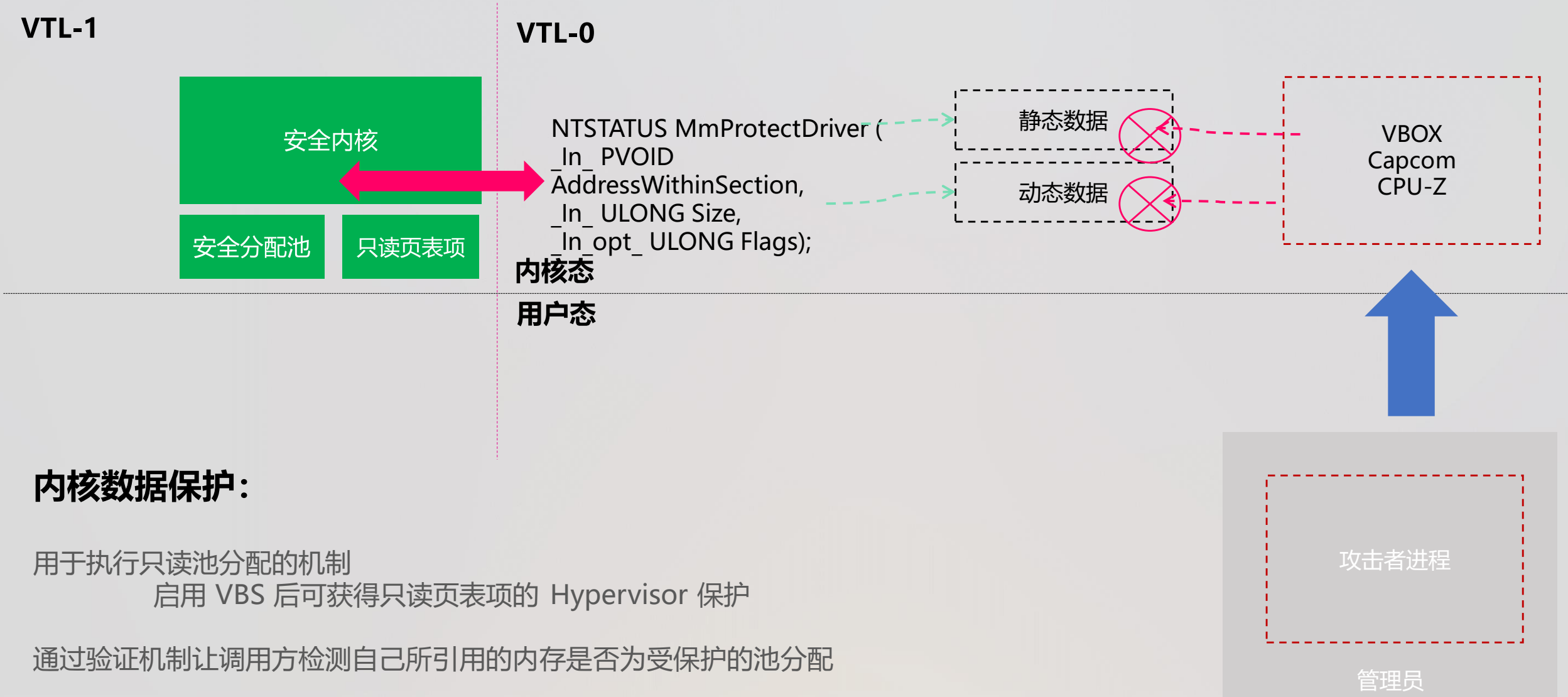


CVE-2016-7256 利用：利用Open type 字体进行权限提升



破坏代码完整性相关的全局变量（来源：FuzzySec）

数据损坏保护



内核数据保护：

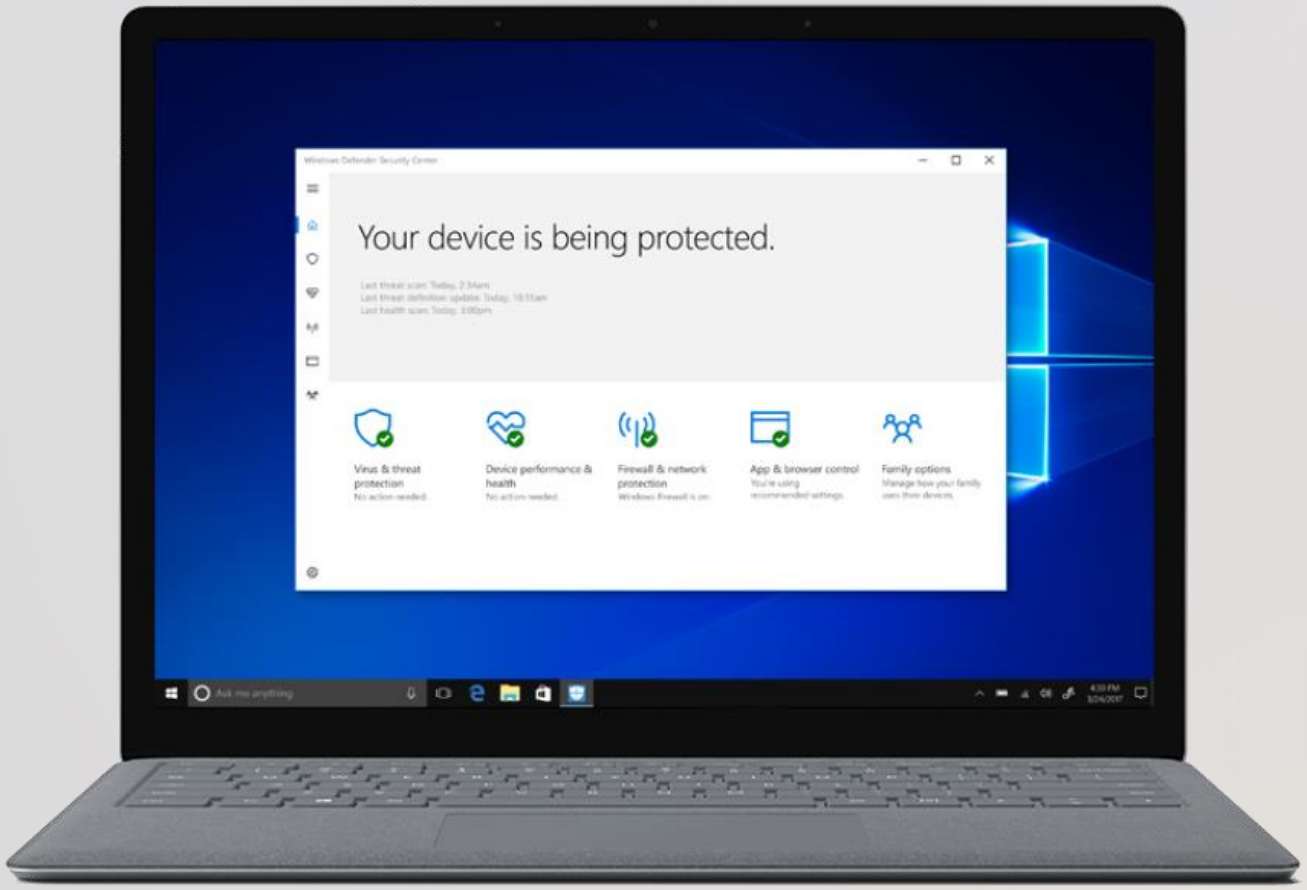
用于执行只读池分配的机制

启用 VBS 后可获得只读页表项的 Hypervisor 保护

通过验证机制让调用方检测自己所引用的内存是否为受保护的池分配

所有应用和系统组件仅具备必须的特权。

“Admin Less”模式



隆重介绍：Admin-less

Admin-less S 模式禁止权限提升

新的标准用户类型可进行某些影响整个设备的改动

标准用户可以更轻松地实现安全性

恶意代码无法在设备上存留。

固件安全问题

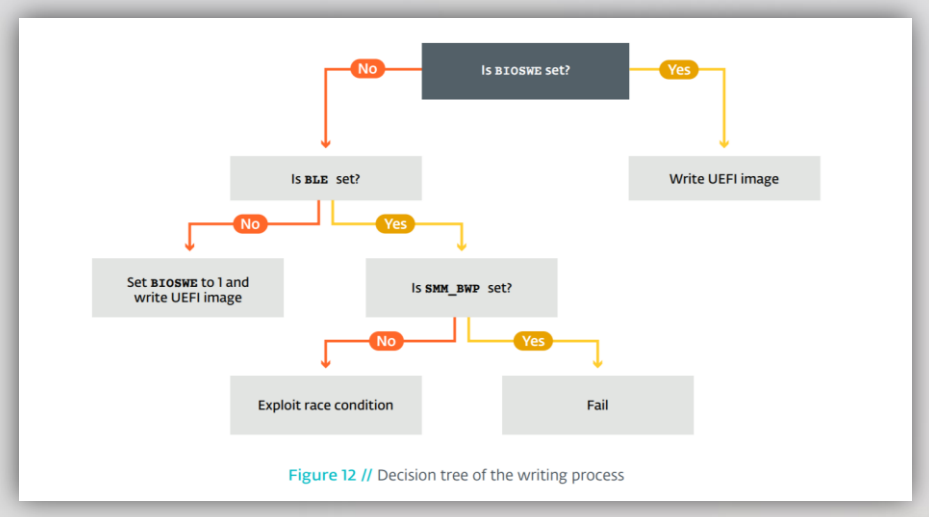
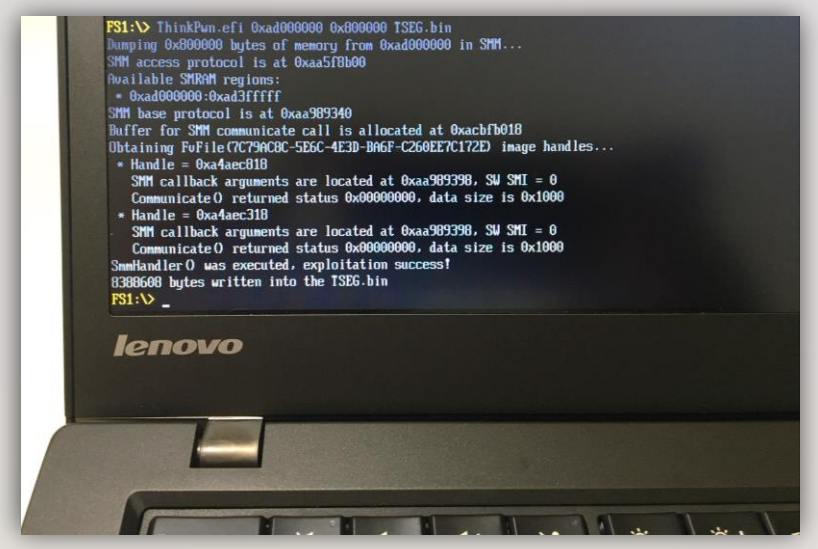


Figure 12 // Decision tree of the writing process

[ESET 发现 SEDNIT/APT28 UEFI 恶意软件]

通过 SMM 攻击绕过 VBS



[“ThinkPWN” 对联想固件的利用]

提高引导过程的安全性

System Guard 与 DRTM 相配合

利用 DRTM（Intel、AMD、QC）通过 Microsoft MLE 执行 TCB 测量

对 UEFI 的“假定入侵”并通过从硬件引导的 MLE 对关键代码和数据进行判定和封印

被测量的值：

- 代码完整性策略
- Hypervisor、内核哈希
- UEFI 变量
- 其他…

零信任

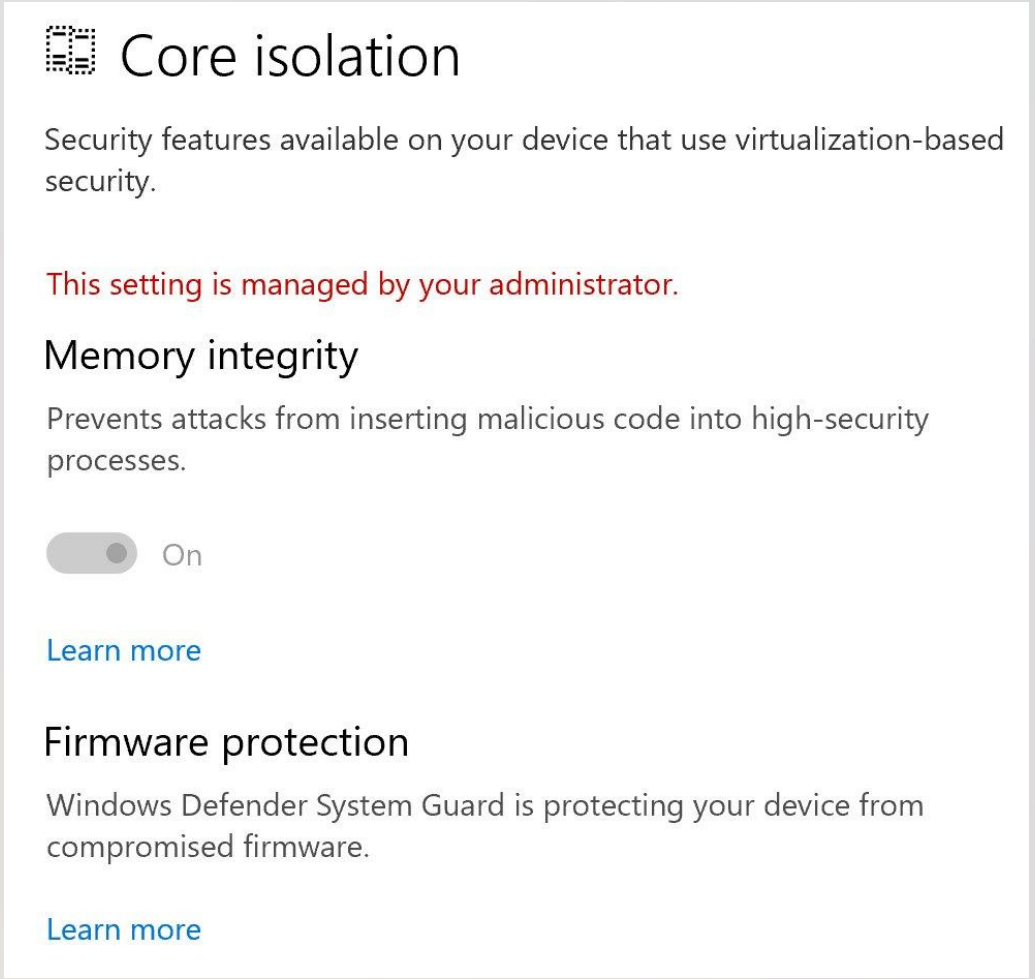
判定 PCR 和 TCG 日志中的密钥属性

通过 System Guard 运行时认证 + Microsoft Conditional Access + WDATP，证实 TCB 组件的安全性

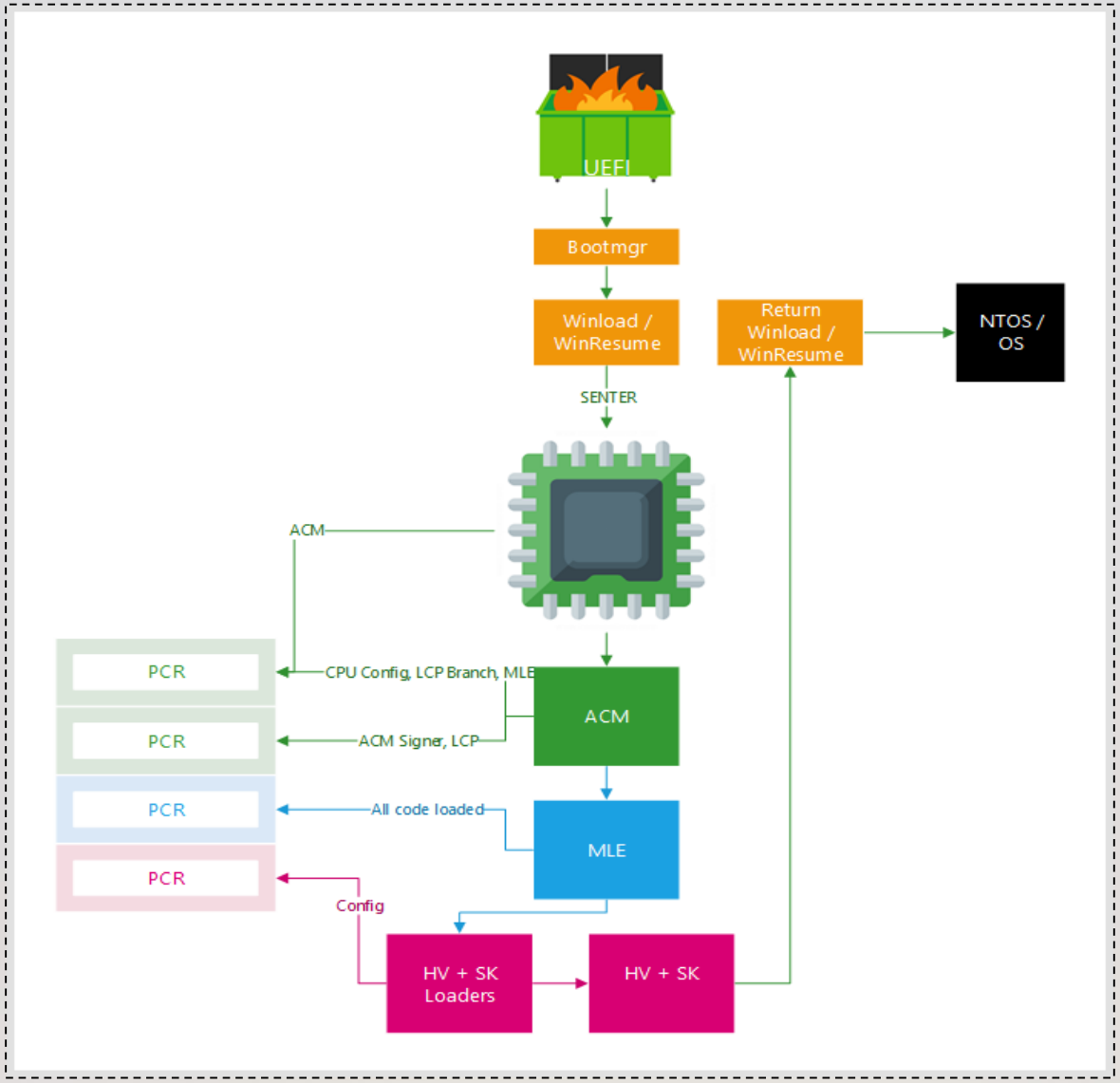
SMM 攻击

可用于篡改 HV 和 SK post-MLE

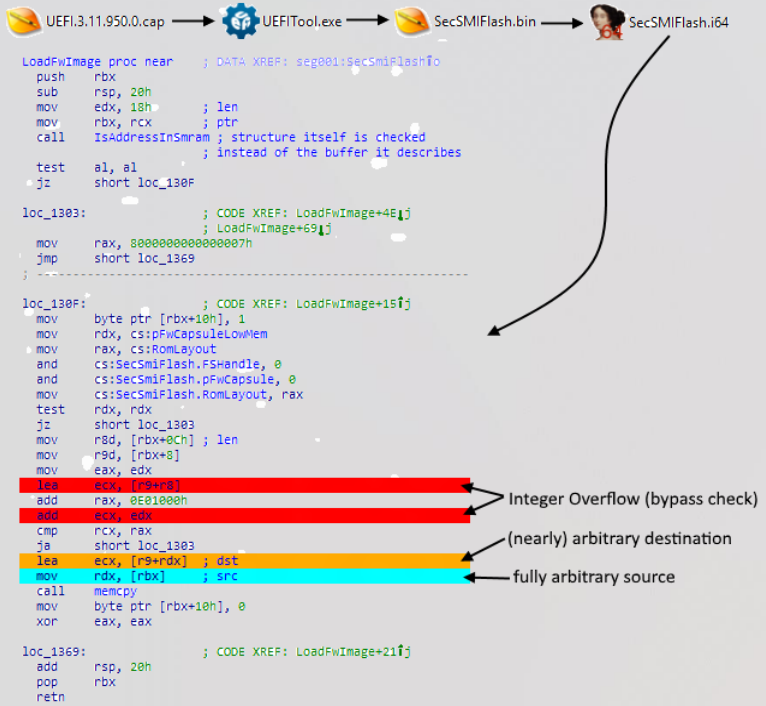
SMM 换页保护 + 认证 正在计划中

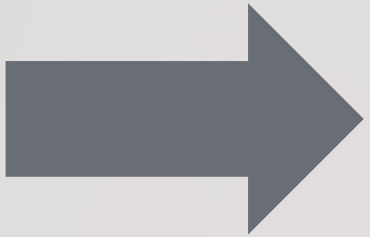


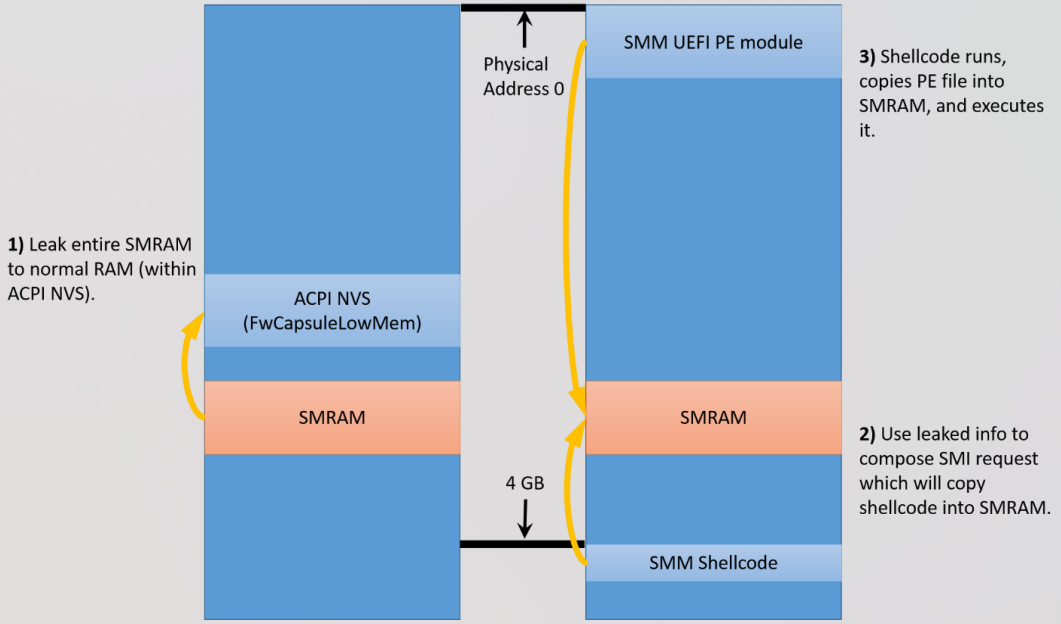
提高引导过程的安全性


UEFI
Bootmgr
Winload / WinResume
Return Winload / WinResume
NTOS / OS
SENTER
ACM
PCR
CPU Config, LCP Branch, MLE
ACM
PCR
ACM Signer, LCP
PCR
All code loaded
MLE
PCR
Config
HV + SK Loaders
HV + SK

提高引导过程的安全性







System Guard 与 DRTM 的配合

外部 研究人员 和 OSR REDTEAM 强调了 SMM 对 DRTM 和 VBS 的风险

SMRAM 中任意代码的执行，可被用于攻击 Hypervisor

SMM 中运行的恶意代码非常难以检测

OSR REDTEAM 所用的 SMM 弱点，已报告给联想

保护 SMM

缓解对 SMM 的利用

Intel Runtime BIOS resilience 为 SMM 提供了如下安全保护：

SMM 入口点锁定

SMM 内所有代码锁定

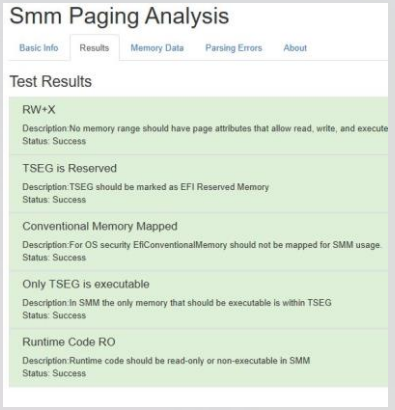
内存映射和页面属性锁定

无法直接从 SMM 访问 OS 和 HV 内存

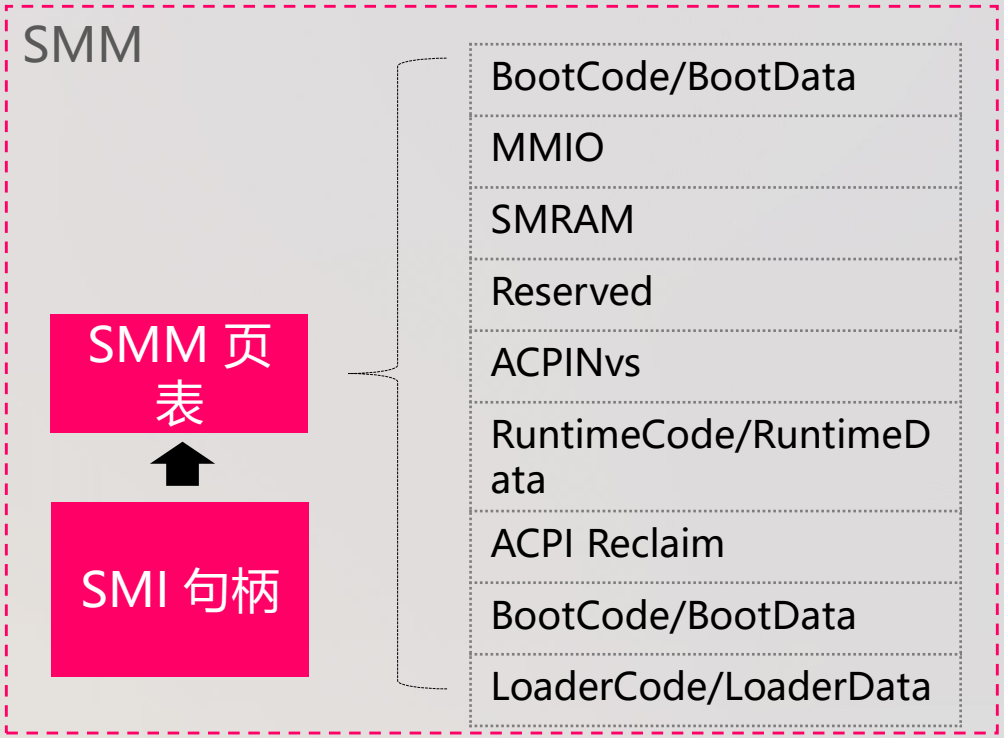
```
//
// Check to see if the CPU supports the SMM Code Access Check feature
// Do not access this MSR unless the CPU supports the SmmRegFeatureControl
//
if ((AsmReadMsr64 (EFI_MSR_SMM_MCA_CAP) & SMM_CODE_ACCESS_CHK_BIT) == 0) {
  mSmmCodeAccessCheckEnable = FALSE;
  return;
}
```

Table 35-34. Additional MSRs Common to Intel® Xeon® Processor D and Intel Xeon Processors E5 v4 Family Based on the Broadwell Microarchitecture

Register Address		Register Name	Scope	Bit Description
Hex	Dec			
17DH	390	MSR_SMM_MCA_CAP	THREAD	Enhanced SMM Capabilities (SMM-RO) Reports SMM capability Enhancement. Accessible only while in SMM.
				57:0 Reserved
				58 SMM_Code_Access_Chk (SMM-RO) If set to 1 indicates that the SMM code access restriction is supported and a host-space interface available to SMM handler.
				59 Long_Flow_Indication (SMM-RO) If set to 1 indicates that the SMM long flow indicator is supported and a host-space interface available to SMM handler.



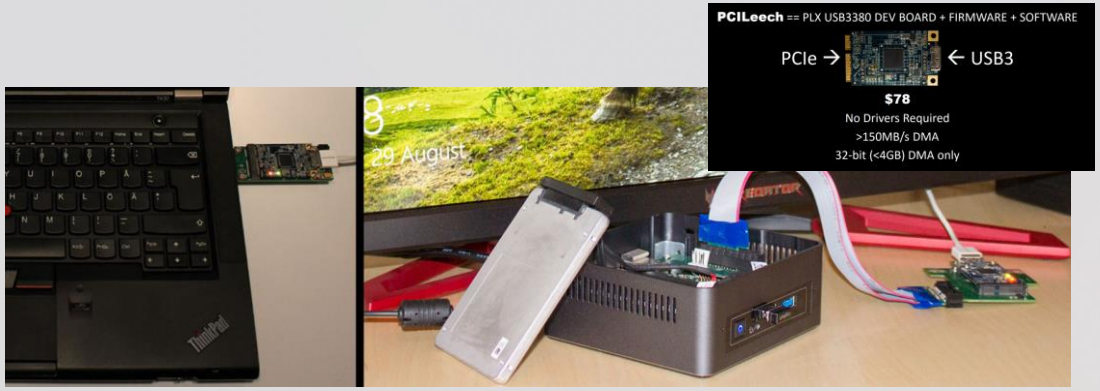
SMM 换页审核



SMM 保护

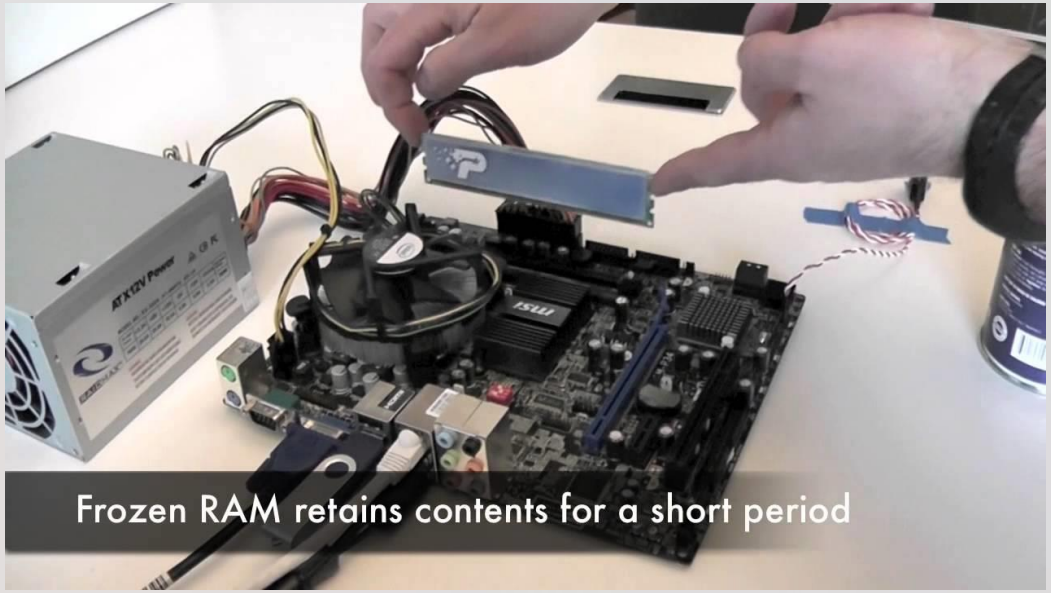
随意通过物理方式访问的攻击者，无法修改设备上的数据或代码。

日益普遍的物理攻击



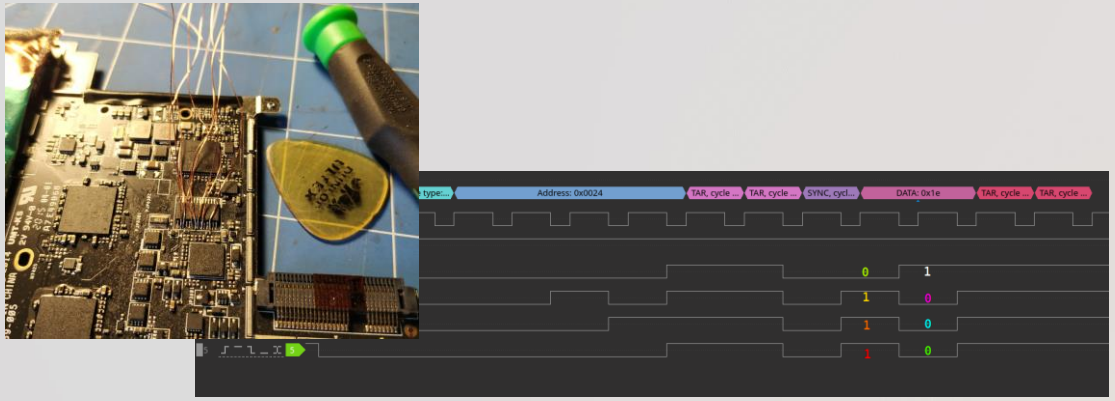
使用 PCILeech 进行 DMA 攻击

来源：1, 2



Bitlocker 冷启动攻击

来源：1



使用 Logic Analyzer 提取 LPC/SPI TPM VMK 密钥

来源：1, 2, 3

Windows DMA 保护

安全目标

防止经由恶意 DMA 攻击所发起的物理攻击对驱动器进行“evil cleaner”

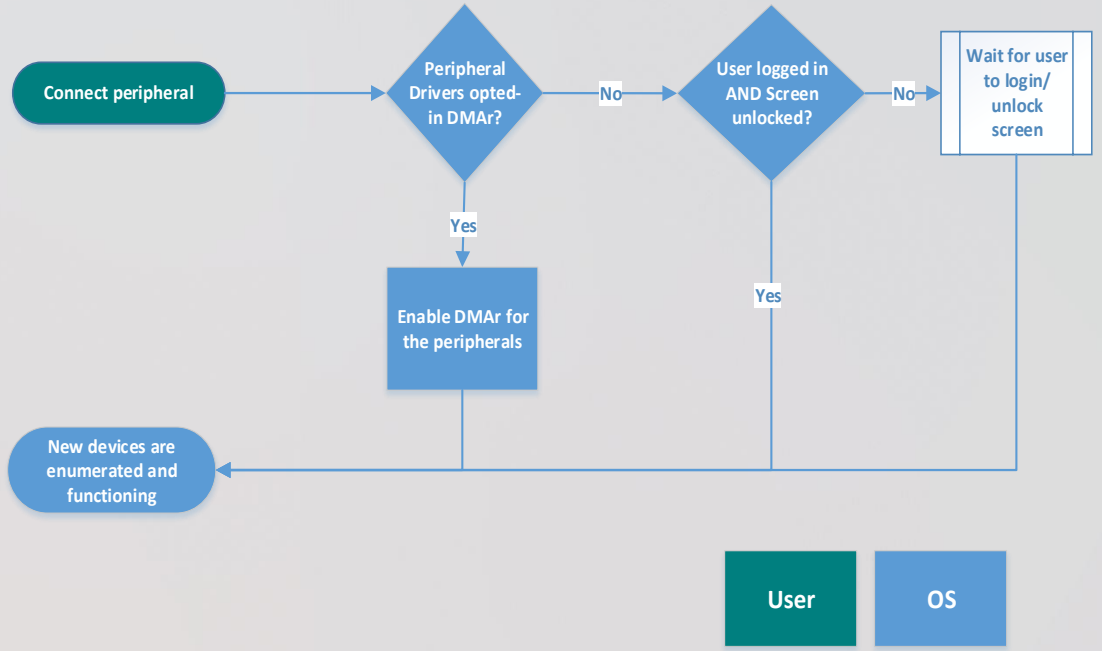
设计细节

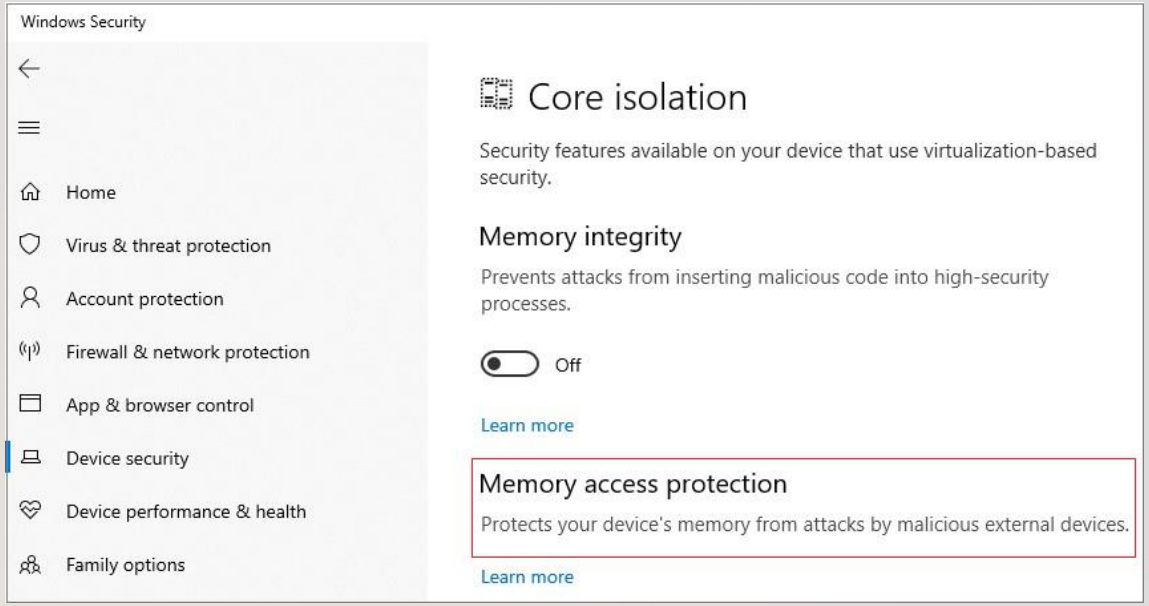
使用 IOMMU 阻止新附加的 Thunderbolt™ 3 设备，在用户登录前禁止进行 DMA 访问

UEFI 可启用 IOMMU 和 BME，该机制可在 Windows 引导前的早期引导阶段生效（参阅 Project Mu）

对于兼容的设备驱动程序，自动启用 DMA 重映射

后续版本中，我们将进一步加固对所有外部 PCI 端口和 cross-silicon 平台的保护





通过加密锁实现的Windows 数据保护

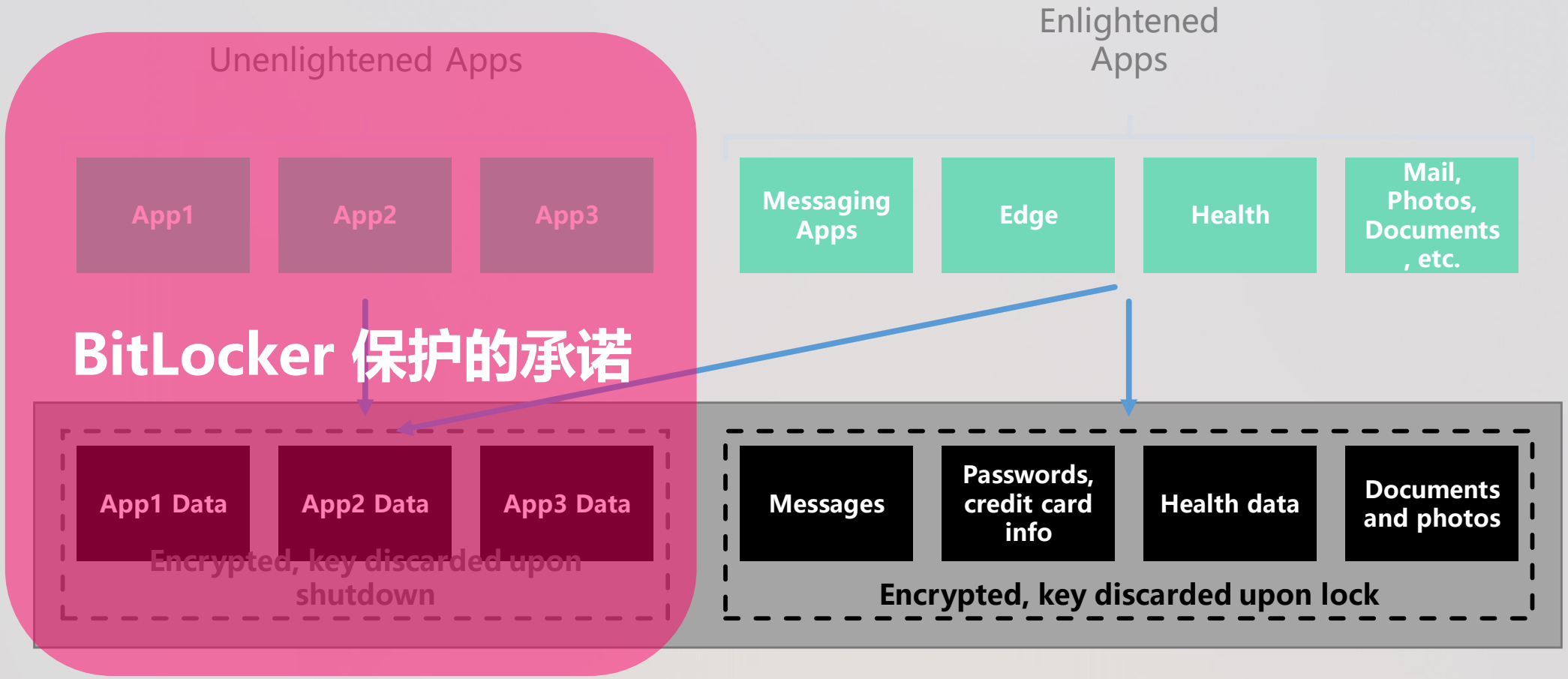
Locked device

Encryption key is removed from memory

Unlocked device

Encryption key is recomputed using user entropy

每文件加密为存储后的文件提供了额外的保护
密钥可从用户的秘密（Hello、生物特征）中生成


Unenlightened Apps
App1
App2
App3
Enlightened Apps
Messaging Apps
Edge
Health
Mail, Photos, Documents, etc.
BitLocker 保护的承诺
App1 Data
App2 Data
App3 Data
Encrypted, key discarded upon shutdown
Messages
Passwords, credit card info
Health data
Documents and photos
Encrypted, key discarded upon lock

用户标识无法被攻陷、嗅探或盗窃。

Windows Hello 和 NGC

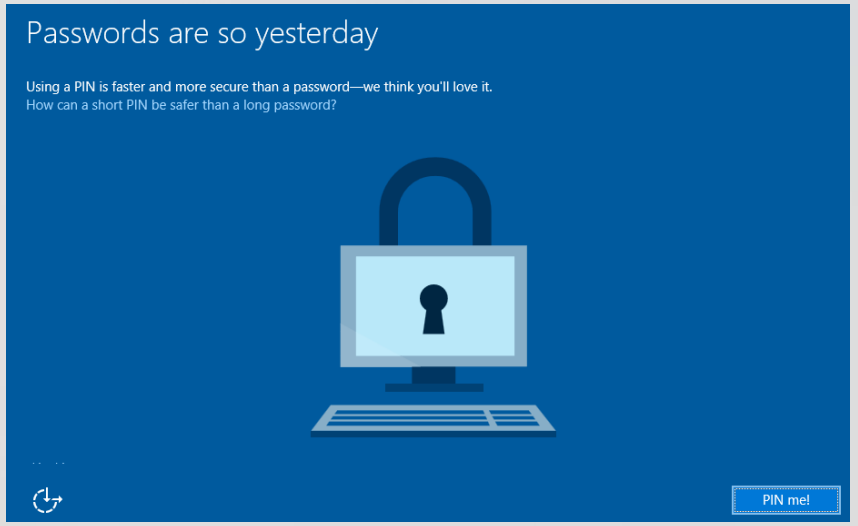
提供生物特征身份验证和硬件支撑的密钥存储
PIN 容易受到恶意管理员的输入过程攻击

改善标识的安全性

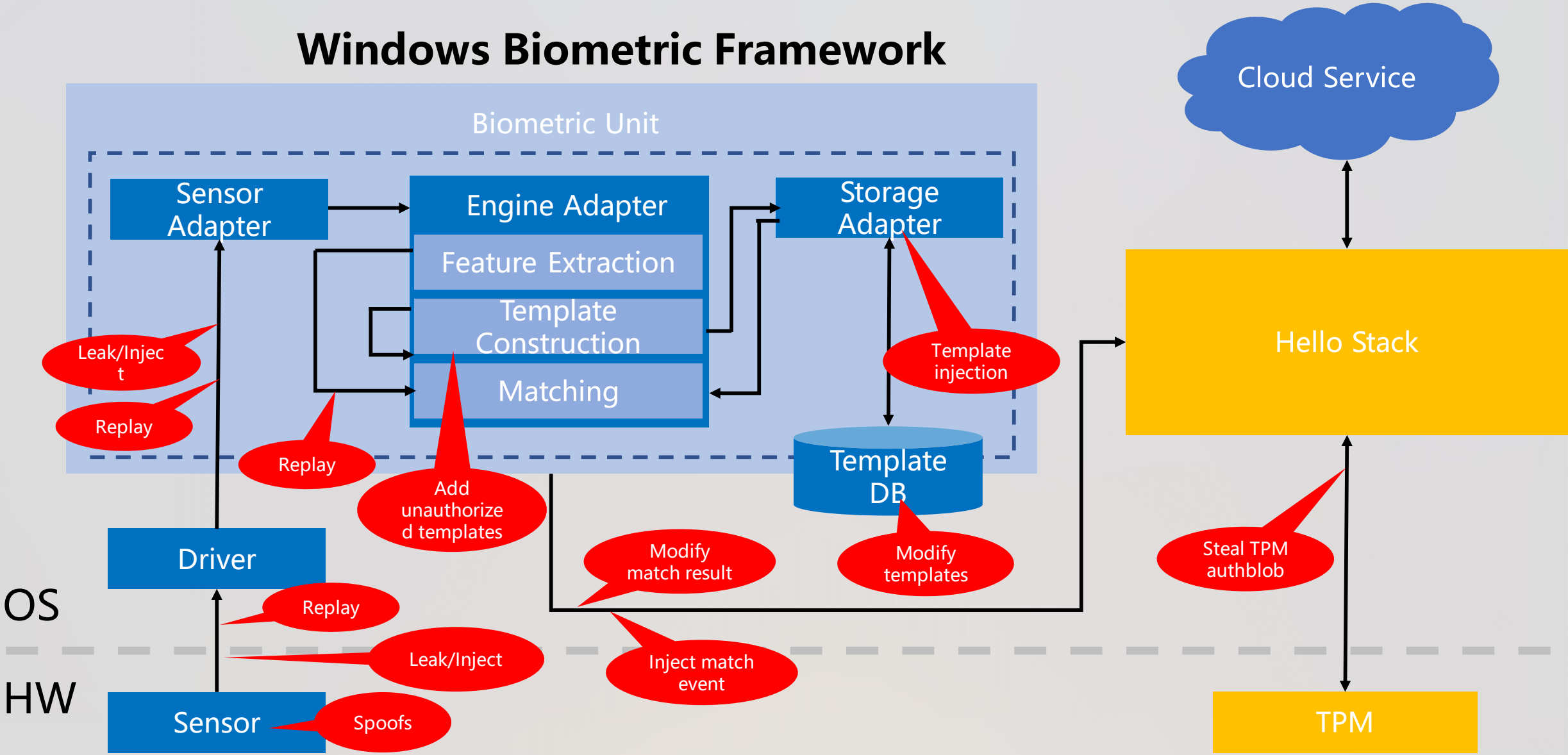
未来版本的 Windows 将包含由虚拟化技术支持的生物特征加固技术

可通过虚拟化技术对数据路径进行生物特征加固

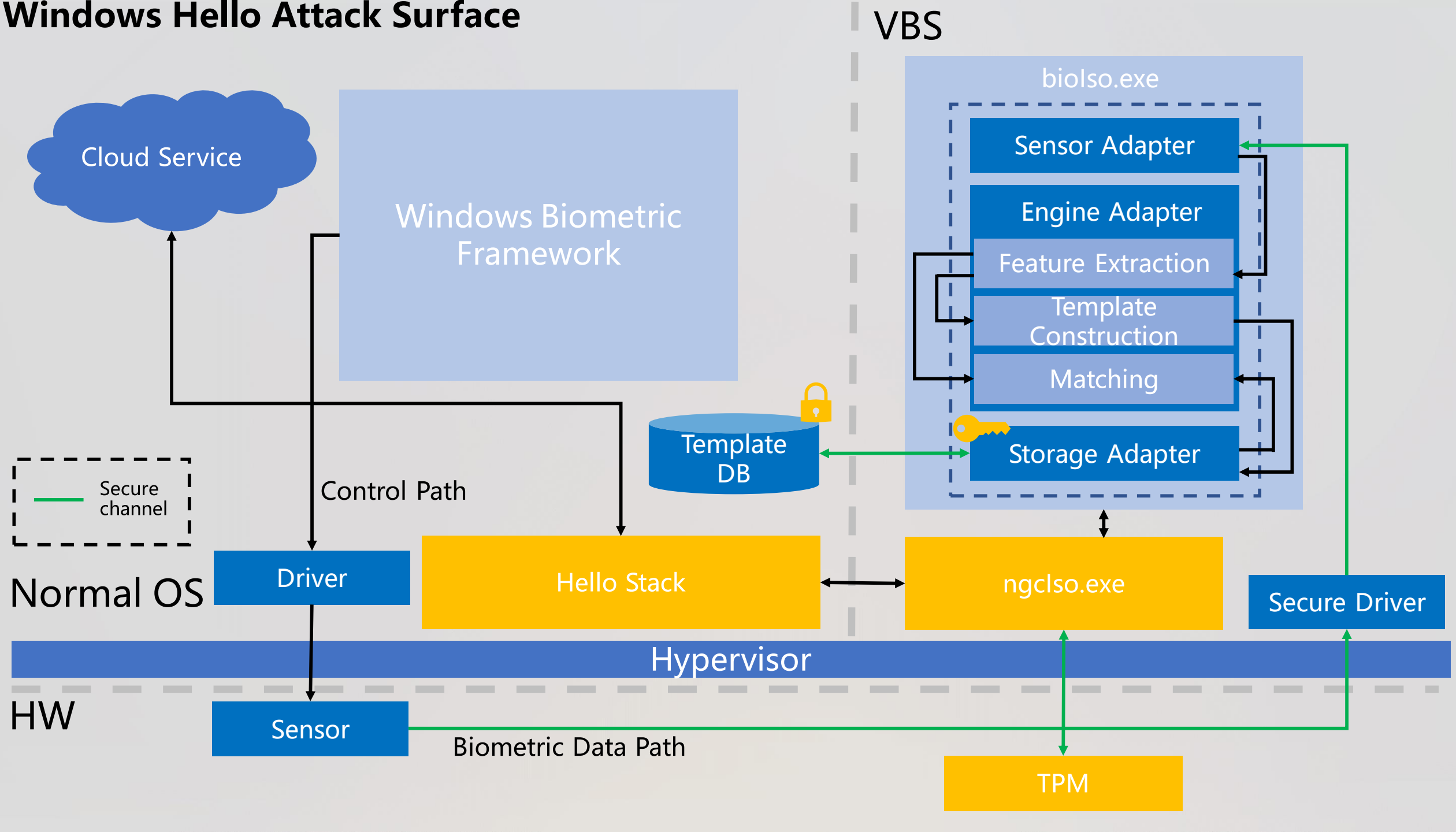
可加固身份证明的发布



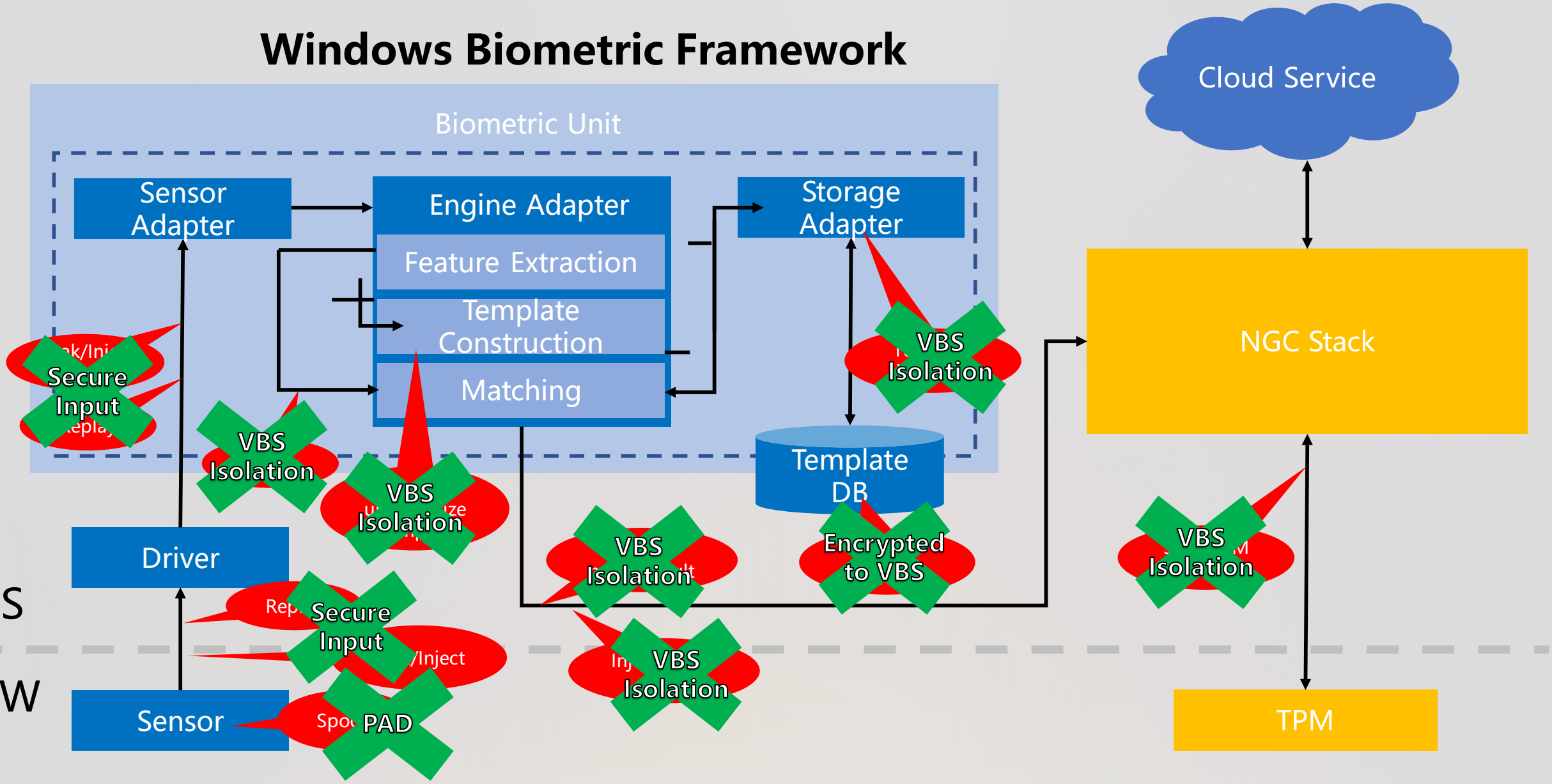
Windows Biometric Framework



Windows Hello Attack Surface



Windows Hello Attack Surface



不只是密码

A web without passwords

Staying secure on the web is more important than ever. We trust web sites to process credit card numbers, save addresses and personal information, and even to handle sensitive records like medical information. All this data is protected by an ancient security model—the password. But passwords are difficult to remember, and are fundamentally insecure—often re-used, and vulnerable to phishing and cracking.

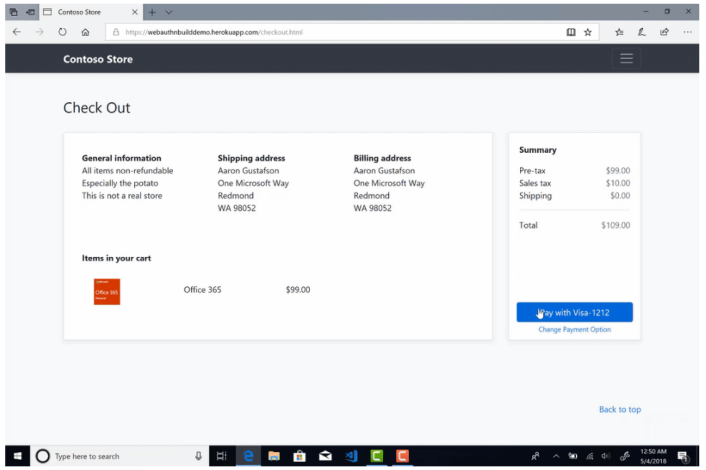
For these reasons, Microsoft has been leading the charge towards a world without passwords, with innovations like Windows Hello biometrics and pioneering work with the FIDO Alliance to create an open standard for passwordless authentication – Web Authentication.

We started this journey in 2016, when we shipped the industry's first preview implementation of the Web Authentication API in Microsoft Edge. Since then, we have been updating our implementation to as we worked with other vendors and the FIDO alliance to develop the standard. In March, the FIDO Alliance announced that the Web Authentication APIs have reached Candidate Recommendation (CR) status in the W3C, a major milestone for the maturity and interoperability of the specification.

Authenticators in Microsoft Edge

Beginning with build 17723, Microsoft Edge supports the CR version of Web Authentication. Our implementation provides the most complete support for Web Authentication to date, with support for a wider variety of authenticators than other browsers.

Windows Hello allows users to authenticate without a password on any Windows 10 device, using biometrics—face and fingerprint recognition—or a PIN number to sign in to web sites. With Windows Hello face recognition, users can log in to sites that support Web Authentication in seconds, with just a glance.



FIDO Alliance and W3C Achieve Major Standards Milestone in Global Effort Towards Simpler, Stronger Authentication on the Web

April 10, 2018

With support from Google Chrome, Microsoft Edge and Mozilla Firefox, FIDO2 Project opens new era of ubiquitous, phishing-resistant, strong authentication to protect web users worldwide

MOUNTAIN VIEW, Calif., and https://www.w3.org/ — April 10, 2018 – The FIDO Alliance and the World Wide Web Consortium (W3C) have achieved a major standards milestone in the global effort to bring simpler yet stronger web authentication to users around the world. The W3C has advanced Web Authentication (WebAuthn), a collaborative effort based on Web API specifications submitted by FIDO to the W3C, to the Candidate Recommendation (CR) stage. The CR is the product of the Web Authentication Working Group, which is comprised of representatives from over 30 member organizations. CR is a precursor to final approval of a web standard, and the W3C has invited online services and web app developers to implement WebAuthn.

WebAuthn defines a standard web API that can be incorporated into browsers and related web platform infrastructure which gives users new methods to securely authenticate on the web, in the browser and across sites and devices. WebAuthn has been developed in coordination with FIDO Alliance and is a core component of the FIDO2 Project along with FIDO's Client to Authenticator Protocol (CTAP) specification. CTAP enables an external authenticator, such as a security key or a mobile phone, to communicate strong authentication credentials locally over USB, Bluetooth or NFC to the user's internet access device (PC or mobile phone). The FIDO2 specifications collectively enable users to authenticate easily to online services with desktop or mobile devices with phishing-resistant security.

违反承诺的举措会被立即发现。

Windows 对篡改一览无余

Windows 的平台篡改检测

在设备引导和持续运行过程中均可检测篡改

按照设计可用于对设备运行状况进行远程评估

从平台层面实现可让大量第三方和应用场景获益

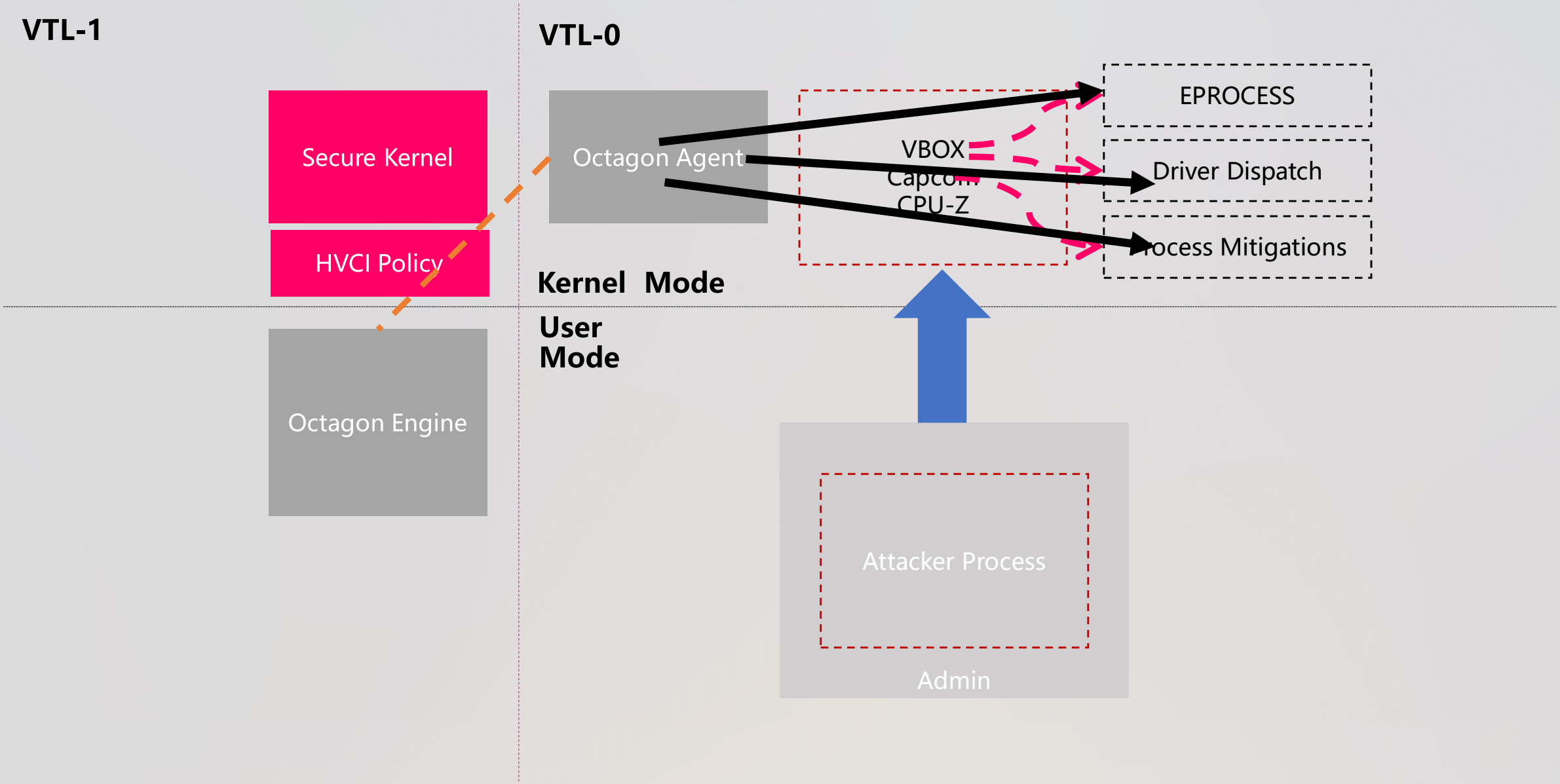
来源于硬件的设备信任

利用 VBS 安全边界提高反篡改的标准

在 Windows 的基础上构建篡改检测架构面临诸多挑战

可扩展的平台组件可通过随后公开发布的 API 进行使用

照片来源：1, 2, 3


VTL-1
VTL-0
Secure Kernel
HVCI Policy
Octagon Engine
Octagon Agent
VBOX
Capcom
CPU-Z
EPROCESS
Driver Dispatch
Process Mitigations
Kernel Mode
User Mode
Attacker Process
Admin

总结

Windows 需要整个社区

平台功能正在快速变化

为了更好地应对新式攻击，Windows 也在快速变革

宏大的目标在于跨越不断成长的威胁模型提供更强大的保障

欢迎研究人员和社区帮我们继续完善

漏洞赏金和征集缓解措施的项目非常重要

我们希望与中国及更多地区的研究人员群体共同努力，更好地了解当前和未来的攻击