WINDOWS 10 安全特性概览

安全研究部 张云海

密级：内部使用

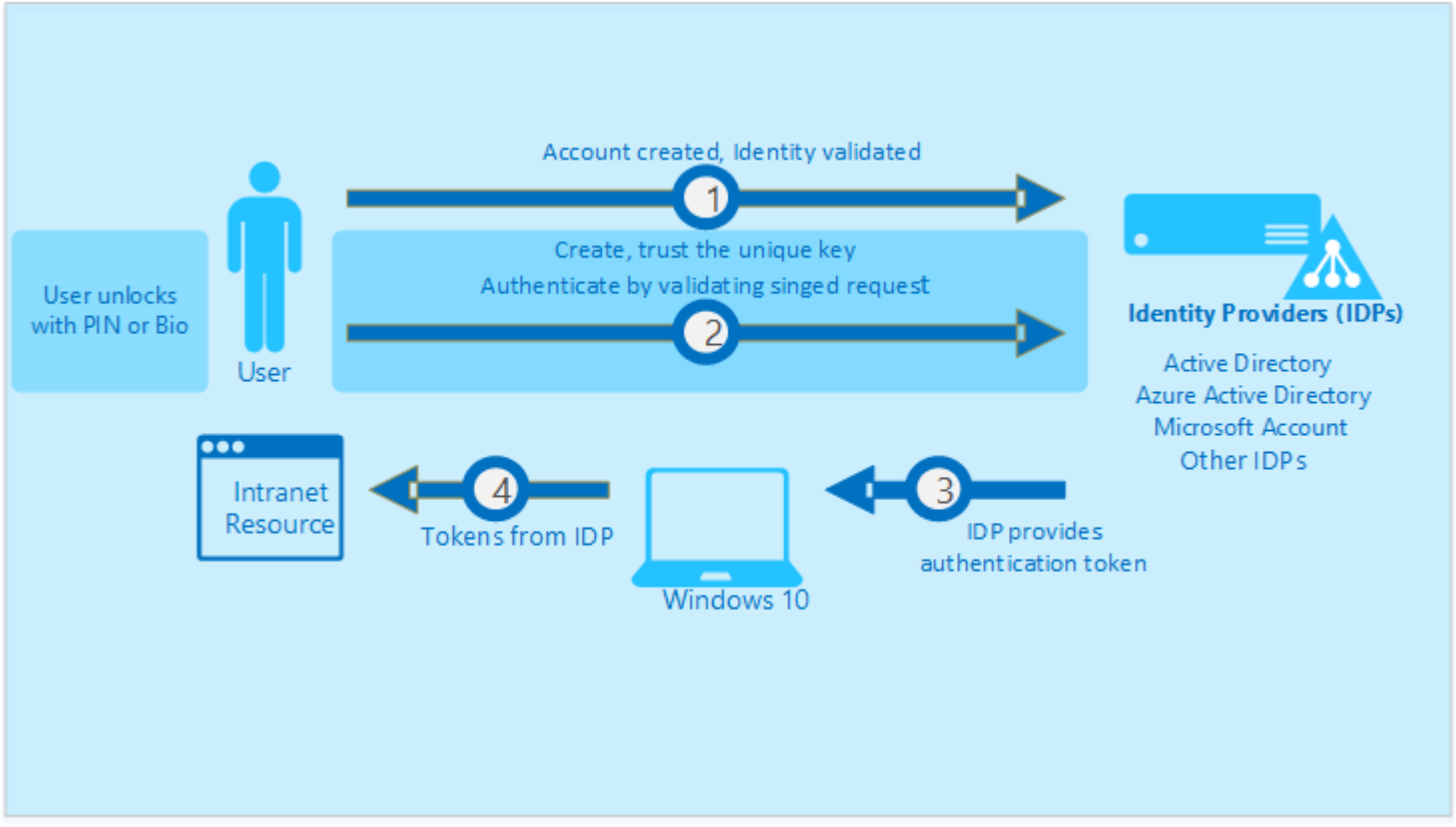
- Windows 10 是微软下一代的操作系统
  - 将于2015年7月29日正式发布
  - 目前有技术预览版供评估

- Windows 10 安全体系

Microsoft Passport

- 强双因素身份验证
  - 注册设备
  - Windows Hello（生物识别）或 PIN
    - 面部识别
    - 虹膜
    - 指纹

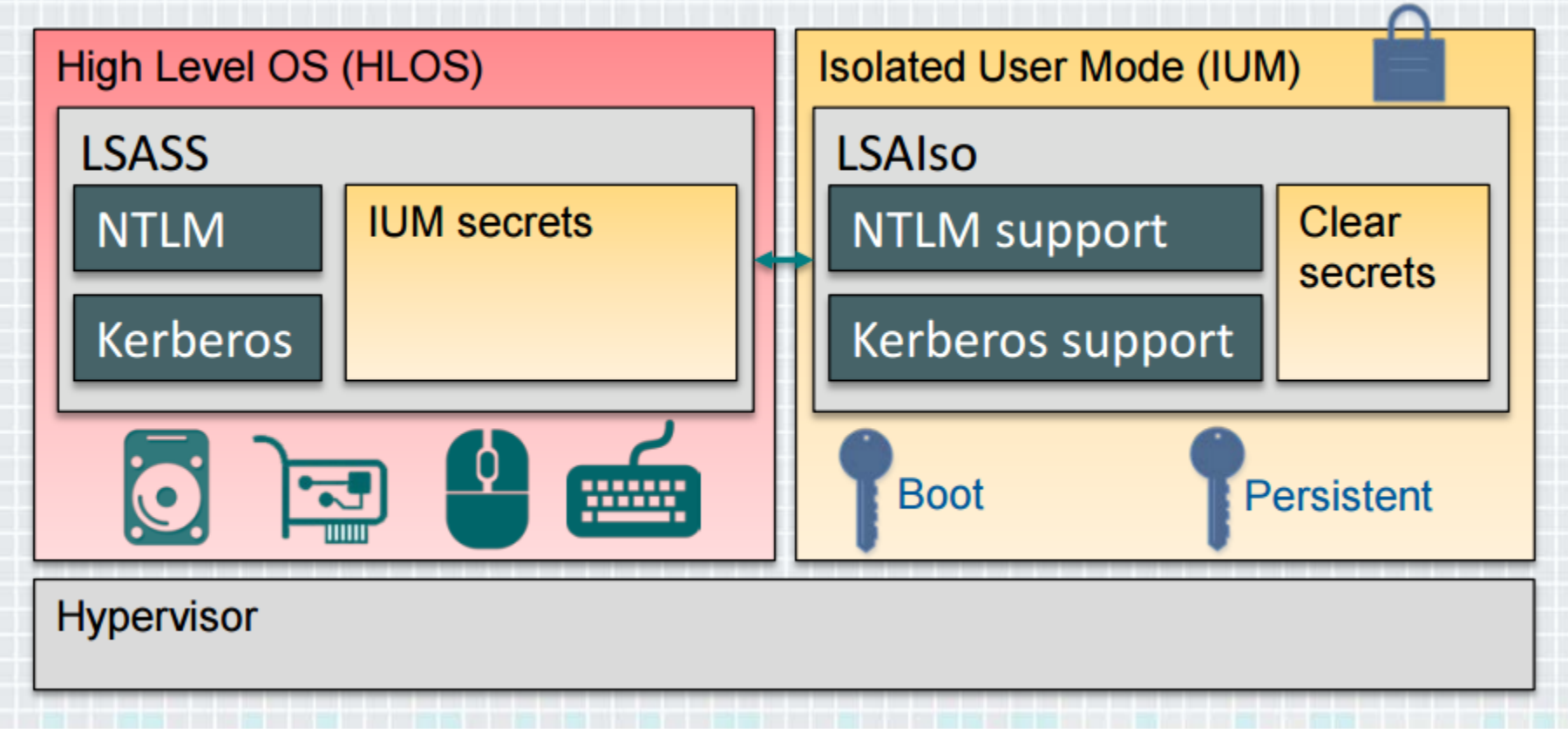
- 兼顾用户便利性与安全性



企业数据保护

- 保护企业数据防止泄漏
  - 持久的企业数据加密
  - 远程擦除设备中的企业数据
  - 控制可访问和使用企业数据的应用
  - 防止数据意外泄露到公共空间
  - 防止数据意外泄露到其他设备

- 隔离用户模式


High Level OS (HLOS)
LSASS
NTLM
Kerberos
IUM secrets
Isolated User Mode (IUM)
LSAIso
NTLM support
Kerberos support
Clear secrets
Boot
Persistent
Hypervisor

- 有效控制允许执行的内容
- 基于签名的保护策略

- Kernel Mode Code Integrity
  - 所有内核模式驱动必须提交到WHDC进行签名
  - 通过EV证书来校验驱动发布者的身份

- User Mode Code Integrity
  - Microsoft Store 签名的应用
  - 特定供应商签名的应用
  - 企业签名的应用
  - Microsoft Device Guard Signing Portal

- 签名类型
  - 嵌入式签名
    - 签名信息保存在二进制文件内
  - 目录签名
    - 对一个或多个二进制文件签名
    - 可独立的管理与部署
    - 保留任何已有的签名

阻止不受信任的字体

- 新的缓解策略：ProcessFontDisablePolicy
  - 启用后禁止加载非系统字体

```
typedef struct _PROCESS_MITIGATION_FONT_DISABLE_POLICY {
    union {
        DWORD Flags;
        struct {
            DWORD DisableNonSystemFonts      : 1;
            DWORD AuditNonSystemFontLoading : 1;
            DWORD ReservedFlags              : 30;
        } DUMMYSTRUCTNAME;
    } DUMMYUNIONNAME;
} PROCESS_MITIGATION_FONT_DISABLE_POLICY, *PPROCESS_MITIGATION_FONT_DISABLE_POLICY;
```

用户模式字体

- 在用户模式完成部分字体处理工作
  - 字体处理复杂而容易产生漏洞
  - 运行在内核模式将使攻击者直接获得系统权限
  - 运行在用户模式可以降低此类漏洞的危害

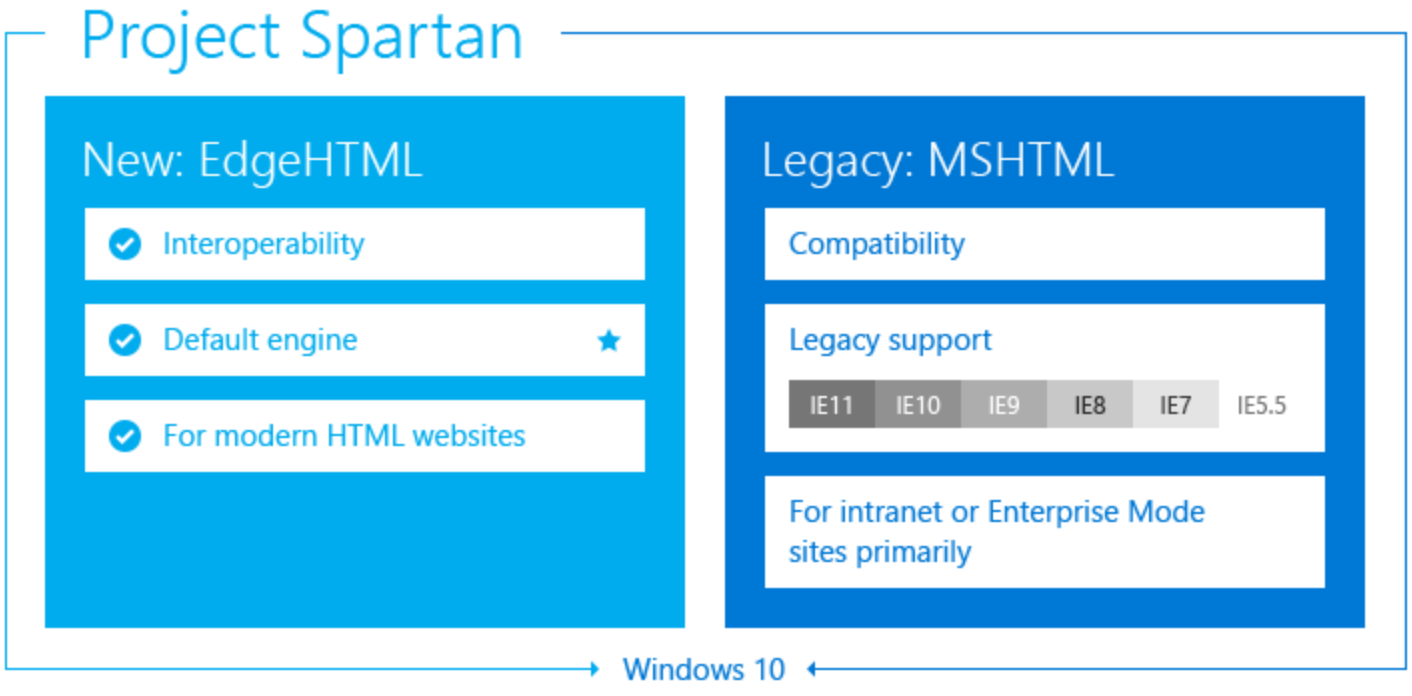
执行流保护

- 在 Windows 8.1 Preview 中首次引入
  - 因兼容性问题在 Windows 8.1 RTM 中禁用
- 在 Windows 10 Technical Preview 中再次启用
- 在 Windows 8.1 Update3 中正式启用

- 技术原理
  - 对间接函数调用的目标进行校验

```
mov     eax,dword ptr [edx]
mov     edi,esp
push    ecx
push    edx
mov     esi,dword ptr [eax+1Ch]
mov     ecx,esi
call    dword ptr [vbscript!__guard_check_icall_fptr (5f67e320)]
call    esi
```

- 替代 IE 成为缺省浏览器



浏览器 Edge

- 渲染引擎
  - MSHTML -> EdgeHTML
- Javascript 引擎
  - JScript9 -> Chakra

- 安全特性
  - 64位系统中缺省为64位
  - 运行在 AppContainer 中
  - 不支持 vbscript
  - 有限支持ActiveX
    - Flash
    - SVG
  - 全面应用执行流保护

Q&A

谢谢！