
Def 2013
第二届
全国网络与信息安全防护峰会
对话·交流·合作

Windows8.1 安全新功能

薛锋
总监，互联网安全
微软公司可信赖计算部

Microsoft

内容

- Windows 8 安全性
- 不断变化的威胁形势
- Windows 8.1 的安全改进

Windows 8 安全功能

阻止恶意软件

确保安全启动
保护代码和核心
保护桌面

保护敏感数据

使用加密技术保护数据

新型访问控制

确保安全登录
安全访问资源

可信硬件

通用可扩展固件接口 (UEFI)

可信平台模块 (TPM)

重新评估威胁

Windows

Windows 8 和 8.1 安全功能

新型访问控制

确保安全登录
安全访问资源

顶级生物识别体验
BYOD 多重身份验证
可信身份和设备
单一登录到服务提供商

阻止恶意软件

确保安全启动
保护代码和核心
保护桌面

可查证的 PC 运行状况
改进了 Windows Defender
改进了 Internet Explorer
改进了系统内核强化

保护敏感数据

使用加密技术保护设备

普及设备加密技术
选择性擦除公司数据

可信硬件

UEFI　　新型生物识别读取器　　TPM

新型硬件

- 可信平台模块 (TPM)

Windows 8.1 中TPM(可信平台模块)

机会

- 显著提高客户和 BYOD 的安全性
- 以创新方式加以利用以应对新型威胁

在 Windows 中的历史

- TPM 当前为可选组件
- 普遍存在于商业设备以及大多数平板电脑中

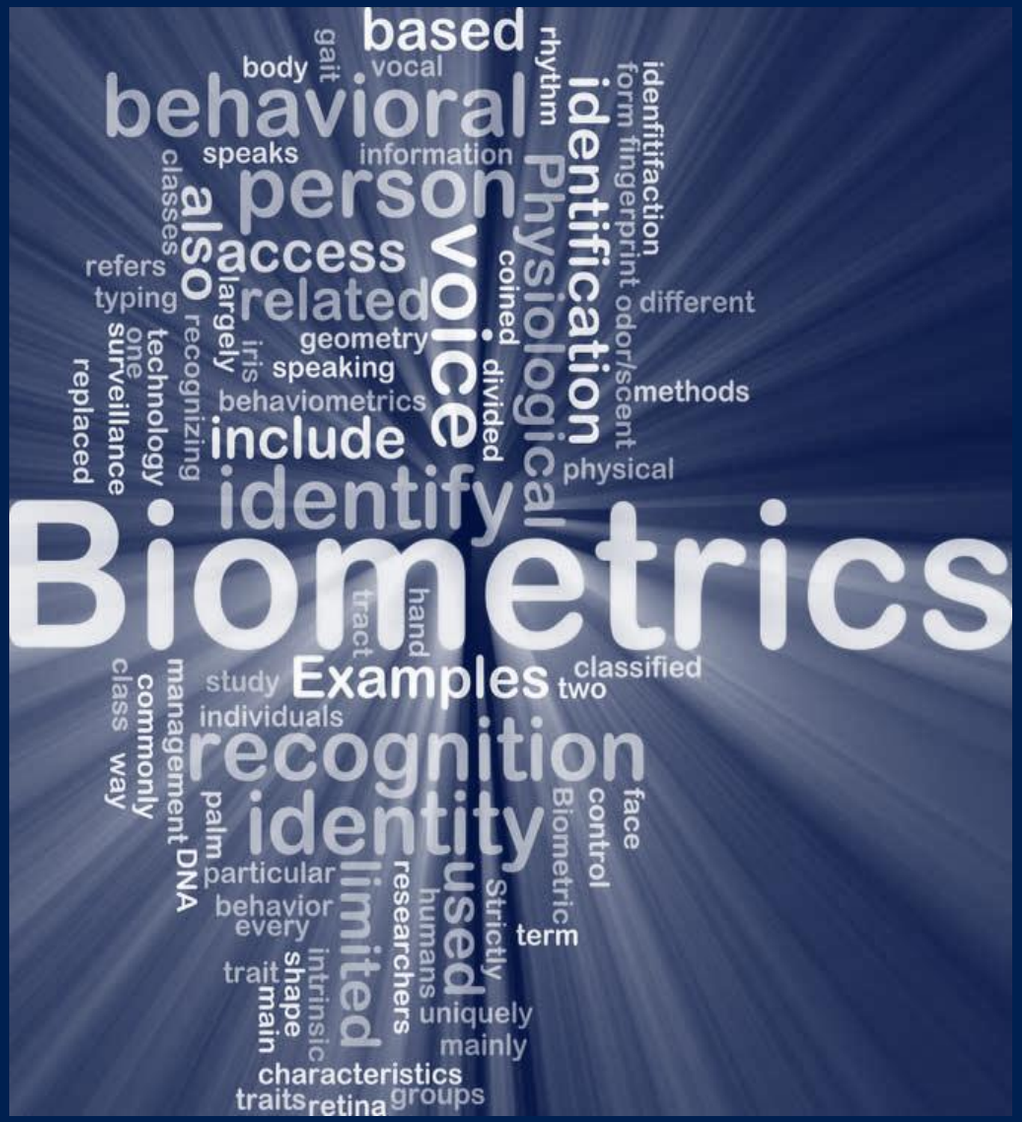
我们在 Windows 8.1 中的目标

- 与 OEM 一起推动“连接待机”体系结构的应用

新型访问控制

- 顶级生物识别体验
- BYOD 多重身份验证
- 可信身份和设备
- 单一登录到服务提供商

Windows 8.1 中的生物识别技术



机会

- 逐步推进替代密码
- 减少不便，改善体验

在 Windows 中的历史

- Windows XP 中首次加入生物识别功能
- Windows 7 中加入 Windows Biometric Framework
- 第三方提供注册服务和驱动程序

应用

- 大多数 PC 未使用，OEM 差异化
- 极少用户体验过

我们在 8.1 中的目标

- 让生物识别技术带来最佳的身份验证体验
- 创造条件让用户喜欢并使用这项技术
- 推动消费者和企业采用这项技术

Windows 8.1 的指纹设备选项

技术选择

- 光学读取器
- 热传导读取器
- 超声波读取器
- 电容读取器 (CMOS)

新型读取器的特点

- 触控
- 活体检测

指纹生物识别端到端支持

- 通用注册体验
  - 电脑设置 -> 用户 -> 创建指纹登录
  - 根据设备功能优化使用体验
- 所有 Windows 体验采用统一的生物识别登录方式
  - Windows 登录
  - 远程访问登录
  - 所有其余身份验证提示（如：UAC）
- “Touch to Buy”功能已添加到：
  - Windows 应用商店
  - Xbox Music
  - Xbox Video

通过生物识别技术保护资源

- 挑战
  - 主要为单用户设计的设备经常需要共享
  - 用户登录设备后就将拥有系统的完全访问权限
  - 通过密码访问应用程序和数据带来太多不便
- 解决方案
  - 能够对应用程序和身份使用“可信用户手势”进行身份验证
  - 适用于注册、登录、购买等行为的指纹生物识别体验
- 情形 – 用户验证用于保护：
  - 应用程序启动过程或应用程序中的特定任务（Windows 应用商店中的应用程序）
  - 能够保护高度机密信息的应用程序
  - 能够在释放凭据之前验证用户状态的应用程序

新型访问控制

- 顶级生物识别体验
- BYOD 多重身份验证
- 可信身份和设备
- 单一登录到服务提供商

虚拟智能卡现可用于 BYOD

- 什么是虚拟智能卡
  - 将 TPM 虚拟化为智能卡，以用于身份验证、加密、签名等作用
  - 解决现有 MFA 解决方案的关键挑战
  - 易于部署、经济高效、在设备上随时待命
- 虚拟智能卡的主要挑战
  - BYOD（未加入域）的注册过程太复杂
- Windows 8.1 的解决方案
  - 通过 API 支持来配置到 BYOD（未加入域；所有体系结构）
  - 与 ISV 合作

新型访问控制

顶级生物识别体验

BYOD 多重身份验证

➡可信身份和设备

单一登录到服务提供商

对于可信赖 PKI 的需求

- 证书可信赖性挑战
  - 难以检测的安全破坏，灾难性的影响
  - 增加了对 PKI 的依赖，导致其成为单一故障点

DigiNotar **破坏**
- 被欺骗发出可信证书

“震网”恶意软件
- 使用盗窃的证书为恶意软件签名

“火焰”恶意软件
- 使用劫持的证书为恶意软件签名

Mimikatz
- 从受害设备导出证书

假设和机会

- 这些破坏依靠的是什么？假设：
  - 看起来未经篡改的证书是可信的
  - 从微软根 CA 计划中的 CA 发出的证书是可信赖的
  - 由哪个 Web 服务器发出可信证书是没有关系的
  - 颁发给客户端的证书是安全的、无法窃取的
- 机会
  - 提高私有和公共 PKI 系统的可信赖性
  - 帮助管理和驱动生态系统内的加密安全性
  - 防止窃取用户和设备身份

保护私有证书和密钥

- 挑战
  - 如果密钥未受硬件保护，则有可能导出密钥
  - 如果能够访问私钥，则表示您拥有该机器或身份
  - 可通过任何设备使用受侵害的私钥（可重现）
  - 今天我们假设这些私钥仍然安全。实际上有时并非如此！
- 解决方案 – TPM KSP + 密钥证明
  - 在私钥与硬件 (TPM) 之间建立强力绑定
  - 创造条件使私钥在导出后无法工作
  - 通过某种方式证明密钥是否通过 TPM 加以保护

保护公用证书和密钥

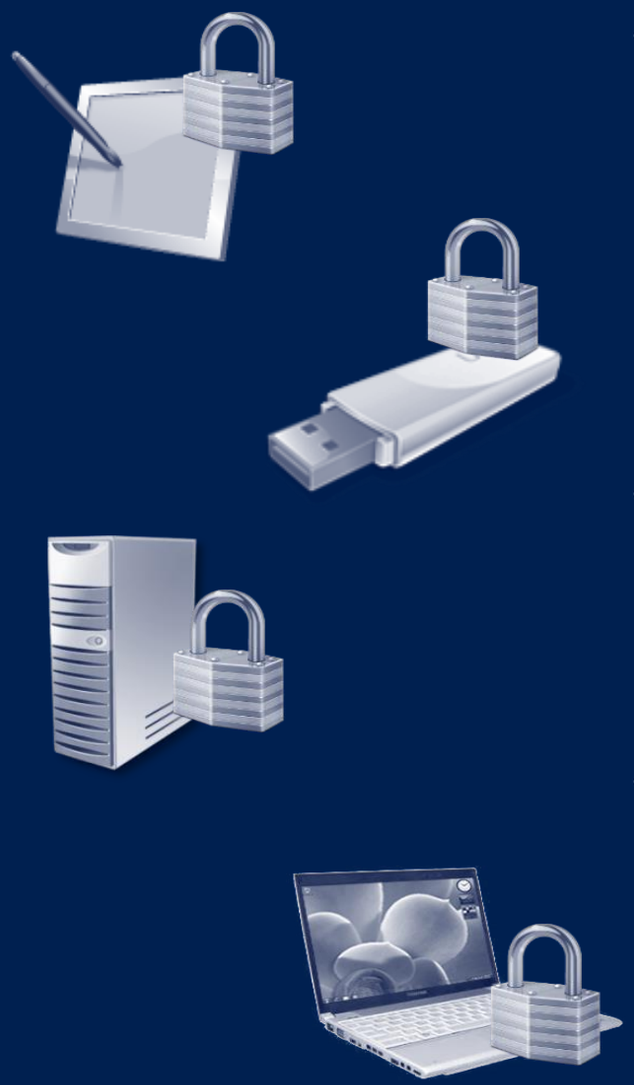
- 我们可以通过哪些措施保护它们？
  - 创建基于云的服务爬网以用于证书遥测
  - 用户选择性加入选项以匿名方式发送证书数据 (SmartScreen)
  - 创建分析服务以检测欺诈性证书
- 对生态系统有何影响？
  - 能够检测意外来源发出的证书
  - 能够调查异常状况并快速启动修复/吊销操作
  - 通过通知 CA 和/或组织来帮助清理生态系统
  - 防止导出和重复使用窃取的身份

保护敏感数据

- 普及设备加密技术

Windows

全盘加密成为主流



- 不断变化的形势
  - 通常仅应用于企业版 Windows
  - 对企业至关重要；增加消费者需求
  - BYOD 使消费者设备进入企业环境
  - 用于保护系统本身，不仅限于数据
- 普及化面临的挑战
  - TPM 很快将成为标准装备，但尚未到达这一步
  - 在低端设备上的性能不够
- 微软的方向
  - 现在 Windows 所有版本均提供设备加密
  - 需要“连接待机”认证设备

设备加密与 BitLocker

- 设备加密
  - 操作系统卷加密是自动化的，并且是现成配置
  - 只要管理员使用微软帐户登录就启用保护
  - 未管理的恢复密钥密码存储在 SkyDrive 中
  - 可对其快速配置以使用 BitLocker 功能（仅限专业和企业版）

- BitLocker 和 BitLocker To Go – Windows专业和企业版
  - 允许加密固定磁盘 (BitLocker) 和可移动磁盘 (BitLocker to Go)
  - 通过映像、管理解决方案或最终用户来启用保护
  - 恢复密钥可存储在 AD 或管理解决方案中

阻止恶意软件

- 可查证的 PC 运行状况
- 改进了 Windows Defender

阻止恶意软件

可查证的 PC 运行状况

➡改进了 Windows Defender 和 Internet Explorer

Windows Defender和IE浏览器的增强功能

- Windows Defender
  - 恶意软件的设计意图几乎都是与世界对话，这是它们的弱点
  - 添加高性能行为监控
  - 识别基本的恶意行为模式（文件、注册表、进程、线程、网络）
  - 将活动日志发送到云进行分析，签名可能随后发出
- IE浏览器
  - 恶意网站尝试以二进制扩展文件（如：ActiveX）来攻击漏洞
  - 二进制扩展文件绕过 AM 直接执行
  - 使用 API 可使反病毒软件解决方案能够在文件执行之前进行扫描

Win8.1安全性应对新威胁

新型访问控制

确保安全登录
安全访问资源

顶级生物识别体验
BYOD 多重身份验证
可信身份和设备

阻止恶意软件

确保安全启动
保护代码和核心
保护桌面

可查证的 PC 运行状况
改进了 Windows Defender
改进了系统内核强化

保护敏感数据

使用加密技术保护设备

普及设备加密技术
选择性擦除公司数据

可信赖硬件

可信平台模块 (TPM) 将在 2014 年得到普及

谢谢！

feng.xue@microsoft.com