BRK3336

Black Belt Security with Windows 10

Sami Laiho
Senior Technical Fellow
Adminize.com / Sovelto

课程安排

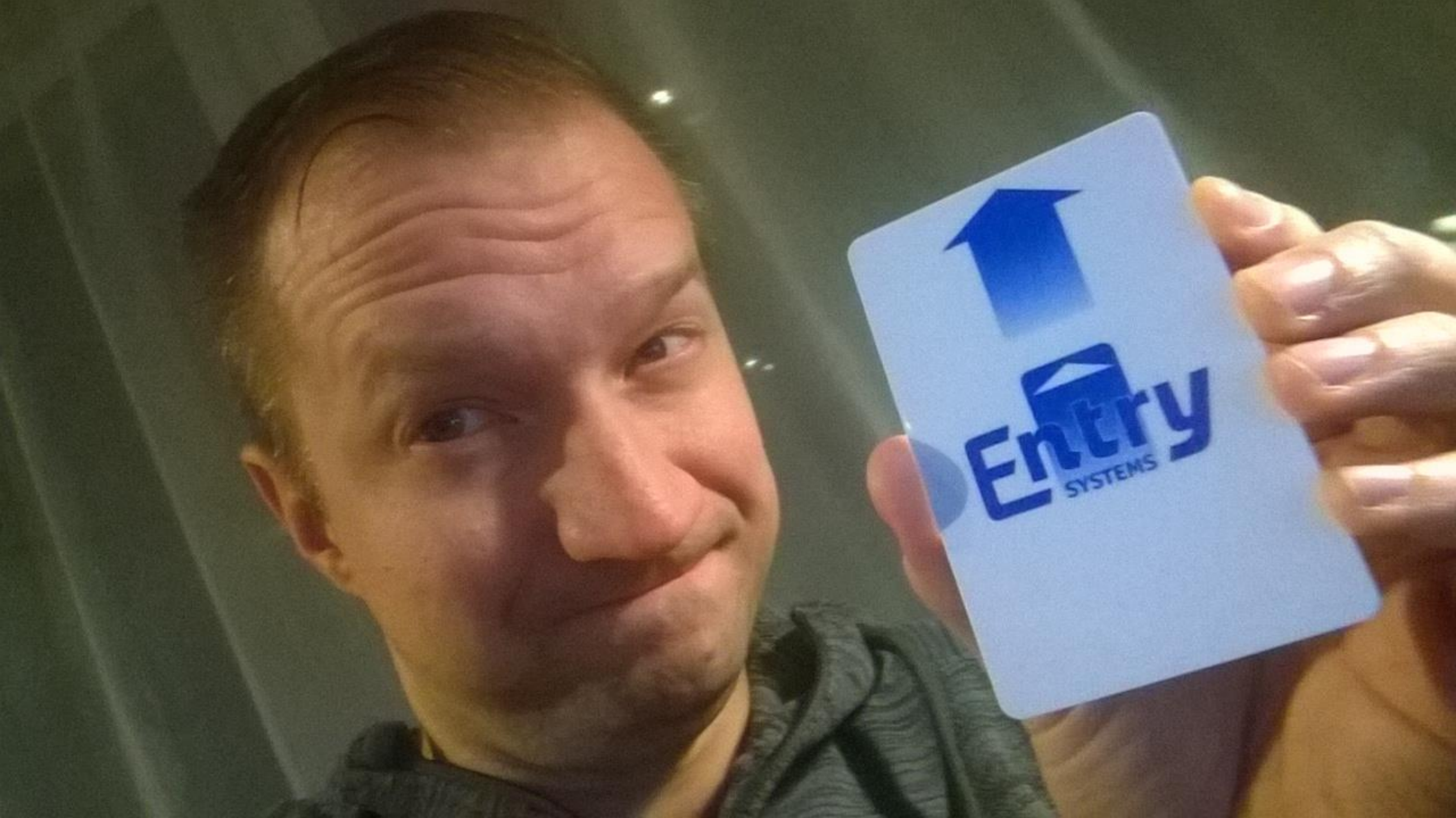
- 安全中的人为因素
- 主动安全防护相较于被动安全防护的优势
- 危害系统的不同方式，如何防止发生危险

人为因素

挪威现状

物理安全与社交工程

- 奥斯陆酒店即将举办 2014 年度欧洲技术大会
  - 我：“您的同事让我来拿一把新钥匙，因为我的钥匙不好用”
  - 她：“我给您做一把新钥匙”
  - 我：“这把木钥匙似乎依然没什么用。您的同事用的是一把塑料钥匙，可能因为材料过厚，所以不能用。您觉得您能给我做一把类似的钥匙吗？”
  - 她：“我需要去后屋检查一下 – 稍等片刻”
  - 她：“这是您的钥匙，但不要告诉任何人您拿到了这把钥匙，因为这是一把万能钥匙，可以打开酒店的任何一扇门”


Entry
SYSTEMS

芬兰现状

芬兰 150M€ Car 购物中心

- 公司 CEO 收到一位英国人的报价，声明向其电汇 3000 万欧元资助项目
- 这笔钱的主人是 Regina Chiluba，赞比亚前总统 Fredrick Chiluba 的遗孀
- CEO 汇出 336000 欧元资助完成现金交易
- 为安全起见，交易冻结
- 这笔钱返还，而后…
- 再次汇出…

芬兰选举

- 一个政党在全国的每一个角落都设置了投票箱...

世界在不断变化

- Symantec、F-Secure 以及其他几乎每一家 AM 公司均发表声明，表示被动解决方案不足以为未来 PC 提供保护
- 我们需要调整重心，变被动为主动

被动解决方案

- 反恶意软件、网络检测服务 (NIS)、软件黑名单...
- 总是努力追赶 – “始终”慢一步！
- 必需先发制人 – “以防万一”

主动解决方案

- 正确权限级别、白名单、防火墙、IPSec…
- 保障贵公司安全高效
- 不要依赖其他公司发现的更新/指纹
- 重要性高于被动解决方案

业界言论

- "仅有 25% 的人具有管理权限"
- "只有我们的笔记本电脑用户具有管理权限"
- "我们不会对内部网络使用防火墙"
- "管理层具有管理权限"
- "我们尝试过白名单，但最终放弃了"
- "MAC 和 Linux 很好 – '因为它们不需要防病毒' "

Windows 主动安全防护

- 加密 - BitLocker
- 有限用户权限
- 不同级别的管理账户
- UAC
- 基于主机的防火墙
- IPSec
- AppLocker 白名单或 Device Guard

我的笔记本电脑现状

- 未启用反恶意软件程序
- 打开所有防火墙端口

我每年有 200 天穿梭于各大机场... 会感到恐惧吗？

完全不会！

- 我不采用被动保护，取而代之的是：
  - AppLocker 白名单 – 所有软件均需要我预先批准
  - 我使用 IPSec – 任何人若不具备证书都不能与我对话
  - 无管理权限 – 我无法禁用自身的保护措施
  - BitLocker – 我可以防止通过物理方式窃取数据，也可以阻止别人入侵我的笔记本电脑操作系统
  - 当前操作系统处于最新状态
  - 正确的硬件 – 无 DMA 端口/接口！

DMA 攻击

- 应用程序可用于
  - 破解密码
  - 窃取 BitLocker 密钥

几项说明

- 为什么使用加密？
- 为什么使用 UAC？
- 为什么不设置管理权限？
- 为什么要为域管理员创建多个级别的用户账户？
- 为什么使用 UAC 还不足够？
- 为什么使用白名单软件？

为什么使用加密

@samilaiho

防范方法

- 强制使用 BitLocker

为什么不为最终用户设置管理权限？

@samilaiho

防范方法

- 如果确实需要提供组策略设置，请更改刷新设置
- 不要为用户提供管理权限！

管理级别过少

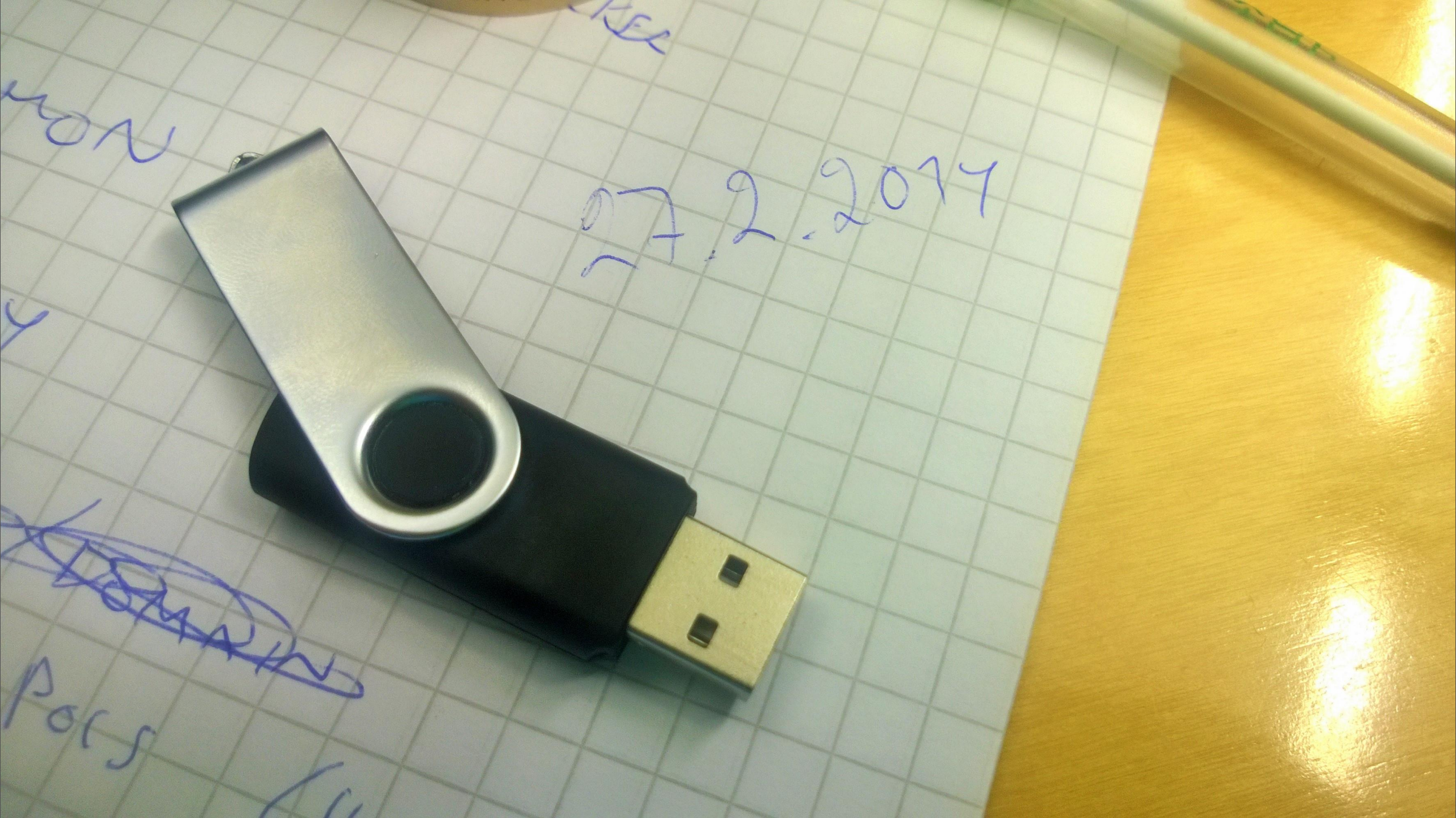
@samilaiho

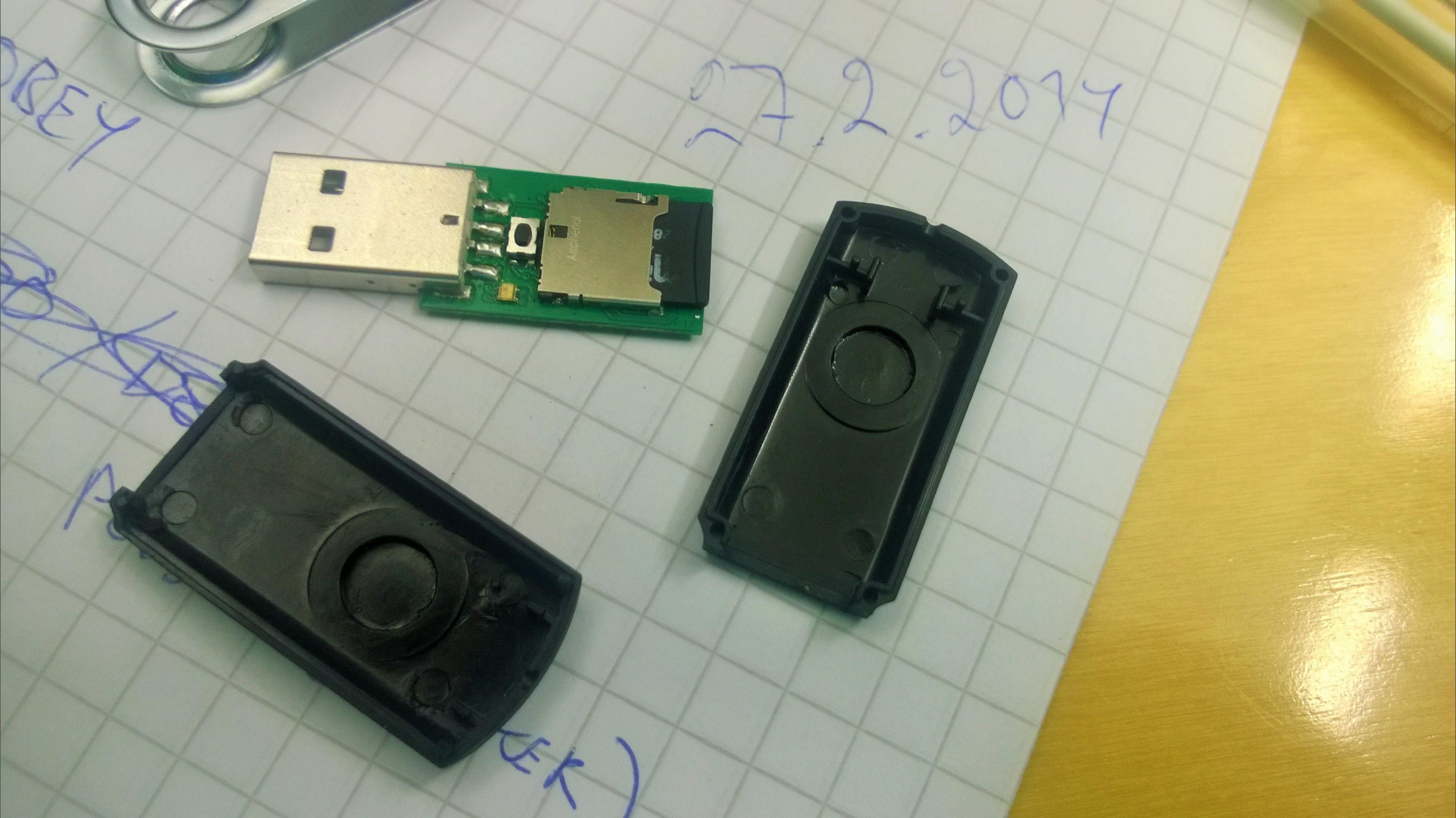
防范方法

- 至少三个域管理员用户账户

为什么使用 UAC 还不足够？

@samilaiho


27.2.2014


27.2.2014

BadUSB

@samilaiho

防范方法

- 始终使用有限用户账户 – 而不仅仅是 UAC！
- 仅使用防篡改设备，并确保其使用签名固件且无法反射
- 对用户进行相关培训
- 更多信息：
  - http://www.zdnet.com/badusb-big-bad-usb-security-problems-ahead-7000032211/
  - https://www.youtube.com/watch?v=nuruzFqMgIw
  - https://github.com/adamcaudill/Psychson
  - https://www.youtube.com/watch?v=xcsxeJz3blI

BadMouse !

@samilaiho

为什么使用白名单软件？

@samilaiho

防范方法

- 使用 AppLocker！ 了解 Device Guard 在 Windows 10 中的应用方法。
- 记得使用 AccessChk 对 AppLocker 安装进行审核！

不用翻译

Microsoft