从微软操作系统的安全探索看反病毒与可信计算的辩证关系

演讲人：李柏松

团队：安天实验室

演讲日期：2014年9月24日

修订日期：2014年9月29日

ISC 2014 中国互联网安全大会

360互联网安全中心

China Internet Security Conference 2014

2014中国互联网安全大会

前言 Preface

反病毒

可信计算

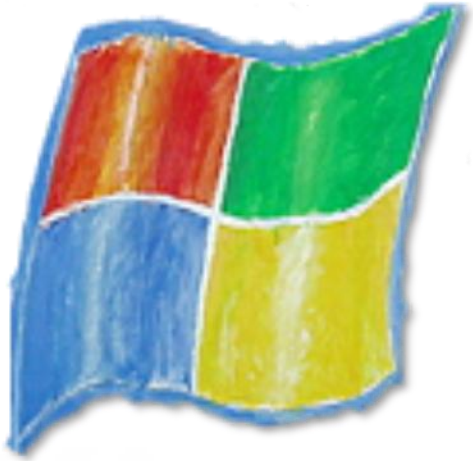
提纲 Outline

微软系统的安全现状与安全特性

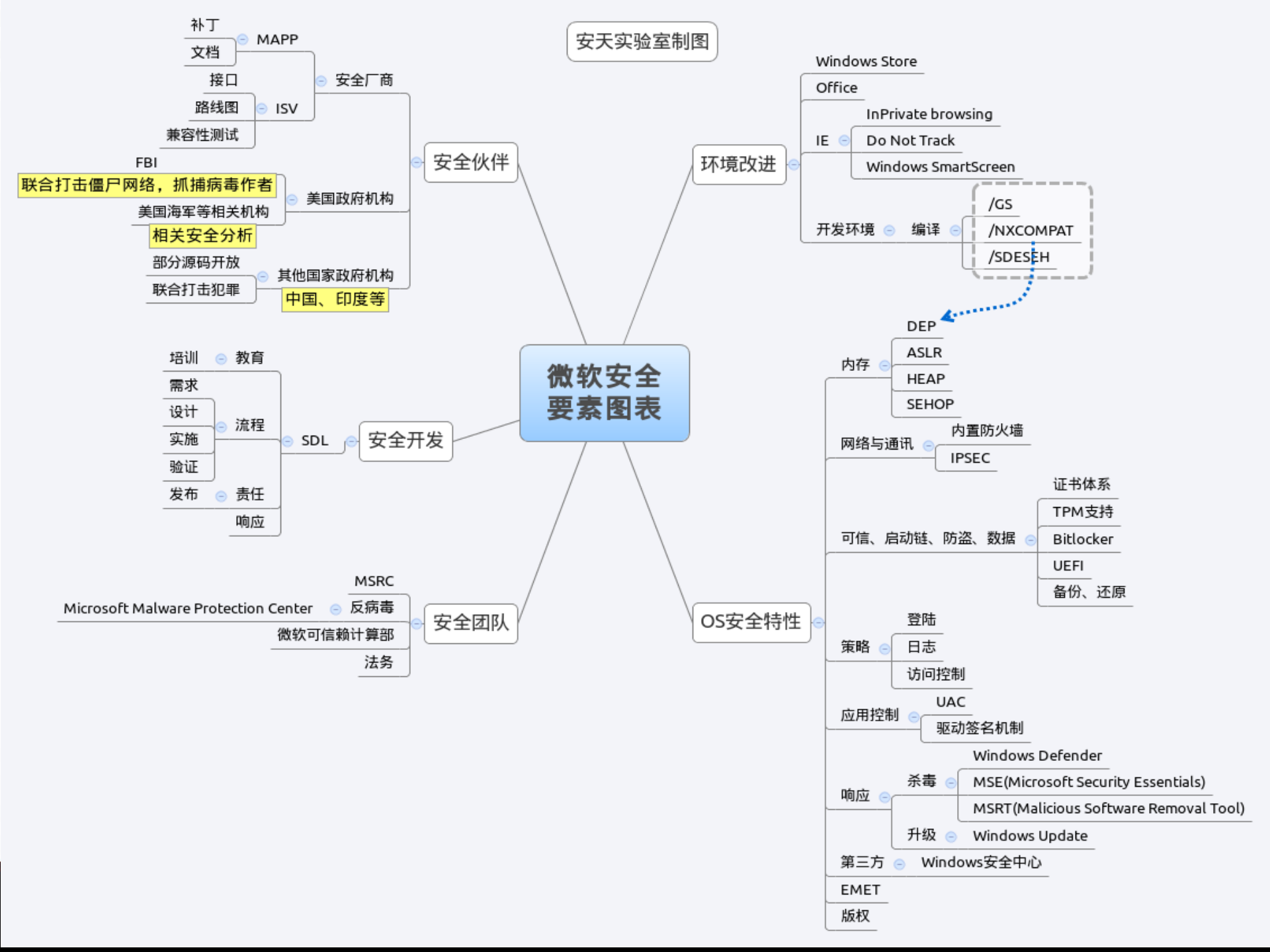
Win7 / 8系统可信计算技术应用

可信计算关键技术实战效果

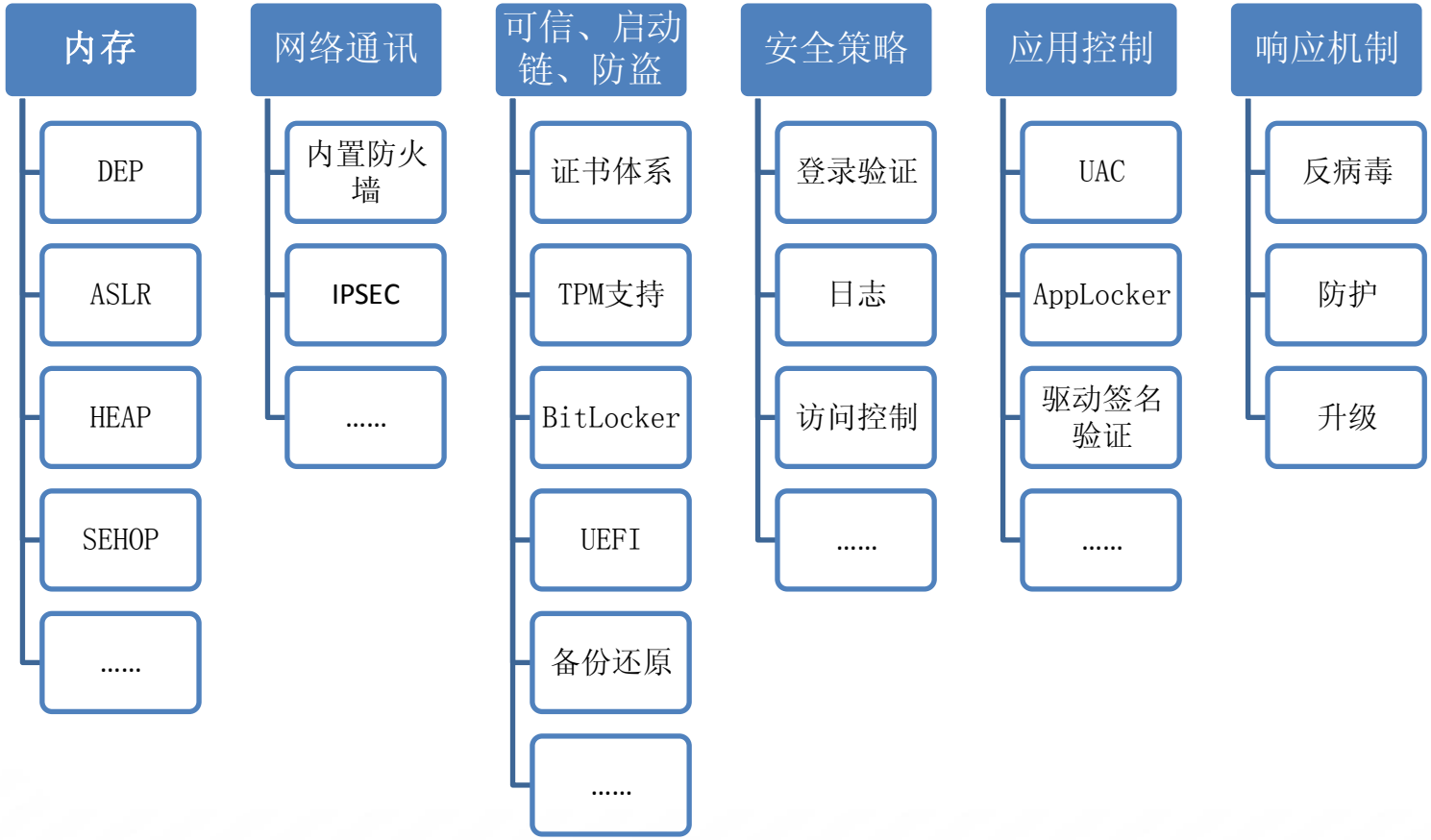
反病毒与可信计算辩证关系



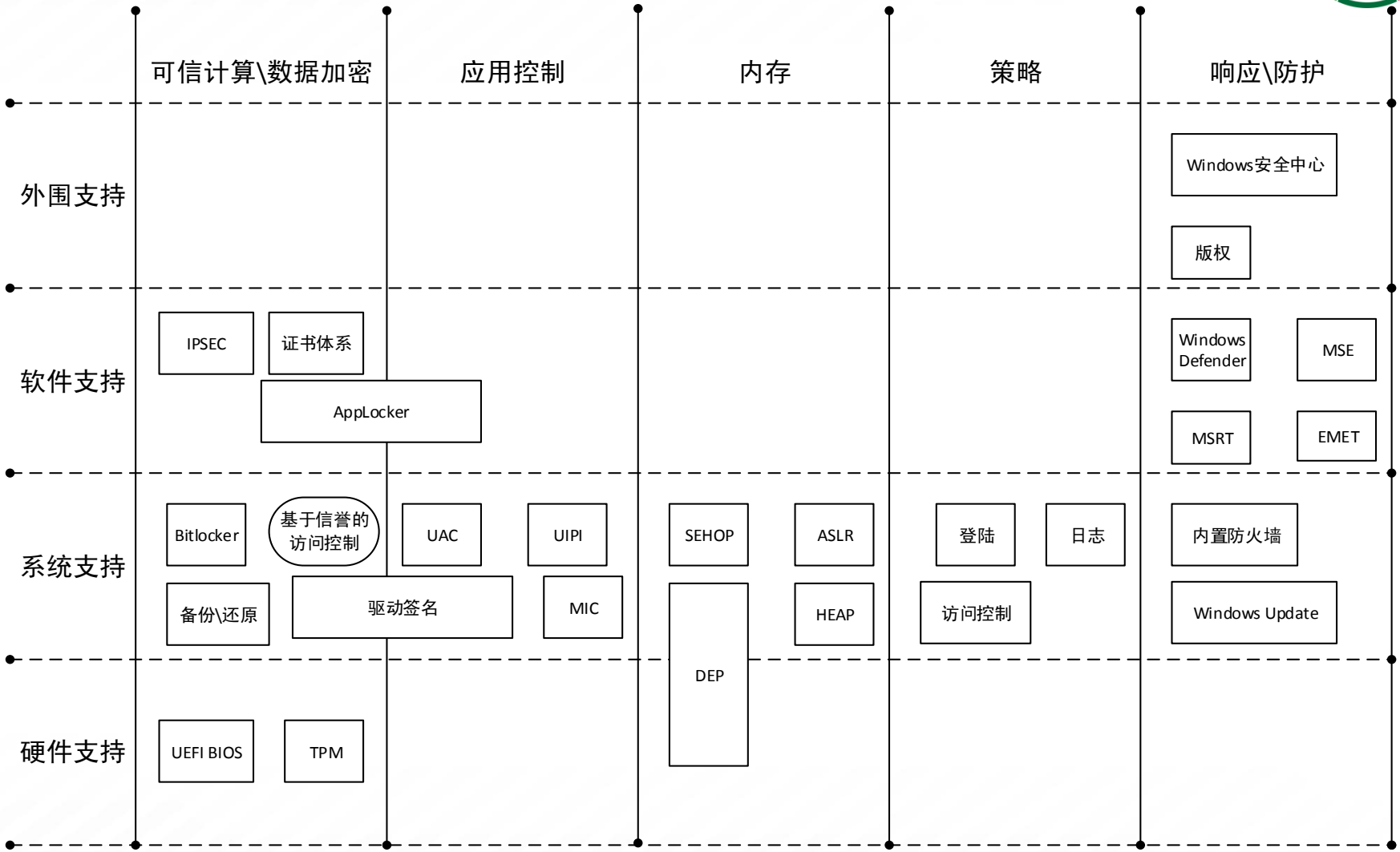
- 微软系统的安全现状
  - 整体安全思路
  - 主要安全特性
  - 安全保护机制


安天实验室制图
微软安全要素图表
安全伙伴
安全厂商
MAPP
补丁
文档
ISV
接口
路线图
兼容性测试
美国政府机构
FBI
联合打击僵尸网络，抓捕病毒作者
美国海军等相关机构
相关安全分析
其他国家政府机构
部分源码开放
联合打击犯罪
中国、印度等
安全开发
SDL
流程
教育
培训
需求
设计
实施
验证
责任
发布
响应
安全团队
MSRC
反病毒
Microsoft Malware Protection Center
微软可信赖计算部
法务
环境改进
Windows Store
Office
IE
InPrivate browsing
Do Not Track
Windows SmartScreen
开发环境
编译
/GS
/NXCOMPAT
/SDESEH
OS安全特性
内存
DEP
ASLR
HEAP
SEHOP
网络与通讯
内置防火墙
IPSEC
可信、启动链、防盗、数据
证书体系
TPM支持
Bitlocker
UEFI
备份、还原
策略
登陆
日志
访问控制
应用控制
UAC
驱动签名机制
响应
杀毒
Windows Defender
MSE(Microsoft Security Essentials)
MSRT(Malicious Software Removal Tool)
升级
Windows Update
第三方
Windows安全中心
EMET
版权

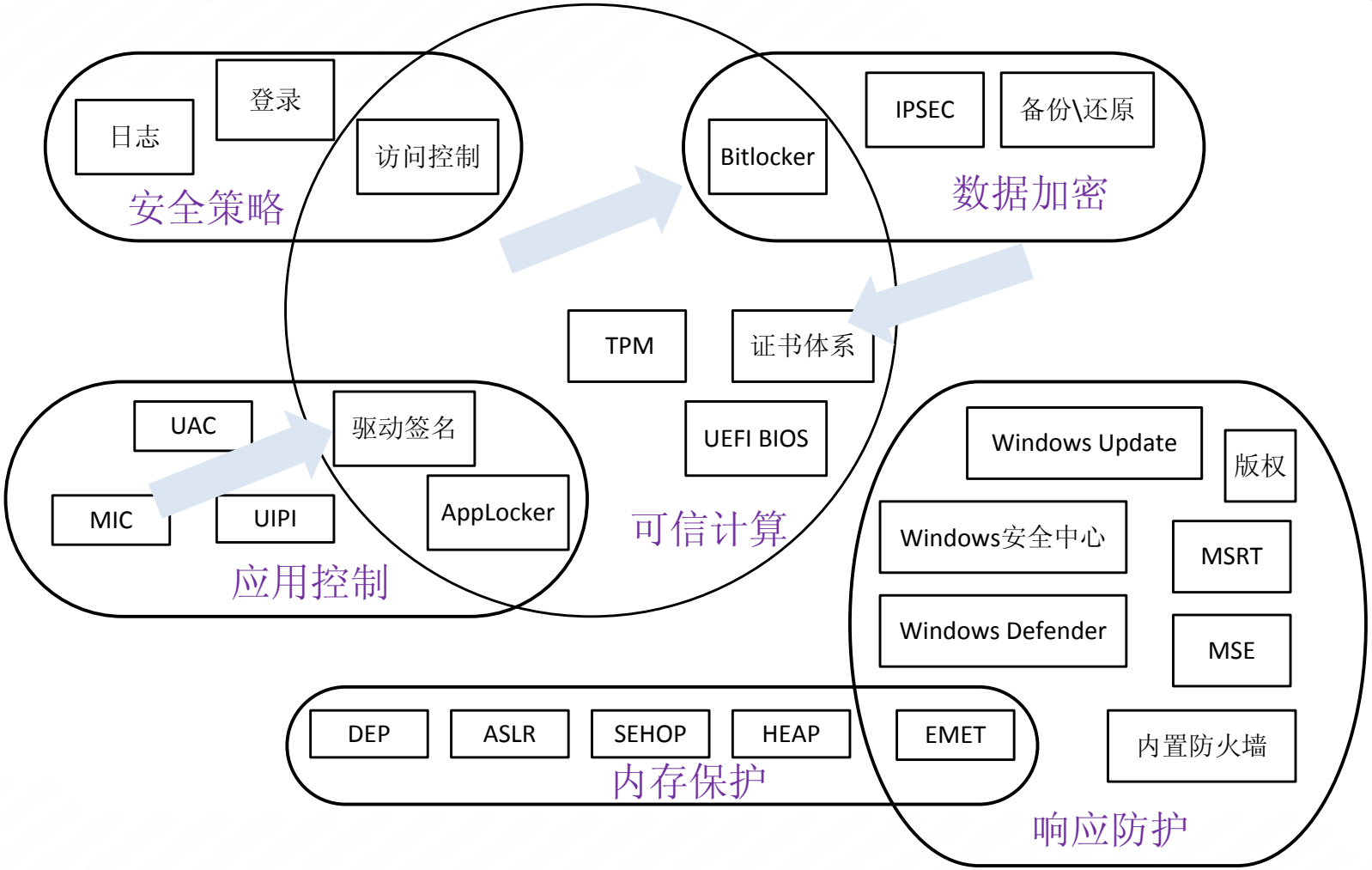
安全特性


内存
DEP
ASLR
HEAP
SEHOP
……
网络通讯
内置防火墙
IPSEC
……
可信、启动链、防盗
证书体系
TPM支持
BitLocker
UEFI
备份还原
……
安全策略
登录验证
日志
访问控制
……
应用控制
UAC
AppLocker
驱动签名验证
……
响应机制
反病毒
防护
升级

微软操作系统安全架构

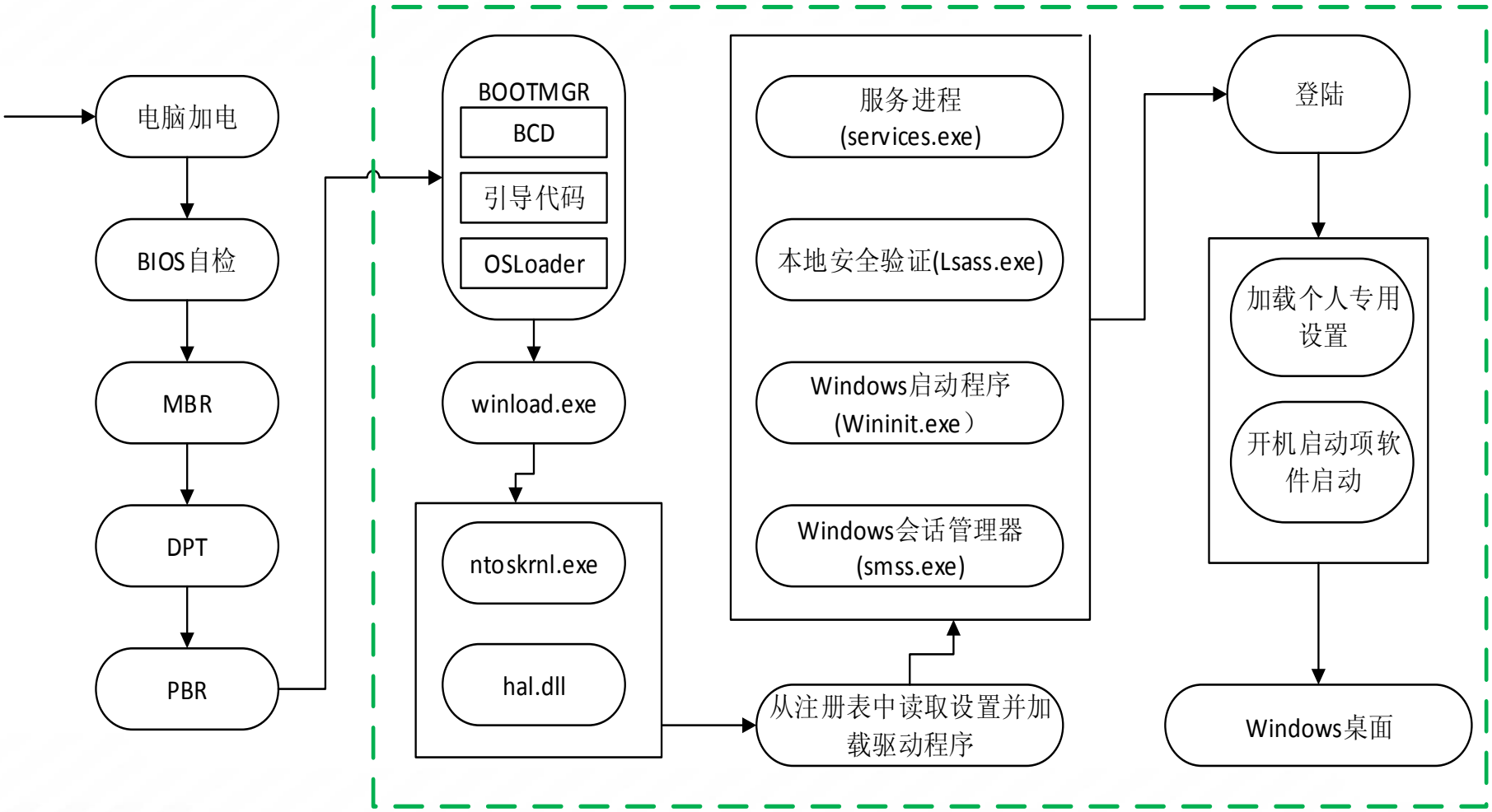

可信计算\数据加密
应用控制
内存
策略
响应\防护
外围支持
软件支持
系统支持
硬件支持
Windows安全中心
版权
IPSEC
证书体系
AppLocker
Windows Defender
MSE
MSRT
EMET
Bitlocker
基于信誉的访问控制
UAC
UIPI
SEHOP
ASLR
登陆
日志
内置防火墙
备份\还原
驱动签名
MIC
DEP
HEAP
访问控制
Windows Update
UEFI BIOS
TPM

Windows保护机制分类

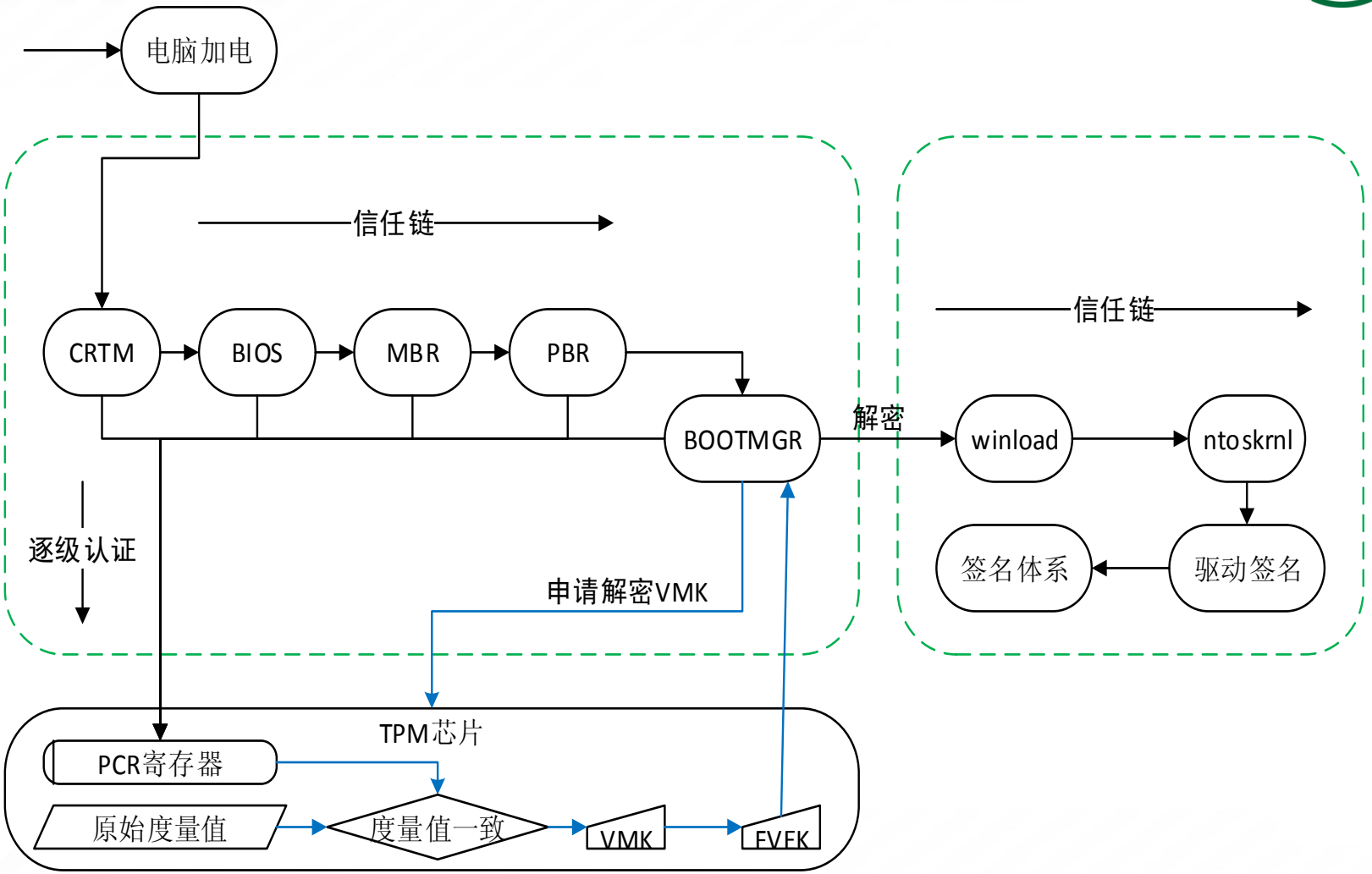


- Win7/8系统可信计算技术应用
  - BitLocker价值
  - 安全启动价值
  - 签名机制价值

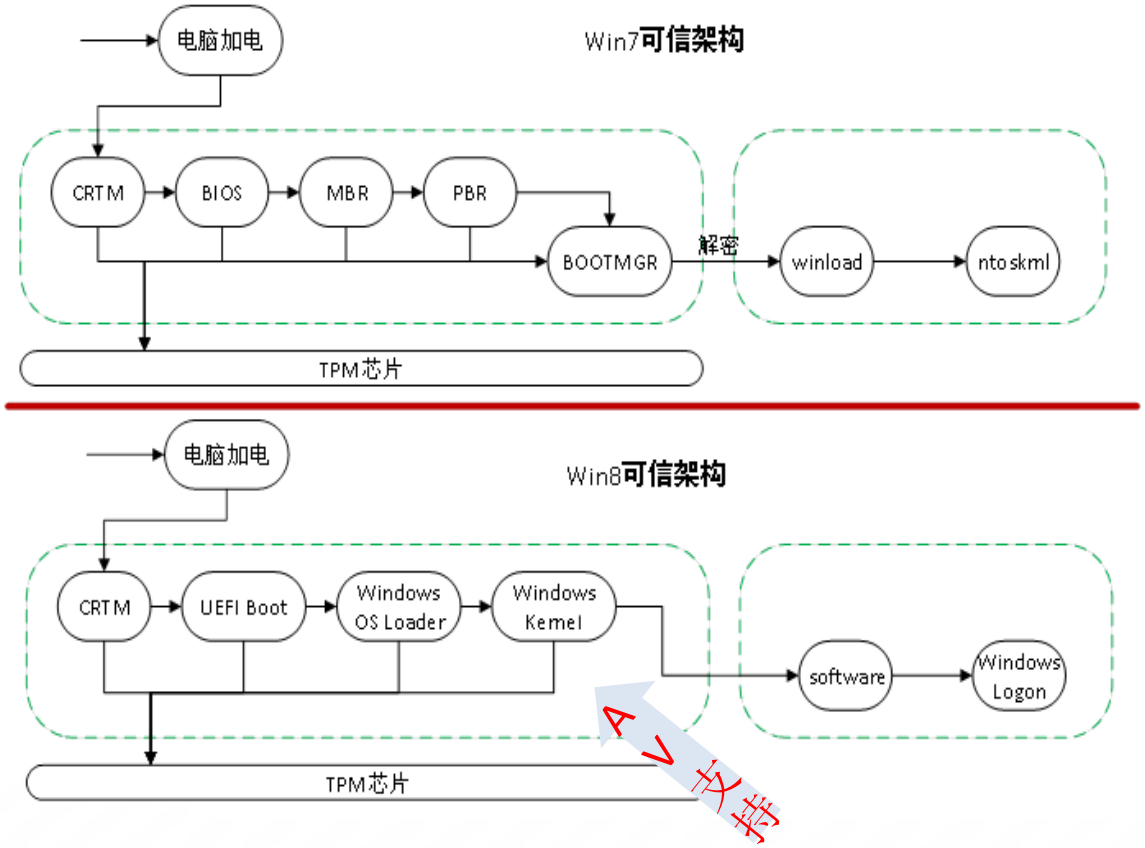
未开启BitLocker保护

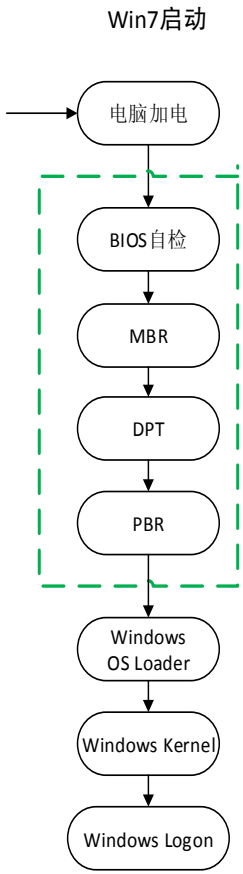


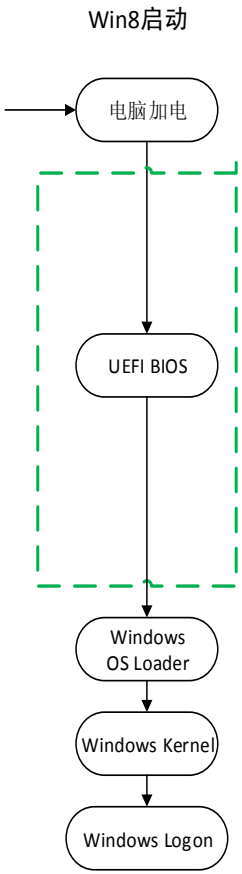
已开启BitLocker保护



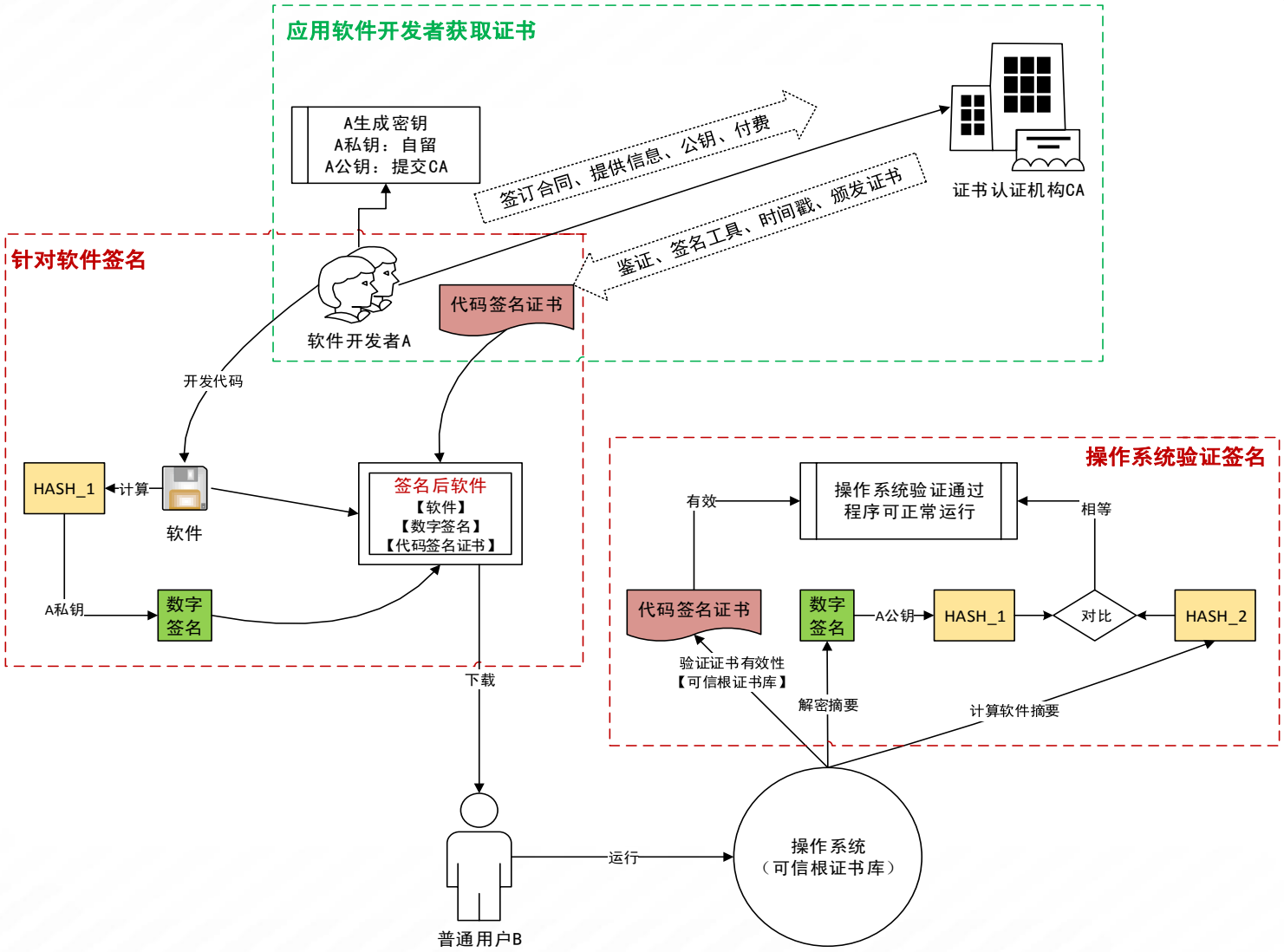
Win8支持的UEFI BIOS



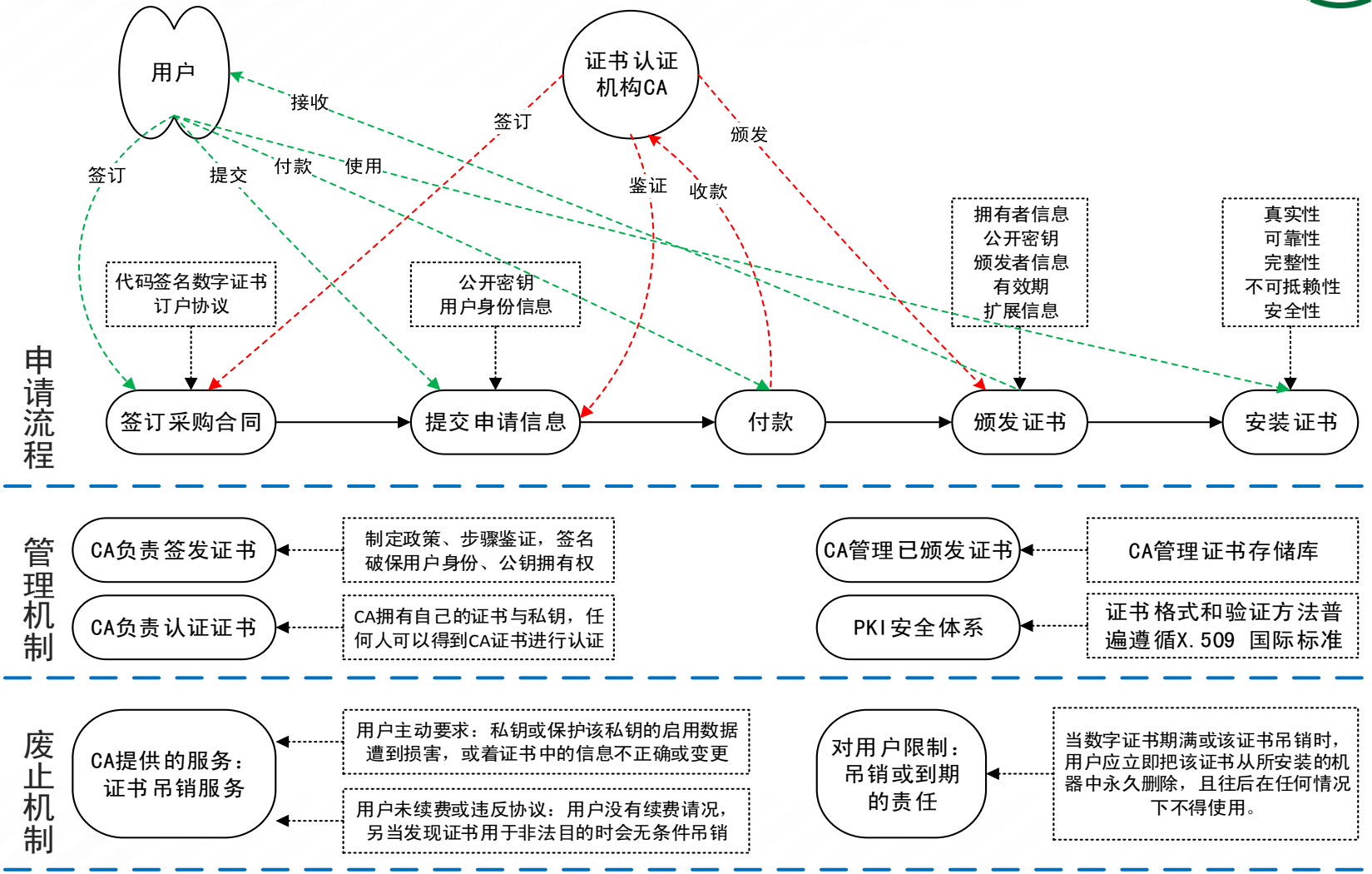




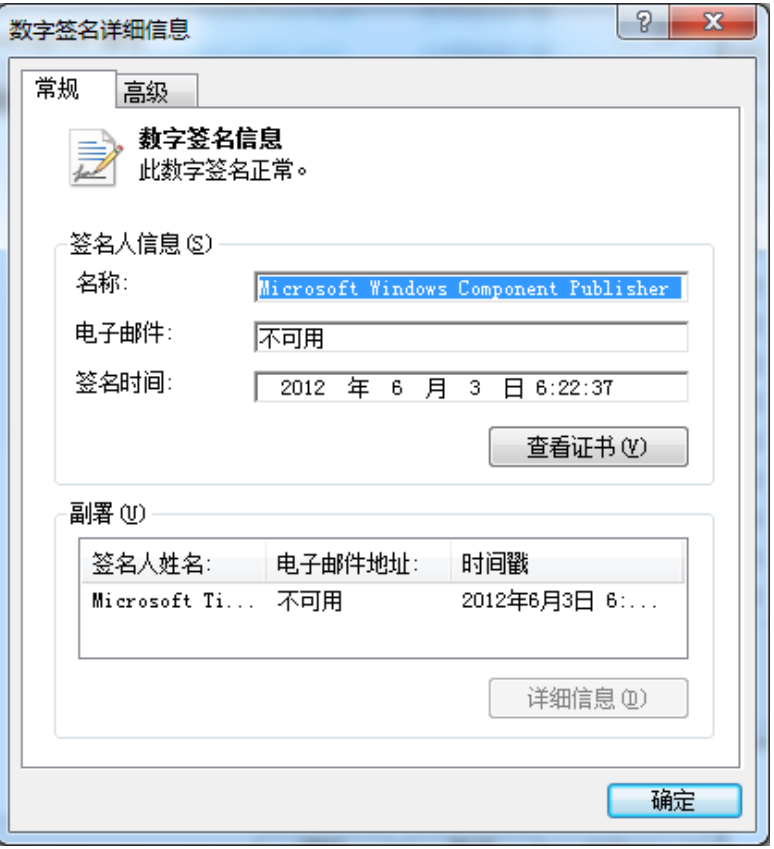
签名验证机理


应用软件开发者获取证书
A生成密钥
A私钥：自留
A公钥：提交CA
签订合同、提供信息、公钥、付费
证书认证机构CA
鉴证、签名工具、时间戳、颁发证书
软件开发者A
代码签名证书
针对软件签名
开发代码
HASH_1
计算
软件
签名后软件
【软件】
【数字签名】
【代码签名证书】
A私钥
数字签名
下载
操作系统验证签名
有效
操作系统验证通过
程序可正常运行
相等
代码签名证书
数字签名
A公钥
HASH_1
对比
HASH_2
验证证书有效性
【可信根证书库】
解密摘要
计算软件摘要
普通用户B
运行
操作系统
（可信根证书库）

证书体系流程


用户
证书认证机构CA
接收
签订
颁发
签订
提交
付款
使用
鉴证
收款
代码签名数字证书
订户协议
公开密钥
用户身份信息
拥有者信息
公开密钥
颁发者信息
有效期
扩展信息
真实性
可靠性
完整性
不可抵赖性
安全性
申请流程
签订采购合同
提交申请信息
付款
颁发证书
安装证书
管理机制
CA负责签发证书
制定政策、步骤鉴证，签名破保用户身份、公钥拥有权
CA负责认证证书
CA拥有自己的证书与私钥，任何人可以得到CA证书进行认证
CA管理已颁发证书
CA管理证书存储库
PKI安全体系
证书格式和验证方法普遍遵循X.509 国际标准
废止机制
CA提供的服务：证书吊销服务
用户主动要求：私钥或保护该私钥的启用数据遭到损害，或着证书中的信息不正确或变更
用户未续费或违反协议：用户没有续费请况，另当发现证书用于非法目的时会无条件吊销
对用户限制：吊销或到期的责任
当数字证书期满或该证书吊销时，用户应立即把该证书从所安装的机器中永久删除，且往后在任何情况下不得使用。

程序签名机制的价值


数字签名详细信息
常规
高级
数字签名信息
此数字签名正常。
签名人信息(S)
名称:
Microsoft Windows Component Publisher
电子邮件:
不可用
签名时间:
2012 年 6 月 3 日 6:22:37
查看证书(V)
副署(U)
签名人姓名:
电子邮件地址:
时间戳
Microsoft Ti...
不可用
2012年6月3日 6:...
详细信息(D)
确定

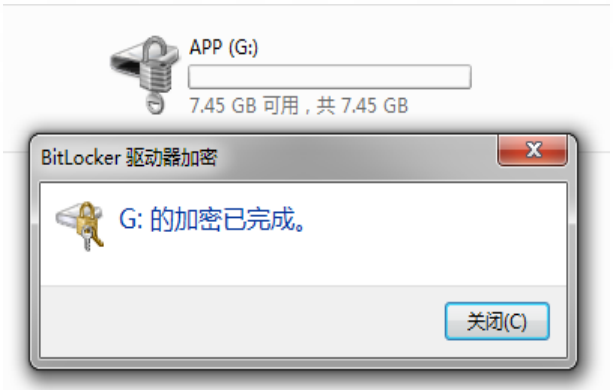

· 规范
· 促进
· 规则
· 收益
· 效率
· 防伪
· 信誉
· 产权
· 防改
· 身份
· 免杀
· 权限
· 可信
· 正确
· 安全
· 身份
· 加载
· 免扰
· TPM
· 稳定

小结 Brief Summary

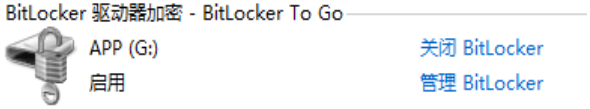
- BitLocker降低了磁盘失窃的数据泄露风险
- 驱动签名验证减少篡改OS驱动的内核劫持攻击
- 程序签名机制涉及支付通道，提高攻击成本

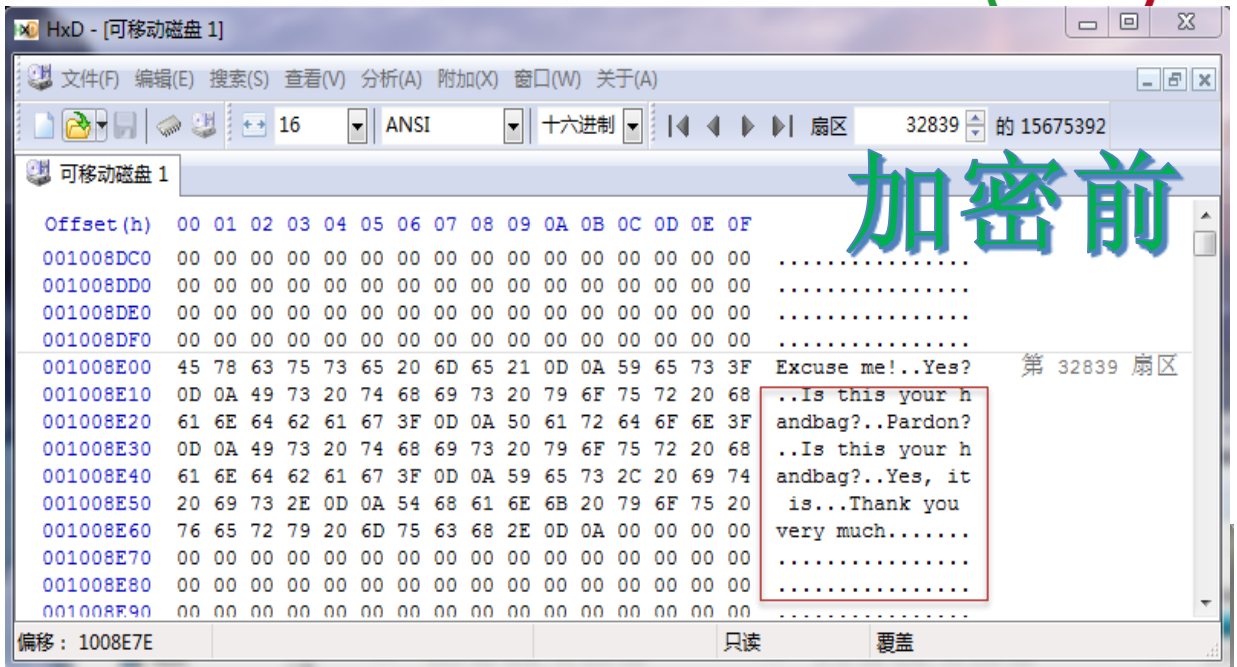
- 关键技术实战效果与价值
  - BitLocker的数据保护
  - 强制驱动签名验证绕过
  - 安全威胁形式的变化
  - 数字签名的盗用问题
  - 可信计算其它实现问题

数据加密前后比较

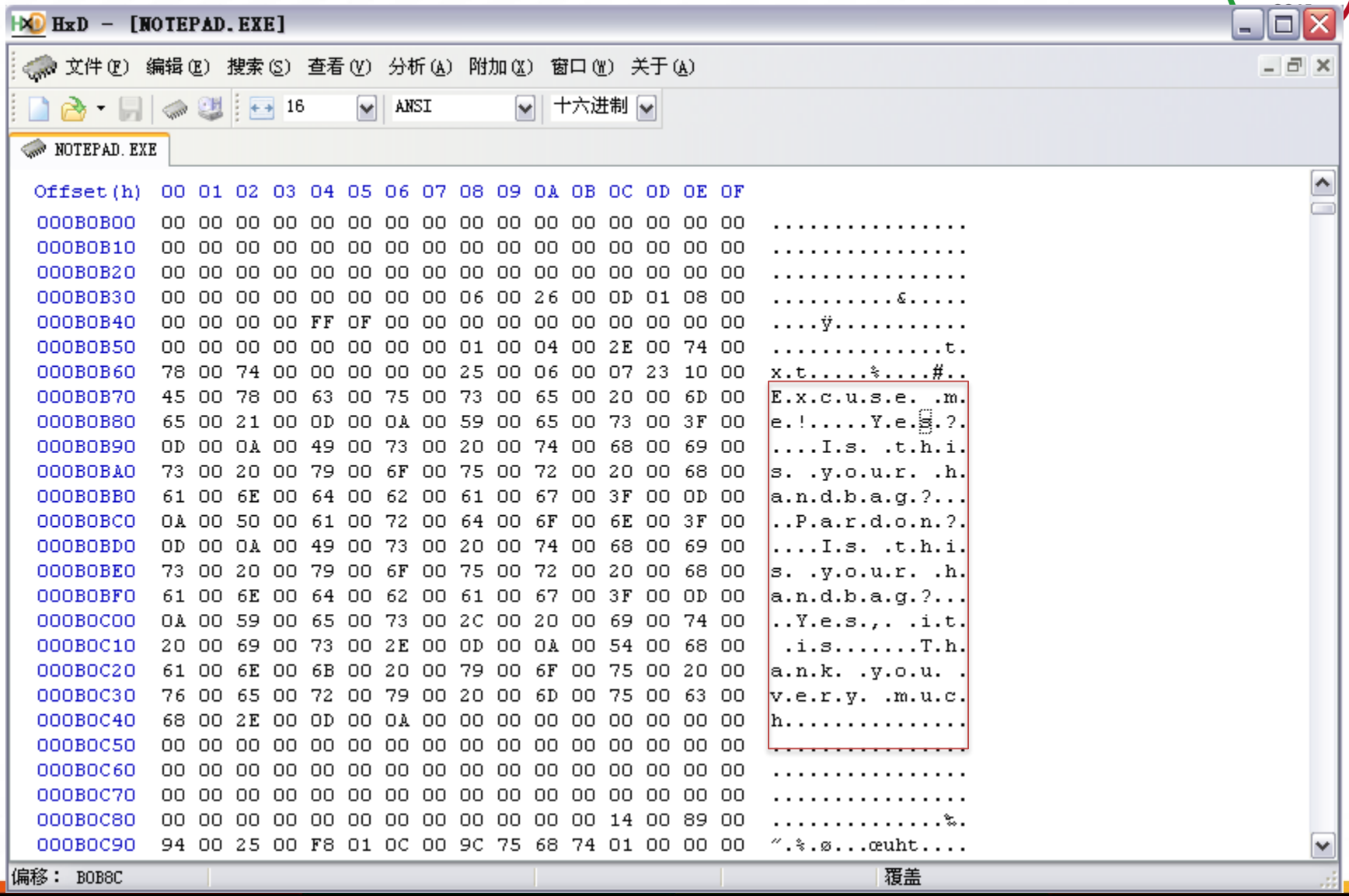


BitLocker加密





内存数据安全性


HxD - [NOTEPAD.EXE]
文件(F) 编辑(E) 搜索(S) 查看(V) 分析(A) 附加(X) 窗口(W) 关于(A)
16
ANSI
十六进制
NOTEPAD.EXE
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000B0B00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000B0B10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000B0B20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000B0B30 00 00 00 00 00 00 00 00 06 00 26 00 0D 01 08 00 ....&.....
000B0B40 00 00 00 00 FF 0F 00 00 00 00 00 00 00 00 00 00 ....ÿ...........
000B0B50 00 00 00 00 00 00 00 00 01 00 04 00 2E 00 74 00 ....t.
000B0B60 78 00 74 00 00 00 00 00 25 00 06 00 07 23 10 00 x.t.....%....#..
000B0B70 45 00 78 00 63 00 75 00 73 00 65 00 20 00 6D 00 E.x.c.u.s.e. .m.
000B0B80 65 00 21 00 0D 00 0A 00 59 00 65 00 73 00 3F 00 e.!.....Y.e.s.?.
000B0B90 0D 00 0A 00 49 00 73 00 20 00 74 00 68 00 69 00 ....I.s. .t.h.i.
000B0BA0 73 00 20 00 79 00 6F 00 75 00 72 00 20 00 68 00 s. .y.o.u.r. .h.
000B0BB0 61 00 6E 00 64 00 62 00 61 00 67 00 3F 00 0D 00 a.n.d.b.a.g.?...
000B0BC0 0A 00 50 00 61 00 72 00 64 00 6F 00 6E 00 3F 00 ..P.a.r.d.o.n.?.
000B0BD0 0D 00 0A 00 49 00 73 00 20 00 74 00 68 00 69 00 ....I.s. .t.h.i.
000B0BE0 73 00 20 00 79 00 6F 00 75 00 72 00 20 00 68 00 s. .y.o.u.r. .h.
000B0BF0 61 00 6E 00 64 00 62 00 61 00 67 00 3F 00 0D 00 a.n.d.b.a.g.?...
000B0C00 0A 00 59 00 65 00 73 00 2C 00 20 00 69 00 74 00 ..Y.e.s.,. .i.t.
000B0C10 20 00 69 00 73 00 2E 00 0D 00 0A 00 54 00 68 00 .i.s.....T.h.
000B0C20 61 00 6E 00 6B 00 20 00 79 00 6F 00 75 00 20 00 a.n.k. .y.o.u. .
000B0C30 76 00 65 00 72 00 79 00 20 00 6D 00 75 00 63 00 v.e.r.y. .m.u.c.
000B0C40 68 00 2E 00 0D 00 0A 00 00 00 00 00 00 00 00 00 h...............
000B0C50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000B0C60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000B0C70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000B0C80 00 00 00 00 00 00 00 00 00 00 00 00 14 00 89 00 ....‰.
000B0C90 94 00 25 00 F8 01 0C 00 9C 75 68 74 01 00 00 00 ”.%.ø...œuht....
偏移： B0B8C
覆盖

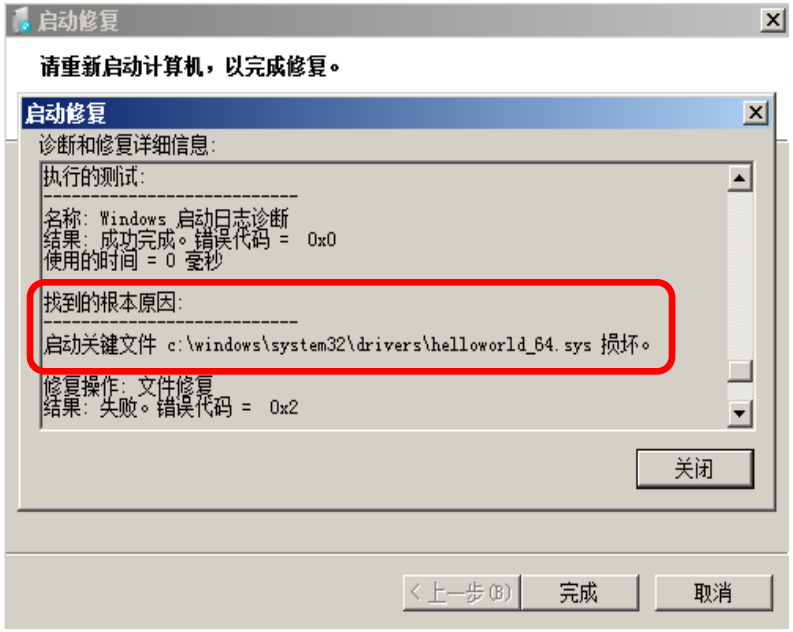
小结 Brief Summary

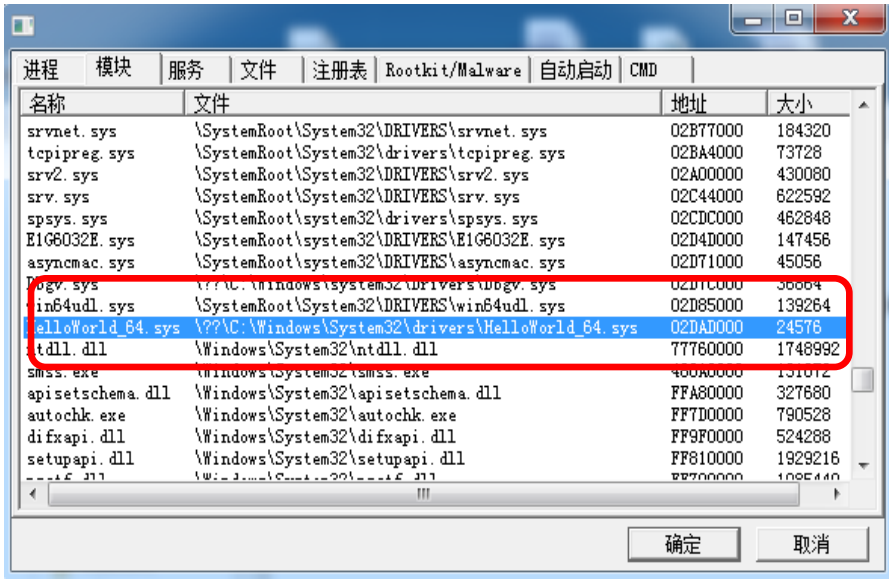
- BitLocker只保证磁盘静态数据安全
- 启动后的安全保障需借助其它机制

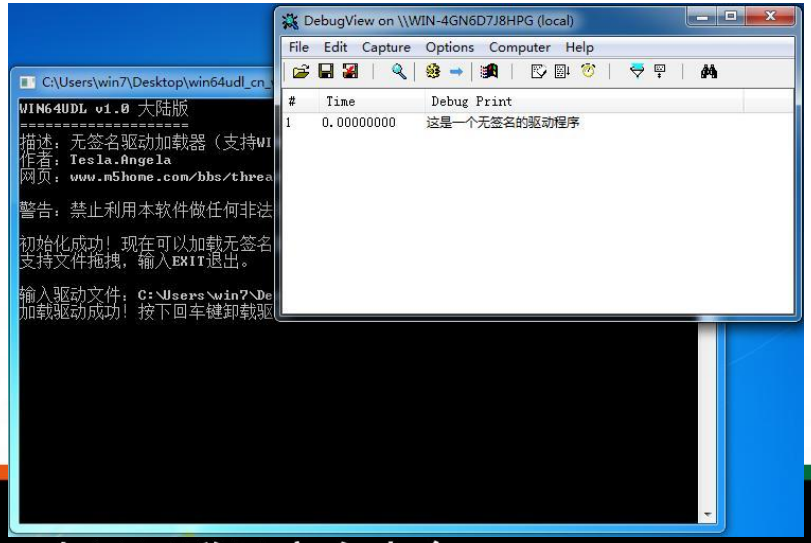
强制驱动签名验证绕过

```
loc_110F0:                              ; CODE XREF: sub_11078+2F↑j
                mov     rax, cs:g_CiOptionsAddr
                mov     cl, [rax]
                mov     cs:original_g_CiOptions_value, cl ; 保存g_CiOptions原来的值
                mov     rcx, cr8
                mov     eax, 2
                mov     cr8, rax        ; 关闭内存写保护
                mov     rax, cr0
                btr     rax, 10h
                mov     cr0, rax
                cli
                mov     rax, cs:g_CiOptionsAddr
                mov     byte ptr [rax], 0 ; 将g_CiOptions的值清零关闭DSE
                mov     rax, cr0
                sti                     ; 开启内存写保护
                bts     rax, 10h
                mov     cr0, rax
                movzx   eax, cl
                jmp     short loc_110E3
; ---------------------------------------------------------------------------
                mov     rax, cr0
                btr     rax, 10h
                mov     cr0, rax
                cli                     ; 关闭内存写保护
                mov     rcx, cs:g_CiOptionsAddr
                mov     al, cs:original_g_CiOptions_value
                mov     [rcx], al       ; 开启DSE
                mov     rax, cr0        ; 开启内存写保护
                sti
                bts     rax, 10h
                mov     cr0, rax
                movzx   eax, dl
```

强制驱动签名验证绕过


启动修复
请重新启动计算机，以完成修复。
启动修复
诊断和修复详细信息:
执行的测试:
名称: Windows 启动日志诊断
结果: 成功完成。错误代码 = 0x0
使用的时间 = 0 毫秒
找到的根本原因:
启动关键文件 c:\windows\system32\drivers\helloworld_64.sys 损坏。
修复操作: 文件修复
结果: 失败。错误代码 = 0x2
关闭
< 上一步(B)
完成
取消


进程
模块
服务
文件
注册表
Rootkit/Malware
自动启动
CMD
名称
文件
地址
大小
srvnet.sys \SystemRoot\System32\DRIVERS\srvnet.sys 02B77000 184320
tcpipreg.sys \SystemRoot\System32\drivers\tcpipreg.sys 02BA4000 73728
srv2.sys \SystemRoot\System32\DRIVERS\srv2.sys 02A00000 430080
srv.sys \SystemRoot\System32\DRIVERS\srv.sys 02C44000 622592
spsys.sys \SystemRoot\system32\drivers\spsys.sys 02CDC000 462848
E1G6032E.sys \SystemRoot\system32\DRIVERS\E1G6032E.sys 02D4D000 147456
asyncmac.sys \SystemRoot\system32\DRIVERS\asyncmac.sys 02D71000 45056
in64udl.sys \SystemRoot\System32\DRIVERS\win64udl.sys 02D85000 139264
elloWorld_64.sys \??\C:\Windows\System32\drivers\HelloWorld_64.sys 02DAD000 24576
tdll.dll \Windows\System32\ntdll.dll 77760000 1748992
apisetschema.dll \Windows\System32\apisetschema.dll FFA80000 327680
autochk.exe \Windows\System32\autochk.exe FF7D0000 790528
difxapi.dll \Windows\System32\difxapi.dll FF9F0000 524288
setupapi.dll \Windows\System32\setupapi.dll FF810000 1929216
确定
取消

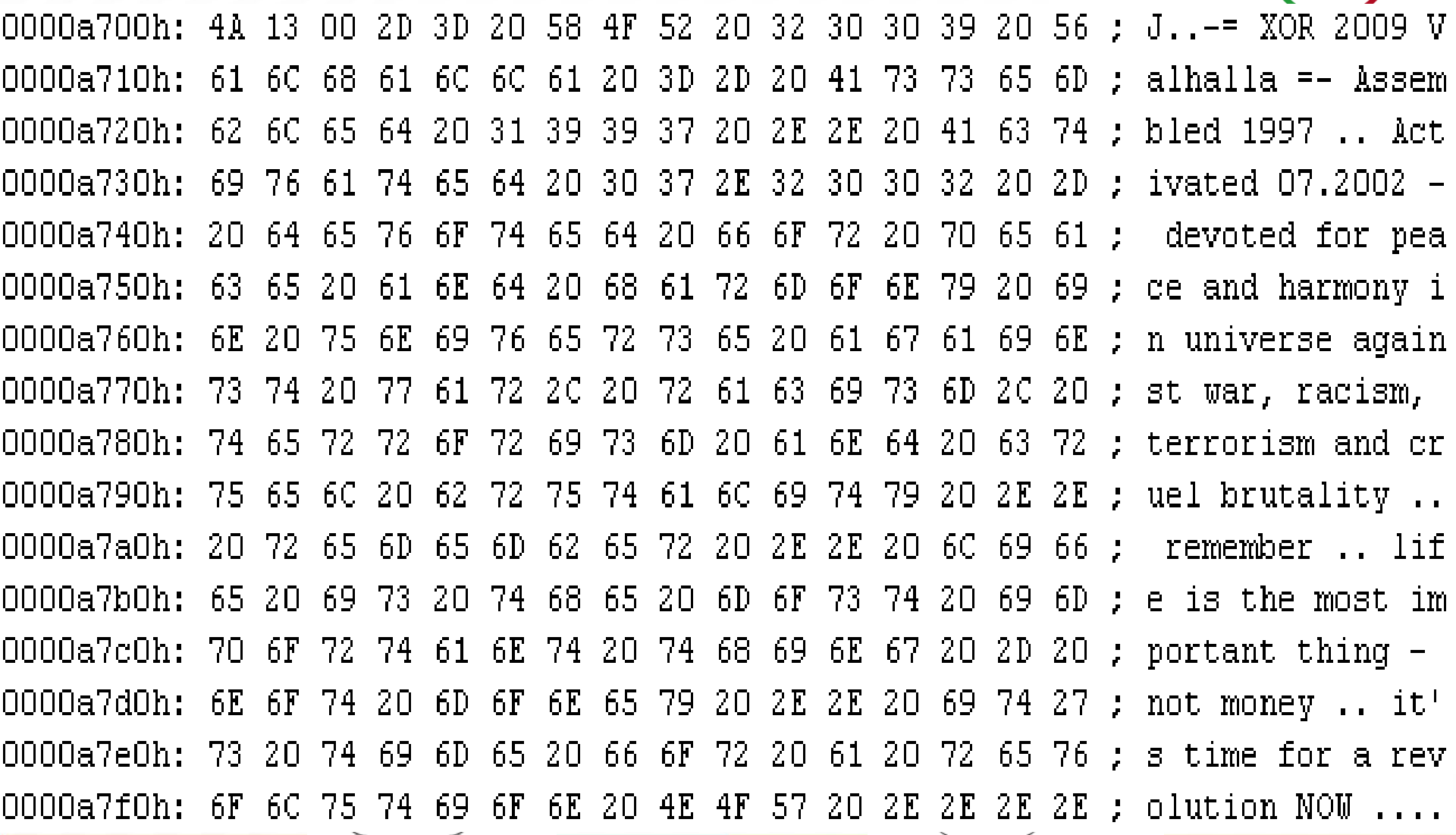

DebugView on \\WIN-4GN6D7J8HPG (local)
File Edit Capture Options Computer Help
Time Debug Print
1 0.00000000 这是一个无签名的驱动程序
C:\Users\win7\Desktop\win64udl_cn_
WIN64UDL v1.0 大陆版
描述：无签名驱动加载器（支持WI
作者：Tesla.Angela
网页：www.m5home.com/bbs/threa
警告：禁止利用本软件做任何非法
初始化成功！现在可以加载无签名
支持文件拖拽，输入EXIT退出。
输入驱动文件：C:\Users\win7\De
加载驱动成功！按下回车键卸载驱


64
Windows 7

小结 Brief Summary

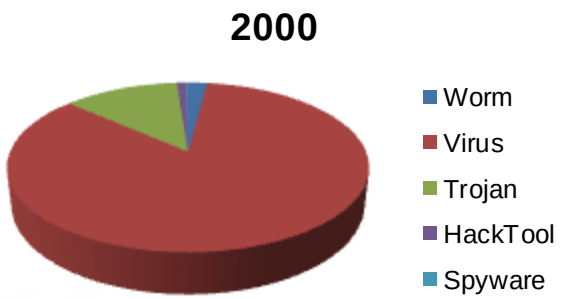
- 强制驱动签名验证实现不够严谨，而且也不可能做到绝对严谨
- 已签名驱动可能有主观恶意
- 已签名驱动可能有实现错误

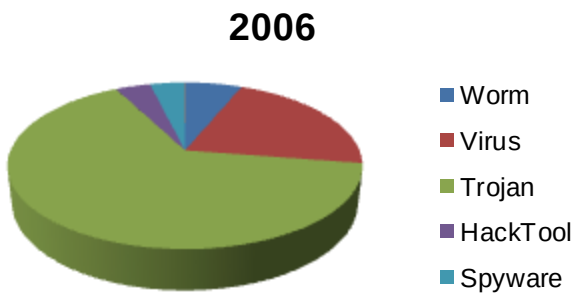
传统感染式恶意代码

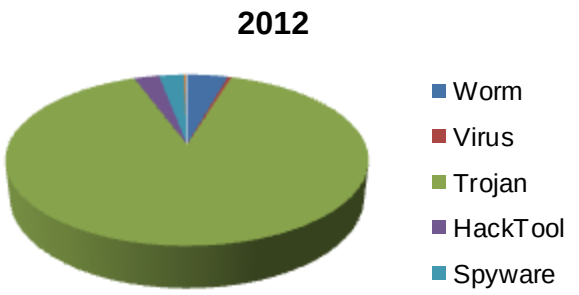

0000a700h: 4A 13 00 2D 3D 20 58 4F 52 20 32 30 30 39 20 56 ; J..-= XOR 2009 V
0000a710h: 61 6C 68 61 6C 6C 61 20 3D 2D 20 41 73 73 65 6D ; alhalla =- Assem
0000a720h: 62 6C 65 64 20 31 39 39 37 20 2E 2E 20 41 63 74 ; bled 1997 .. Act
0000a730h: 69 76 61 74 65 64 20 30 37 2E 32 30 30 32 20 2D ; ivated 07.2002 -
0000a740h: 20 64 65 76 6F 74 65 64 20 66 6F 72 20 70 65 61 ; devoted for pea
0000a750h: 63 65 20 61 6E 64 20 68 61 72 6D 6F 6E 79 20 69 ; ce and harmony i
0000a760h: 6E 20 75 6E 69 76 65 72 73 65 20 61 67 61 69 6E ; n universe again
0000a770h: 73 74 20 77 61 72 2C 20 72 61 63 69 73 6D 2C 20 ; st war, racism,
0000a780h: 74 65 72 72 6F 72 69 73 6D 20 61 6E 64 20 63 72 ; terrorism and cr
0000a790h: 75 65 6C 20 62 72 75 74 61 6C 69 74 79 20 2E 2E ; uel brutality ..
0000a7a0h: 20 72 65 6D 65 6D 62 65 72 20 2E 2E 20 6C 69 66 ; remember .. lif
0000a7b0h: 65 20 69 73 20 74 68 65 20 6D 6F 73 74 20 69 6D ; e is the most im
0000a7c0h: 70 6F 72 74 61 6E 74 20 74 68 69 6E 67 20 2D 20 ; portant thing -
0000a7d0h: 6E 6F 74 20 6D 6F 6E 65 79 20 2E 2E 20 69 74 27 ; not money .. it'
0000a7e0h: 73 20 74 69 6D 65 20 66 6F 72 20 61 20 72 65 76 ; s time for a rev
0000a7f0h: 6F 6C 75 74 69 6F 6E 20 4E 4F 57 20 2E 2E 2E 2E ; olution NOW ....

2000 ~ 2012恶意代码演变

年份/家族数	2000	2006	2012
Worm	512	8109	354049
Virus	21006	27760	29940
Trojan	3066	84811	7262094
HackTool	260	4968	217502
Spyware	37	4899	214570
RiskWare	0	88	25800







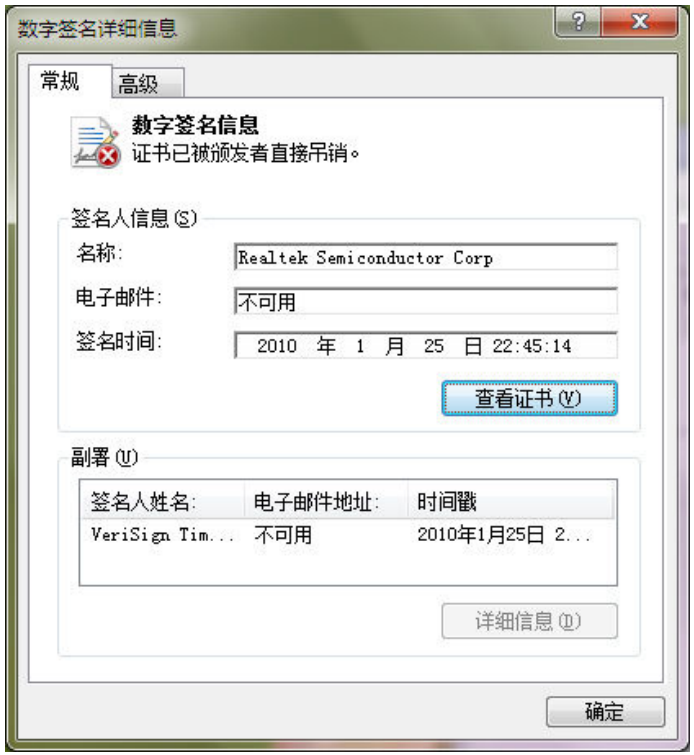
小结 Brief Summary

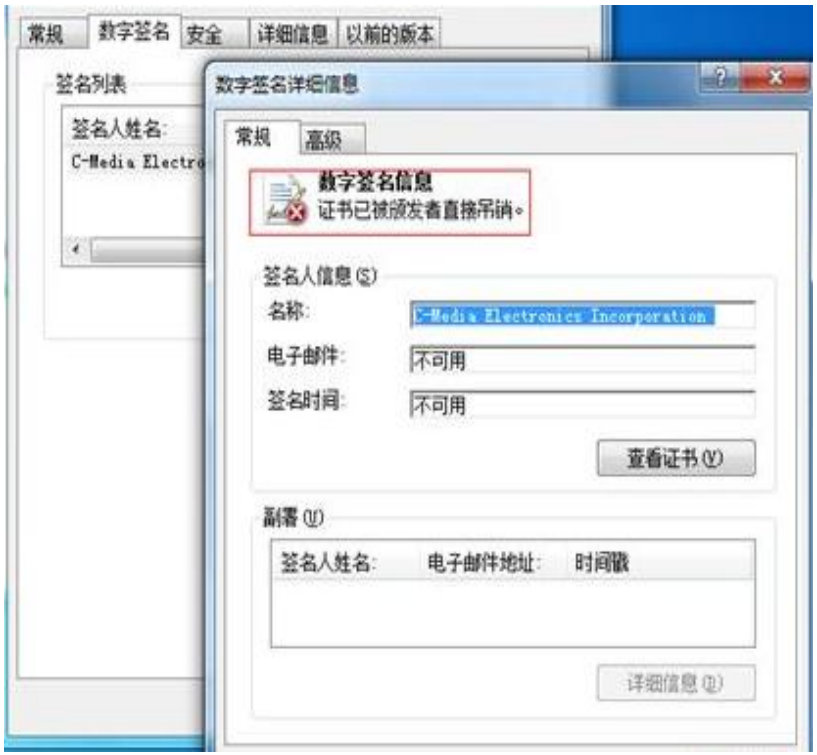
- 被感染式病毒感染后程序签名会被破坏
- 禁止签名无效程序运行可防止感染传播
- 但目前主流安全威胁不再是感染式病毒
- 而是不具备感染性的木马，其可能带有签名
- 有趣的是——感染式病毒也可以自带签名证书

APT攻击中的证书盗用

REALTEK

Cmedia
C-MEDIA ELECTRONICS INC.





证书盗用问题

2011年Winnti组织

公司	国家
ESTsoft Corp	韩国
Kog Co., Ltd.	韩国
LivePlex Corp	韩国/ 菲律宾
MGAME Corp	韩国
Rosso Index KK	日本
Sesisoft	韩国
Wemade	日本/韩国/美国
YNK Japan	日本
Guangzhou YuanLuo	中国
Fantasy Technology Corp	中国
Neowiz	韩国

2014年Poisoned Hurricane行动

公司	国家
MOCOMSYS INC	韩国
PIXELPLUS CO. LTD.	韩国
Police Mutual Aid Association	韩国
QTI INTERNATIONAL INC	韩国
Ssangyong Motor Co.	韩国
Jtc	韩国

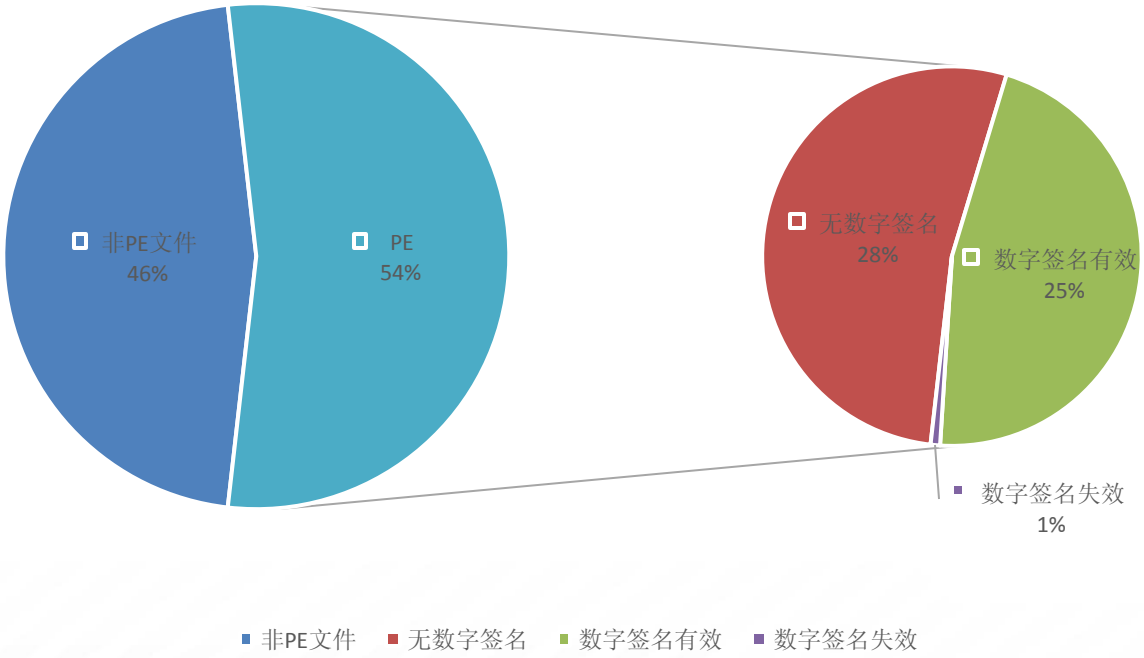
2011年发现的Duqu具有窃取证书功能

2012年发现的Flame利用哈希碰撞伪造微软证书

恶意代码使用签名统计

针对2014年07月12日Virustotal样本：
含恶意代码文件73111个
非PE文件：33921个，46%占比
无数字签名文件：20715，28%占比
数字签名有效文件：18160，25%占比
数字签名无效文件：315，1%占比
其中数字签名无效文件包括：

1. 证书被吊销
2. 签名破损
3. 签名时间过期
4. 签名无效
5. 文件尾感染病毒



小结 Brief Summary

- 主流软件厂商数字签名亦存在被盗用现象
- 近半数PE恶意程序具有（有效的）数字签名
- 被滥用的签名不能得到及时处理

可信计算在Win7/8中应用

理论	信任根->信任链
	逐层测量认证
	扩大到整个系统
现实	安全启动
	TPM芯片+BitLocker加密
效果	减少内核劫持攻击
	降低数据泄密风险

可信计算实现中的问题 - 1

环节	问题
签名验证	CVE-2013-3900 WinVerifyTrust 函数处理可移植可执行文件 (PE) 的 Windows Authenticode 签名验证的方式中存在一个远程执行代码漏洞。
签名验证	CVE-2013-3869 X.509证书分析的实施中存在一个拒绝服务漏洞，该漏洞可能导致受影响的Web服务停止响应。
签名验证	CVE-2013-2153 Apache Santuario 漏洞，攻击者可借助Signature中的Reference元素绕过签名验证。
签名验证	CVE-2013-1336 Microsoft .NET Framework漏洞，当Microsoft .NET Framework无法正确验证特制XML文件的签名时存在一个欺骗漏洞。成功利用此漏洞的攻击者可能会修改XML文件的内容，而不会使与文件相关联的签名无效。

可信计算实现中的问题 - 2

环节	问题
签名验证	CVE-2011-2993 Mozilla Firefox 4.x至5版本的JAR文件数字签名的实现没有阻止未签名JavaScript代码对签名代码的调用，导致远程攻击者可以通过特制的网站绕过同源策略并获得特权。
签名验证	CVE-2009-3875 Java Runtime Environment(JRE)的MessageDigest.isEqual函数允许远程攻击者借助与"时序攻击漏洞"相关的未加规定向量，骗取基于HMAC的数字签名，并可能绕过鉴别。
签名验证	CVE-2008-5100 Microsoft .NET Framework 中的strong name(SN)implementation依赖于公共密钥数字签名的一个DLL文件路径名，而不是DLL文件本身，可被绕过。

可信计算实现中的问题 - 3

环节	问题
签名验证	CVE-2007-2218 Windows的安全通道(SChannel)库在实现客户端SSLv3握手协议时，校验服务器端数字签名实现错误，存在单字节堆溢出漏洞，远程攻击者可能利用此漏洞控制服务器或造成拒绝服务。
签名验证	CVE-2003-1363 微软的文件保护系统(WFP)错误地信任CA根服务器发布签名证书，导致攻击者可以自建一个使用根CA数字签名的程序来欺骗文件保护系统。

可信计算实现中的问题 - 4

环节	问题
Bitlocker应用	CVE-2010-3145 在Microsoft Windows Vista SP1和SP2中的Backup Manager的sdclt.exe中使用的BitLocker Drive Encryption API中存在不可信搜索路径漏洞。本地用户可以借助当前工作目录中的fveapi.dll木马文件获取特权。
Bitlocker应用	CVE-2008-3893 Windows Vista SP1之前的版本中的Microsoft Bitlocker在BIOS键盘缓冲区内储存pre-boot权限密码而且不会在使用后清空该缓冲区，本地用户可以通过读取与该缓冲区有关的物理内存位置来获得敏感信息。
UEFI BIOS实现	CVE-2014-4859 EDK2是一个提供了统一可扩展固件接口的参考实现（UEFI）的开源项目。EDK2中存在本地整数溢出漏洞。攻击者可利用该漏洞以系统固件权限执行任意代码。也可能造成拒绝服务。

可信计算实现中的问题 - 5

环节	问题
AppLocker应用	CVE-2011-4434 Microsoft Windows 多个版本中存在不能准确实施AppLocker规则，使攻击者可借助应用程序中的宏或脚本语言绕过访问限制。该漏洞已在Microsoft Office applications和SANDBOX_INERT以及LOAD_IGNORE_CODE_AUTHZ_LEVEL中被证实。
TPM实现	CVE-2011-1162 The tpm_read function in the Linux kernel 2.6 does not properly clear memory, which might allow local users to read the results of the previous TPM command.
TPM实现	CVE-2011-1160 The tpm_open function in drivers/char/tpm/tpm.c in the Linux kernel before 2.6.39 does not initialize a certain buffer, which allows local users to obtain potentially sensitive information from kernel memory via unspecified vectors.

可信计算实现中的问题 - 6

环节	问题
TPM实现	TPM Reset Attack If an attacker really wanted to keep from disturbing the rest of the platform, they could physically isolate the TPM from the platform and drive the reset line only on the TPM . Either way, we could ultimately take a platform in an untrusted configuration and put it into a trusted one.
TPM实现	Cloaking Malware with the Trusted Platform Module Malware can use the Trusted Platform Module to make its computation significantly more difficult to analyze. Even though the TPM was intended to increase the security of computer systems, it can undermine computer security when used by malware.

可信计算的有效与无效

有价值的

- 引导链安全
- 被盗
- 感染式病毒
- 部分Rootkit
- 发现非签名应用
- ……

难以应对的

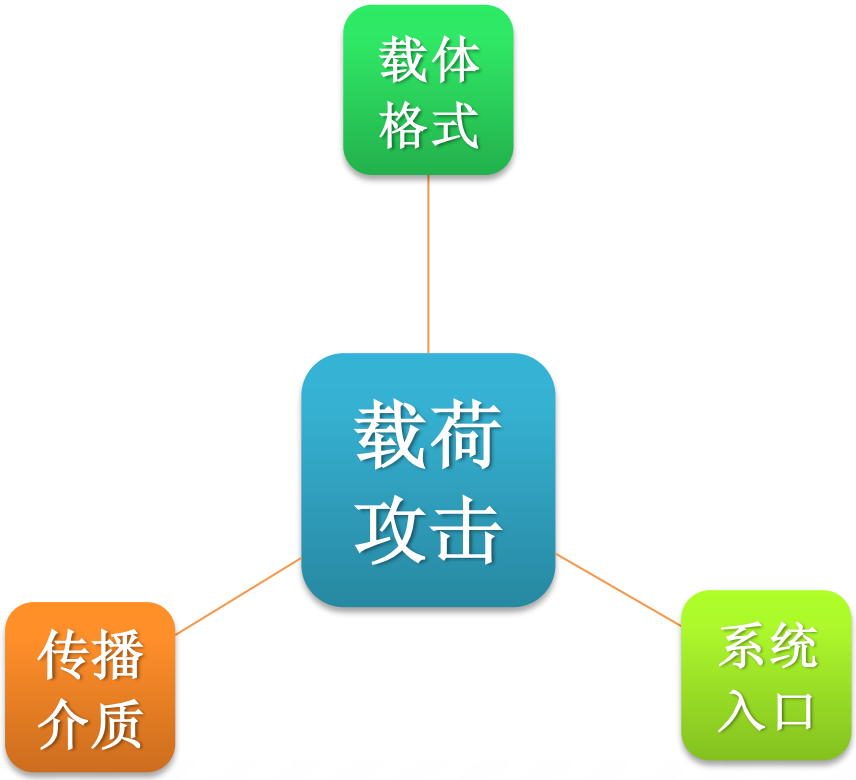
- 带有签名的二进制恶意代码
- 宏病毒
- 脚本病毒
- 溢出和注入
- Sql注入
- Shell
- Webshell

可信的困局

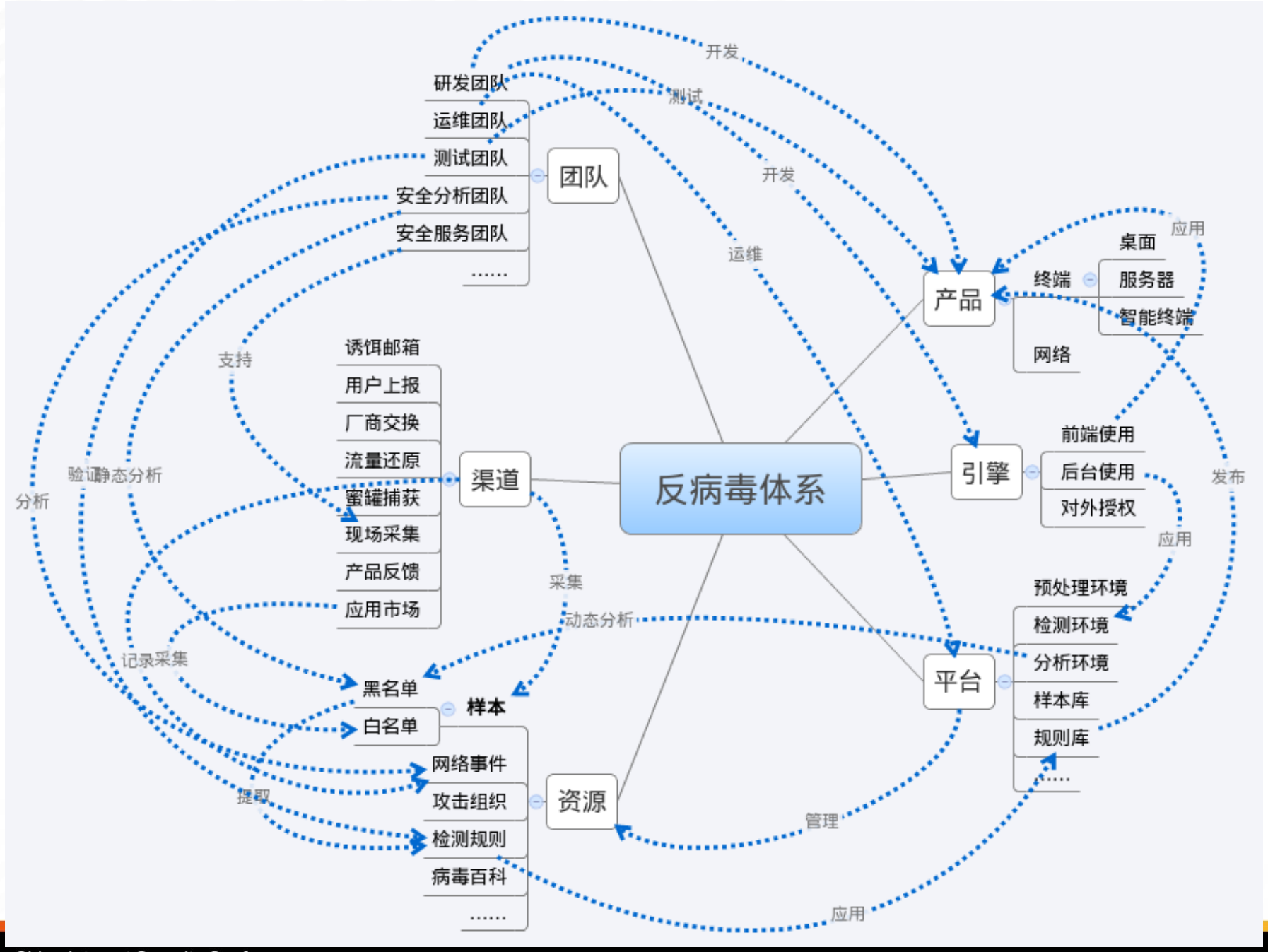
- Trustworthy Conputing Group(2002-2014)
  - 9月19日微软拆分可信赖计算部门

- 反病毒与可信辩证关系
  - 安全的规律
  - 反病毒的价值
  - 反病毒与可信计算的关系

从载荷攻击看安全的规律



- 科恩范式：**恶意代码与正常程序的区别，没有数学级形式化方法，攻击者和正常用户间，就更不可能有这种形式化方法。**
- 应用可以运行，攻击载荷即可运行。
- 应用可以签名，攻击载荷即可签名。
- 用户可以登录，攻击者即可尝试。
- 在数据获取能力上，应用和系统没有本质区别


反病毒体系
团队
研发团队
运维团队
测试团队
安全分析团队
安全服务团队
……
渠道
诱饵邮箱
用户上报
厂商交换
流量还原
蜜罐捕获
现场采集
产品反馈
应用市场
资源
样本
黑名单
白名单
网络事件
攻击组织
检测规则
病毒百科
……
产品
终端
桌面
服务器
智能终端
网络
引擎
前端使用
后台使用
对外授权
平台
预处理环境
检测环境
分析环境
样本库
规则库
……
开发
测试
开发
运维
应用
支持
验证
静态分析
分析
采集
动态分析
记录采集
提取
管理
应用
发布
应用

反病毒体系 - 扩展场景


工业控制系统仿真环境
工业控制系统仿真环境能够真实体现工控系统的组成结构和主要场合工控环境的展示。
本系统包含了运行环境
计算机及网络系统
现场控制区域

反病毒的价值

- 安全威胁检测能力
- 安全威胁影响评估
- 安全事件鉴定能力
- 安全事件关联分析
- 安全事件响应能力

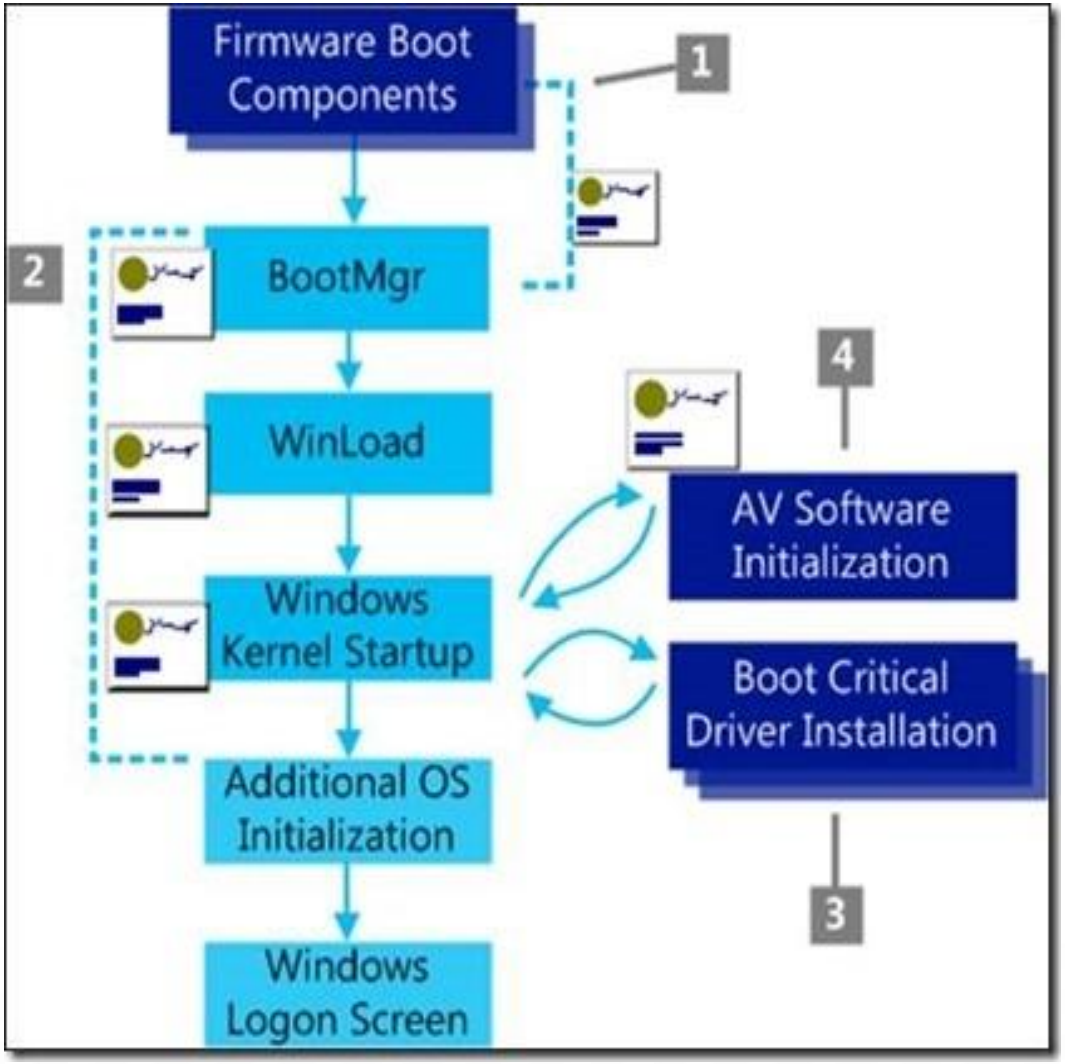
反病毒也需要可信架构保证

微软安全中心注册机制可被病毒利用

反病毒也需要可信架构保证

- 传统安全中心机制，易被恶意代码所利用
- 操作系统与反病毒采用私密接口互动
- 将可靠反病毒厂商加入可信链是更安全的作法

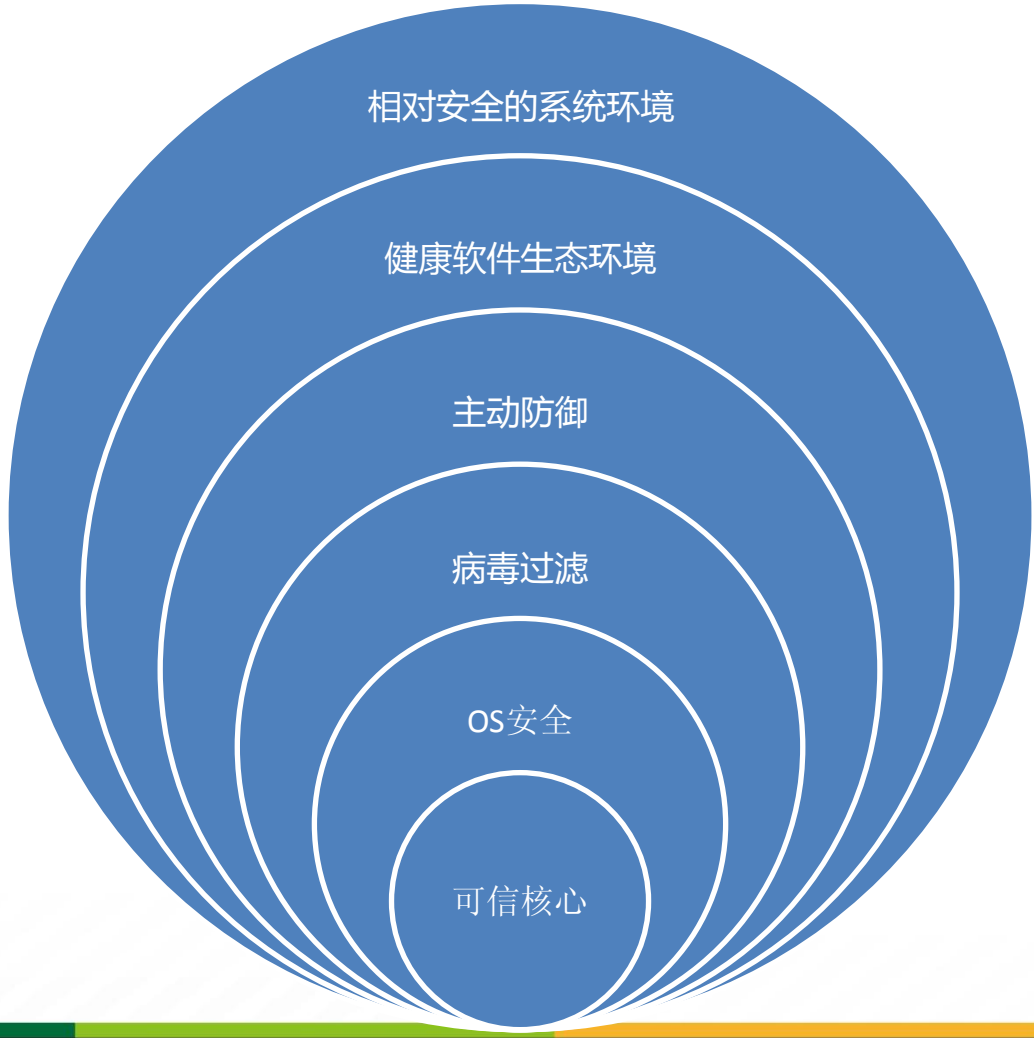
微软已经做出尝试



1. 固件校验UEFI可执行文件及OS加载器，确保其可信
2. 启动组件校验各待加载组件（非受信组件不被加载）
3. 校验启动关键驱动
4. 先于其它驱动，检查并加载反病毒软件

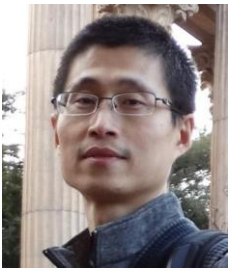
结论

唯有可信架构、主动防御、反病毒能力、软件生态体系等因素都得到充分强化，才能够带给我们一个相对安全的系统环境



Thanks

不懂网络安全的人是幸福的人
而我们的责任是保护他们的幸福
——引自《安天团队宣言》



libaisong@antiy.cn

420318

weibo.com/libaisong75