

Vulnerabilities in Full/Virtual Disk Encryption Products

Neil Kettle

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

neil@digit-security.com - *Digit Security Ltd*

SEC-T '10



The screenshot shows a Yahoo! search interface for the UK & IRELAND region. The search bar contains "digit-labs.org". Below the search bar, there are radio buttons for "the Web", "only in UK", and "only in Ireland", with "the Web" selected. On the left side, there are buttons for "View Notes (1)" and "SafeSearch - Off". The search results show 10,900 results for "digit-labs.org". The first result is titled "digit-labs.org | 2010" and includes a warning icon and text: "Warning: Dangerous Downloads". The snippet below the warning reads: "computer ... mu-b/digit-labs.org 'Your face, your ass, what's the difference?' home. research ... © Copyright digit-labs.org 1999-2010 - all rights reserved. Valid XHTML, CSS ...". At the bottom of the snippet, there is a link to "www.digit-labs.org - Cached".

November, 2007 - January 9, 2011

OUTLINE

AGENDA

FAQ

- FAQ - Why Bother?

- FAQ - Why Bother With Drivers?

- Random Info

DISCLAIMER

PRODUCTS & VULNERABILITIES

- Generic Driver Design

- Products & Vulnerabilities

- Vulnerability Matrix

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.*

The self-aggrandising endorsement of shoddily implemented 'security' software by self proclaimed 'expert' 'security' Companies and the UK Government who turn a blind eye to its use.

FAQ - 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 be embarrassed.

FAQ - 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 be embarrassed.

Citrix/Cisco - Deterministic Network Extender (DNE) & 95%+ Win32 VPN clients as a corollary.

```
82.108.142.194 - - "GET /files/exploits/dne2000-call.exe HTTP/1.1" 404 299
```

```
lorenz: mu-b$ whois 82.108.142.194 | grep netname
```

```
netname: NGS
```

FAQ - 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 be embarrassed.

Authentium, Inc SafeCentral & Information Risk Management’s (IRM) “world-renowned security testing team [...] evaluate[d] SafeCentral” [1]. Authentium, Inc were “ecstatic to see that SafeCentral met or exceeded every claim, and indeed is ‘certified’ to provide true privacy when transacting online” [1].



FAQ - 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 be embarrassed.

To find out the truth of Information Risk Management's 'certifi[cation]', visit <http://www.digit-labs.org/files/otherstuff/unsafecentral/>.



FAQ - WHY BOTHER?

- ▶ To prove the following,
- ▶ Thesis #1: “Third Party Windows Kernel drivers are **really** terrible.”
- ▶ Thesis #2: ‘Sales pitches’ and slogans are little more than blatant self-adulation, in the best-case; outright propaganda and lies, in the worst-case.
- ▶ Thesis #3: The first and second theses are so obviously **true**, it takes a really “good education” not to see it.
- ▶ Thesis #4: No matter how trivial any implementation is to break, the fact that it is breakable will elicit **no** response from vendors or otherwise.

FAQ - WHY BOTHER?

- ▶ To prove the following,
- ▶ Thesis #1: “Third Party Windows Kernel drivers are **really** terrible.”
- ▶ Thesis #2: ‘Sales pitches’ and slogans are little more than blatant self-adulation, in the best-case; outright propaganda and lies, in the worst-case.
- ▶ Thesis #3: The first and second theses are so obviously **true**, it takes a really “good education” not to see it.
- ▶ Thesis #4: No matter how trivial any implementation is to break, the fact that it is breakable will elicit **no** response from vendors or otherwise.

FAQ - WHY BOTHER?

- ▶ To prove the following,
- ▶ Thesis #1: “Third Party Windows Kernel drivers are **really** terrible.”
- ▶ Thesis #2: ‘Sales pitches’ and slogans are little more than blatant self-adulation, in the best-case; outright propaganda and lies, in the worst-case.
- ▶ Thesis #3: The first and second theses are so obviously **true**, it takes a really “good education” not to see it.
- ▶ Thesis #4: No matter how trivial any implementation is to break, the fact that it is breakable will elicit **no** response from vendors or otherwise.

FAQ - WHY BOTHER?

- ▶ To prove the following,
- ▶ Thesis #1: “Third Party Windows Kernel drivers are **really** terrible.”
- ▶ Thesis #2: ‘Sales pitches’ and slogans are little more than blatant self-adulation, in the best-case; outright propaganda and lies, in the worst-case.
- ▶ Thesis #3: The first and second theses are so obviously **true**, it takes a really “good education” not to see it.
- ▶ Thesis #4: No matter how trivial any implementation is to break, the fact that it is breakable will elicit **no** response from vendors or otherwise.

FAQ - WHY BOTHER?

- ▶ To prove the following,
- ▶ Thesis #1: “Third Party Windows Kernel drivers are **really** terrible.”
- ▶ Thesis #2: ‘Sales pitches’ and slogans are little more than blatant self-adulation, in the best-case; outright propaganda and lies, in the worst-case.
- ▶ Thesis #3: The first and second theses are so obviously **true**, it takes a really “good education” not to see it.
- ▶ Thesis #4: No matter how trivial any implementation is to break, the fact that it is breakable will elicit **no** response from vendors or otherwise.

FAQ - WHY BOTHER?

- ▶ If our theses hold,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
 - suggestions as to what Information Risk Management's (IRM) "world-renowned security testing team" members were missing are always welcome.
- ▶ Kernel hacking is interesting and fun! and easy given the above,
 - "Hello we are researchers that look for holes in your OS. We have found some, but guess what we already told people how to exploit them." The researchers should be arrested for not notifying Apple of the potential risk, so they would have time to patch the vulnerability [sic]."
 - Kernel exploits aren't worth much on the open market, but 'backdoored' full-disk encryption bootblocks are.

FAQ - WHY BOTHER?

- ▶ If our theses hold,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
 - suggestions as to what Information Risk Management's (IRM) "world-renowned security testing team" members were missing are always welcome.
- ▶ Kernel hacking is interesting and fun! and easy given the above,
 - ""Hello we are researchers that look for holes in your OS. We have found some, but guess what we already told people how to exploit them." The researchers should be arrested for not notifying Apple of the potential risk, so they would have time to patch the vulnerability [*sic*]."
 - Kernel exploits aren't worth much on the open market, but 'backdoored' full-disk encryption bootblocks are.

FAQ - WHY BOTHER?

- ▶ If our theses hold,
 - if it takes longer than an hour to find a bug, your either blind or doing something wrong.
 - suggestions as to what Information Risk Management's (IRM) "world-renowned security testing team" members were missing are always welcome.
- ▶ Kernel hacking is interesting and fun! and easy given the above,
 - ""Hello we are researchers that look for holes in your OS. We have found some, but guess what we already told people how to exploit them." The researchers should be arrested for not notifying Apple of the potential risk, so they would have time to patch the vulnerability [*sic*]."
 - Kernel exploits aren't worth much on the open market, but 'backdoored' full-disk encryption bootblocks are.

FAQ - WHY BOTHER WITH DRIVERS?

- ▶ In software encryption, the driver **is** the implementation!
 - attacking the drivers is a much more likely attack vector than the much publicised “Cryogenically frozen RAM bypasses all disk encryption methods” [2].
- ▶ A potentially unhealthy personal interest in cryptography/cryptographic implementations,
 - particularly those of ‘interesting’ or ‘unknown’ origin, hence ‘unhealthy’.

FAQ - WHY BOTHER WITH DRIVERS?

- ▶ In software encryption, the driver **is** the implementation!
 - attacking the drivers is a much more likely attack vector than the much publicised “Cryogenically frozen RAM bypasses all disk encryption methods” [2].
- ▶ A potentially unhealthy personal interest in cryptography/cryptographic implementations,
 - particularly those of ‘interesting’ or ‘unknown’ origin, hence ‘unhealthy’.

RANDOM INFO

- ▶ Research commenced November, 2007
 - very slow going!
 - I don't have the time (fortunately for the vendors)
- ▶ First product 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 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



"[listen], I have made alot of money out of selling DESlock. [...] we get alot of threats, emails and alike, how do we know you are not an eastern european terrorist?"
- David Tomlinson, Director

RANDOM INFO



“ohhh you must be the bot farmer that threatened to down our web-site?”

- David Tomlinson, Director

(whilst impersonating a salesman @Infosec '09)

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 ~~s~~ 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 ~~s~~ 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;” [3] (“3.2.7 Changes [...] - Updated the Licence agreement and Patent information” [4]).

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

PRODUCTS & VULNERABILITIES

DESlock⁺

SOPHOS

SecurStar

COMPUTER

SECURITY

 **Jetico** Protection made perfect.

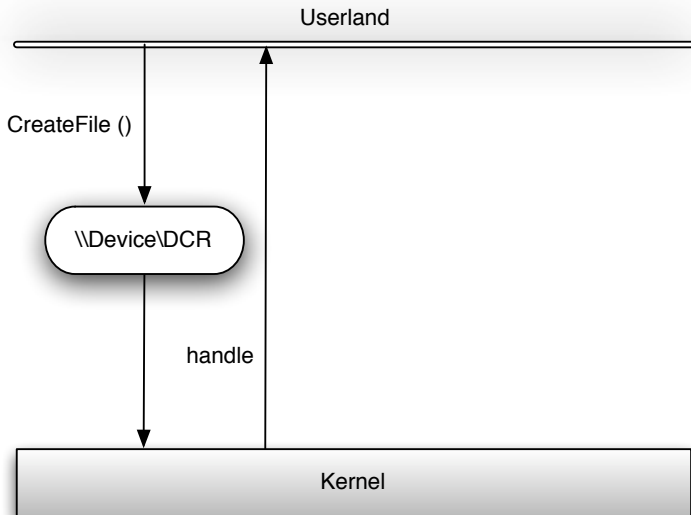
#becrypt



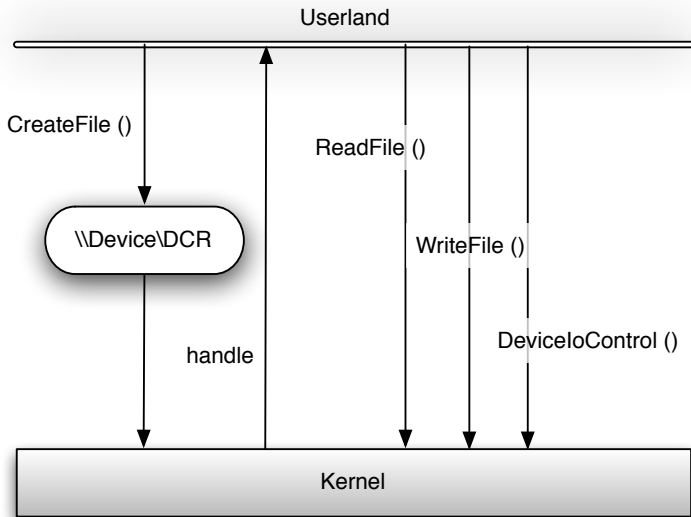
PRODUCTS & VULNERABILITIES

- ▶ ... but first a little background,
 - simple and generic driver design.
- ▶ bugs categorised as per “Common Driver Reliability Issues” [5].

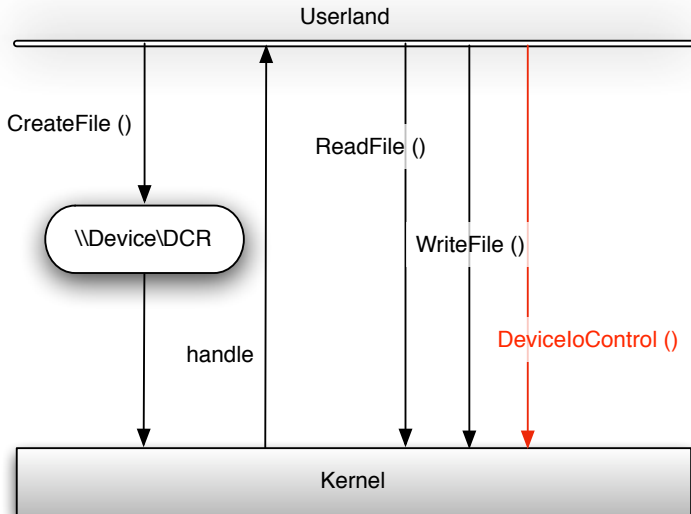
GENERIC DRIVER DESIGN



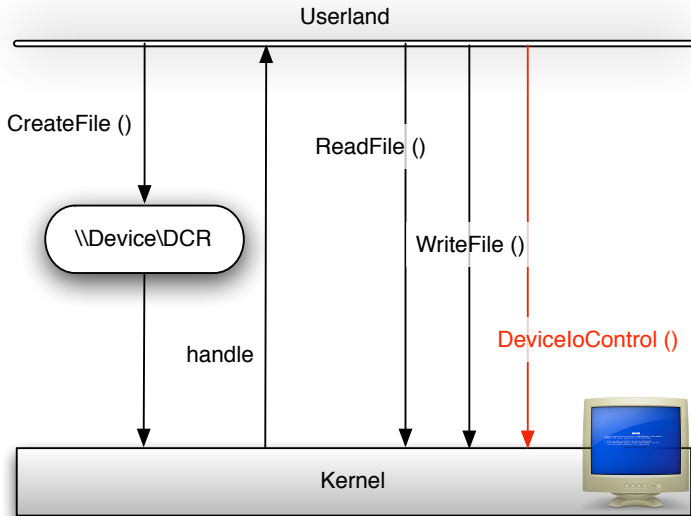
GENERIC DRIVER DESIGN



GENERIC DRIVER DESIGN



GENERIC DRIVER DESIGN



DEVICEIOCONTROL FUNCTION

► DeviceIoControl Function

Sends a control code directly to a specified device driver, causing the corresponding device to perform the corresponding operation.

```
BOOL WINAPI DeviceIoControl(  
    __in        HANDLE hDevice,  
    __in        DWORD dwIoControlCode,  
    __in_opt    LPVOID lpInBuffer,  
    __in        DWORD nInBufferSize,  
    __out_opt   LPVOID lpOutBuffer,  
    __in        DWORD nOutBufferSize,  
    __out_opt   LPDWORD lpBytesReturned,  
    __inout_opt LPOVERLAPPED lpOverlapped  
);
```

1. DESLOCK⁺

- ▶ DESlock⁺ v3.2.7/4.1.10
- ▶ 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” [6], Director: “David Tomlinson”,
 - Data Encryption Systems Ltd, founded by “Len Jones” [6] who “[is] ex-Navy Communications, then GCHQ” [6] in 1985.



DESlock⁺



1. DESLOCK⁺

- ▶ DESlock⁺ v3.2.7/4.1.10
- ▶ 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" [6], Director: "David Tomlinson",
 - Data Encryption Systems Ltd, founded by "Len Jones" [6] who "[is] ex-Navy Communications, then GCHQ" [6] in 1985.

DESlock⁺



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 screenshot displays a Windows command prompt window and the Windows Task Manager. The command prompt shows 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 Guest.

Command Prompt Output:

```

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:\>
  
```

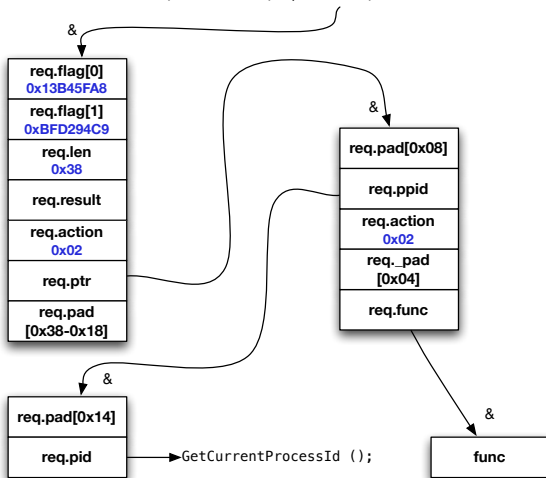
Windows Task Manager - Processes Tab:

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
msdtc.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

Windows Task Manager Summary: Processes: 34 | CPU Usage: 5% | Commit Charge: 121M / 1881M

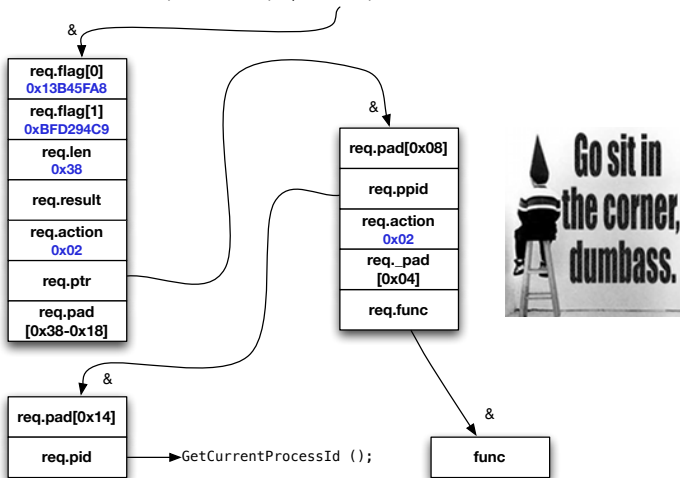
USER-MODE ADDRESSES IN KERNEL-MODE CODE

```
DeviceIoControl (... , 0x80012010, lpInbuffer, ...);
```



USER-MODE ADDRESSES IN KERNEL-MODE CODE

```
DeviceIoControl (... , 0x80012010, lpInbuffer, ...);
```



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" [7]
 - 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." [7]
 - 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" [7]
 - 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." [7]
 - 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” [7]
 - 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.” [7]
 - Principle developer is Shaun Hollingworth.



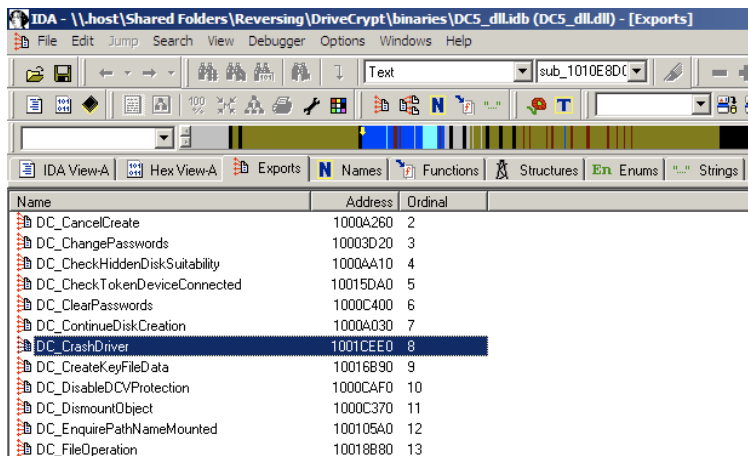
2. DRIVECRYPT

“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).” [8]

Clients



USER-MODE ADDRESSES IN KERNEL-MODE CODE



IDA - \\.\host\Shared Folders\Reversing\DriveCrypt\binaries\DC5_dll.lib (DC5_dll.dll) - [Exports]

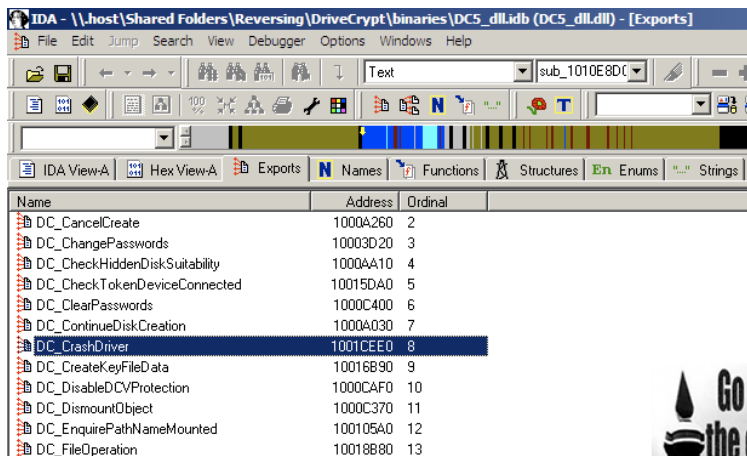
File Edit Jump Search View Debugger Options Windows Help

Text sub_1010E8DC

IDA View-A Hex View-A Exports Names Functions Structures Enums Strings

Name	Address	Ordinal
DC_CancelCreate	1000A260	2
DC_ChangePasswords	10003D20	3
DC_CheckHiddenDiskSuitability	1000AA10	4
DC_CheckTokenDeviceConnected	10015DA0	5
DC_ClearPasswords	1000C400	6
DC_ContinueDiskCreation	1000A030	7
DC_CrashDriver	1001CEE0	8
DC_CreateKeyFileData	10016890	9
DC_DisableDCVProtection	1000CAF0	10
DC_DismountObject	1000C370	11
DC_EnquirePathNameMounted	100105A0	12
DC_FileOperation	10018880	13

USER-MODE ADDRESSES IN KERNEL-MODE CODE



IDA - \\.\host\Shared Folders\Reversing\DriveCrypt\binaries\DC5_dll.lib (DC5_dll.dll) - [Exports]

File Edit Jump Search View Debugger Options Windows Help

Text sub_1010E8DC

IDA View-A Hex View-A Exports Names Functions Structures Enums Strings

Name	Address	Ordinal
DC_CancelCreate	1000A260	2
DC_ChangePasswords	10003D20	3
DC_CheckHiddenDiskSuitability	1000AA10	4
DC_CheckTokenDeviceConnected	10015DA0	5
DC_ClearPasswords	1000C400	6
DC_ContinueDiskCreation	1000A030	7
DC_CrashDriver	1001CEE0	8
DC_CreateKeyFileData	10016890	9
DC_DisableDCVProtection	1000CAF0	10
DC_DismountObject	1000C370	11
DC_EnquirePathNameMounted	100105A0	12
DC_FileOperation	10018880	13



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

Windows Task Manager

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

```

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

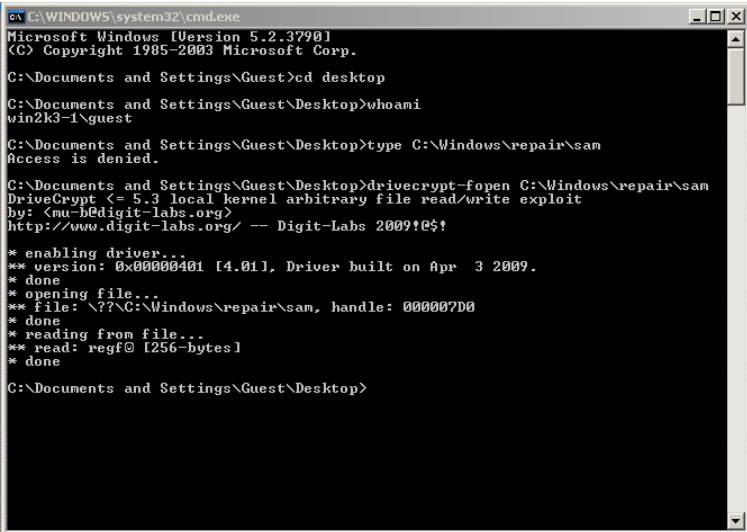
C:\Documents and Settings\Guest\Desktop>
  
```

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

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>
```

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. 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

FAILING TO VALIDATE VARIABLE-LENGTH BUFFERS

The screenshot displays a Windows XP desktop with two windows open. The left window is a command prompt titled 'C:\WINDOWS\system32\cmd.exe'. It shows the execution of a command: `safeguard-pdisk-overflow-v2`. The output indicates a successful overflow of a PrivateDiskM.sys kernel buffer, resulting in system authority. The right window is the Windows Task Manager, showing a list of running processes with columns for Image Name, PID, User Name, CPU, and Mem Usage.

```

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
neill-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!05!

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!05!

* 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:\>

```

Windows Task Manager

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
dpddd.exe	3252	Guest	00	6,064 K
TPAutoConnect.exe	3060	Guest	00	3,672 K
explorer.exe	3032	Guest	00	15,032 K
httsrv.exe	2448		00	3,044 K
wmpvse.exe	1956		00	4,912 K
dhost.exe	1632		00	6,924 K
TPAutoConnSvc.exe	1524		00	3,808 K
svchost.exe	1488		00	4,016 K
VMwareService.exe	1356		00	5,696 K
svchost.exe	1264		00	1,256 K
svchost.exe	1212		00	1,960 K
DCRServ.exe	1192		00	1,336 K
dpasrv.exe	1176		00	1,832 K
msdct.exe	1076		00	4,132 K

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

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>
```

4. SAFEBIT

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



4. SAFEBIT

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



4. SAFEBIT

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



MEMORY LEAKS

The screenshot displays a Windows XP desktop environment. On the left, a command prompt window is open, showing the execution of a program named 'safebit-memleak'. The output indicates that the program is running on a local kernel DoS PoC and is consuming 100% of the CPU and 276 MB of memory. On the right, the Windows Task Manager is open to the Performance tab, which shows the system's resource usage. The CPU usage is at 100%, and the Commit Charge is at 276M / 1881M. The Task Manager also displays various system statistics, including handles, threads, processes, physical memory, and kernel memory usage.

```

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

CPU Usage	100 %
PF Usage	276 MB

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

5. BESTCRYPT - **NEW!**

- ▶ BestCrypt v8.20.5
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista, 7 (32/64-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by Jetico Inc,
 - Founded in 1995, supplied and used “in over 100 countries by government and military agencies, national laboratories” [9].
 - “Jetico’s data protection software was used in the White House by Bill Clintons administration because this fact was published in the U.S. press.” [9]



5. BESTCRYPT - **NEW!**

- ▶ BestCrypt v8.20.5
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista, 7 (32/64-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by Jetico Inc,
 - Founded in 1995, supplied and used “in over 100 countries by government and military agencies, national laboratories” [9].
 - “Jetico’s data protection software was used in the White House by Bill Clintons administration because this fact was published in the U.S. press.” [9]



5. BESTCRYPT - **NEW!**

- ▶ BestCrypt v8.20.5
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista, 7 (32/64-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by Jetico Inc,
 - Founded in 1995, supplied and used “in over 100 countries by government and military agencies, national laboratories” [9].
 - “Jetico’s data protection software was used in the White House by Bill Clintons administration because this fact was published in the U.S. press.” [9]



NULL DEREFERENCES

```
00010EAF mov     eax, [ebp+arg_0] ; arg_0 == NULL
00010EB2 mov     eax, [eax+28h]
00010EB5 mov     ebx, [ebp+Irp]
00010EB8 mov     esi, [ebx+60h]
00010EBB mov     [ebp+arg_0], eax
00010EBE lea     eax, [esi-24h]
00010EC1 mov     edi, eax
00010EC3 push   7
00010EC5 pop    ecx
00010EC6 rep  movsd
00010EC8 mov     byte ptr [eax+3], 0
00010ECC mov     eax, [ebx+60h]
00010ECF sub     eax, 24h
00010ED2 lea     ecx, [ebp+Event]
00010ED5 mov     dword ptr [eax+1Ch], offset sub_10CDC
00010EDC mov     [eax+20h], ecx
00010EDF mov     byte ptr [eax+3], 0E0h
00010EE3 mov     eax, [ebp+arg_0]
00010EE6 mov     ecx, [eax+4] ; DeviceObject
00010EE9 mov     edx, ebx ; Irp
00010EEB call   ds:IoCallDriver
```

6. BECRYPT - **NEW!**

- ▶ BeCrypt Disk Protect v5.5.0
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista, 7 (32/64-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by Bcrypt Ltd,
 - Founded in 2001 by Bernard Parsons and Nigel Lee [10].
 - Used to "protect customers in a number of key Government areas, including Central Government, Defence, Law Enforcement, and Customs and Excise." [10]
 - DE-FACTO standard of UK Government & ATLAS Project.



#becrypt®



6. BECRYPT - **NEW!**

- ▶ BeCrypt Disk Protect v5.5.0
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista, 7 (32/64-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by Becrypt Ltd,
 - Founded in 2001 by Bernard Parsons and Nigel Lee [10].
 - Used to "protect customers in a number of key Government areas, including Central Government, Defence, Law Enforcement, and Customs and Excise." [10]
 - DE-FACTO standard of UK Government & ATLAS Project.

The logo for Becrypt, featuring a purple hash symbol followed by the word "becrypt" in a lowercase, sans-serif font. The hash symbol has a small registered trademark symbol (®) to its upper right.

6. BECRYPT - **NEW!**

- ▶ BeCrypt Disk Protect v5.5.0
- ▶ Supports: Microsoft Windows™ 2000 Professional, XP, Vista, 7 (32/64-bit)
- ▶ Provides: File/Virtual Disk (VDE)/Full Disk Encryption (FDE)
- ▶ Developed by Becrypt Ltd,
 - Founded in 2001 by Bernard Parsons and Nigel Lee [10].
 - Used to “protect customers in a number of key Government areas, including Central Government, Defence, Law Enforcement, and Customs and Excise.” [10]
 - DE-FACTO standard of UK Government & ATLAS Project.

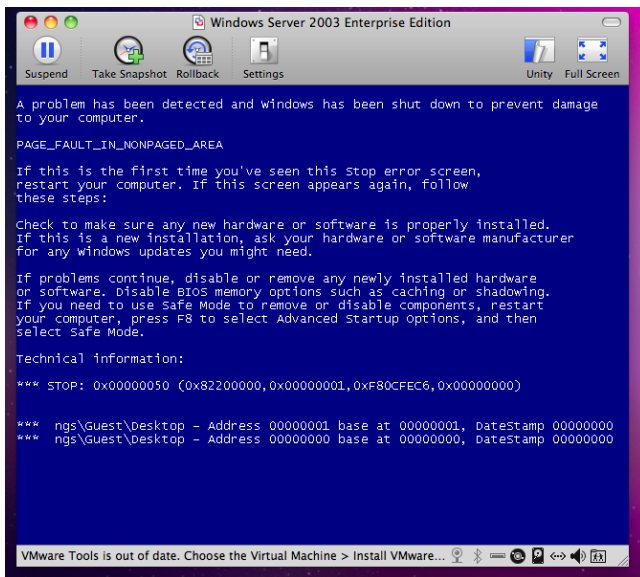
The logo for Becrypt, featuring a purple hashtag symbol followed by the word "becrypt" in a lowercase, sans-serif font. The letter "b" has a small registered trademark symbol (®) to its upper right.

INTEGER OVERFLOWS

```
00018E50 loc_18E50:           ; ecx == lpInBuffer
00018E50 mov     ecx, [ecx]
00018E52 lea   ebx, [ebx+ecx-1]
00018E56 imul  ebx, 0C8h
00018E5C add   ebx, eax
00018E5E mov   [ebp+var_38], ebx
00018E61 push  50524342h      ; Tag
00018E66 push  ebx           ; NumberOfBytes
00018E67 push  0             ; PoolType
00018E69 call  ds:ExAllocatePoolWithTag
00018E6F mov   edi, eax
00018E71 mov   [ebp+var_30], edi
00018E74 test  edi, edi
00018E76 jnz   short loc_18E84
```

```
00018E84 loc_18E84:           ; size_t
00018E84 push  dword_39FF4
00018E8A push  dword_39FF0   ; void *
00018E90 push  edi           ; void *
00018E91 call  memcpy
00018E96 add   esp, 0Ch
00018E99 and   [ebp+var_20], 0
00018E9D mov   eax, [edi]
00018E9F mov   [ebp+var_24], eax
```

INTEGER OVERFLOWS

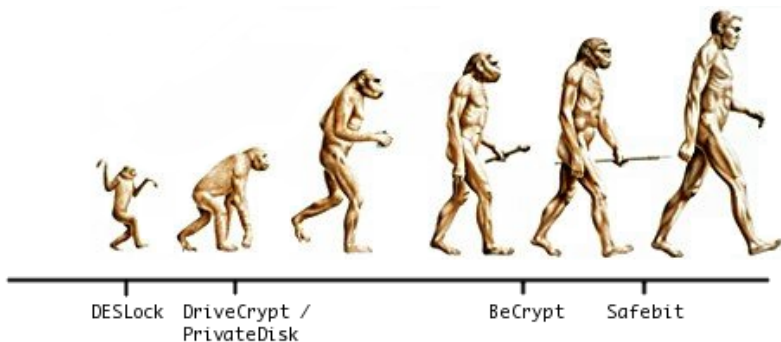


VULNERABILITIES

	DoS	Mem Leak	Logic Flaw	Code Exec
DESlock ⁺				
DriveCrypt				
PrivateDisk				
SafeBit				
BestCrypt				
BeCrypt				

Table: Vulnerability table, severity increasing from left to right.

VULNERABILITIES



CONCLUSIONS

- ▶ Thesis #1 & #2 -
 - 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.
- ▶ Thesis #3 -
 - Obviously holds since only ideologues and salesman believe extra software provides a solution to the problem of too much software/complexity.

CONCLUSIONS

- ▶ Thesis #1 & #2 -
 - 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.
- ▶ Thesis #3 -
 - Obviously holds since only ideologues and salesman believe **extra** software provides a solution to the problem of **too much software/complexity**.

CONCLUSIONS

- ▶ Thesis #4 -
 - The coordinated release of 10+ exploits for numerous FDE/VDE implementations elicited precisely **zero** comment in the 'security' press,
 - and only 2 patches from vendors, both of which were DESlock⁺ (one of which didn't actually fix anything).
- ▶ 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

- ▶ Thesis #4 -
 - The coordinated release of 10+ exploits for numerous FDE/VDE implementations elicited precisely **zero** comment in the 'security' press,
 - and only 2 patches from vendors, both of which were DESlock⁺ (one of which didn't actually fix anything).
- ▶ 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),
 - Check Point Full Disk Encryption
 - Portcullis Guardian Angel - **no copy available!**
 - PGP
 - SafeHouse

CONCLUSIONS

- ▶ Of course, further products are of interest (in order of importance),
 - Check Point Full Disk Encryption
 - Portcullis Guardian Angel - **no copy available!**
 - PGP
 - SafeHouse

CHALLENGE

*[...] 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/> [11]*

REFERENCES I



Authentium Inc.

Testing Confirms SafeCentral Security.

<http://tinyurl.com/37y6an4>, 2009.



ZDNet.

Cryogenically frozen RAM bypasses all disk encryption methods.

<http://tinyurl.com/29ca7t7>, 2008.



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.

REFERENCES II



Microsoft Corporation.

Common Driver Reliability Issues.

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



SecurStar GmbH.

References.

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

REFERENCES III



Jetico Inc.

Mission.

<http://www.jetico.com/mission/>, 2010.



Becrypt Ltd.

About Us - Software Encryption Products.

<http://www.becrypt.com/emea/About-Us>, 2010.



Portcullis Computer Security Ltd.

Guardian Angel celebrates its 20th birthday with the latest CAPS approval.

<http://tinyurl.com/339191k>, 2006.