[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
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...

A Crypto Nerd's Imagination:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

What Would Actually Happen:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
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”.
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”.
Why Bother?

- A personal interest in cryptography/cryptographic implementations,
- Kernel hacking is interesting and fun!
  - sits a-top of Justine Aitels “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 Aitels “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.
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\textsuperscript{TM} 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”,

![DESlock\(^+\) Logo](DESlock.png)
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”,
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”,
1. **DESlock⁺**

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

[DESlock⁺ logo]
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**,
  - 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,
  - 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,
  - 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]
2. DriveCrypt

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

- Encryption modes,
  - 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,**
  - 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”.

![SecurStar Computer Security](image-url)
2. DriveCrypt

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

- Encryption modes,
  - 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”.

SecurStar COMPUTER SECURITY
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).
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).
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).
3. SafeGuard PrivateDisk

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

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

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

- SafeBit (no version numbers!)
- Supports: Microsoft Windows\textsuperscript{TM} 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.
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

Kernel

Userland

\Device\DCR

CreateFile()

handle

REFERENCES
Generic Driver Design

Userland

\Device\DCR
handle
CreateFile ()

Kernel

ReadFile ()

WriteFile ()

DeviceIoControl ()
Generic Driver Design

Kernel

Userland

\Device\DCR

handle

CreateFile ()

ReadFile ()

WriteFile ()

DeviceIoControl ()

REFERENCES
**Generic Driver Design**
DriveCrypt - IOCTL
DriveCrypt - IOCTL

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

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

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-udiptokn
DESlock* <= 4.0.4 local kernel ring0 SYSTEM exploit
by: <num-b@digit-labs.org> http://www.digit-labs.org/ -- Digit-Labs 2009!!!
Usage: deslock-udiptokn <processid to elevate>
C:\>deslock-udiptokn 1795
DESlock* <= 4.0.4 local kernel ring0 SYSTEM exploit
by: <num-b@digit-labs.org> http://www.digit-labs.org/ -- Digit-Labs 2009!!!
* allocated page: 0x55550000 [65536-bytes]
* allocdisk.sys base: 0xF0D5000
* overwrit 160xP005CPU 4-bytes.. done
* jumping.. done
* hmmm, you didn’t STOP the box????
C:\\\whoami
nt authority\system
C:\>
"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
Failing to Validate Variable-Length Buffers
“[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
MEMORY LEAKS

Windows Task Manager

- CPU Usage: 100%
- Page File Usage: 276 MB
- Physical Memory (K):
  - Total: 785824
  - Available: 462100
  - System Cache: 96604
- Commit Charge (K):
  - Total: 282880
  - Limit: 1927124
  - Peak: 284636
- Processes: 29
- CPU Usage: 100%
- Commit Charge: 276M / 1881M
Logic Flaws

![Image of command prompt output]

```cmd
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-i\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!@$!
Usage: safeguard-pdisk-write-header <volume file>
C:\Documents and Settings\Guest\Desktop>safeguard-pdisk-write-header C:\Documents and Settings\Administrator\My Documents\Important.vol
Utimaco Safeware AG - SafeGuard PrivateDisk write header exploit
by: <mu-b@digit-labs.org>
http://www.digit-labs.org/ -- Digit-Labs 2008!@$!
* 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

<table>
<thead>
<tr>
<th></th>
<th>DeviceName</th>
<th>bounded</th>
<th>unbounded</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESlock⁺</td>
<td>DLKFDisk_Control</td>
<td>&gt; 1000000000</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td></td>
<td>DLKPFSD_Device</td>
<td>&gt; 1000000000</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td></td>
<td>DLPCryptCore</td>
<td>&gt; 1000000000</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td></td>
<td>DLPTokenWalter0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DriveCrypt</td>
<td>DCR</td>
<td>&lt; 4096</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td></td>
<td>DCVP</td>
<td>&lt; 32</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td>PrivateDisk</td>
<td>PrivateDisk</td>
<td>&gt; 1000000000</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td>SafeBit</td>
<td>hidedir</td>
<td>&lt; 32</td>
<td>&gt; 1000000000</td>
</tr>
<tr>
<td></td>
<td>vdisk</td>
<td>&lt; 32</td>
<td>&gt; 1000000000</td>
</tr>
</tbody>
</table>

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 $\geq$ 10, OpenSolaris installation on a machine with a hardware crypto device, you’re probably already owned.
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 $\geq$ 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 $\geq 10$, 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 CESG LOGFIRE algorithm. LOGFIRE is the new CESG one way password encryption algorithm that cannot be reverse engineered.
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 CESG LOGFIRE algorithm. LOGFIRE is the new CESG one way password encryption algorithm that cannot be reverse engineered.
REFERENCES I

Data Encryption Systems Ltd.
DESlock EULA.

Data Encryption Systems Ltd.
DESlock Release Note.

D. Tomlinson.
David Tomlinson Ses Gov Technology.

SecurStar GmbH.
About SecurStar.
REFERENCES II

- **SecurStar GmbH.**
  References.

- **Microsoft Corporation.**
  Common Driver Reliability Issues.

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