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

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/un safecentral/.
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, you’re 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”.
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”.
“[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
"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.
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/](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;” [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
Products & Vulnerabilities

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

Diagram showing the interaction between Userland and Kernel. The diagram includes:
- Userland
- Kernel
- `CreateFile()` function
- `\Device\DCR`
- `handle`

The diagram illustrates how a file operation is performed from Userland to Kernel.
**GENERIC DRIVER DESIGN**

```
\Device\DCR
handle
CreateFile ()
ReadFile ()
WriteFile ()
DeviceIoControl ()
```
**Generic Driver Design**

- **Kernel**
- **Userland**
  - `CreateFile()`
  - `DeviceIoControl()`
  - `ReadFile()`
  - `WriteFile()`
  - `\Device\DCR`
  - Handle

This diagram illustrates the interaction between the Kernel and Userland, with specific functions and a device handle. The `DeviceIoControl()` function is highlighted, indicating a key operation within this design.
**Generic Driver Design**

```
\Device\DCR
handle
CreateFile ()
ReadFile ()
WriteFile ()
DeviceIoControl ()
```
DeviceIoControl Function

- DeviceIoControl Function

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

```c
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”,
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”,
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”,
“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

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:\\whoami
win2k3-1\guest
C:\\deglack-udlptokn
DESl0ck* <= 4.0.4 local kernel ring0 SYSTEM exploit
dby: <www-digit-labs.org>/ -- Digit-Labs 2009!!$
Usage: deslock-udlptokn <processid to elevate>
C:\\\deglack-udlptokn 1795
DESl0ck* <= 4.0.4 local kernel ring0 SYSTEM exploit
dby: <www-digit-labs.org>/ -- Digit-Labs 2009!!$
* allocated page: 0x55550000 [65536 bytes]
* dlhfisk.sys base: 0x7005000
* overwriting 0x7005000cpu 4-bytes!!! done
* jumping.. done
* hmmm, you didn’t STOP the box????
C:\\\whoami
nt authority\system
C:\\>
DeviceIoControl (.., 0x80012010, lpInbuffer, ...);

GetCurrentProcessId ();
User-Mode Addresses in Kernel-Mode Code

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

GetCurrentProcessId ();

func
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]
User-Mode Addresses in Kernel-Mode Code
## User-Mode Addresses in Kernel-Mode Code

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Ordinal</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC_CancelCreate</td>
<td>1000A260</td>
<td>2</td>
</tr>
<tr>
<td>DC_ChangePasswords</td>
<td>10003D20</td>
<td>3</td>
</tr>
<tr>
<td>DC_CheckHiddenDiskSuitability</td>
<td>1000A10</td>
<td>4</td>
</tr>
<tr>
<td>DC_CheckTokenDeviceConnected</td>
<td>10015DA0</td>
<td>5</td>
</tr>
<tr>
<td>DC_ClearPasswords</td>
<td>1000C400</td>
<td>6</td>
</tr>
<tr>
<td>DC_ContinueDiskCreation</td>
<td>1000A030</td>
<td>7</td>
</tr>
<tr>
<td><strong>DC_CrashDriver</strong></td>
<td><strong>1001CEE0</strong></td>
<td><strong>8</strong></td>
</tr>
<tr>
<td>DC_CreateKeyFileData</td>
<td>10016B90</td>
<td>9</td>
</tr>
<tr>
<td>DC_DisableDCVProtection</td>
<td>1000CAF0</td>
<td>10</td>
</tr>
<tr>
<td>DC_DismountObject</td>
<td>1000C370</td>
<td>11</td>
</tr>
<tr>
<td>DC_EnquirePathNameMounted</td>
<td>100105A0</td>
<td>12</td>
</tr>
<tr>
<td>DC_FileOperation</td>
<td>10018B80</td>
<td>13</td>
</tr>
</tbody>
</table>
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
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

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-b@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. 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).
Failing to Validate Variable-Length Buffers
LOGIC FLAWS
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<sup>TM</sup> 2000 Professional, XP, Vista (32-bit)
- Provides: File/Virtual Disk Encryption (VDE)
- Developed by SafeBit.
MEMORY LEAKS
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 Clinton’s 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

```assembly
00010EAF mov  eax, [ebp+arg_0] ; arg_0 == NULL
00010EB2 mov  eax, [eax+28h]
00010EB5 mov  ebx, [ebp+Irps]
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
00010EC9 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:IoifCallDriver
```
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.
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.
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.
INTEGER OVERFLOWS
A problem has been detected and Windows has been shut down to prevent damage to your computer.

**PAGE_FAULT_IN_NONPAGED_AREA**

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

**Technical information:**

```plaintext
*** STOP: 0x00000050 (0x82200000, 0x0000001, 0xF80CFEC6, 0x00000000)

*** ngs\Guest\Desktop - Address 00000001 base at 00000001, DateStamp 00000000
*** ngs\Guest\Desktop - Address 00000000 base at 00000000, DateStamp 00000000
```

VMware Tools is out of date. Choose the Virtual Machine > Install VMware...
## Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>DoS</th>
<th>Mem Leak</th>
<th>Logic Flaw</th>
<th>Code Exec</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESlock+</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DriveCrypt</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>PrivateDisk</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SafeBit</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>BestCrypt</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>BeCrypt</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

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

DESLock  DriveCrypt / PrivateDisk  BeCrypt  Safebit
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
[...] 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

Authentium Inc.
Testing Confirms SafeCentral Security.

ZDNet.
Cryogenically frozen RAM bypasses all disk encryption methods.

Data Encryption Systems Ltd.
DESlock EULA.

Data Encryption Systems Ltd.
DESlock Release Note.
REFERENCES II


REFERENCES III

Jetico Inc.
Mission.

Becrypt Ltd.
About Us - Software Encryption Products.

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