

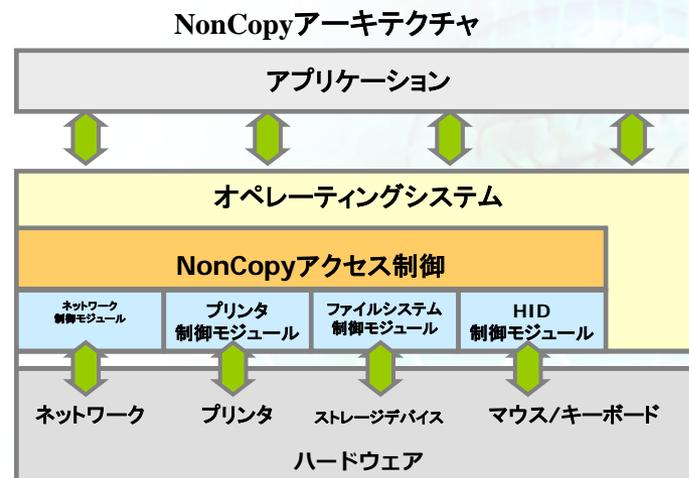
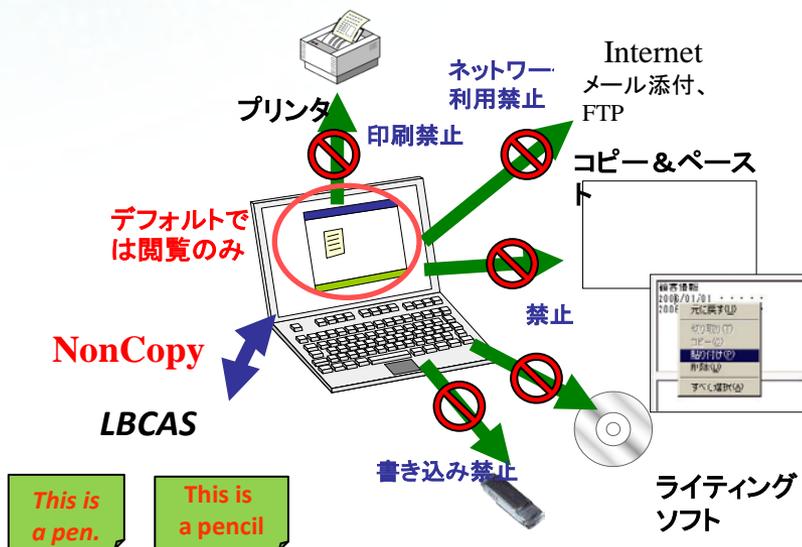
Bitvisorをベースとした 既存Windowsのドライバメモリ保護

須崎 有康、八木 豊志樹、古原 和邦、
石山 智祥、村上 純一、鵜飼 裕司

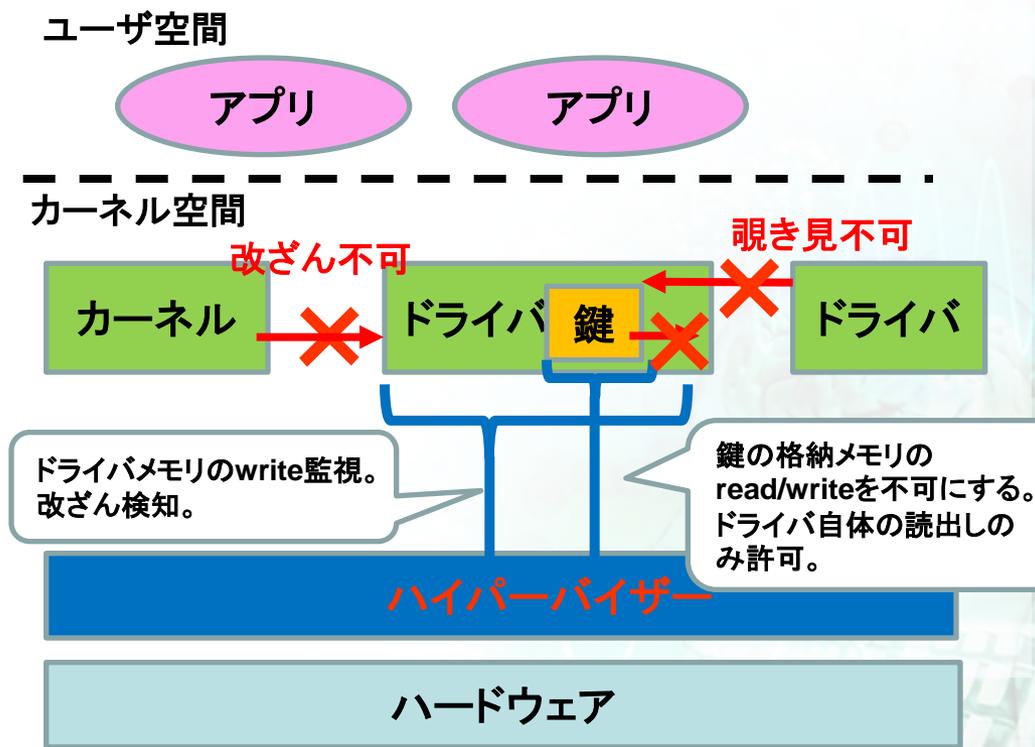
(独)産業技術総合研究所 セキュアシステム研究部門
フォティーンフォティ技術研究所

- 背景
 - ドライバメモリを守る理由
- ドライバメモリ保護に必要な技術
 - インストール済みのOSの外部から挿入可能なハイパーバイザー
 - VM Introspection
 - 関連研究
- 現状
 - メモリの保護はStealth breakpointsを活用
- 改善計画
- まとめ

- クライアントおよびサーバ双方からの情報漏えいを防止するアクセス制御技術の研究開発
 - 総務省による戦略的情報通信研究開発推進制度(SCOPE) H23-25
 - 産総研、サイエンスパーク、(FFRI)
- Windows上でアクセス制御を行うNonCopy (サイエンスパーク社製品)を活用
 - NonCopyはドライバによりファイルコピー、Screen Cut&Paste、印刷などを行うWindows APIを抑制する。



- ドライバの中に暗号鍵がある。ドライバは長時間メモリに滞在するため、漏えいの危険性がある。
 - メモリに長期滞在するデータの危険性は[Chow, USENIX Sec 04]より指摘されている。
- ハイパーバイザーでOSの下位よりドライバを監視して不正アクセスを防御する。
 - ハイパーバイザーで守ることで、OSをだます攻撃にも対応する。



ドライバメモリ保護に 必要な技術

- ハイパーバイザーに必要な技術
 1. インストール済みのOSに対して外部から挿入可能なハイパーバイザー
 2. VM Introspection
- 関連研究

- 多くのハイパーバイザーは複数OSを1台のマシンで起動するために使われている
 - 例: IaaSクラウド
- 問題点
 - ホストOSが必要
 - 管理ソフトウェアの大規模化
 - VMware ESXiは5.xよりホストOS無しになったが、管理サーバが必要
 - 基本的にデバイスがホストOSの管理下になる
 - VMデバイスモデルが固定
 - デバイスはVM中の仮想デバイスで共有される
 - プレインストールのOSとは異なる
 - Xen, KVM, QEMUはQEMU Deviceモデルが標準

既存のOSへの ハイパーバイザー挿入

- 既存のOSが想定している物理デバイスをVM環境内で提供する必要がある。
 - VMデバイスモデルが同じにできればよい
 - 各PC毎にデバイスをモデルを用意しなければならない
 - VMからデバイスを直接アクセス
 - I/O PassThrough。ハードウェアが限定。ハイパーバイザーでも対応が必要
 - Para-PassThrough。Bitvisorで提供される

Windowsドライバ保護に必要な技術 2(VM Introspection)

- ハイパーバイザーがドライバの動作、メモリ空間を認識する必要がある。
 - 守るべきドライバが組み込まれたことの認識
 - Linux: create_module, init_module システムコールなど
 - Windows: NtLoadDriver システムコールなど。
 - 守るべきメモリ空間の認識
 - 各種の実装あり。

VM Introspection

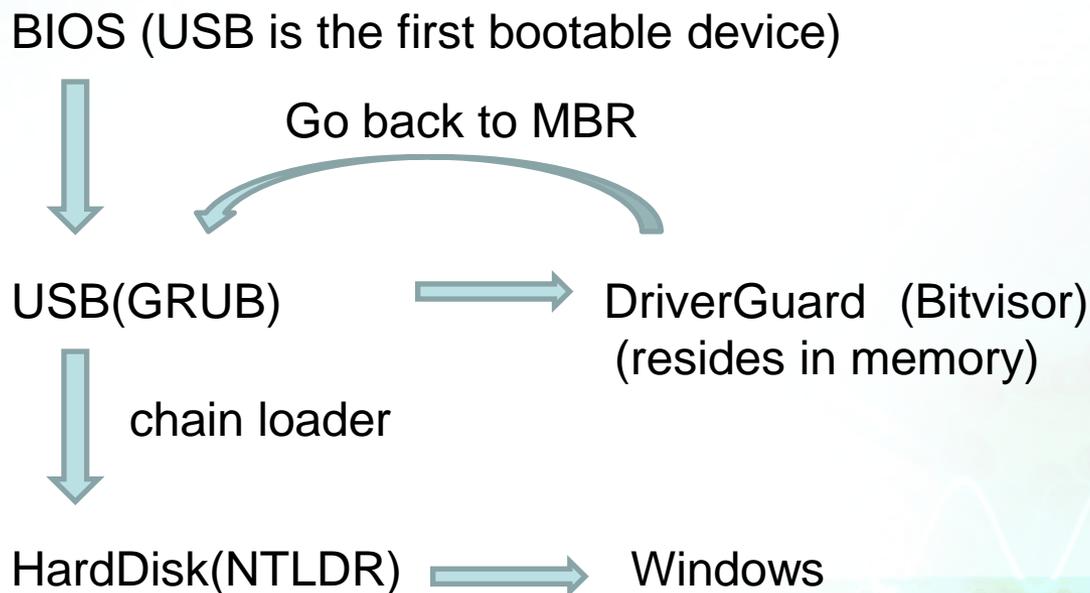
- **Ether** [GITech Wenke Leeグループ, CCS'08]
 - XenベースのVM Introspection。オープンソース。対象OSはWindows XP SP2
 - <http://ether.gtisc.gatech.edu/source.html>
- **GreenKiller** [FFRI Junichi Murakami, BlackHat'08]
 - BitvisorベースのVM Introspection。対象OSはWindows XP SP3
- **Alkanet** [立命館大学 大月さん、毛利先生, CSS'11]
 - Bitvisorベースのシステムコールトレース。対象OSはWindows XP SP3

- Nooks [M.Swift, SOSPP'03]
 - 障害時にリカバリーがメイン。
- HUKO[NDSS'11]
 - 信頼できないドライバの保護。ドライバ用のメモリ空間とカーネル用のメモリ空間の分離。CR3の値を変える。
- Windows7の Driver Isolation
 - プリンタがメイン。
- OS2
 - IA32アーキテクチャの4つのリング構造でカーネルとデバイスドライバを分ける。

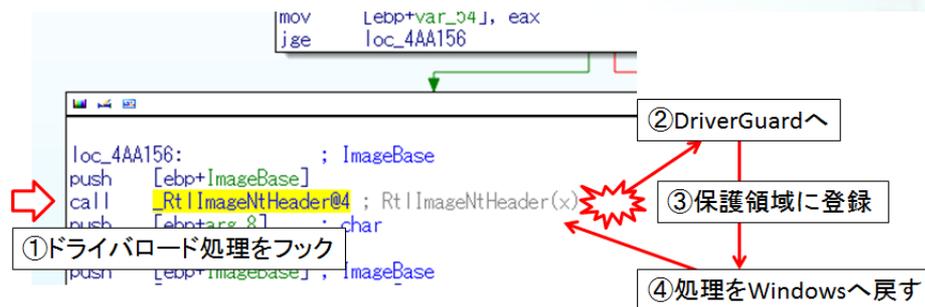
ドライバメモリを保護する ハイパーバイザー

- 既存OSへの挿入可能性、VM Introspectionを考慮してGreen Killerベースで開発。
 - **DriverGuard と命名。**
- 動作手順
 - USBからハイパーバイザーを起動後、ハードディスクOSの起動
 - ハイパーバイザーのドライバ認識
 - 保護するメモリ領域の認識
 - 攻撃に対する防衛
 - Stealth Breakpoints技術

- ハードディスクにインストール済みのOSに対して、起動時にDriverGuardを挿入する
 - Chain load技術
 - 類似の技術にはLinuxのkexecシステムコールを使ったkbootがある。PS3Linuxで使われていた。



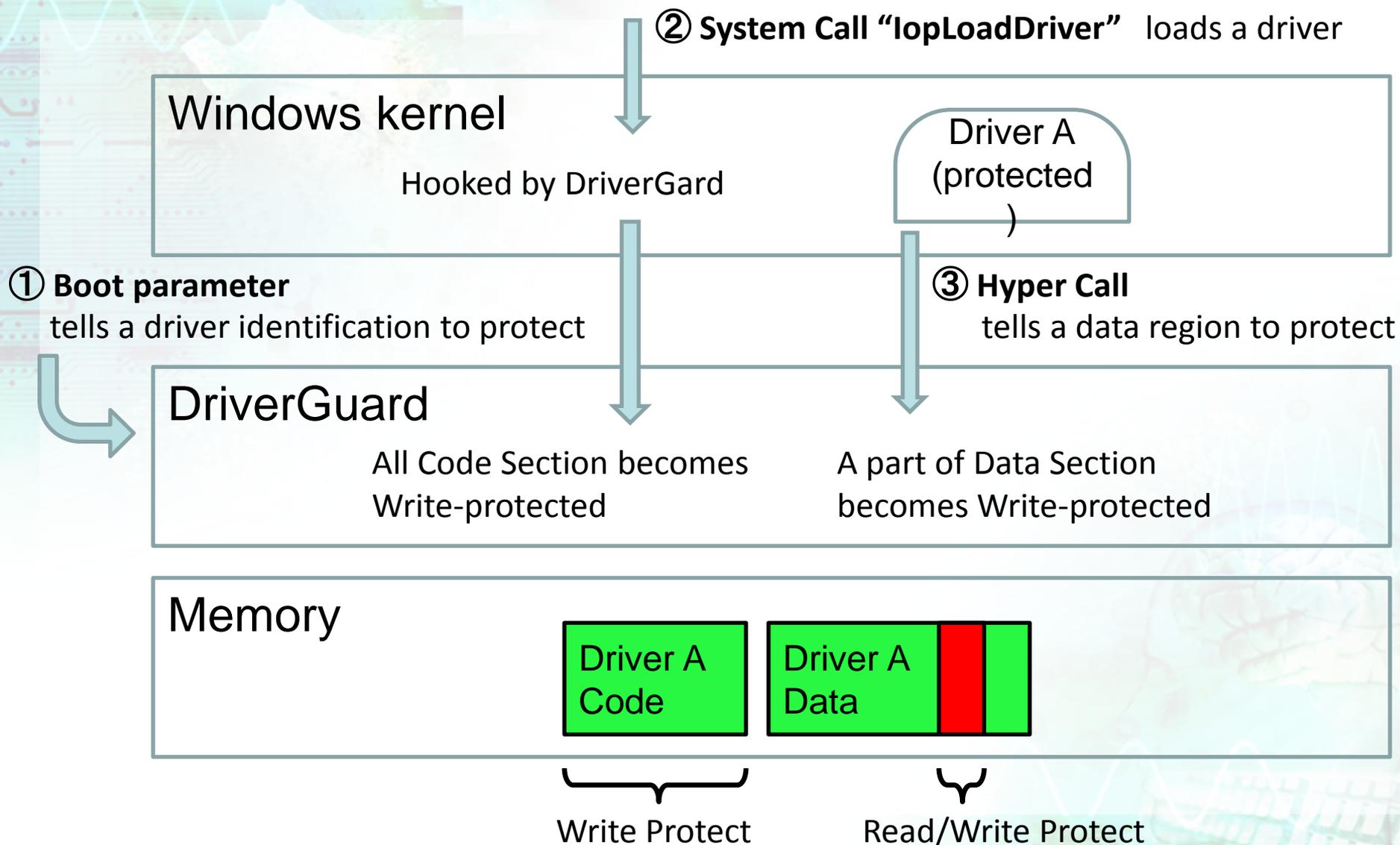
- DriverGuardではGreenKillerによるWindowsの解析を利用
- 起動時に守るべきドライバの認識
 - ドライバのIDとしてはタイムスタンプをIDとする
 - ドライバはntkrnlpa.exeのLoadDriver関数を通るため、この関数をフック。
 - フックはint 03H (0xCC)命令例に置き換えることで例外をDriverGuardに通知。



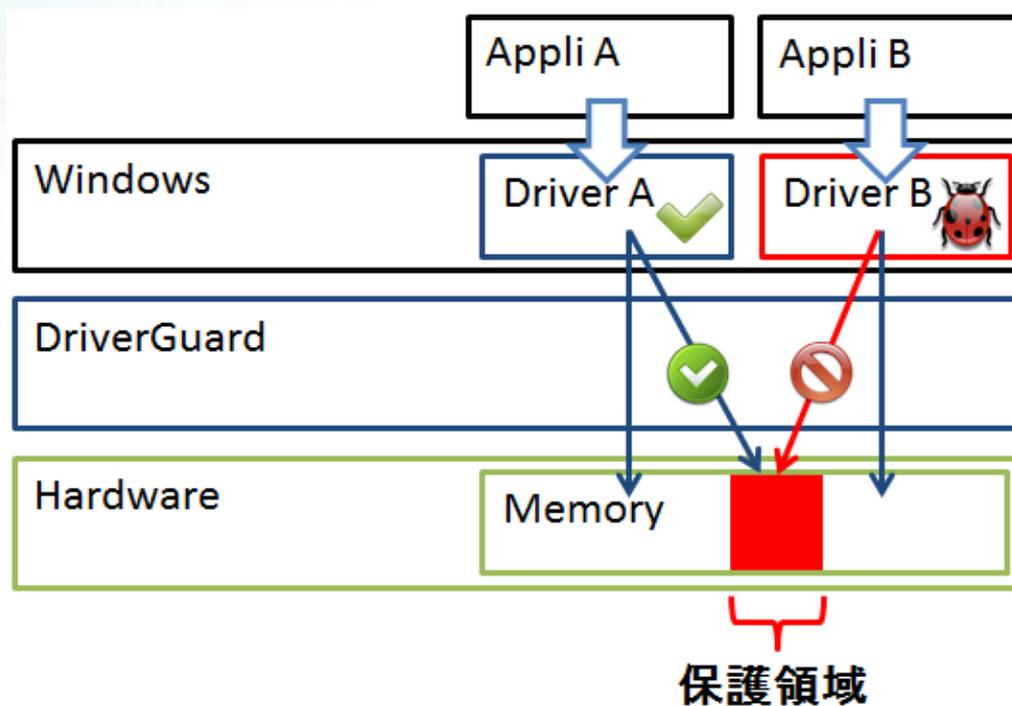
現在の実装 2/2

- 守るべきメモリ空間はドライバからのハイパーコールで通知
 - ドライバの改変が必要
- 現在対象のNonCopyではExAllocatePoolWithTagで保護対象のメモリを確保していたが、他の領域で保護対象にできる

保護手順



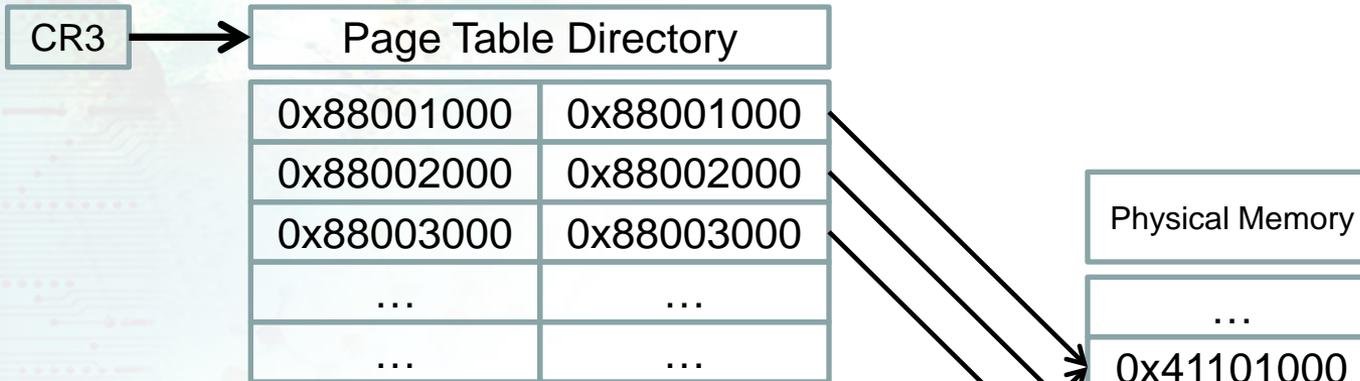
- 本来のドライバ以外から攻撃を検出
 - カーネル内で同じメモリ空間のドライバからの攻撃



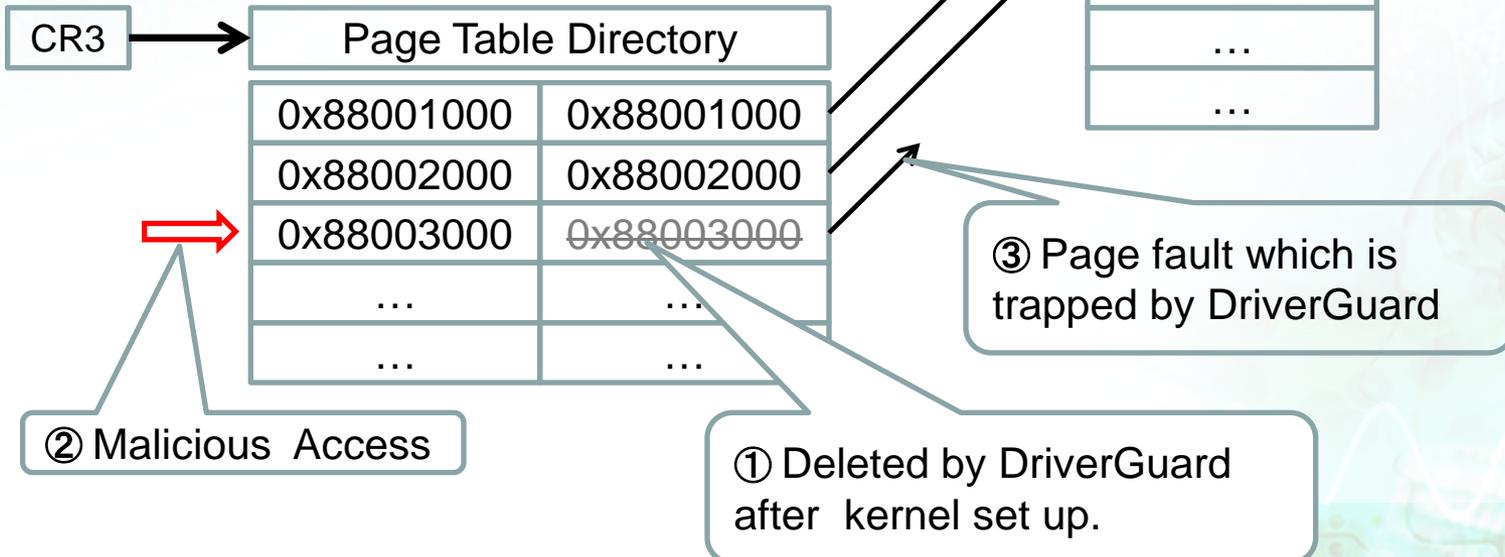
- **Stealth Breakpoints [ACSAC'05]の技術の活用**
 - INT 03H (0xCC)に置き換えずにBreakpointの機能を実現。メモリ内容を変えないため、攻撃者から検出され難い。
 - ハイパーバイザーが守るべきメモリを管理するページテーブルを空にし、アクセスが起こるたびにページフォルトを起こす。
 -
 - ページフォルトをハイパーバイザーが捉え、正しいアクセスか検証。問題が無ければアクセスを許す。
 - **問題点**
 - 保護対象は4KBページ単位。
 - 保護対象外でも4KBページ内のアクセスは全て検証されてしまう。

Stealth Breakpoints

Process A (Normal)



Process B (Malicious)



攻撃検出後の動作

- 問題を起こしたプロセスをとらえ、無限ループにする
 - Low IRQL(Interrupt ReQuest Level)で無限ループのすることにより、他のプロセスは実行可能。但し、現状ではCPUをかなり食うので他のプロセスは遅くなる。

動作例1

ログ表示ツールによる
Bitvisor(DriverGuard)
の動作確認

```

C:\> cd driverguard\#dbesh.exe
> log
Starting BitVisor...
Copyright (c) 2007, 2008 University of Tsukuba
All rights reserved.
4183866368 bytes (3990 MiB) RAM available.
VMM will use 0xB5400000-0xBD400000 (128 MiB).
ACPI DMAR found.

.....
Disable ACPI S3
ACPI MCFG cleared.
Initing Virtual Ethernet (VE) for VPN Client Module...
Virtual Ethernet (VE): Ok.
Module not found.
Processor 0 (BSP)
SVM is not available.
Processor 0 2261005032 Hz
Loading drivers.
AES/AES-XTS Encryption Engine initialized (AES=openssl)
Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.
PCI: finding devices ..... 25 devices found
Starting a virtual machine.
gkiller_do_movcr0:185: set WP-bit on CRO initial time
get_ntoskrnl_base:383:
-- more --

```

イメージ名	ユーザー名	C...	メモリ使..
alg.exe	LOCAL SERVICE	00	4,292 K
conime.exe	rcis	00	5,216 K
dbesh.exe	rcis	00	1,272 K
wsontfy.exe	SYSTEM	00	3,408 K
SPWATCHI.exe		00	8,448 K
SynTPLpr.exe		00	4,088 K
ctfmon.exe		00	4,744 K
TPOSDSVC.exe		00	7,160 K
TPOSDSVC.exe		00	7,184 K
wuauclt.exe		00	7,776 K
hkcmd.exe		00	6,468 K
taskmgr.exe		02	7,140 K
SUService.exe		00	12,128 K
igfxtray.exe		00	4,748 K
acs.exe		00	7,648 K
TPHKSVC.exe		00	5,840 K
tphkload.exe		00	5,184 K
svchost.exe		00	4,504 K
virtscrl.exe		00	5,804 K
spoolsv.exe		00	5,488 K
NCPMUI.exe		00	8,316 K
tvtsched.exe		00	6,128 K
svchost.exe		00	4,604 K
NCTRAY.exe		00	11,804 K
svchost.exe		00	4,324 K
tvt_reg_monitor_sv...		00	3,728 K
Application VISTA ...		00	4,564 K
s Resources, Inc.		00	20,780 K
igfxpers.exe		00	5,552 K
svchost.exe		00	4,228 K
NCUPSVC.exe		00	5,552 K
scheduler_proxy.e...		00	4,228 K
SynTPEnh.exe		00	8,888 K
wmiprvse.exe		00	8,844 K
svchost.exe		00	5,008 K
svchost.exe		00	5,708 K
ibmpmsvc.exe		00	2,196 K
lsass.exe		00	6,884 K
services.exe		00	4,372 K
winlogon.exe		00	2,676 K
NCAGSVC.exe		00	19,992 K
TPScorex.exe		00	5,432 K
TPONSCR.exe		00	5,532 K
csrss.exe		02	5,444 K
explorer.exe		00	21,848 K
smss.exe		00	444 K
mounter.exe		00	1,200 K
DWADSVC.exe		00	5,164 K
		02	260 K
ms...		05	28 K

詳細

- Lhaplus ショートカット 1 KB
- bitvisor.elf.OUT OUT ファイル 12,876 KB
- bitvisor.elf.SAFE SAFE ファイル 12,876 KB
- drg_config.exe drg_config ffr
- readme.txt テキストドキュメント 1 KB

コンピュータが危険にさらされている可能性があります。

- 自動更新が無効になっています。
- ウイルス対策ソフトウェアがインストールされていない可能性があります。

問題を解決するには、このバルーンをクリックしてください。

スタート | NonCopy LBCAS デモ | driverguard | C:\> cd driverguard\#dbesh... | 10:56

動作例2

```

C:\>driverguard\%dbgsh.exe
get_ntoskrnl_base:383:
get_ntoskrnl_base:392: VMCS_GUEST_IDTR_BASE: 0x8003f400
get_ntoskrnl_base:396: guest_idt[0x2e].handler: 0x8053f000
get_ntoskrnl_base:399: searching kernel base from: 0x8043f000
gkiller_do_movcr0:187: kernel_base:0x804d9000
init_nt_api:439: image_base=0x804d9000
gkiller_add_pd:497: start:0x804d9000 end:0x806d5380
gkiller_do_movcr0:196: Hooked ExAllocatePool
gkiller_do_movcr0:203: Hooked ExFreePoolWith
gkiller_do_breakpoint:237: called ExAllocate
auth_loading_driver:302: TimeDateStamp:0x480
auth_loading_driver:302: TimeDateStamp:0x4f4
auth_loading_driver:302: TimeDateStamp:0x4ea065a4
auth_loading_driver:302: TimeDateStamp:0x480254ce
auth_loading_driver:302: TimeDateStamp:0x4eadf2a2
gkiller_add_ro:511: start:0xb9b89000 end:0xb9b89424
gkiller_add_pd:497: start:0xb9b89000 end:0xb9b89424

コマンド プロンプト - dgtest.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\rcis>cd %driverguard

C:\driverguard>dgtest.exe
LoadDriver : LoadDriver 'DGTEST.sys'
LoadDriver : Driver loaded.
Load driver completed.
0: end
1: read test
2: write test
>2
addr(0xXXXXXXXX) : 0xb9b89000
  
```

保護アドレスの確認

攻撃ツールからの保護
アドレスへの書き込み

イメージ名	ユーザー名	C...	メモリ使...
acs.exe		00	7,648 K
alg.exe	LOCAL SERVICE	00	4,288 K
cmd.exe	rcis	00	3,456 K
conime.exe	rcis	00	5,260 K
csrss.exe		00	6,772 K
ctfmon.exe		00	4,876 K
dbgsh.exe	rcis	00	1,272 K
dgtest.exe	rcis	00	1,288 K
DWADSVC.exe		00	5,164 K
explorer.exe		00	22,828 K
hkcmd.exe		00	472 K
ibmpmsvc.exe		00	
igfxpers.exe		00	
igfxtray.exe		00	
lsass.exe		00	
mounter.exe		00	
mspaint.exe		00	
NCAGSVC.exe		00	
NCPMUI.exe		00	
NCTRAY.exe		00	
NCUPSVC.exe		00	
scheduler_proxy.e...		00	
services.exe		00	7,128 K
smss.exe		00	444 K
spoolsv.exe		00	5,496 K
SPWATCH1.exe		00	8,448 K
SUService.exe		00	12,128 K
svchost.exe		00	5,696 K
svchost.exe		00	5,020 K
svchost.exe		00	22,092 K
svchost.exe		00	4,316 K
svchost.exe		00	4,612 K
svchost.exe		00	4,504 K
svchost.exe		00	5,008 K
SynTPEnh.exe	SYSTEM	00	8,940 K
SynTPLpr.exe		00	4,096 K
System		00	260 K
System Idle Proce...	SYSTEM	97	28 K
taskmgr.exe		02	7,232 K
tphkload.exe		00	5,184 K
TPHKSVC.exe		00	5,840 K
TPONSCR.exe		00	5,544 K
TPOSDSVC.exe		00	7,192 K
TPOSDSVC.exe		00	7,168 K
TpScrx.exe		00	5,444 K
tvt_reg_monitor_sv...		02	3,728 K
tvtshed.exe		00	6,124 K
utilman.exe		00	5,044 K

攻撃ツールのCPU
攻撃前使用量 (0%)

動作例3

```

C:\>C:\driverguard\%dbgsh.exe
get_ntoskrnl_base:383:
get_ntoskrnl_base:392: VMCS_GUEST_IDTR_BASE: 0x8003f400
get_ntoskrnl_base:396: guest_idt[0x2e].handler: 0x8053f000
get_ntoskrnl_base:399: searching kernel base from: 0x8043f000
gkiller_do_movcr0:187: kernel_base:0x804d9000
init_nt_api:439: image_base=0x804d9000
gkiller_add_pd:497: start:0x804d9000 end:0x806d5380
gkiller_do_movcr0:196: Hooked ExAllocatePool
gkiller_do_movcr0:203: Hooked ExFreePoolWith
gkiller_do_breakpoint:237: called ExAllocate
auth_loading_driver:302: TimeDateStamp:0x480254ce
auth_loading_driver:302: TimeDateStamp:0x4f406000
auth_loading_driver:302: TimeDateStamp:0x4ea065a4
auth_loading_driver:302: TimeDateStamp:0x480254ce
auth_loading_driver:302: TimeDateStamp:0x4eadf2a2
gkiller_add_ro:511: start:0xb9b89000 end:0xb9b89424
gkiller_add_pd:497: start:0xb9b89000 end:0xb9b89424
  
```

保護アドレスの確認

```

C:\>コマンド プロンプト - dgtest.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\rcis>cd %driverguard

C:\driverguard>dgtest.exe
LoadDriver : LoadDriver 'DGTEST.sys'
LoadDriver : Driver loaded.
Load driver completed.
0: end
1: read test
2: write test
>2
addr(0xFFFFFFFF) : 0xb9b89000
  
```

攻撃ツールからの保護
アドレスへの書き込み

イメージ名	ユーザー名	C...	メモリ使...
acs.exe		00	7,652 K
alg.exe	LOCAL SERVICE	00	4,288 K
cmd.exe	rcis	00	3,456 K
conime.exe	rcis	00	5,260 K
csrss.exe		00	6,772 K
ctfmon.exe		00	4,876 K
dbgsh.exe	rcis	00	1,272 K
dgtest.exe	rcis	98	1,292 K
DWADSVC.exe		00	5,164 K
explorer.exe		00	22,824 K
hkcmd.exe		00	5,468 K
ibmpmsvc.exe		00	...
igfxpers.exe		00	...
igfxtray.exe		00	...
lsass.exe		00	...
mouner.exe		00	...
mspaint.exe	rcis	00	...
NCAGSVC.exe		00	...
NCPMUI.exe		00	...
NCTRAY.exe		00	...
NCUPSVC.exe		00	...
scheduler_proxy.e...		00	...
services.exe		00	...
smss.exe		00	...
spoolsv.exe		00	...
SPWATCH1.exe		00	...
SUService.exe		00	...
svchost.exe	SYSTEM	00	...
SynTPEnh.exe		00	...
SynTPLpr.exe		00	...
System		00	...
System Idle Proce...	SYSTEM	00	...
taskmgr.exe		02	7,232 K
tphkload.exe		00	5,184 K
TPHKSVC.exe		00	5,840 K
TPONSCRExe		00	5,544 K
TPOSDSVC.exe		00	7,192 K
TPOSDSVC.exe		00	7,168 K
TpScrx.exe		00	5,444 K
tvt_reg_monitor_sv...		00	3,728 K
tvt sched.exe		00	6,124 K
...		00	5,944 K

攻撃ツールのCPU
 攻撃後使用量
**(98%)Low IRQLに
 よる無限ループ**
 他のアプリも使えま
 すが、遅くなります。

現在DriverGuardの制約事項

- OSはWindowsXP SP3のみ
- BIOSの設定によりマルチプロセッサをDisabled(無効)とする
- OSの設定により仮想メモリ機能を無効の状態とする
- OSの設定によりPSE(Page Size Extension)を無効の状態とする
- 保護領域のアドレス通知をすべて受け取るまでは保護領域は守れない
- OSであるWindowsXP SP3をアップデートした場合は動作を保証できない

- ドライバのIDとしてタイムスタンプは不適切
 - 実装が容易だが、改ざんされる恐れあり。
- ドライバでHyperCallする必要がある
 - ドライバの改良が必要
- 警告確認がCPUの負荷の向上で判り難い
 - ユーザ空間にハイパーバイザーの状態をポーリングする手法も考慮したが、これが改ざんされる(検出漏れ)恐れがある

改良予定

- ドライバの識別子としてドライバコードのSHA1とする
 - ハイパーバイザーでSHA1の計算が必要
- ドライバの守るべき領域をヒープメモリとする
 - ヒープメモリをハイパーバイザーが実行時に検出する必要あり
 - ヒープは頻繁にアクセスされないと想定
- OSと非依存の警告
 - 悪意のあるアクセスを検出した場合、OSと非依存の警告
 - ハイパーバイザーがビープ音を鳴らすことやビデオドライバへの直接警告する
 - Bitvisor 1.3で入った機能。(電通大の大山先生のADvisor)
 - 現状では対象ビデオカードが限定。Intel 945GMはちょっと古い？

- Windowsを対象としたドライバメモリの情報漏えいを防ぐ、DriverGuardの提案
 - Bitvisorベースとすることで、任意のインストール済みOSに対して、起動時にハイパーバイザーを挿入する
 - Driverを理解するためにVM Introspection機能のあるGreenKillerの活用
 - Stealth Breakpointsによるアクセス検出