



Covert Debugging

Circumventing Software
Armoring Techniques

Offensive Computing, LLC

Danny Quist
Valsmith

dquist@offensivecomputing.net

valsmith@offensivecomputing.net



Danny Quist

- Offensive Computing, Cofounder
- PhD Student at New Mexico Tech
- Reverse Engineer
- Exploit Development
- cDc/NSF



Valsmith

- Offensive Computing, Cofounder
- Malware Analyst/Reverse Engineer
- Metasploit Contributor
- Penetration Tester/Exploit developer
- cDc/NSF



Offensive Computing, LLC

- **Community Contributions**
 - Free access to malware samples
 - Largest open malware site on the Internet
 - 350k hits per month
- **Business Services**
 - Customized malware analysis
 - Large malware data-mining / access
 - Reverse Engineering



Introduction

- Debugging Malware is a powerful tool
 - Trace Runtime Performance
 - Monitor API Calls
 - Dynamic Analysis == Automation
- Malware is getting good at preventing it
 - Debugger Detection
 - VM Detection
 - Legitimate Software Pioneered these Techniques



Overview of Talk

- Software Armoring Techniques
- Covert Debugging Requirements
- Dynamic Instrumentation for Debugging
- OS Pagefault Assisted Covert Debugging
- Application – Generic Autounpacking
- Results



Software Armoring

- Packing/Encryption
- VM Detection
- SEH Tricks
- Debugger Detection
- Shifting Decode Frame
- Example: Microsoft's Patchguard

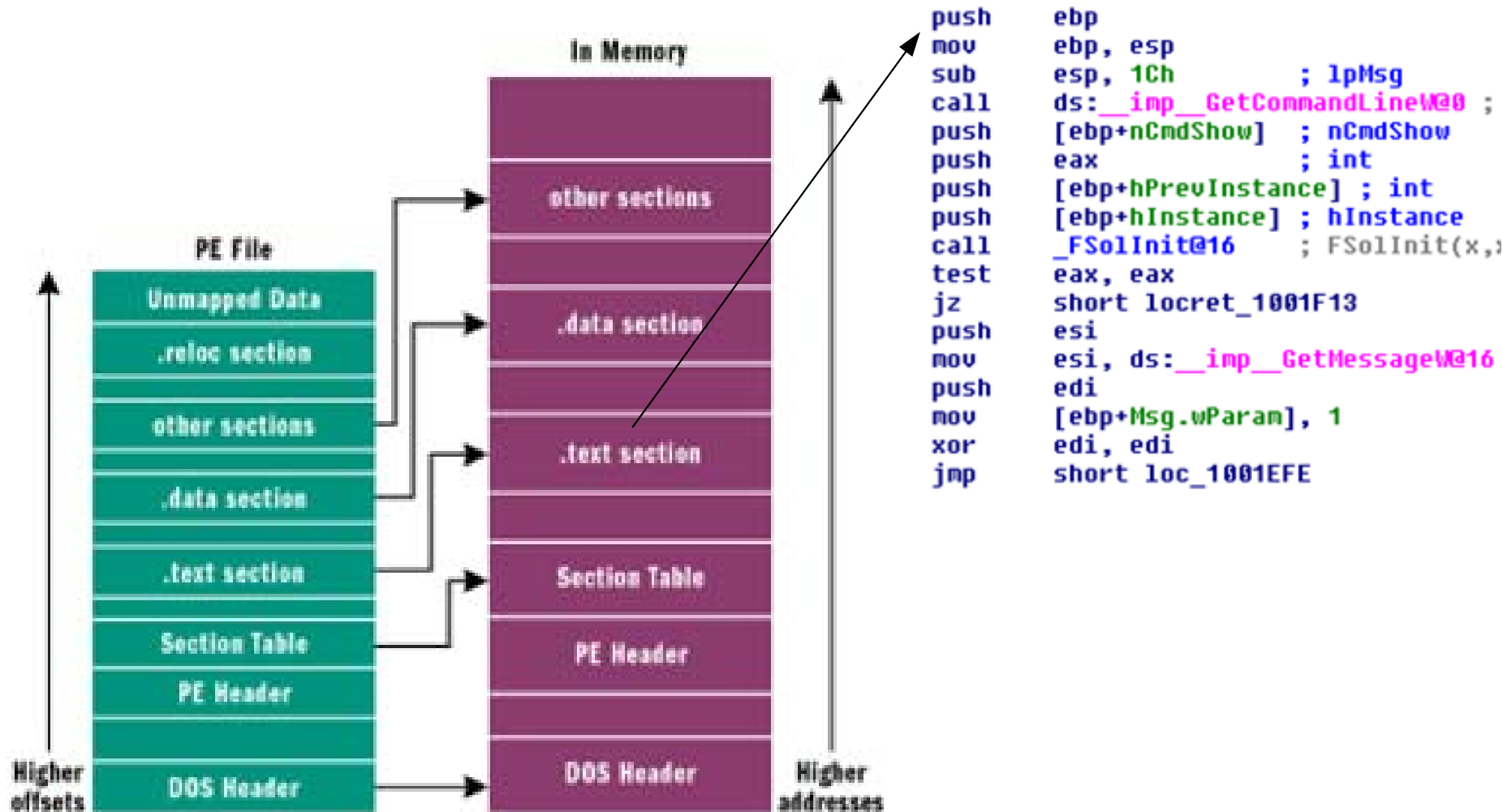


Packing/Encryption

- Self-modifying Code
 - Small Decoder Stub
 - Decompresses the main executable
 - Restores imports
- Play Tricks with Portable Executables
 - Hide the Imports
 - Obscure relocations
 - Encrypt/compress the executable

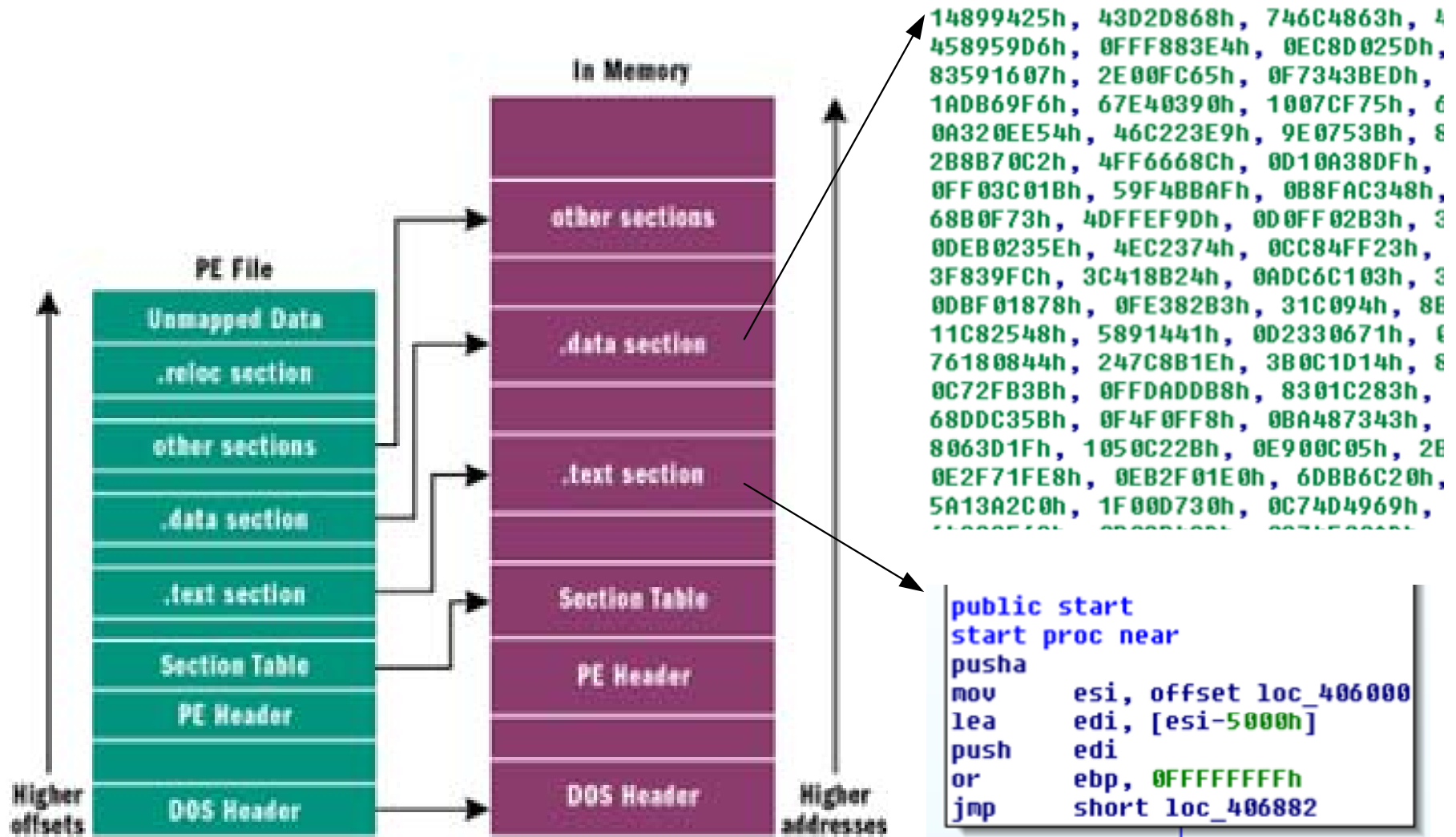


Normal PE File





Packed PE File





Virtual Machine Detection

- Single instruction detection
 - SLDT, SGDT, SIDT
 - See: Redpill, Scoopy-Doo, OCVmdetect
- Instructions for Privileged/Unprivileged CPU mode
 - VMs try to be efficient, some instructions insecure
 - Do not fully emulate x86 bug for bug



Debugger Detection

- Windows API
 - IsDebuggerPresent() API call
 - Checks PEB for magic bit (EFLAGS)
 - Bit toggling works
- Timing Attacks
 - Issue RDTSC instruction, compare to known values
 - Amazingly effective



Debugger Detection (cont.)

- Breakpoint Detection
 - Int3 (0xCC) Instruction Scanning
 - Checksumming of executable
- Hardware Debugging Detection
 - Check CPU Flags for debug bit
- SoftICE Detection
 - Modification of Int3 Scanning



SEH Tricks

- Structured Exception Handler
- Used to handle error in running code
- Malware will overload this function to unpack code
- Debugger thinks SEH exceptions are for it
- Debugger dies



Shifting Decode Frames

- Execution is split at the basic block level
- Block is decoded, executed, and then encoded again
- Hard to defeat!
- Implemented in Patchguard for Vista 64 and Windows Server 2003 64-bit



So What?

- These are all variations on a theme
- There should be a generic way to debug
- Need to modify at a fundamental level
- Solution should be:
 - Generic – Work across set of executables
 - Efficient – Good performance for non-debug
 - Undetectable (as much as possible)
 - Extensible – Automation is the key



Software Armoring Achilles Heel

If it executes,
it can be unpacked.



Unpacking

- How an Unpacker Works:
 - Writes to an area of memory (decode)
 - Memory is read from (execute)
 - More writes to memory (optional re-encoding)
- CPU Only Executes Machine Code
- This process can be monitored
- Unpacking is directly related to timing
 - At some point, it ***must*** be unpacked



Manual Unpacking Process

- Consists of several stages
 - Identify Packer Type
 - Find OEP or get process to unpacked state in memory
 - Dump process memory to file
 - Fixup file / rebuild Import Address Table (IAT)
 - Ensure file can now be analyzed



Manual Unpacking Process

- Several methods to identify packer type
 - Peid
 - Msfpecan / OffensiveComputing.net
 - Manually look at section names
 - Other packer scanners like
 - Protection-id
 - Pe-scan



Manual Unpacking Process

The screenshot displays a Windows desktop environment. In the background, there is a browser window titled "Offensive Computing" showing a "RETRIEVING DATA" status. In the foreground, the PEID v0.94 application is open, analyzing a file named "C:\packers\upx1.20_calc.exe". The application shows the following details:

- File: C:\packers\upx1.20_calc.exe
- Entrypoint: 00020310
- EP Section: UPX1
- File Offset: 00007710
- First Bytes: 60, BE, 00, 90
- Linker Info: 7.0
- Subsystem: Win32 GUI
- Match: UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo

Below the PEID window, a Metasploit terminal window is visible, showing the following command and output:

```
msf > msfpescan -f upx_scrambler_calc.exe -S
upx_scrambler_calc.exe: UPX-Scrambler RC v1.x [667] (1 matches)
```



Manual Unpacking Process

- Methods to find OEP / unpacked memory
 - OllyScripts
 - <http://www.tuts4you.com>
 - <http://www.openrce.org>
 - OEP finder tools
 - OEP finders for specific packers
 - OEP Finder (very limited)
 - PE Tools / LordPe
 - PEiD generic OEP finder



Manual Unpacking Process

The screenshot displays the OllyDbg interface for the file `upx1.20_calc.exe`. The CPU window shows the main thread at address `01012475` with the instruction `PUSH 70`, which is highlighted as the OEP (Original Entry Point). A comment for this instruction reads: "This is the OEP! Found By : fly".

Overlaid on the interface are several utility windows:

- OllyScript**: A message box stating "Just : OEP ! Plz Dump and Fix IAT . Good Luck".
- PEiD v0.94**: A window showing analysis results for `C:\packers\upx1.20_calc.exe`. It identifies the entrypoint as `00020310`, the EP section as `UPX1`, and the subsystem as `Win32 GUI`. It also lists the linker version as `7.0`.
- Generic OEP Finder FX [v0.8 Beta]**: A window showing the analysis progress at 100% and a list of possible OEPs. The first entry is `01012475`.
- GenOEP**: A small window confirming the found OEP: `01012475`.

The main disassembly window shows the following instructions:

Address	Hex dump	Disassembly	Comment
01012475	6A 70	PUSH 70	This is the OEP! Found By : fly
01012477	68 E0150001	PUSH upx1_20_.010015E0	
0101249E	75 12	JNZ SHORT upx1_20_.010124A0	
010124A0	0FB741 18	MOVZX EAX, WORD PTR [EAX]	
010124A4	3D 0B010000	CMP EAX, 10B	
010124A9	74 10	JZ SHORT upx1_20_.010124B0	
010124AB	3D 00000000	CMP EAX, 0	
010124B0	74 05	JZ SHORT upx1_20_.010124B5	
010124B2	895D	MOV EDI, EDI	
010124B5	EB 20	MOV EBX, EBX	
010124B7	83B9	MOV ECX, ECX	
010124BE	76 F0	JLE SHORT upx1_20_.010124C0	
010124C0	33C0	XOR EAX, EAX	



Manual Unpacking Process

– Dump process memory to file

- OllyDump
- LordPE
- Custom tools

– Example:

```
void DumpProcMem(unsigned int ImageBase, unsigned int ImageSize, LPSTR filename,
LPSTR pid) {
    SIZE_T ReadBytes = 0; SIZE_T WriteBytes = 0;
    unsigned char * buffer = (unsigned char *) calloc(ImageSize, 1);
    HANDLE hProcess = OpenProcess(PROCESS_VM_READ, FALSE, (DWORD)atoi(pid));
    ReadProcessMemory(hProcess, (LPCVOID) ImageBase, buffer, ImageSize,
&ReadBytes);
    HANDLE hFile = CreateFile(TEXT("oc_dumped_image.exe"),
        GENERIC_READ|GENERIC_WRITE,
        0,
        NULL,
        OPEN_ALWAYS,
        FILE_ATTRIBUTE_NORMAL,
        NULL);
    WriteFile(hFile, buffer, ImageSize, &WriteBytes, NULL);
}
```




Manual Unpacking Process

The screenshot displays the OllyDbg interface with several windows open during the manual unpacking process:

- OllyDump - upx1.20_calc.exe**: A dialog box for dumping a section of the executable. It shows the Start Address (1000000), Size (28000), Entry Point (20310), and Base of Code (19000). A table of sections is visible:

Section	Virtual Size	Virtual Offset	Raw Size	Raw Offset	Characteristics
UPX0	00018000	00001000	00018000	00001000	E0000080
UPX1	00008000	00019000	00008000	00019000	E0000040
.rsrc	00007000	00021000	00007000	00021000	C0000040

- LordPE Deluxe [by yoda]**: A PE editor window showing a list of loaded processes and their PE images. The process `c:\packers\upx1.20_calc.exe` is selected, showing its ImageBase (01000000) and ImageSize (00028000).
- Rebuild Status**: A dialog box reporting the progress of the unpacking process. It indicates that the dump is done, relocation is present, and the file is minimized to 92%. The process concludes with "Rebuilding finished."

The background shows the OllyDbg disassembly window with the instruction `PUSH 2` at address `010124E1` and `CALL [100120C]` at `010124E3`.



Manual Unpacking Process

- Fixup file / rebuild Import Address Table (IAT)
 - ImportRec probably best tool
 - Revirgin by +TsehP
 - Manually with a hex editor (tedious)
- IAT contains list of functions imported
 - Very useful for understanding capabilities

Address	Ordinal	Name	Library
01001214		??1type_info@@@UAE@xZ	msvcrt
01001210		??3@YAXPAX@Z	msvcrt
01001220		?terminate@@@YAXZ	msvcrt
010010B8		CallWindowProcW	USER32
010010F0		CharNextA	USER32
0100111C		CharNextW	USER32
010010B0		CheckDlgButton	USER32
01001144		CheckMenuItem	USER32
01001148		CheckMenuRadioItem	USER32
0100110C		CheckRadioButton	USER32
010010...		ChildWindowFromPoint	USER32
010010F4		CloseClipboard	USER32
0100106C		CloseHandle	KERNEL32
0100116C		CreateDialogParamW	USER32



Manual Unpacking Process

The screenshot shows the manual unpacking process. In the background, a Windows Explorer window displays the path `c:\bin\reversing\lordpe\lordpe.exe` with PID 00000168. The foreground features two main windows:

- Import REConstructor v1.6 FINAL (C) 2001-2003 MackT/uCF**: This window is used to attach to an active process and import functions. The process `c:\packers\upx1.20_calc.exe (000003AC)` is selected. A list of imported functions is shown, including `advapi32.dll`, `gdi32.dll`, `kernel32.dll`, `shell32.dll`, `user32.dll`, and `msvcrt.dll`. The log indicates that 6 modules and 84 functions were imported, and a new section was added successfully. The IAT Infos needed section shows OEP `00020310`, RVA `00001000`, and Size `00000228`. The New Import Infos (IID+ASCII+LOADER) section shows RVA `00000000` and Size `00000830`. Buttons for "Load Tree", "Save Tree", "Get Imports", and "Fix Dump" are visible.
- Revirgin by +Tsehp 1.5 public version**: This window is used to attach to a module. The process `upx1.20_calc.exe` is selected. The "IAT Critical Values" section shows OEP `01020310`, RVA `00001000`, and Length `00000228`. The "IT Values + generator" section shows RVA and Length fields. The "Show IAT referers" and "Autofix sections + IT paste" checkboxes are checked. The "Mangled Scheme" checkbox is unchecked, with a high limit of `10000000`. Buttons for "Fetch IAT", "Tracer", and "generate!" are visible.

The status bar at the bottom indicates the process `upx1.20_calc.exe` is in "Imports View" and "Import Edit disabled".



Manual Unpacking Process

- Ensure file can now be analyzed
- Clean disassembly should be available
- IAT should be visible
- Functions should be found
- Strings clear and useful
- Manual unpacking process can be tedious
- Hardest part is generally finding the OEP



Manual Unpacking Process

IDA - C:\packers\unpacked\upx1.20_calc_lordPE_dumped_exe

File Edit Jump Search View Debugger Options Windows Help

IDA View-A

```
UPX0:01010B13 arg_4 = dword ptr 0Ch
UPX0:01010B13
UPX0:01010B13 push ebp
UPX0:01010B14 mov ebp, esp
UPX0:01010B16 mov edx, [ebp+8]
UPX0:01010B19 mov ecx, [ebp+4]
UPX0:01010B1C mov eax, [edx+8]
UPX0:01010B1F sub eax, [ecx+8]
UPX0:01010B22 push esi
UPX0:01010B23 mov esi, [ecx+4]
UPX0:01010B26 push edi
UPX0:01010B27 mov edi, [edx+4]
UPX0:01010B2A sub eax, esi
UPX0:01010B2C add eax, edi
UPX0:01010B2E jns short loc_1
```

Imports

Address	Ordinal	Name	Library
01028000		RegOpenKeyExA	advapi32
01028004		RegQueryValueExA	advapi32
01028008		RegCloseKey	advapi32
01028010		SetBkColor	gdi32
01028014		SetTextColor	gdi32
01028018		SetBkMode	gdi32
01028020		GetModuleHandleA	kernel32
01028024		LoadLibraryA	kernel32
01028028		GetProcAddress	kernel32
0102802C		GlobalCompact	kernel32
01028030		GlobalAlloc	kernel32
01028034		GlobalFree	kernel32
01028038		GlobalReAlloc	kernel32
0102803C		IstrcmpW	kernel32
01028040		Sleep	kernel32
01028044		WriteProfileStringW	kernel32
01028048		GetStartupInfoA	kernel32
0102804C		GlobalSize	kernel32
01028050		GlobalUnlock	kernel32
01028054		CreateEventW	kernel32
01028058		CreateThread	kernel32
0102805C		ResetEvent	kernel32
01028060		IstrcpynW	kernel32
01028064		SetEvent	kernel32
01028068		WaitForSingleObject	kernel32
0102806C		CloseHandle	kernel32
01028070		IstrcatW	kernel32
01028074		IstrlenW	kernel32
01028078		LocalReAlloc	kernel32
0102807C		LocalFree	kernel32
01028080		LocalAlloc	kernel32
01028084		GetProfileStringW	kernel32
01028088		GlobalLock	kernel32

Names window

Name	Address
a0123456789abcd	01
all	01
al4	01
aw4	01
aAWhatSThis?	01
start	01
RegOpenKeyExA	01
RegQueryValueExA	01
RegCloseKey	01
SetBkColor	01
SetTextColor	01
SetBkMode	01
GetModuleHandleA	01
LoadLibraryA	01

Functions window

Function name	Segment	Start	Length	R	F	L	S	B	T
sub_10013D1	UPX0	010013D1	0000002E	R
sub_10013FF	UPX0	010013FF	00000025	R
sub_1001424	UPX0	01001424	000000D5	R	.	.	.	B	.
sub_10014F9	UPX0	010014F9	00000129	R	.	.	.	B	.
sub_10016F2	UPX0	010016F2	00000036	R
sub_10017B2	UPX0	010017B2	00000052	R
sub_1001804	UPX0	01001804	00000047	R
sub_10034FC	UPX0	010034FC	00000052	R
sub_100356C	UPX0	0100356C	00000052	R
sub_1003641	UPX0	01003641	00000018	R
sub_10036B4	UPX0	010036B4	00000110	R	.	.	.	B	.
sub_10037C4	UPX0	010037C4	00000352	R	.	.	.	B	.
sub_1003BA0	UPX0	01003BA0	000000AD	R	.	.	.	B	.
sub_1003C4D	UPX0	01003C4D	0000002B	R
sub_1003C78	UPX0	01003C78	00000048	R
sub_1004332	UPX0	01004332	0000001B	R
sub_100446A	UPX0	0100446A	00000027	R
sub_1004491	UPX0	01004491	00000027	R

Strings window

Offset	Type	String
000A	C	gdi32.dll
000B	C	SetBkColor
000C	C	SetTextColor
000D	C	SetBkMode
000E	C	kernel32.dll
0011	C	GetModuleHandleA
001D	C	LoadLibraryA
001F	C	GetProcAddress
002C	C	GlobalCompact
0032	C	WriteProfileStringW
003A	C	GetStartupInfoA
0048	C	ResetEvent
0058	C	trcpynW
0067	C	SetEvent



Unpacking: The Algorithm

- Track written memory
- If that memory is executed, it's unpacked
- Must monitor:
 - Memory writes
 - Memory Executions
- Break on execute useful here
- Automate the process



Dynamic Instrumentation

- Allows a running process to be monitored
- Intel PIN
 - Uses Just-In-Time compiler to insert analysis code
 - Retains consistency of executable
 - Pintools – Use API to analyze code
 - Good control of execution
 - Instruction
 - Memory access
 - Basic block
 - Process Attaching / Detaching



Dynamic Instrumentation

- Instruction tracing for the following packers
 - Armadillo
 - Aspack
 - FSG
 - MEW
 - PECompact
 - Telock
 - UPX
- Created Simple Hello World Application
- Graphed results with Oreas GDE

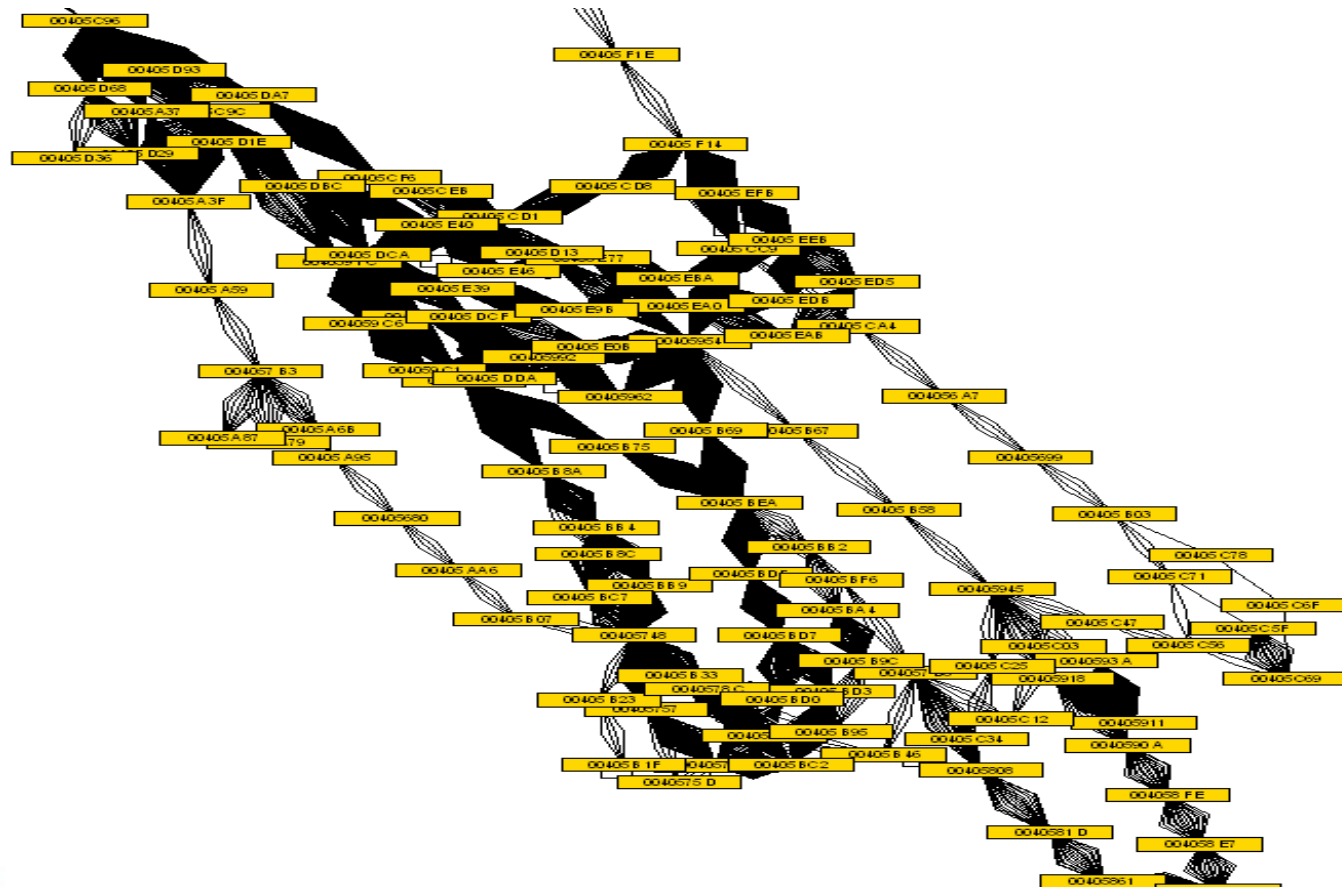


Aspack 2.12



Results

- Unpacking loop is easy to find





Dynamic Instrumentation Results

- Generic Algorithm Described Previously works well
- All address verified by manual unpacking
- Addresses display clustering, which must be taken into account
- Attach / Detach is effective for taking memory snapshots of an executable



Dynamic Instrumentation Problems

- Detectable
 - Memory checksums
 - Signature scanning
- Extend this to work generically, non-detectably
- Slow – ~1,000 times slower than native
- Need faster implementation



Towards a Solution

- Core operating system component that:
 - Monitors all memory
 - Intercepts memory accesses
 - Fast Interception and Logging
 - Fundamental part of OS



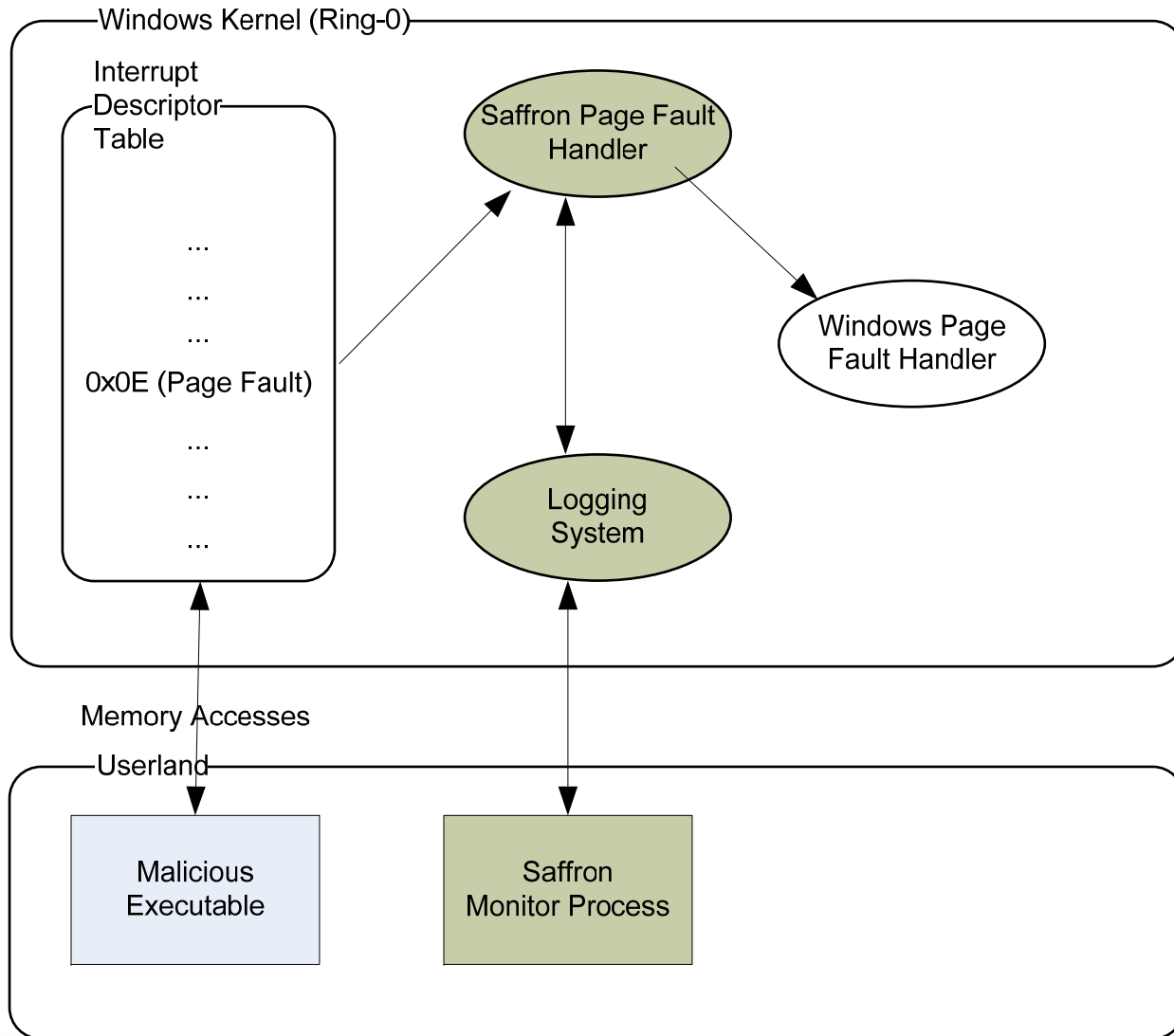
Introducing Saffron

- Intel PIN and Hybrid Page Fault Handler
- Extension of OllyBonE Kernel Code
- Designed for 32-bit Intel x86 CPUs
- Replaces Windows 0x0E Trap Handler
- Logs memory accesses





Saffron System Implementation





Virtual Memory Translation

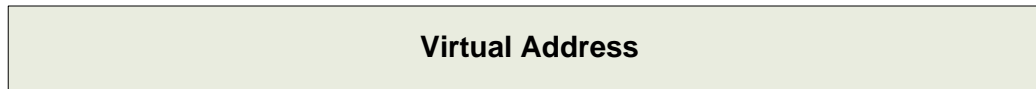
- Each process has its own memory
- Memory must be translate from Virtual to Physical Address
- Non-PAE 32bit Processors use 2 page indexes and a byte index
- Each process has its own Page Directory



Example Memory Translation

31

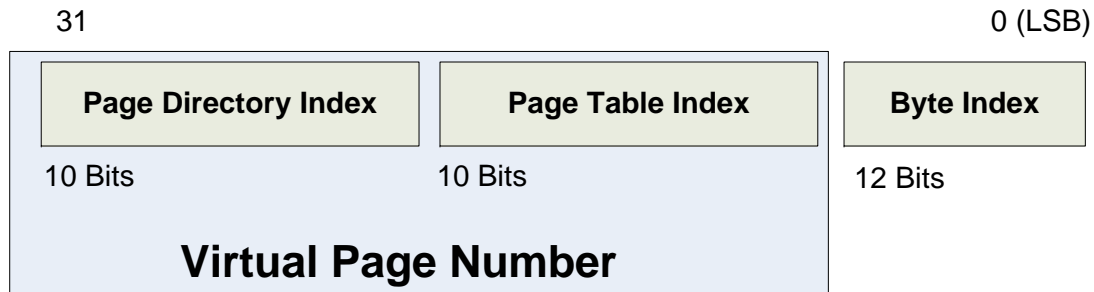
0 (LSB)



CPU References Virtual Memory Address

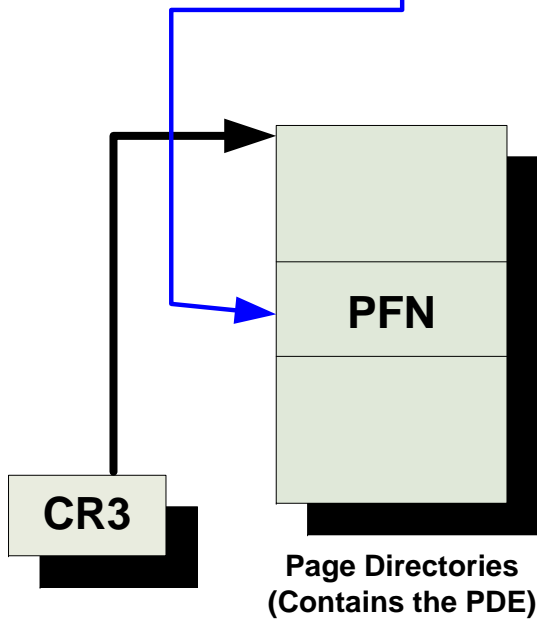
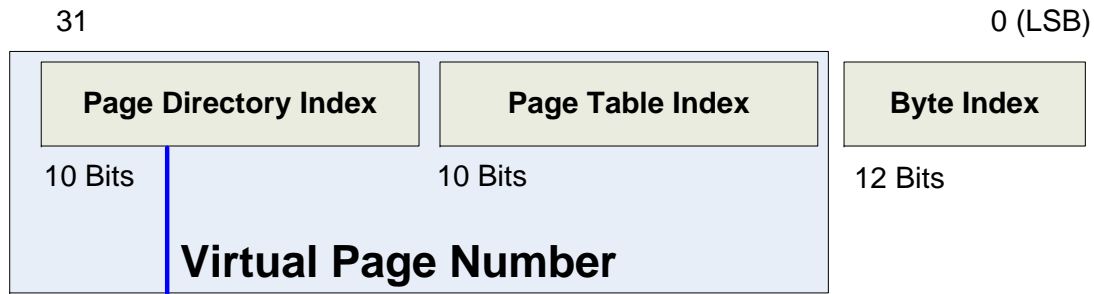


Example Memory Translation





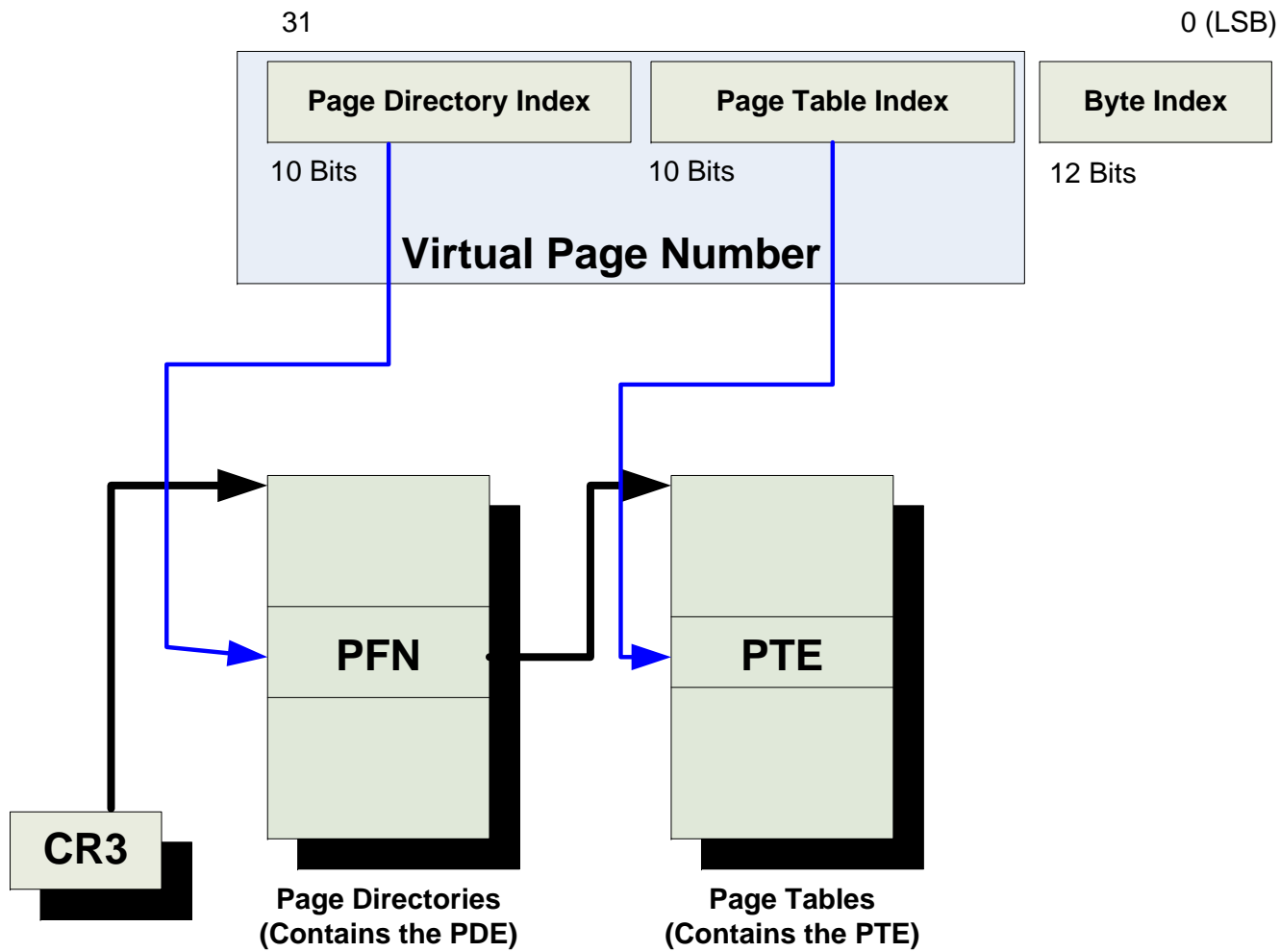
Example Memory Translation



CR3 contains process Page Directories

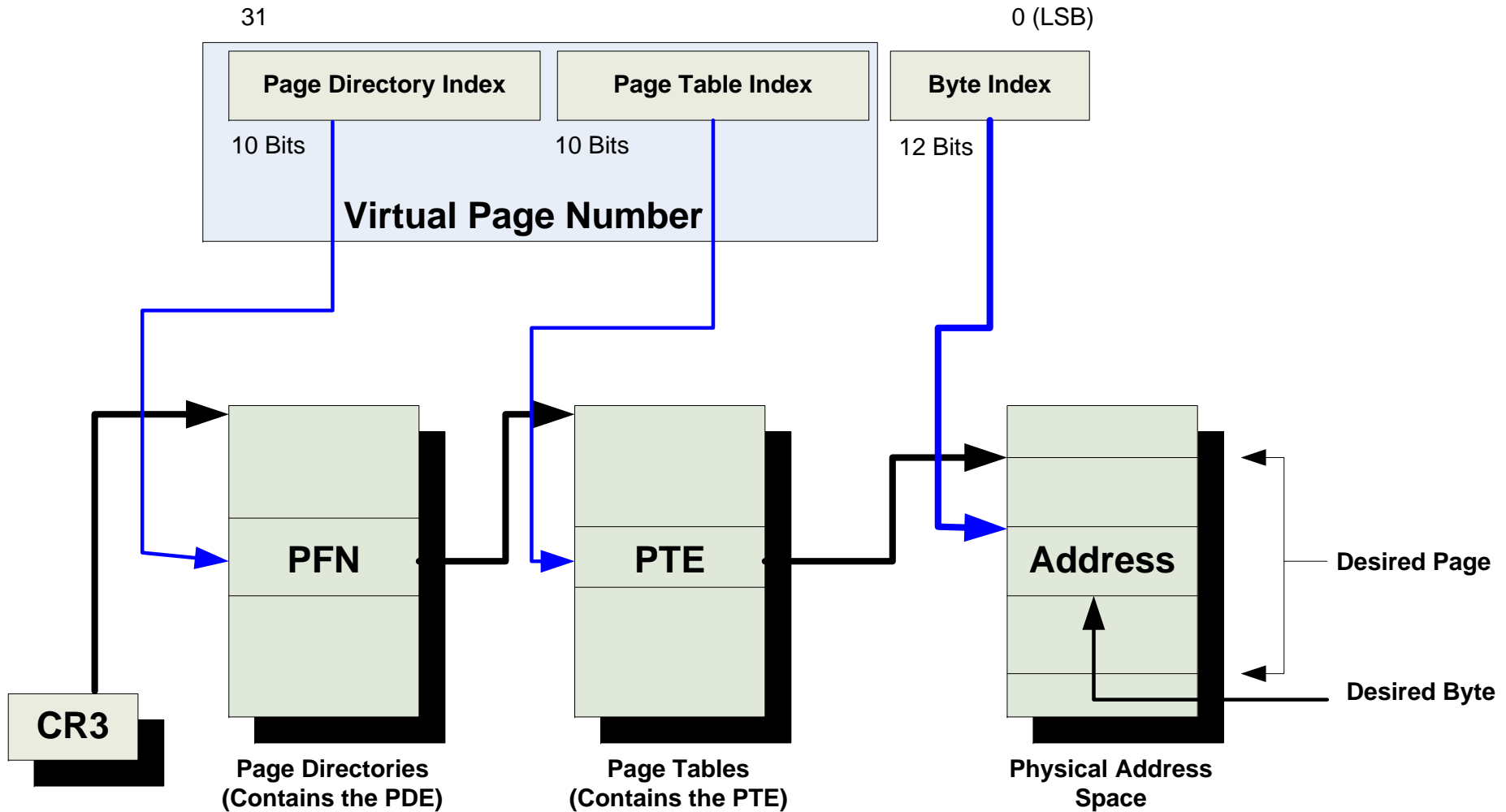


Example Memory Translation





Example Memory Translation





MMU Data Structures

- Page Directory Entry is hardware defined
 - Contains permissions, present bit, etc.
- Page Table Entry also hardware defined
 - Permissions (Ring0 vs. all others)
 - Present bit (paged to disk or not)
 - “User” defined bits (for OS)



Virtual Address Translation

- TLB is major source of optimization
- Hardware resolves as much as possible
- Invokes page fault handler when
 - Page is not loaded in RAM
 - Incorrect privileges
 - Loaded, but mapped with demand paging
 - Address is not legal (out-of-range)
- All indicated by special fields



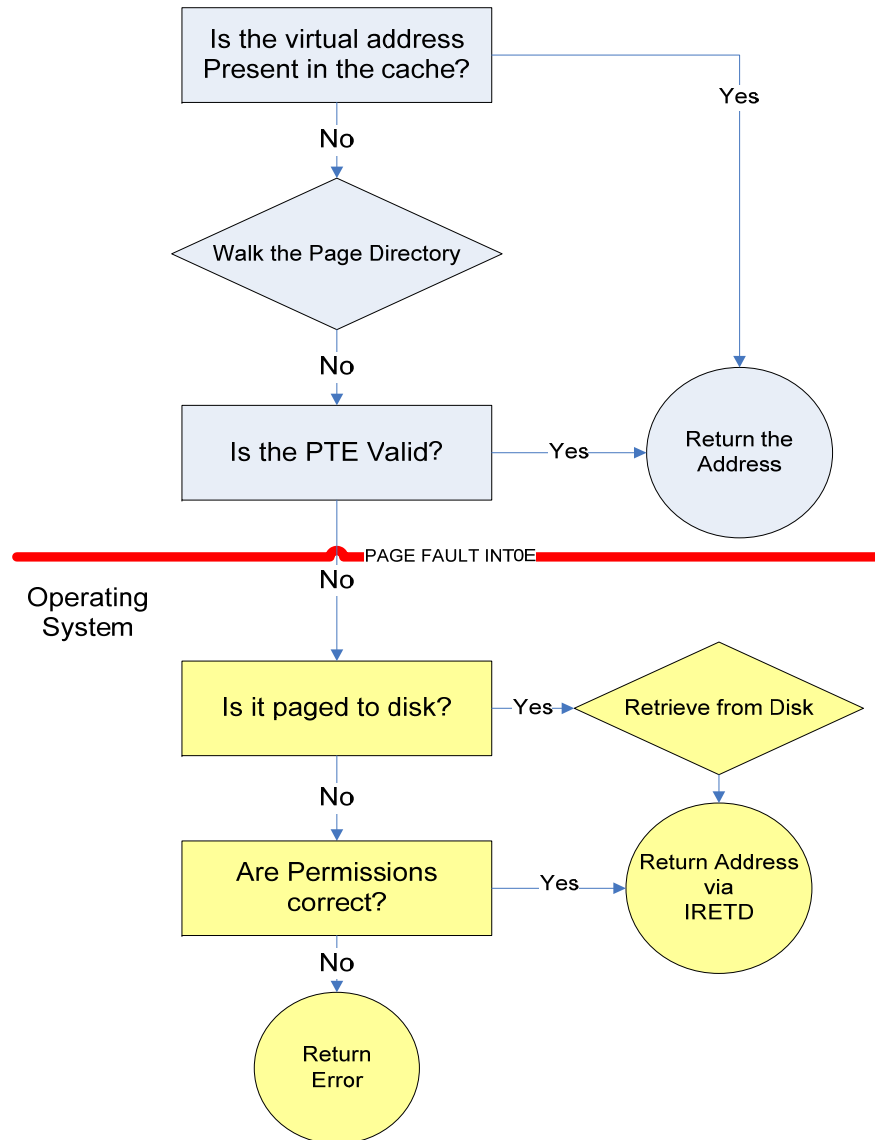
Intel TLB Implementation

- Two TLBs maintained
 - Data - DTLB
 - Instructions – ITLB
- ITLB more optimized than DTLB
 - Less lookups for ITLB == faster code
 - DTLB accessed less



Offensive Computing - Malware Intelligence

Hardware





Process Monitoring

- Overloading of supervisor bit in page fault handler
- All process memory must be found
- Iterate through all pages for a process
 - Windows application memory
0x00000000 – 0x7FFFFFFF
- Mark supervisor bit on each valid PTE
- Invalidate the page in the TLB with INVLPG
- Hook heap allocation so new pages are watched



Trap to Page Fault Handler

- Determine if a watched process
- Unset the supervisor bit
- Loads the memory into the TLB
- Resets supervisor bit



Results

- Memory accesses are visible
- Reads, writes, and executes are exposed
- Program execution can be tracked, controlled
- Memory reads, writes are extremely apparent
- Executions only show for each individual page



Modifying the Autounpacker

- Watch for written pages
- Monitor for executions into that page
- Mark page as Original Entry Point
- Dump memory of the process



Video Demo of Unpacking

- Demonstrate Saffron



Autounpacker Results

- Effective method for bypassing debugger attacks
 - SEH decode problem is easily solved
 - Memory checksum
 - No process memory is modified
 - p0wn3d!!!
- Shifting decode frame
 - Slight modification under development, but effective



Future Work

- Develop full-fledged API
- Problems
 - Sometimes all page markings are lost
 - Still detectable at some level



Questions?

- Paper, presentation available at

www.offensivecomputing.net

