Ether: Malware Analysis via Hardware Virtualization Extensions

Enrico Galli

September 21, 2010

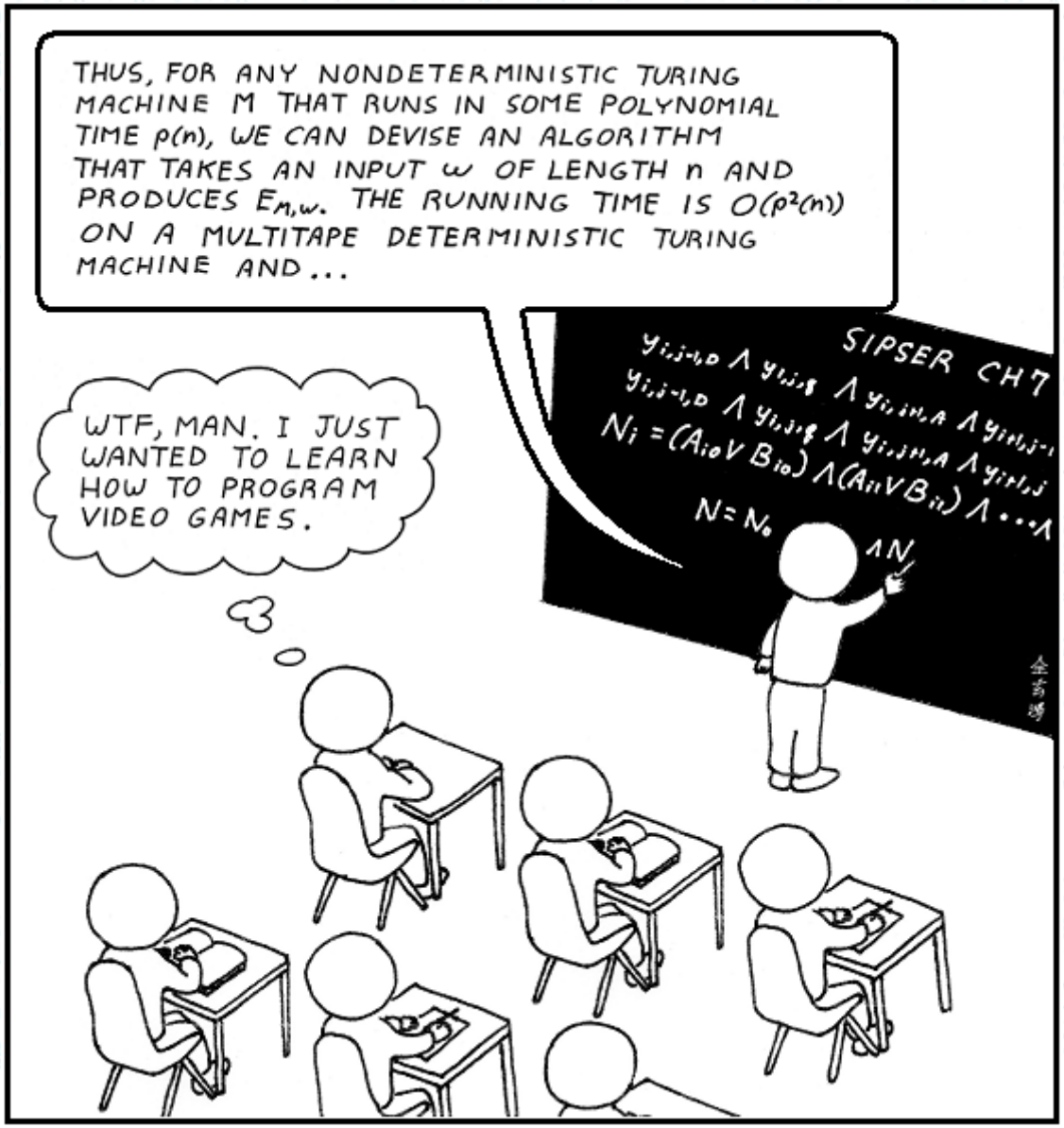
Introduction

- Background and Related Work
- Formal Foundations
- Implementation:Ether
- Experiments and Evaluation

Background and Related Work

- The malware problem
- Current techniques
  - System: Virtualization and Emulation
  - OS: Kernel Module
  - API: Hooking and/or virtualization
- Malware is getting smarter

Formal Foundations



Transparent Malware Analysis

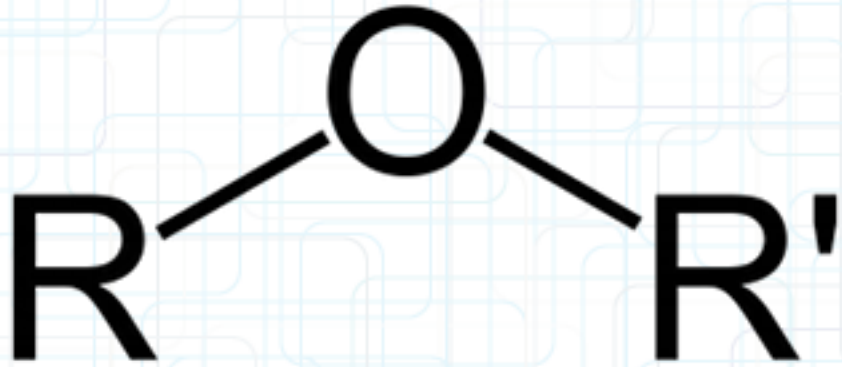
If run a program under an environment with an analyzer, it should run the same instructions that it would have if the analyzer was not present.

Requirements for Transparency

1. Higher Privileges
2. No non-privileged side effects
3. Identical Basic Instruction Execution Semantics
4. Transparent Exception Handling
5. Identical Measurements of Time

Implementation: Ether

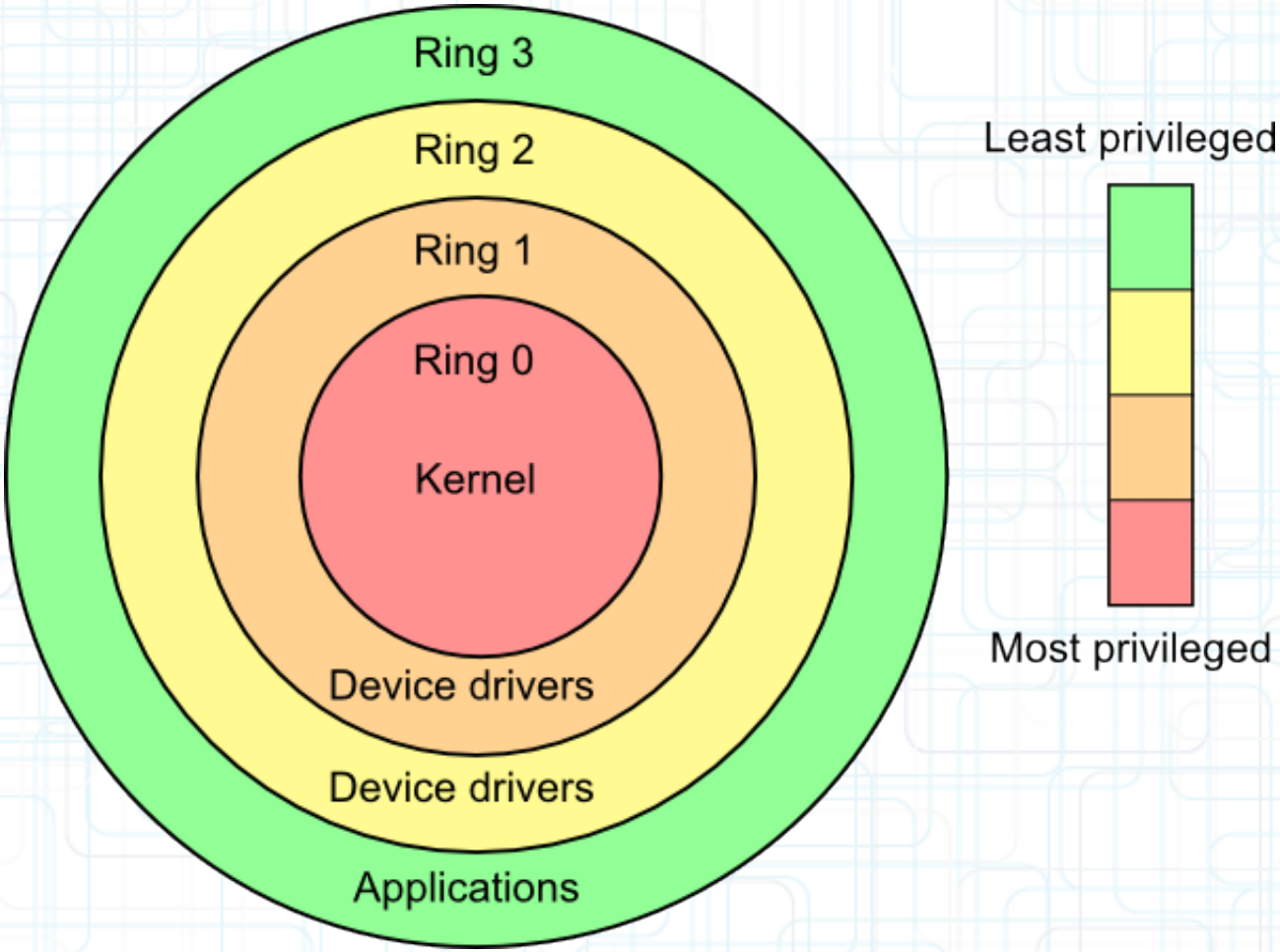
- Environment
- Analyzer Architecture
- Using Intel VT for Malware Analysis
- Maintaining Analyzer Transparency
- Potential Attacks



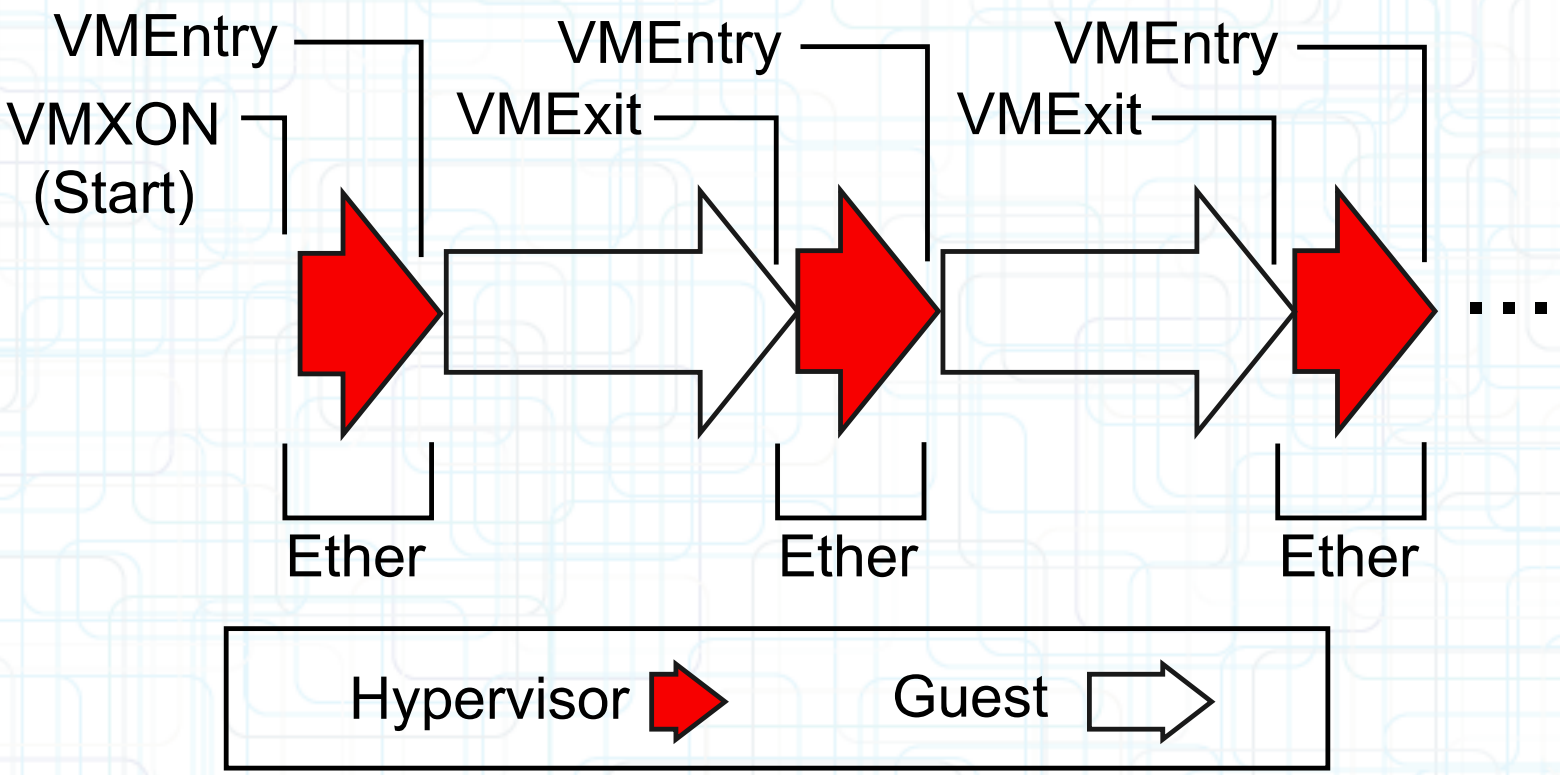
Environment

- Ether is built on top of Xen
  - Hypervisor
  - One Dom0 with access to the hardware
  - Multiple DomUs virtualized
- Intel VT hardware virtualization extensions

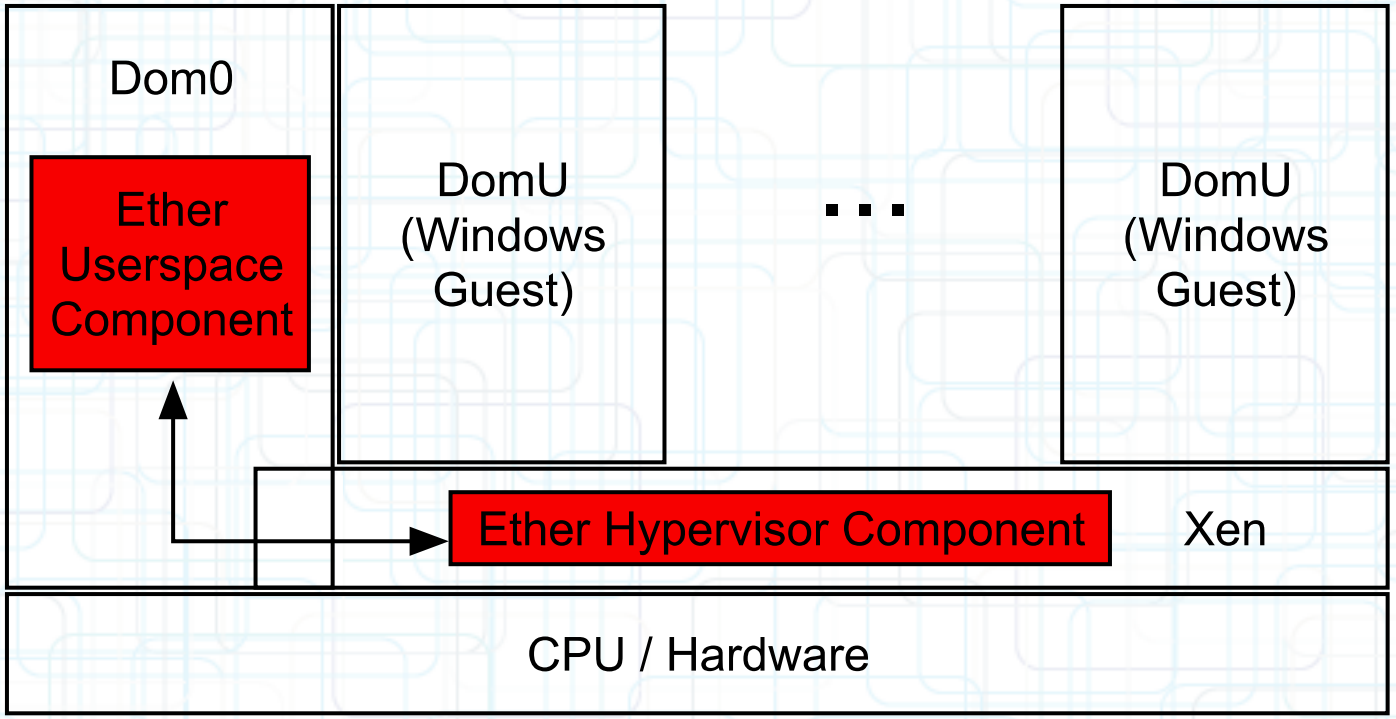
Intel VT


Ring 3
Ring 2
Ring 1
Ring 0
Kernel
Device drivers
Device drivers
Applications
Least privileged
Most privileged

Intel VT(cont.)



Analyzer Architecture



Using Intel VT for Malware Analysis

- Coarse-grained: Systems calls
- Fine-grained: Instructions
- Intel VT was not originally designed for malware analysis

Using Intel VT for Malware Analysis(cont.)

- Monitoring Instruction Execution
  - Set the trap flag
- Monitoring Memory Writes
  - Shadow page tables
- Monitoring System Call Execution
  - Replace SYSENTER_EIP_MSR
- Limiting Scope to a Chosen Process
  - VMExit on page directory entry accessed

Maintaining Analyzer Transparency

- Hiding the trap flag
  - Control instructions
- Page Table Modification
  - Shadow page tables
- SYSENTER_EIP_MSR
  - Control all access to register

Potential Attacks

- In-memory presence
- CPU registers
- Memory Protection
- Privileged Instruction Handling
- Instruction Emulation
- Timing Attacks
  - Some Intel VT support

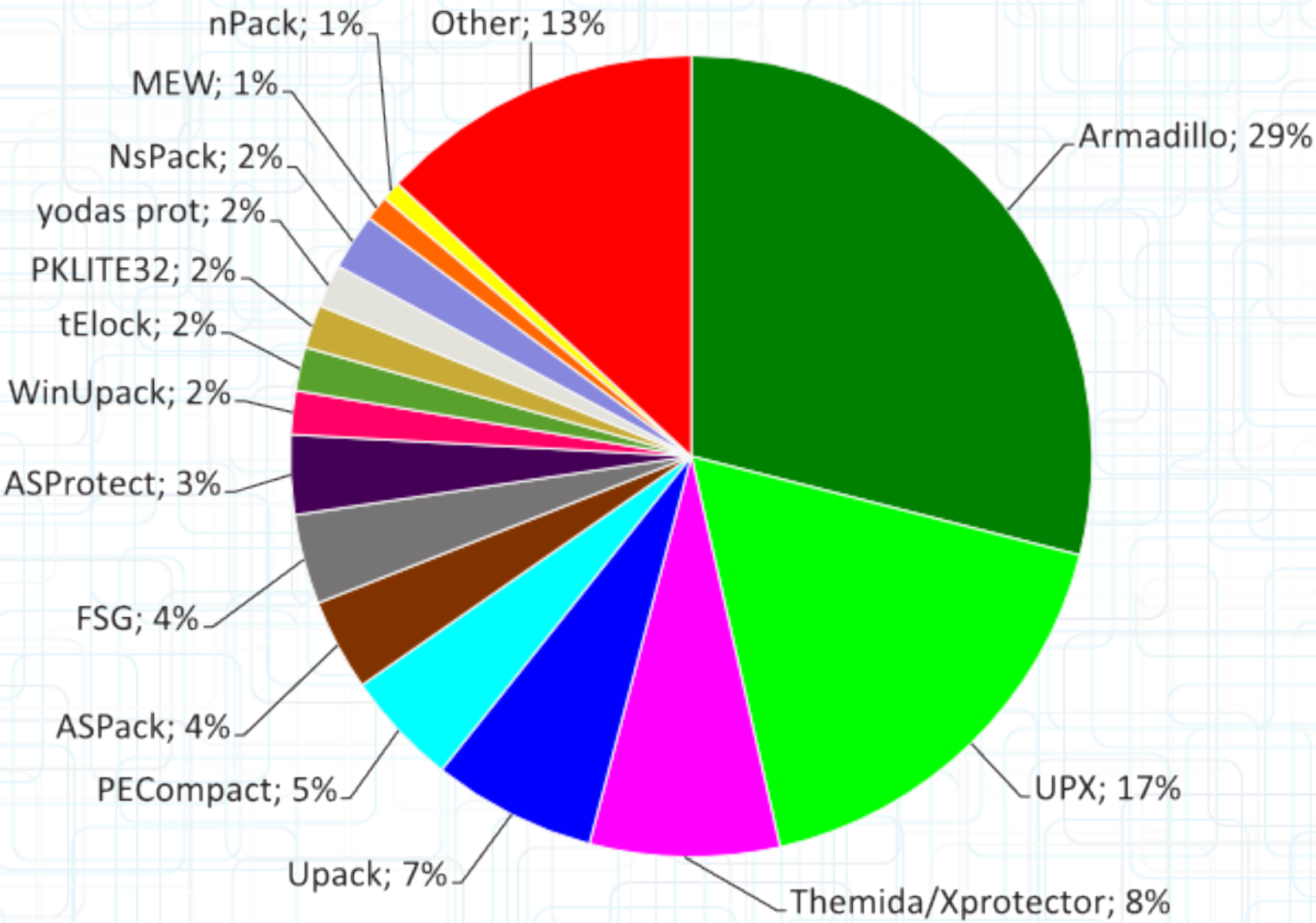
Experiments and Evaluation

- Fine-grained Tracing: EtherUnpack
- Coarse-grained Tracing: EtherTrace

Fine-grained Tracing: EtherUnpack

- Test to see if packers are able to find weaknesses in Ether's transparency
- Searched for a 32 bytes string starting at a fixed offset
  - No Windows API calls
- Performance
  - Not for real-time analysis
  - Forensic tool

Sample Distribution



EtherUnpack: Results

Packing Tool	EtherUnpack	Renovo	PolyUnpack
Armadillo	yes	no	no
Aspack	yes	yes	no
Asprotect	yes	yes	yes
FSG	yes	yes	yes
MEW	yes	yes	yes
Molebox	yes	yes	no
Morphine	yes	yes	yes
Obsidium	yes	no	no
PECompact	yes	yes	no
Themida	yes	yes	no
Themida VM	yes	no	no
UPX	yes	yes	yes
UPX S	yes	yes	yes
WinUPack	yes	yes	no
yoda's Prot.	yes	yes	no

Coarse-grained Tracing: EtherTrace

- Evaluate Ether's ability to do coarse-grained tracing
- Methodology
  - Created an executable with a list of Windows API calls
  - Packed it with top 15 packers
  - Test accuracy and performance

EtherTrace: Effectiveness

Packing Tool	EtherTrace	Anubis	Norman
None	yes	yes	yes
Armadillo	yes	no	no
UPX	yes	yes	yes
Upack	yes	yes	yes
Themida	yes	yes	yes
PECompact	yes	yes	yes
ASPack	yes	yes	yes
FSG	yes	yes	yes
ASProtect	yes	no	yes
WinUpack	yes	yes	yes
tElock	yes	no	yes
PKLITE32	yes	yes	yes
yoda's Prot.	yes	yes	no
NsPack	yes	yes	yes
MEW	yes	yes	yes
nPack	yes	yes	yes
RLPack	yes	yes	yes
RCryptor	yes	yes	yes

EtherTrace: Performance

Benchmark	Untraced	Traced	Change
HTMLRender	0.97 pg/s	0.62 pg/s	35.95%
FileDecrypt	64.87 MB/s	64.09 MB/s	1.19%
HDD	11.34 MB/s	8.14 MB/s	28.29%
TextEdit	68.83 pg/s	19.37 pg/s	71.86%
Image	14.86 MPix/s	14.69 MPix/s	1.12%
FileCompress	2.7 MB/s	2.66 MB/s	1.67%
FileEncrypt	16.07 MB/s	15.53 MB/s	3.39%
VirusScan	11.14 MB/s	11.09 MB/s	0.41%
MemLatency	7.75 MAcc/s	3.12 MAcc/s	59.8%
RARTime	40.87 s	45.29 s	10.81%

Conclusion

- Ether was able to stay transparent to malware
- Future work: Improve resilience to
  - Timing attacks
  - Memory hierarchy

Questions?