

# Get Your Head Out of the Clouds: The Illusion of Confidentiality & Privacy



Vincent E. Urias, William MS Stout, Caleb Loverro and Brian Van Leeuwen

PRESENTED BY

Vince Urias and Caleb Loverro



Introduction

Thwarting Encryption At-Rest and In-Motion

- Through Virtual Machine Introspection

Addressing Transparency

Conclusions

- Suggested Mitigations

Numerous government and industry entities are moving to the cloud

- Adopt a shared-security responsibility model

According to NIST, security controls for confidentiality and integrity for data-at-rest and in-motion are based on encryption.

For SaaS/PaaS, CSP may access unencrypted data/keys

IaaS may provide customer full control of encryption mechanisms and keys

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Network controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Host infrastructure	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Physical security	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer

For IaaS, a CSP should not have carte blanche access to virtual machine (VM) data

- Does the CSP have tools to access to the guest OS?
- Can the CSP access plain-text (PT) data in the guest OS?
- With undetected access, claims to confidentiality and privacy are null.

This research efforts attempts to show that:

- Network and disk encryption in the cloud may not be sufficient.
- Hypervisor-based approaches may be leveraged to gain access to information.
- Mitigations do exist and should be implemented.



Privacy & Confidentiality are based on user's trust of the CSP

- IaaS may provide more confidence since user owns encryption piece

However, through virtual machine introspection (VMI), that trust may be for naught

What we will cover:

- Understanding VMI
- By-passing Encryption through hypervisor-assisted VMI
- Extracting TLS keys from a browser
- Extracting encryption keys from LSASS
- Passing keys for decryption in-motion
- Transparently decrypting filesystems



2003: VMI created to provide an architecture for IDS

- Virtual Machine Monitor (VMM) named Livewire

VMI applications include augmenting network-based systems, enforcing security policies on VMs, performance monitoring, cybersecurity efforts (e.g., malware execution), whitelisting, etc.

- LibVMI, Volatility, Rekall, ...

Four methodologies:

1. In-VM
2. Out-of-VM Delivered
3. **Out-of-VM Derived**
4. Hybrid Techniques



VMI approach used largely based on Out-of-VM  
Derived.

- Hook handling of VM-Exit by VM to hypervisor
- Can gain execution in VMX mode
  - Control execution state
  - Read memory of the currently exited VM
- Can do memory reads, or modify state of VM



## THWARTING ENCRYPTION:

### By-passing encryption through hypervisor-assisted VMI

Any hypervisor can be used to bypass encryption

- Set breakpoints, log system calls, etc., gather I/O buffers before they are passed from userspace to kernel

Implemented VMI for several hypervisors (no using hypervisor-built APIs) for:

- Setting breakpoints
- Parsing binaries
- Enumerating process information
- Hooking any/all system calls

Custom interfaces allow ability to change guest state or execution, including full control over structs like VMCS.



## THWARTING ENCRYPTION: Extracting TLS keys from a browser

Likely many ways to accomplish this, discussed is just one approach that requires little understanding of Firefox code, and without having to re-implement crypto code/libs.

Function: PK11\_ExtractKeyValue

- Dumps PK11SymKey structure

ID'ing keys of interest:

- Functions: PK11-PubWrapSymKey, PK11\_FreeSymKey
- Breakpoint allows enumeration of addresses of any PK11SymKey structure

All done in real-time with affecting the guest browser.

## THWARTING ENCRYPTION: Extracting encryption keys from LSASS

Windows systems and Cryptography API: Next Gen (CNG) – Edge, IE, Remote Desktop, server applications.

Leverage knowledge of EPROCESS struct to link the name lasass.exe to directory table base (page table or CR3)

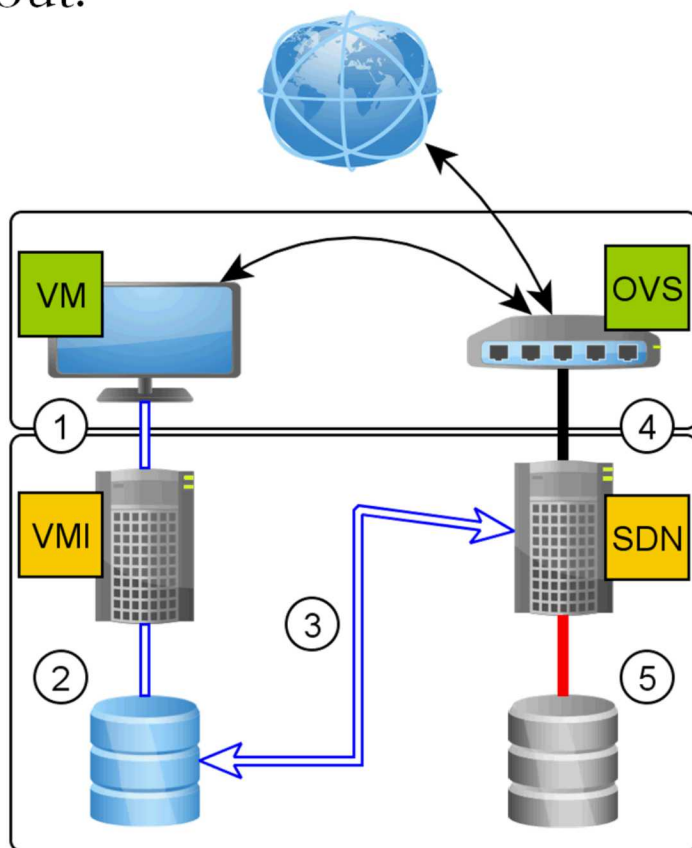
- Local Security Authority Subsystem Service (LSASS) – repository for all session keys
- VMI tool isolates guest page tables and EPT, to enumerate ring3-available memory in the LSASS process
- Keys ID'd via two 4-byte magic values and a C++ object

Code runs in hypervisor context and periodically scans memory for new copies of said structs

Output can then be passed to other tools such as RDP-Replay, Wireshark, or an inline decryption mechanism

# THWARTING ENCRYPTION: Passing keys for decryption in-motion

Using key material from previous methods, decryption of network traffic is carried out.



```

decrypted SSL data (583 bytes):
0000 47 45 54 20 2f 63 6c 69 65 6e 74 5f 73 74 6f 72 GET /client stor
0010 61 67 65 2f 61 31 32 35 33 37 35 35 30 39 2e 68 age/al25375509.h
0020 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP/1.1..Ho
0030 73 74 3a 20 61 31 32 35 33 37 35 35 30 39 2e 63 st: al25375509.c
0040 64 6e 2e 6f 70 74 69 6d 69 7a 65 6c 79 2e 63 6f dn.optimizely.co
0050 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d m..User-Agent: M
0060 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 ozilla/5.0 (Wind
0070 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 69 6e 36 ows NT 6.1; Win6
0080 34 3b 20 78 36 34 3b 20 72 76 3a 35 33 2e 30 29 4; x64; rv:53.0)
0090 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/20100101
00a0 46 69 72 65 66 6f 70 2f 35 33 2e 30 0d 0a 41 63 Firefox/53.0..Ac
00b0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: text/html,
00c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d application/xhtm
00d0 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,application
00e0 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b n/xml;q=0.9,*/*;
00f0 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8..Accept-La
0100 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e nguage: en-US,en
0110 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5..Accept-E
0120 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, Re
0130 65 66 6c 61 74 65 2c 20 62 72 0d 0a 52 65 66 65 eflate, br..Refe
0140 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 77 72 e rer: http://www.
0150 63 6e 6e 2e 63 6f 6d 2f 0d 0a 43 6f 6f 6b 69 65 cnn.com/.Cookie
0160 3a 20 63 64 6e 3d 68 74 74 70 25 33 61 25 32 66 : cdn=http%3a%2f
0170 25 32 66 61 6b 61 6d 61 69 25 33 61 64 73 64 25 %2fakamai%3adsd%
0180 34 30 63 64 6e 2e 6f 70 74 69 6d 69 7a 65 6c 79 40cdn.optimizely
0190 2e 63 6f 6d 25 32 66 6a 73 25 32 66 31 33 31 37 .com%2fjs%2f1317
01a0 38 38 30 35 33 2e 6a 73 0d 0a 43 6f 6e 6e 65 63 88053.js..Connec
01b0 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: keep-alive
01c0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ..Upgrade-Insecu
01d0 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Requests: 1..
01e0 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69 6e 63 If-Modified-Sinc
01f0 65 3a 20 54 75 65 2c 20 32 33 20 4d 61 79 20 32 e: Tue, 23 May 2
0200 30 31 37 20 30 3a 35 32 3a 32 38 20 47 4d 54 017 00:52:28 GMT
0210 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a ..If-None-Match:
0220 20 22 37 63 38 65 38 62 38 39 37 64 37 39 39 31 "7c8e8b897d7991
0230 34 35 38 65 62 30 38 31 33 39 33 65 35 31 63 33 458eb081393e51c3
0240 31 66 22 0d 0a 0d 0a 1f*....
  
```

Each block of plaintext network traffic as output from the decryption function are classified as either frame, reassembled TCP, or decrypted SSL. A packetizer function consumes each of these classified blocks to reconstruct entire TCP segments and streams, maintaining all the application layer flag and option settings, whilst updating the lower level attributes (such as CRC calculations). This updated, plaintext session traffic is then output to the decrypt tap

## THWARTING ENCRYPTION: Transparently decrypting filesystems

By monitoring `sys_read` on Linux or `NtReadFile` on Windows, VMI tool can gather data out of file buffers on most encrypted filesystems.

- Encryption generally takes place a lower layer than that of the system call

Encrypted files at rest → contents are not copied into buffers and passed to system calls

- However, mod'ing args or redirecting guest execution can produce results by “tricking” the OS to read a file it would otherwise not have touched
- Allows VMI tool to read contents of arbitrary files on an encrypted volume at will

Can the cloud user detect if VMI is being used by the CSP?

- Hypothesis: A VMI may impact VM or instance performance

Experiment design based on two experiments regarding encrypted data at-rest and in-motion.

Network Test Factors

Factor-1	Factor-2	Factor-2 Levels
No VMI FF Key Extraction LSASS Key Extraction	Pay Load Size	1K, 500KB, 1MB
	Cipher Suite	(*), (+)

Host Test Factors

Factor-1	Factor-2	Factor-2 Levels
No VMI With VMI	File Read	1MB, 10MB, 100MB
	File Write	1MB, 10MB, 100MB

\*TLS ECDHE ECDSA WITH AES 128 GCM SHA256

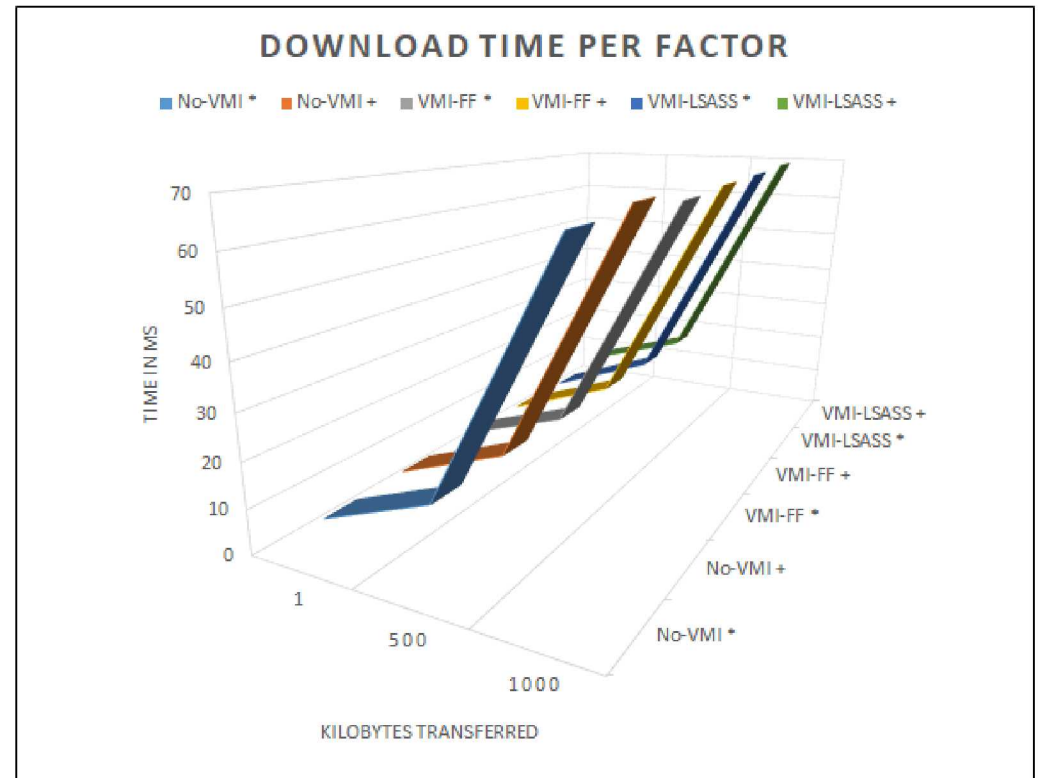
+TLS ECDHE ECDSA WITH AES 256 CBC SHA



X-axis: number of bytes transferred (file size)

Y-axis: the average time to download.

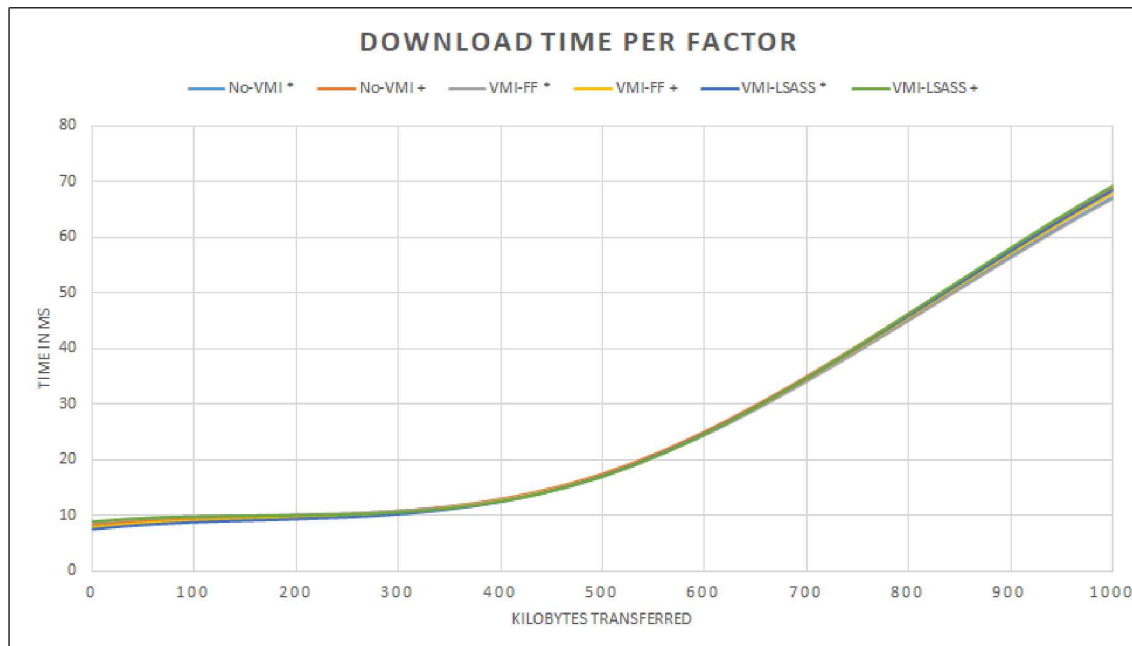
The times for each factor combination are almost identical. (Actual values are on the next slide).



NETWORK EXPERIMENT RESULTS (ALL TIMES IN MILLISECONDS.)

<b>No-VMI*</b>	<b>1KB</b>	<b>500KB</b>	<b>1MB</b>	<b>VMI-FF*</b>	<b>1KB</b>	<b>500KB</b>	<b>1MB</b>	<b>VMI-L*</b>	<b>1KB</b>	<b>500KB</b>	<b>1MB</b>
Mean	7.99	17.19	67.17	Mean	8.85	17.12	66.81	Mean	7.54	17.00	68.32
Std Dev	1.95	2.28	3.21	Std Dev	2.07	1.91	2.94	Std Dev	1.79	1.88	2.43
<b>No-VMI+</b>	<b>1KB</b>	<b>500KB</b>	<b>1MB</b>	<b>VMI-FF+</b>	<b>1KB</b>	<b>500KB</b>	<b>1MB</b>	<b>VMI-L+</b>	<b>1KB</b>	<b>500KB</b>	<b>1MB</b>
Mean	8.34	17.42	68.77	Mean	8.01	17.21	67.80	Mean	9.00	17.03	69.24
Std Dev	1.97	2.38	2.98	Std Dev	2.30	1.99	3.01	Std Dev	1.55	2.31	2.33

Means times to download the files, and their standard deviations, are very similar





For host-based experiment, t-test used to compare the data sets; lack of VMI used as the population – Null hypothesis is that with VMI enabled, observations shall not be significantly different than without VMI.

HOST TEST RESULTS: FILE WRITE

<b>No-VMI</b>	<b>1 MB (ms)</b>	<b>10 MB (ms)</b>	<b>100 MB (ms)</b>
Mean	8.50	12.167	75.58
Std Dev	2.77	2.68	4.75
<b>VMI</b>	<b>1 MB (ms)</b>	<b>10 MB (ms)</b>	<b>100 MB (ms)</b>
Mean	8.44	11.79	76.97
Std Dev	2.77	3.42	5.48

HOST TEST RESULTS: FILE READS

<b>No-VMI</b>	<b>1 MB (ms)</b>	<b>10 MB (ms)</b>	<b>100 MB (ms)</b>
Mean	29.78	71.37	653.14
Std Dev	5.79	7.47	15.71
<b>VMI</b>	<b>1 MB (ms)</b>	<b>10 MB (ms)</b>	<b>100 MB (ms)</b>
Mean	28.18	73.24	660.14
Std Dev	6.14	6.59	21.45

Write 1MB:	$p = 0.914046758$
Write 10MB:	$p = 0.646450549$
Write 100MB:	$p = 0.308094339$
Read 1MB:	$p = 0.313688073$
Read 10MB:	$p = 0.317179742$
Read 100MB:	$p = 0.162026589$

Considering all of the p-values being higher than a 0.05 significance, we can accept the null hypothesis that there is no significant difference between file reading and writing with or without VMI running.

AMD Secure Encrypted Virtualization (SEV) and SEV with Encrypted State

- Requires support from the virtualized OS

Intel Software Guard Extensions (SGX) to create a Trusted Execution Environment (TEE)

- Creates enclaves running in isolated hardware-encrypted memory
- High overhead, limited set of instructions (based on rings)
- Limitations of encrypted memory (Encrypted Page Cache)

Hypervisor Architectures, e.g., Hyper-V or Azure

- Hypervisor boot sequence (root partition), view of system memory by hypervisor
- Can leverage VT-d to prevent DMA, and EPT to block memory access

Use EPT and VT-d to protect guest memory

- Thwarts LSASS attack
- Not done by default in many hypervisors
  - Hyper-V may have ability to do so with Virtual Trust Levels (VTL)



Several inherent risks to the protection of user data in IaaS environments

Encryption may not be the ultimate safeguarding mechanism to ensure confidentiality and privacy of data

Transparent decryption of data at-rest and in-motion, transparently, is possible.

Knowledge, awareness, and implementing mitigations where possible may help to build trust in an untrusted environment.

# Get Your Head Out of the Clouds: The Illusion of Confidentiality & Privacy



*PRESENTED BY*

Vince Urias and Caleb Loverro



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.