SAND2018-12963C

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

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.

OVERVIEW

- Introduction
- Thwarting Encryption At-Rest and In-Motion
  - Through Virtual Machine Introspection
- Addressing Transparency
- Conclusions
  - Suggested Mitigations

INTRODUCTION

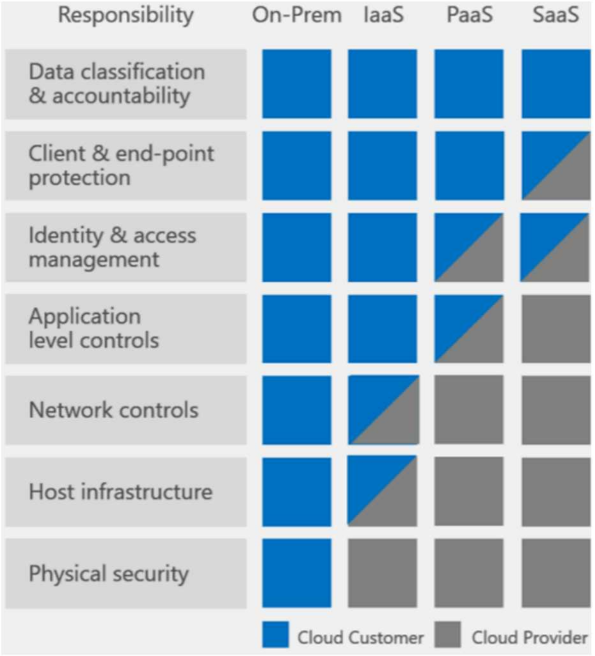
Numerous government and industry entities are moving to the cloud

- 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



INTRODUCTION

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.

THWARTING ENCRYPTION

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

THWARTING ENCRYPTION:
Understanding VMI

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

THWARTING ENCRYPTION:
Understanding VMI

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)

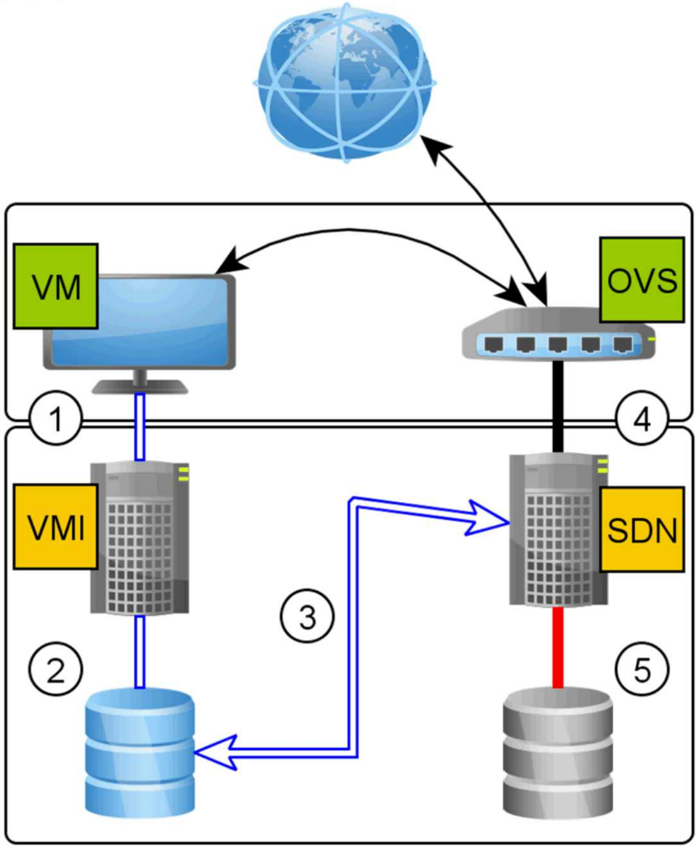
- Local Security Authority Subsystem Service (LSASS) – repository for all session keys
- VMI tool isolates guest page tables and EPT, to enumerate ring3-available memory in the LSASS process
- Keys ID'd via two 4-byte magic values and a C++ object

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.



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 Linus 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

TRANSPARENCY

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

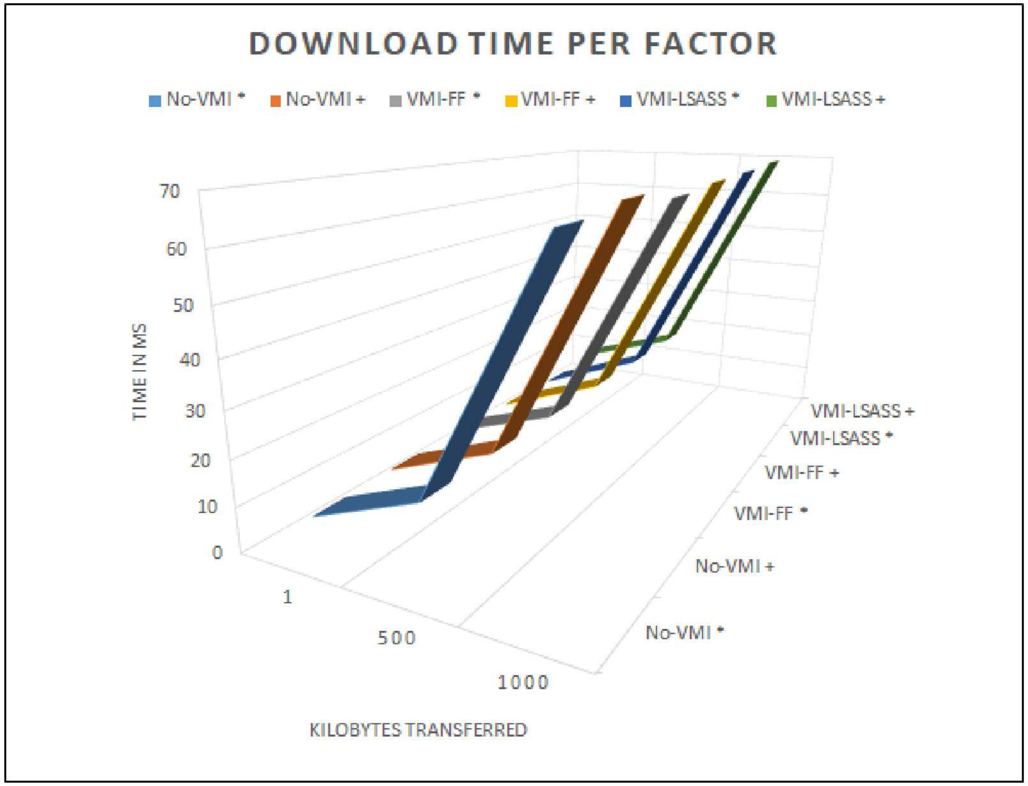
*TLS ECDHE ECDSA WITH AES 128 GCM SHA256
+TLS ECDHE ECDSA WITH AES 256 CBC SHA

TRANSPARENCY

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).

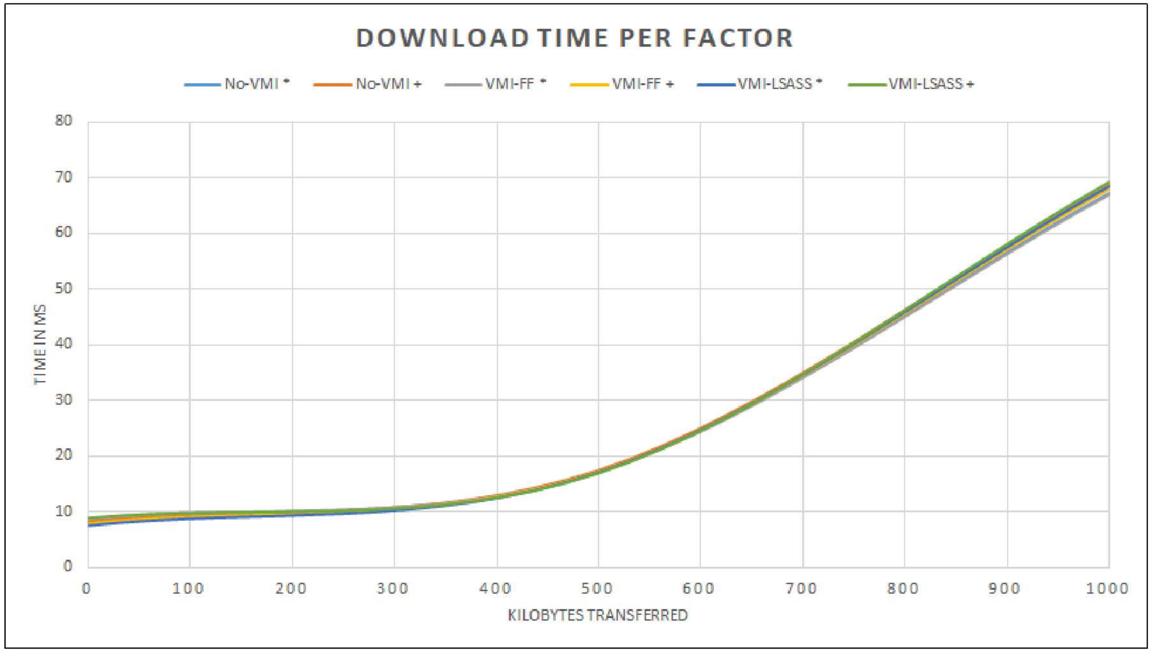


TRANSPARENCY

NETWORK EXPERIMENT RESULTS (ALL TIMES IN MILLISECONDS.)

No-VMI*	1KB	500KB	1MB	VMI-FF*	1KB	500KB	1MB	VMI-L*	1KB	500KB	1MB
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
No-VMI+	**1KB**	**500KB**	**1MB**	**VMI-FF+**	**1KB**	**500KB**	**1MB**	**VMI-L+**	**1KB**	**500KB**	**1MB**
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



TRANSPARENCY

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

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

HOST TEST RESULTS: FILE READS

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

TRANSPARENCY

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.

CONCLUSION AND MITIGATIONS

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)

CONCLUSIONS

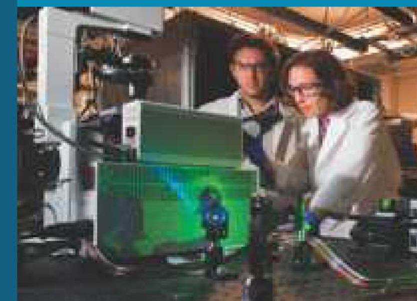
Several inherent risks to the protection of user data in IaaS environments

Encryption may not the ultimate safeguarding mechanism to ensure confidential 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.