All You Ever Wanted to Know About Virtual Machine Introspection: Hands-on Labs and Conclusion

Zhiqiang Lin

Department of Computer Sciences
The University of Texas at Dallas

August 24^{th}, 2015

Outline

1. Hands-on-Labs
2. Conclusion
3. Reference

Outline

1. Hands-on-Labs

2. Conclusion

3. Reference

Hands-on Labs

1. Using kernel debugging tool (redhat `crash` utility) to inspect kernel states
2. Using volatility tool to perform memory introspection

Linux memory introspection w/ crash

```
root@debian:~/crash# ./run-crash.sh

crash 4.1.2
Copyright (C) 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009  Red Hat, Inc.
GNU gdb 6.1
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i686-pc-linux-gnu"...

crash: cannot set context for pid: 8257
      KERNEL: ./vmlinux-2.6.18sa
    DUMPFILE: /tmp/crash/mem
        CPUS: 1
        DATE: Wed Jan 27 14:19:01 2010
      UPTIME: 2 days, 02:47:14
LOAD AVERAGE: 0.22, 0.07, 0.02
       TASKS: 92
    NODENAME: hope
     RELEASE: 2.6.18sa
     VERSION: #1 SMP Wed Jan 6 00:41:44 EST 2010
     MACHINE: i686  (2127 Mhz)
      MEMORY: 255.9 MB
         PID: 0
     COMMAND: "swapper"
        TASK: c035dc00  [THREAD_INFO: c0426000]
         CPU: 0
       STATE: TASK_RUNNING (ACTIVE)
```

Linux memory introspection w/ `crash`

```
crash> help

*              files          mod            runq           union
alias          foreach        mount          search         vm
ascii          fuser          net            set            vtop
bt             gdb            p              sig            waitq
btop           help           ps             struct         whatis
dev            irq            pte            swap           wr
dis            kmem           ptob           sym            q
eval           list           ptov           sys
exit           log            rd             task
extend         mach           repeat         timer

crash version: 4.1.2    gdb version: 6.1
For help on any command above, enter "help <command>".
For help on input options, enter "help input".
For help on output options, enter "help output".

CRSEOF
crash>
```

Windows Memory Forensics with Volatility

```
root@debian:~/volatility-2.4# vol.py -h
Volatility Foundation Volatility Framework 2.4
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the timezone for displaying timestamps
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --output-file=OUTPUT_FILE
                        write output in this file
  -v, --verbose         Verbose information
  -g KDBG, --kdbg=KDBG  Specify a specific KDBG virtual address
  -k KPCR, --kpcr=KPCR  Specify a specific KPCR address

        Supported Plugin Commands:

                apihooks        Detect API hooks in process and kernel memory
                atoms           Print session and window station atom tables
                atomscan        Pool scanner for atom tables
```

Windows Memory Forensics with Volatility

```
root@debian:~/windows# vol.py pslist -f hidden_process.img
Volatility Foundation Volatility Framework 2.4
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------
0x819cc830 System                    4      0     51      254 ------      0
0x817e4670 smss.exe                360      4      3       19 ------      0 2008-11-26 07:38:
0x8181bd78 csrss.exe               596    360     10      322      0      0 2008-11-26 07:38:
0x8182b100 winlogon.exe            620    360     16      503      0      0 2008-11-26 07:38:
0x8183ba78 services.exe            672    620     15      245      0      0 2008-11-26 07:38:
...

root@debian:~/windows# vol.py psscan -f hidden_process.img
Volatility Foundation Volatility Framework 2.4
Offset(P)          Name                PID   PPID PDB        Time created                   T
------------------ ---------------- ------ ------ ---------- ------------------------------ -
0x000000000181b748 alg.exe             992    660 0x08140260 2008-11-15 23:43:25 UTC+0000
0x0000000001843b28 wuauclt.exe        1372   1064 0x08140180 2008-11-26 07:39:38 UTC+0000
0x000000000184e3a8 wscntfy.exe         560   1064 0x081402a0 2008-11-26 07:44:57 UTC+0000
...
root@debian:~/windows# vol.py psxview -f hidden_process.img
Volatility Foundation Volatility Framework 2.4
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd E
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- -
0x01a2b100 winlogon.exe            620 True   True   True     True   True  True    True
0x01a3d360 svchost.exe             932 True   True   True     True   True  True    True
```

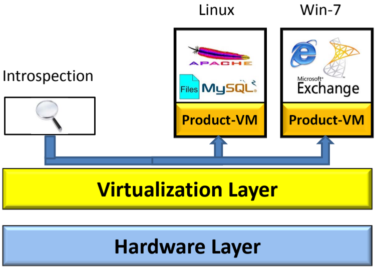
Outline

1. Hands-on-Labs

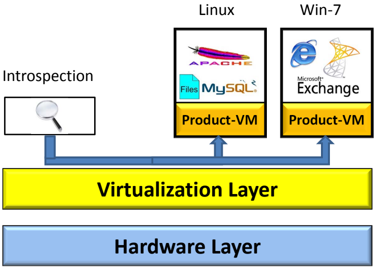
2. Conclusion

3. Reference

Virtual Machine Introspection

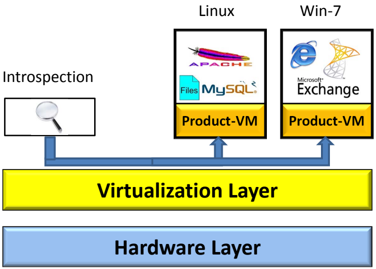


Virtual Machine Introspection



- Isolation, portability, reliability, trustworthiness, automation, security, transparency ...

Virtual Machine Introspection



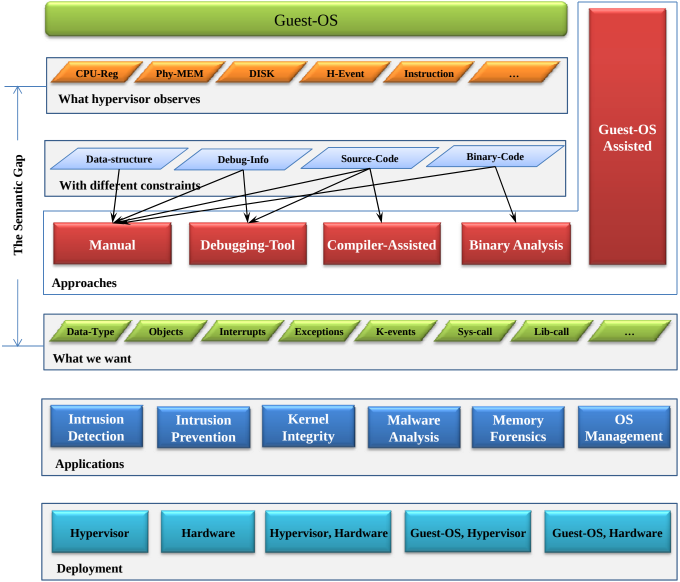
- Isolation, portability, reliability, trustworthiness, automation, security, transparency ...

- Virtual Machine Introspection
- Virtual Machine (Re)Configuration, Repair
- Automated Out-of-VM Management via HyperShell

Future Directions

1. Protecting the Hypervisor Itself
   - Pushing one layer down to hardware
   - Improving the hypervisor code
   - Deprivilege the hypervisor
2. Providing High Fidelity Hypervisor
3. Complete Memory Monitoring (including swapped memory)
4. Complete Disk Monitoring (including FDE protected disk)
5. Beyond Read-Only Introspection
6. Beyond the guest OS kernel and traditional platform (e.g., mobile)

Take Away



Guest-OS

CPU-Reg · Phy-MEM · DISK · H-Event · Instruction · …

What hypervisor observes

Data-structure · Debug-Info · Source-Code · Binary-Code

With different constraints

Manual · Debugging-Tool · Compiler-Assisted · Binary Analysis

Guest-OS Assisted

Approaches

The Semantic Gap

Data-Type · Objects · Interrupts · Exceptions · K-events · Sys-call · Lib-call · …

What we want

Intrusion Detection · Intrusion Prevention · Kernel Integrity · Malware Analysis · Memory Forensics · OS Management

Applications

Hypervisor · Hardware · Hypervisor, Hardware · Guest-OS, Hypervisor · Guest-OS, Hardware

Deployment

Outline

1. Hands-on-Labs
2. Conclusion
3. Reference

References I

2006.
Implementing and Detecting a PCI Rootkit.
(2006).
http://www.blackhat.com/presentations/bh-dc-07/Heasman/Paper/bh-dc-07-Heasman-WP.pdf.

Martín Abadi, Mihai Budiu, Úlfar Erlingsson, and Jay Ligatti. 2005.
Control-flow Integrity. In Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS '05). ACM, New York, NY, USA, 340–353.
DOI:http://dx.doi.org/10.1145/1102120.1102165

Keith Adams and Ole Agesen. 2006.
A Comparison of Software and Hardware Techniques for x86 Virtualization. In Proceedings of the 12th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS XII). 2–13.
DOI:http://dx.doi.org/10.1145/1168919.1168860

David Anderson. 2003.
White Paper: Red Hat Crash Utility.
(2003).
http://people.redhat.com/anderson/crash_whitepaper/.

A.M. Azab, Peng Ning, E.C. Sezer, and Xiaolan Zhang. 2009.
HIMA: A Hypervisor-Based Integrity Measurement Agent. In Computer Security Applications Conference, 2009. ACSAC '09. Annual. 461–470.
DOI:http://dx.doi.org/10.1109/ACSAC.2009.50

References II

Ahmed M. Azab, Peng Ning, Jitesh Shah, Quan Chen, Rohan Bhutkar, Guruprasad Ganesh, Jia Ma, and Wenbo Shen. 2014.
Hypervision Across Worlds: Real-time Kernel Protection from the ARM TrustZone Secure World. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). ACM, New York, NY, USA, 90–102.
DOI:http://dx.doi.org/10.1145/2660267.2660350

Ahmed M. Azab, Peng Ning, Zhi Wang, Xuxian Jiang, Xiaolan Zhang, and Nathan C. Skalsky. 2010.
HyperSentry: enabling stealthy in-context measurement of hypervisor integrity. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). 38–49.
DOI:http://dx.doi.org/10.1145/1866307.1866313

Arati Baliga, Vinod Ganapathy, and Liviu Iftode. 2008.
Automatic Inference and Enforcement of Kernel Data Structure Invariants. In Proceedings of the 2008 Annual Computer Security Applications Conference (ACSAC '08). IEEE Computer Society, Washington, DC, USA, 77–86.
DOI:http://dx.doi.org/10.1109/ACSAC.2008.29

Davide Balzarotti, Marco Cova, Christoph Karlberger, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. 2010.
Efficient Detection of Split Personalities in Malware. In 17th Annual Network and Distributed System Security Symposium (NDSS 2010).
http://www.isoc.org/isoc/conferences/ndss/10/pdf/24.pdf

Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield. 2003.
Xen and the art of virtualization. In Proceedings of the nineteenth ACM symposium on Operating systems principles (SOSP '03). 164–177.
DOI:http://dx.doi.org/10.1145/945445.945462

References III

Ulrich Bayer, Paolo Milani Comparetti, Clemens Hlauschek, Christopher Krügel, and Engin Kirda. 2009.
Scalable, Behavior-Based Malware Clustering. In Proceedings of the 2009 Annual Network and Distributed System Security Symposium (NDSS).
http://www.isoc.org/isoc/conferences/ndss/09/pdf/11.pdf

Antonio Bianchi, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. 2012.
Blacksheep: detecting compromised hosts in homogeneous crowds. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, Raleigh, North Carolina, USA, 341–352.
DOI:http://dx.doi.org/10.1145/2382196.2382234

Matt Bishop. 2002.
Computer Security: Art and Science (1 ed.).
Addison-Wesley Professional.

Martim Carbone, Matthew Conover, Bruce Montague, and Wenke Lee. 2012.
Secure and robust monitoring of virtual machines through guest-assisted introspection. In Proceedings of the 15th international conference on Research in Attacks, Intrusions, and Defenses (RAID'12). 22–41.
DOI:http://dx.doi.org/10.1007/978-3-642-33338-5_2

Martim Carbone, Weidong Cui, Long Lu, Wenke Lee, Marcus Peinado, and Xuxian Jiang. 2009.
Mapping kernel objects to enable systematic integrity checking. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). 555–565.
DOI:http://dx.doi.org/10.1145/1653662.1653729

Peter M. Chen and Brian D. Noble. 2001.
When Virtual Is Better Than Real. In Proceedings of the Eighth Workshop on Hot Topics in Operating Systems (HOTOS '01). 133–.
http://dl.acm.org/citation.cfm?id=874075.876409

References IV

- Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmanyam, Carl A. Waldspurger, Dan Boneh, Jeffrey Dwoskin, and Dan R.K. Ports. 2008.
  Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems. In Proceedings of the 13th international conference on Architectural support for programming languages and operating systems (ASPLOS XIII). ACM, New York, NY, USA, 2–13.
  DOI:http://dx.doi.org/10.1145/1353536.1346284

- Weidong Cui, Marcus Peinado, Zhilei Xu, and Ellick Chan. 2012.
  Tracking rootkit footprints with a practical memory analysis system. In Proceedings of the 21st USENIX conference on Security symposium (Security'12). 42–42.
  http://dl.acm.org/citation.cfm?id=2362793.2362835

- Robert Denz and Stephen Taylor. 2013.
  A survey on securing the virtual cloud.
  Journal of Cloud Computing 2, 1 (2013), 1–9.

- Edsger W. Dijkstra. 1968.
  The structure of the THE-multiprogramming system.
  Commun. ACM 11 (May 1968), 341–346.
  Issue 5. DOI:http://dx.doi.org/10.1145/357980.357999

- Artem Dinaburg, Paul Royal, Monirul Sharif, and Wenke Lee. 2008.
  Ether: malware analysis via hardware virtualization extensions. In Proceedings of the 15th ACM conference on Computer and communications security (CCS '08). 51–62.
  DOI:http://dx.doi.org/10.1145/1455770.1455779

References V

Brendan Dolan-Gavitt, Tim Leek, Josh Hodosh, and Wenke Lee. 2013.
Tappan Zee (North) Bridge: Mining Memory Accesses for Introspection. In Proceedings of the ACM Conference on Computer and Communications Security (CCS). ACM, New York, NY, USA.
DOI:http://dx.doi.org/10.1145/2508859.2516697

Brendan Dolan-Gavitt, Tim Leek, Michael Zhivich, Jonathon Giffin, and Wenke Lee. 2011a.
Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. In Proceedings of 2011 IEEE Symposium on Security and Privacy. IEEE Computer Society, Oakland, CA, USA, 297–312.
DOI:http://dx.doi.org/10.1109/SP.2011.11

Brendan Dolan-Gavitt, Bryan Payne, and Wenke Lee. 2011b.
Leveraging Forensic Tools for Virtual Machine Introspection.
Technical Report; GT-CS-11-05 (2011).

Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. 2009.
Robust Signatures for Kernel Data Structures. In Proceedings of the ACM Conference on Computer and Communications Security (CCS). ACM, New York, NY, USA.
DOI:http://dx.doi.org/10.1145/1653662.1653730

M. Egele, C. Kruegel, E. Kirda, H. Yin, and D. Song. 2007.
Dynamic Spyware Analysis. In Proceedings of the 2007 Usenix Annual Conference (Usenix'07). USENIX Association.
http://dl.acm.org/citation.cfm?id=1364385.1364403

Shawn Embleton, Sherri Sparks, and Cliff Zou. 2008.
SMM rootkits: a new breed of OS independent malware. In Proceedings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08). Article 11, 12 pages.
DOI:http://dx.doi.org/10.1145/1460877.1460892

References VI

S. Forrest, S.A. Hofmeyr, A. Somayaji, and T.A. Longstaff. 1996.
A sense of self for Unix processes. In Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on. 120–128.
DOI:http://dx.doi.org/10.1109/SECPRI.1996.502675

T. Fraser, M.R. Evenson, and W.A. Arbaugh. 2008.
VICI Virtual Machine Introspection for Cognitive Immunity. In Computer Security Applications Conference, 2008. ACSAC 2008. Annual. 87–96.
DOI:http://dx.doi.org/10.1109/ACSAC.2008.33

Yangchun Fu and Zhiqiang Lin. 2012.
Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection. In 2012 IEEE Symposium on Security and Privacy. IEEE Computer Society, 586–600.
DOI:http://dx.doi.org/10.1109/SP.2012.40

Yangchun Fu and Zhiqiang Lin. 2013a.
Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection. ACM Trans. Inf. Syst. Secur. 16, 2 (2013).
DOI:http://dx.doi.org/10.1145/2505124

Yangchun Fu and Zhiqiang Lin. 2013b.
EXTERIOR: using a dual-VM based external shell for guest-OS introspection, configuration, and recovery. In Proceedings of the 9th ACM SIGPLAN/SIGOPS international conference on Virtual execution environments (VEE '13). 97–110.
DOI:http://dx.doi.org/10.1145/2451512.2451534

References VII

Yangchun Fu, Zhiqiang Lin, and Kevin Hamlen. 2013.
Subverting Systems Authentication with Context-aware, Reactive Virtual Machine Introspection. In Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC'13). New Orleans, Louisiana.
DOI:http://dx.doi.org/10.1145/2523649.2523664

Yangchun Fu, Junyuan Zeng, and Zhiqiang Lin. 2014.
HYPERSHELL: A Practical Hypervisor Layer Guest OS Shell for Automated in-VM Management. In Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference (USENIX ATC'14). USENIX Association, Berkeley, CA, USA, 85–96.
http://dl.acm.org/citation.cfm?id=2643634.2643644

Tal Garfinkel and Mendel Rosenblum. 2003.
A virtual machine introspection based architecture for intrusion detection. In Proceedings Network and Distributed Systems Security Symposium (NDSS'03).
http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/13.pdf

Zhongshu Gu, Zhui Deng, Dongyan Xu, and Xuxian Jiang. 2011.
Process Implanting: A New Active Introspection Framework for Virtualization. In Proceedings of the 2011 IEEE 30th International Symposium on Reliable Distributed Systems (SRDS '11). 147–156.
DOI:http://dx.doi.org/10.1109/SRDS.2011.26

Brian Hay and Kara Nance. 2008.
Forensics examination of volatile system data using virtual introspection.
SIGOPS Operating System Review 42 (April 2008), 74–82.
Issue 3. DOI:http://dx.doi.org/10.1145/1368506.1368517

References VIII

Jennia Hizver and Tzi-cker Chiueh. 2014.
Real-time Deep Virtual Machine Introspection and Its Applications. In Proceedings of the 10th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE '14). ACM, New York, NY, USA, 3–14.
DOI:http://dx.doi.org/10.1145/2576195.2576196

Owen S. Hofmann, Alan M. Dunn, Sangman Kim, Indrajit Roy, and Emmett Witchel. 2011.
Ensuring operating system kernel integrity with OSck. In Proceedings of the sixteenth international conference on Architectural support for programming languages and operating systems (ASPLOS XVI). 279–290.
DOI:http://dx.doi.org/10.1145/1950365.1950398

Bhushan Jain, Mirza Basim Baig, Dongli Zhang, Donald E Porter, and Radu Sion. 2014.
SoK: Introspections on Trust and the Semantic Gap.
(2014).
DOI:http://dx.doi.org/10.1109/SP.2014.45

Xuxian Jiang and Xinyuan Wang. 2007.
"Out-of-the-Box" monitoring of VM-based high-interaction honeypots. In Proceedings of the 10th international conference on Recent advances in intrusion detection (RAID'07). 198–218.
DOI:http://dx.doi.org/10.1007/978-3-540-74320-0_11

Xuxian Jiang, Xinyuan Wang, and Dongyan Xu. 2007.
Stealthy malware detection through vmm-based out-of-the-box semantic view reconstruction. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07). Alexandria, Virginia, USA, 128–138.
DOI:http://dx.doi.org/10.1145/1315245.1315262

References IX

Stephen T. Jones, Andrea C. Arpaci-Dusseau, and Remzi H. Arpaci-Dusseau. 2006.
Antfarm: tracking processes in a virtual machine environment. In Proceedings of the annual conference on USENIX '06 Annual Technical Conference.
http://dl.acm.org/citation.cfm?id=1267359.1267360

Stephen T. Jones, Andrea C. Arpaci-Dusseau, and Remzi H. Arpaci-Dusseau. 2008.
VMM-based hidden process detection and identification using Lycosid. In Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments (VEE '08). 91–100.
DOI:http://dx.doi.org/10.1145/1346256.1346269

Ashlesha Joshi, Samuel T. King, George W. Dunlap, and Peter M. Chen. 2005.
Detecting past and present intrusions through vulnerability-specific predicates. In Proceedings of the twentieth ACM symposium on Operating systems principles (SOSP '05). ACM, 91–104.
DOI:http://dx.doi.org/10.1145/1095809.1095820

Eric Keller, Jakub Szefer, Jennifer Rexford, and Ruby B. Lee. 2010.
NoHype: virtualized cloud infrastructure without the virtualization. In Proceedings of the 37th annual international symposium on Computer architecture (ISCA '10). 350–361.
DOI:http://dx.doi.org/10.1145/1816038.1816010

Gene H. Kim and Eugene H. Spafford. 1994.
The design and implementation of tripwire: a file system integrity checker. In Proceedings of the 2nd ACM Conference on Computer and Communications Security (CCS'94). ACM, Fairfax, Virginia, United States, 18–29.
DOI:http://dx.doi.org/10.1145/191177.191183

References X

Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, and Jacob R. Lorch. 2006.
SubVirt: Implementing malware with virtual machines. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP '06). 314–327.
DOI:http://dx.doi.org/10.1109/SP.2006.38

Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. 2009.
seL4: formal verification of an OS kernel. In Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles. ACM, 207–220.
DOI:http://dx.doi.org/10.1145/1629575.1629596

Srinivas Krishnan, Kevin Z. Snow, and Fabian Monrose. 2010.
Trail of bytes: efficient support for forensic analysis. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, 50–60.
DOI:http://dx.doi.org/10.1145/1866307.1866314

Stephen Kuhn and Stephen Taylor. 2011.
A survey of forensic analysis in virtualized environments.
Dartmouth College, Hanover, New Hampshire, Tech. Rep (2011).

Andrea Lanzi, Monirul I. Sharif, and Wenke Lee. 2009.
K-Tracer: A System for Extracting Kernel Malware Behavior. In Proceedings of the 2009 Annual Network and Distributed System Security Symposium (NDSS).
http://www.isoc.org/isoc/conferences/ndss/09/pdf/12.pdf

References XI

Ben Laurie and Abe Singer. 2008.
Choose the red pill and the blue pill: A position paper. In Proceedings of the 2008 Workshop on New Security Paradigms. ACM, New York, NY, USA, 127–133.
DOI:http://dx.doi.org/10.1145/1595676.1595695

Hojoon Lee, Hyungon Moon, Daehee Jang, Kihwan Kim, Jihoon Lee, Yunheung Paek, and Brent ByungHoon Kang. 2013.
KI-Mon: a hardware-assisted event-triggered monitoring platform for mutable kernel object. In Proceedings of the 22nd USENIX conference on Security. USENIX Association, 511–526.
http://dl.acm.org/citation.cfm?id=2534766.2534810

Wenhao Li, Yubin Xia, Haibo Chen, Binyu Zang, and Haibing Guan. 2015.
Reducing World Switches in Virtualized Environment with Flexible Cross-world Calls. In Proceedings of the 42Nd Annual International Symposium on Computer Architecture (ISCA '15). ACM, New York, NY, USA, 375–387.
DOI:http://dx.doi.org/10.1145/2749469.2750406

Zhiqiang Lin. 2013.
Toward Guest OS Writable Virtual Machine Introspection.
VMware Technical Journal 2, 2 (2013).

Zhiqiang Lin, Junghwan Rhee, Xiangyu Zhang, Dongyan Xu, and Xuxian Jiang. 2011.
SigGraph: Brute Force Scanning of Kernel Data Structure Instances Using Graph-based Signatures. In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS'11). San Diego, CA.
http://www.isoc.org/isoc/conferences/ndss/11/pdf/3_3.pdf

References XII

Lionel Litty, H. Andrés Lagar-Cavilla, and David Lie. 2008.
Hypervisor support for identifying covertly executing binaries. In Proceedings of the 17th conference on Security symposium (SS'08). 243–258.
http://dl.acm.org/citation.cfm?id=1496711.1496728

Yutao Liu, Yubin Xia, Haibing Guan, Binyu Zang, and Haibo Chen. 2014.
Concurrent and consistent virtual machine introspection with hardware transactional memory. In High Performance Computer Architecture (HPCA), 2014 IEEE 20th International Symposium on. IEEE, 416–427.
DOI:http://dx.doi.org/10.1109/HPCA.2014.6835951

Ziyi Liu, JongHyuk Lee, Junyuan Zeng, Yuanfeng Wen, Zhiqiang Lin, and Weidong Shi. 2013.
CPU transparent protection of OS kernel and hypervisor integrity with programmable DRAM. In Proceedings of the 40th Annual International Symposium on Computer Architecture (ISCA '13). 392–403.
DOI:http://dx.doi.org/10.1145/2485922.2485956

Lorenzo Martignoni, Stephen McCamant, Pongsin Poosankam, Dawn Song, and Petros Maniatis. 2012.
Path-exploration lifting: hi-fi tests for lo-fi emulators. In Proceedings of the seventeenth international conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS XVII). London, England, UK, 337–348.
DOI:http://dx.doi.org/10.1145/2150976.2151012

Hyungon Moon, Hojoon Lee, Jihoon Lee, Kihwan Kim, Yunheung Paek, and Brent Byunghoon Kang. 2012.
Vigilare: toward snoop-based kernel integrity monitor. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). 28–37.
DOI:http://dx.doi.org/10.1145/2382196.2382202

References XIII

George C. Necula, Scott McPeak, Shree Prakash Rahul, and Westley Weimer. 2002.
CIL: Intermediate Language and Tools for Analysis and Transformation of C Programs. In Proceedings of the 11th International Conference on Compiler Construction (CC '02). 213–228.
http://dl.acm.org/citation.cfm?id=647478.727796

A.M. Nguyen, N. Schear, HeeDong Jung, A. Godiyal, S.T. King, and H.D. Nguyen. 2009.
MAVMM: Lightweight and Purpose Built VMM for Malware Analysis. In Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC'09). 441–450.
DOI:http://dx.doi.org/10.1109/ACSAC.2009.48

Daniela Oliveira and Shyhtsun Felix Wu. 2009.
Protecting Kernel Code and Data with a Virtualization-Aware Collaborative Operating System. In Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC'09). 451–460.
DOI:http://dx.doi.org/10.1109/ACSAC.2009.49

Roberto Paleari, Lorenzo Martignoni, Emanuele Passerini, Drew Davidson, Matt Fredrikson, Jon Giffin, and Somesh Jha. 2010.
Automatic generation of remediation procedures for malware infections. In Proceedings of the 19th USENIX conference on Security.
http://dl.acm.org/citation.cfm?id=1929820.1929856

Bryan D. Payne, Martim Carbone, and Wenke Lee. 2007.
Secure and Flexible Monitoring of Virtual Machines. In Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC 2007).
DOI:http://dx.doi.org/10.1109/ACSAC.2007.10

References XIV

Bryan D. Payne, Martim Carbone, Monirul I. Sharif, and Wenke Lee. 2008.
Lares: An Architecture for Secure Active Monitoring Using Virtualization. In Proceedings of 2008 IEEE Symposium on Security and Privacy. IEEE Computer Society, Washington, DC, USA, 233–247.
DOI:http://dx.doi.org/10.1109/SP.2008.24

Nick L. Petroni, Jr., Timothy Fraser, Jesus Molina, and William A. Arbaugh. 2004.
Copilot - A coprocessor-based kernel runtime integrity monitor. In Proceedings of the 13th USENIX Security Symposium. San Diego, CA, 179–194.
http://dl.acm.org/citation.cfm?id=1251375.1251388

Nick L. Petroni, Jr., Timothy Fraser, AAron Walters, and William A. Arbaugh. 2006.
An architecture for specification-based detection of semantic integrity violations in kernel dynamic data. In Proceedings of the 15th conference on USENIX Security Symposium. USENIX Association.
http://dl.acm.org/citation.cfm?id=1267336.1267356

Nick L. Petroni, Jr. and Michael Hicks. 2007.
Automated detection of persistent kernel control-flow attacks. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). ACM, 103–115.
DOI:http://dx.doi.org/10.1145/1315245.1315260

Gerald J. Popek and Robert P. Goldberg. 1974.
Formal requirements for virtualizable third generation architectures.
Commun. ACM 17, 7 (1974), 412–421.
DOI:http://dx.doi.org/10.1145/361011.361073

References XV

Aravind Prakash, Eknath Venkataramani, Heng Yin, and Zhiqiang Lin. 2013.
Manipulating Semantic Values in Kernel Data Structures: Attack Assessments and Implications. In Proceedings of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks(DSN-PDS 2013). Budapest, Hungary.
DOI:http://dx.doi.org/10.1109/DSN.2013.6575344

Aravind Prakash, Eknath Venkataramani, Heng Yin, and Zhiqiang Lin. 2014.
On the Trustworthiness of Memory Analysis—An Empirical Study from the Perspective of Binary Execution. IEEE Transactions on Dependable and Secure Computing (2014).
DOI:http://dx.doi.org/10.1109/TDSC.2014.2366464

Junghwan Rhee, Zhiqiang Lin, and Dongyan Xu. 2011.
Characterizing Kernel Malware Behavior with Kernel Data Access Patterns. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. Hong Kong.
DOI:http://dx.doi.org/10.1145/1966913.1966940

Junghwan Rhee, Ryan Riley, Dongyan Xu, and Xuxian Jiang. 2010.
Kernel malware analysis with un-tampered and temporal views of dynamic kernel memory. In Proceedings of the 13th international conference on Recent advances in intrusion detection (RAID'10). 178–197.
http://dl.acm.org/citation.cfm?id=1894166.1894179

Ryan Riley, Xuxian Jiang, and Dongyan Xu. 2008.
Guest-Transparent Prevention of Kernel Rootkits with VMM-Based Memory Shadowing. In Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection (RAID '08). 1–20.
DOI:http://dx.doi.org/10.1007/978-3-540-87403-4_1

References XVI

Ryan Riley, Xuxian Jiang, and Dongyan Xu. 2009.
Multi-aspect profiling of kernel rootkit behavior. In Proceedings of the 4th ACM European conference on Computer systems (EuroSys '09). 47–60.
DOI:http://dx.doi.org/10.1145/1519065.1519072

Alireza Saberi, Yangchun Fu, and Zhiqiang Lin. 2014.
Hybrid-Bridge: Efficiently Bridging the Semantic-Gap in Virtual Machine Introspection via Decoupled Execution and Training Memoization. In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14). San Diego, CA.
http://www.internetsociety.org/doc/
hybrid-bridge-efficiently-bridging-semantic-gap-virtual-machine-introspection-decouple

Arvind Seshadri, Mark Luk, Ning Qu, and Adrian Perrig. 2007.
SecVisor: a tiny hypervisor to provide lifetime kernel code integrity for commodity OSes. In Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles (SOSP '07). ACM, New York, NY, USA, 335–350.
DOI:http://dx.doi.org/10.1145/1294261.1294294

Monirul I. Sharif, Wenke Lee, Weidong Cui, and Andrea Lanzi. 2009.
Secure in-VM monitoring using hardware virtualization. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). 477–487.
DOI:http://dx.doi.org/10.1145/1653662.1653720

Kevin Snow, Srinivas Krishnan, Fabian Monrose, and Niels Provos. 2011.
ShellOS: Enabling fast detection and forensic analysis of code injection attacks. In Proceedings of the 20th USENIX Security Symposium.
http://static.usenix.org/events/sec11/tech/full_papers/Snow.pdf

References XVII

Deepa Srinivasan, Zhi Wang, Xuxian Jiang, and Dongyan Xu. 2011.
Process out-grafting: an efficient "out-of-VM" approach for fine-grained process execution monitoring. In Proceedings of the 18th ACM conference on Computer and communications security (CCS'11). ACM, Chicago, Illinois, USA, 363–374.
DOI:http://dx.doi.org/10.1145/2046707.2046751

Abhinav Srivastava and Jonathon Giffin. 2011.
Efficient monitoring of untrusted kernel-mode execution. In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS 2011).
http://www.isoc.org/isoc/conferences/ndss/11/pdf/3_2.pdf

Abhinav Srivastava and Jonathon Giffin. 2012.
Efficient protection of kernel data structures via object partitioning. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). ACM, Orlando, Florida, 429–438.
DOI:http://dx.doi.org/10.1145/2420950.2421012

Udo Steinberg and Bernhard Kauer. 2010.
NOVA: a microhypervisor-based secure virtualization architecture. In Proceedings of the 5th European conference on Computer systems (EuroSys '10). 209–222.
DOI:http://dx.doi.org/10.1145/1755913.1755935

Jakub Szefer, Eric Keller, Ruby B. Lee, and Jennifer Rexford. 2011.
Eliminating the hypervisor attack surface for a more secure cloud. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). ACM, 401–412.
DOI:http://dx.doi.org/10.1145/2046707.2046754

References XVIII

Donghai Tian, Qiang Zeng, Dinghao Wu, Peng Liu 0005, and Changzhen Hu. 2012.
Kruiser: Semi-synchronized Non-blocking Concurrent Kernel Heap Buffer Overflow Monitoring. In Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS 2012).
http://www.internetsociety.org/kruiser-semi-synchronized-non-blocking-concurrent-kernel-heap-buffer-overflow-monitori

Amit Vasudevan, Sagar Chaki, Limin Jia, Jonathan McCune, James Newsome, and Anupam Datta. 2013.
Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework. In Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP '13). IEEE Computer Society, Washington, DC, USA, 430–444.
DOI:http://dx.doi.org/10.1109/SP.2013.36

Amit Vasudevan and Ramesh Yerraballi. 2006.
Cobra: Fine-grained Malware Analysis using Stealth Localized-executions. In Proceedings of the 2006 IEEE Symposium on Security and Privacy. 264–279.
DOI:http://dx.doi.org/10.1109/SP.2006.9

Jiang Wang, Angelos Stavrou, and Anup Ghosh. 2010.
HyperCheck: a hardware-assisted integrity monitor. In Proceedings of the 13th international conference on Recent advances in intrusion detection (RAID'10). 158–177.
http://dl.acm.org/citation.cfm?id=1894166.1894178

Zhi Wang and Xuxian Jiang. 2010.
HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity. In Security and Privacy (SP), 2010 IEEE Symposium on. 380–395.
DOI:http://dx.doi.org/10.1109/SP.2010.30

References XIX

- Zhi Wang, Xuxian Jiang, Weidong Cui, and Peng Ning. 2009.
  Countering kernel rootkits with lightweight hook protection. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). 545–554.
  DOI:http://dx.doi.org/10.1145/1653662.1653728
- Zhi Wang, Xuxian Jiang, Weidong Cui, and Xinyuan Wang. 2008.
  Countering Persistent Kernel Rootkits through Systematic Hook Discovery. In Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection (RAID '08). Cambridge, MA, USA, 21–38.
  DOI:http://dx.doi.org/10.1007/978-3-540-87403-4_2
- Zhi Wang, Chiachih Wu, Michael Grace, and Xuxian Jiang. 2012.
  Isolating commodity hosted hypervisors with HyperLock. In Proceedings of the 7th ACM european conference on Computer Systems (EuroSys '12). ACM, 127–140.
  DOI:http://dx.doi.org/10.1145/2168836.2168850
- Rafal Wojtczuk. 2008.
  Subverting the Xen hypervisor. In Black Hat Technical Security Conf. Las Vegas, Nevada.
- Chiachih Wu, Zhi Wang, and Xuxian Jiang. 2013.
  Taming Hosted Hypervisors with (Mostly) Deprivileged Execution. In Proceedings of the Network and Distributed System Security Symposium (NDSS).
  http://internetsociety.org/doc/taming-hosted-hypervisors-mostly-deprivileged-execution

References XX

Rui Wu, Ping Chen, Peng Liu, and Bing Mao. 2014.
System Call Redirection: A Practical Approach to Meeting Real-World Virtual Machine Introspection Needs. In Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. 574–585.
DOI:http://dx.doi.org/10.1109/DSN.2014.59

Yubin Xia, Yutao Liu, and Haibo Chen. 2013.
Architecture Support for Guest-transparent VM Protection from Untrusted Hypervisor and Physical Attacks. In Proceedings of the 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA) (HPCA '13). IEEE Computer Society, Washington, DC, USA, 246–257.
DOI:http://dx.doi.org/10.1109/HPCA.2013.6522323

Xi Xiong, Donghai Tian, and Peng Liu. 2011.
Practical Protection of Kernel Integrity for Commodity OS from Untrusted Extensions. In NDSS.
http://www.isoc.org/isoc/conferences/ndss/11/pdf/3_1.pdf

Chaoting Xuan, John A. Copeland, and Raheem A. Beyah. 2009.
Toward Revealing Kernel Malware Behavior in Virtual Execution Environments.. In Proceedings of the 12th international symposium on Recent Advances in Intrusion Detection. 304–325.
DOI:http://dx.doi.org/10.1007/978-3-642-04342-0_16

Lok-Kwong Yan, Manjukumar Jayachandra, Mu Zhang, and Heng Yin. 2012.
V2E: Combining Hardware Virtualization and Softwareemulation for Transparent and Extensible Malware Analysis. In Proceedings of the 8th ACM SIGPLAN/SIGOPS Conference on Virtual Execution Environments (VEE '12). ACM, New York, NY, USA, 227–238.
DOI:http://dx.doi.org/10.1145/2151024.2151053

References XXI

Lok Kwong Yan and Heng Yin. 2012.
DroidScope: seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis. In Proceedings of the 21st USENIX conference on Security symposium (Security'12). 29–29.
http://dl.acm.org/citation.cfm?id=2362793.2362822

Jean Yang and Chris Hawblitzel. 2010.
Safe to the last instruction: automated verification of a type-safe operating system. In Proceedings of the 2010 ACM SIGPLAN conference on Programming language design and implementation (PLDI '10). ACM, New York, NY, USA, 99–110.
DOI:http://dx.doi.org/10.1145/1806596.1806610

Heng Yin, Zhenkai Liang, and Dawn Song. 2008.
HookFinder: Identifying and Understanding Malware Hooking Behaviors. In Proceedings of the 2008 Annual Network and Distributed System Security Symposium (NDSS).
http://www.isoc.org/isoc/conferences/ndss/08/papers/15_hookfinder_identifying.pdf

Heng Yin, Dawn Song, Manuel Egele, Christopher Kruegel, and Engin Kirda. 2007.
Panorama: capturing system-wide information flow for malware detection and analysis. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). 116–127.
http://doi.acm.org/10.1145/1315245.1315261

Fengzhe Zhang, Jin Chen, Haibo Chen, and Binyu Zang. 2011.
CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (SOSP '11). 203–216.
DOI:http://dx.doi.org/10.1145/2043556.2043576

References XXII

Shengzhi Zhang, Xiaoqi Jia, Peng Liu, and Jiwu Jing. 2010.
Cross-layer comprehensive intrusion harm analysis for production workload server systems. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10). 297–306.
DOI:http://dx.doi.org/10.1145/1920261.1920306

Yajin Zhou and Xuxian Jiang. 2012.
Dissecting Android Malware: Characterization and Evolution. In Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP'12). IEEE Computer Society, Washington, DC, USA, 95–109.
DOI:http://dx.doi.org/10.1109/SP.2012.16