[3] McAfee Threats Report: Fourth Quarter 2010. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf. [last accessed: May 2011].

[4] QEMU. http://www.qemu.org. [last accessed: May 2011].

[5] UPX: The Ultimate Packer for eXecutables. http://upx.sourceforge.net. [last accessed: May 2011].

[6] Adams, K., and Agesen, O. 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* (2006).

[7] AMD. AMD-V Nested Paging. *AMD White Paper* (2008).

[8] Azab, A. M., Ning, P., Sezer, E. C., and Zhang, X. HIMA: A Hypervisor-Based Integrity Measurement Agent. In *Proceedings of the 25th Annual Computer Security Applications Conference* (2009).

[9] Bayer, U., Kruegel, C., and Kirda, E. TTAnalyze: A Tool for Analyzing Malware. In *Proceedings of the 15th Annual Conference of the European Institute for Computer Antivirus Research* (2006).

[10] cker Chiueh, T., Conover, M., Lu, M., and Montague, B. Stealthy Deployment and Execution of In-Guest Kernel Agents. In *BlackHat 2009*.

[11] Dinaburg, A., Royal, P., Sharif, M., and Lee, W. Ether: Malware Analysis via Hardware Virtualization Extensions. In *Proceedings of the 15th ACM Conference on Computer and Communications Security* (2008).

[12] Dolan-Gavitt, B., Leek, T., Zhivich, M., Giffin, J., and Lee, W. Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection. In *Proceedings of the 32nd IEEE Symposium on Security and Privacy* (2011).

[13] Forrest, S., Hofmeyr, S., and Somayaji, A. The Evolution of System-Call Monitoring. In *Proceedings of the 24th Annual Computer Security Applications Conference* (2008).

[14] Garfinkel, T., Pfaff, B., and Rosenblum, M. Ostia: A Delegating Architecture for Secure System Call Interposition. In *Proceedings of the 11th Annual Network and Distributed System Security Symposium* (2004).

[15] Garfinkel, T., and Rosenblum, M. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In *Proceedings of the 10th Annual Network and Distributed Systems Security Symposium* (2003).

[16] Goldberg, I., Wagner, D., Thomas, R., and Brewer, E. A. A Secure Environment for Untrusted Helper Applications: Confining the Wily Hacker. In *Proceedings of the 6th USENIX Security Symposium* (1996).

[17] Guo, F., Ferrie, P., and Chiueh, T.-c. A Study of the Packer Problem and Its Solutions. In *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection*. (2008).

[18] Intel. Intel Virtualization Technology: Hardware Support for Efficient Processor Virtualization. *Intel(R) Technology Journal 10*, 3 (2006).

[19] Intel. *Intel 64 and IA-32 Architectures Software Developerś Manual Volume 3: System Programming Guide, Part 1 and Part 2*, (2010).

[20] Jiang, X., and Wang, X. "Out-of-the-Box" Monitoring of VM-Based High-Interaction Honeypots. In *Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection* (2007).

[21] Jiang, X., Wang, X., and Xu, D. 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* (2007).

[22] Gu, Z., Deng, Z., Xu, D., and Jiang, X. Process Implanting: A New Active Introspection Framework for Virtualization. In *Proceedings of the 30th IEEE Symposium on Reliable Distributed Systems* (2011).

[23] Joshi, A., King, S. T., Dunlap, G. W., and Chen, P. M. Detecting Past and Present Intrusions through Vulnerability-specific Predicates. In *Proceedings of the 20th ACM Symposium on Operating Systems Principles* (2005).

[24] King, S. T., and Chen, P. M. Backtracking Intrusions. In *Proceedings of the 19th ACM Symposium on Operating Systems Principles* (2003).

[25] Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R., Norrish, M., Sewell, T., Tuch, H., and Winwood, S. seL4: Formal Verification of an OS Kernel. In *Proceedings of the 22nd Symposium on Operating Systems Principles* (2009).

[26] Martignoni, L., Christodorescu, M., and Jha, S. OmniUnpack: Fast, Generic, and Safe Unpacking of Malware. In *Proceedings of the 23rd Annual Computer Security Applications Conference* (2007).

[27] Martignoni, L., Paleari, R., and Bruschi, D. A Framework for Behavior-Based Malware Analysis in the Cloud. In *Proceedings of the 5th International Conference on Information Systems Security* (2009).

[28] Nuttall, M. A Brief Survey of Systems Providing Process or Object Migration Facilities. *ACM SIGOPS Operating Systems Review 28* (1994).

[29] Osman, S., Subhraveti, D., Su, G., and Nieh, J. The Design and Implementation of Zap: a System for Migrating Computing Environments. *ACM SIGOPS Operating Systems Review 36* (2002).

[30] Payne, B., de Carbone, M., and Lee, W. Secure and Flexible Monitoring of Virtual Machines. In *Proceedings of the 23rd Annual Computer Security Applications Conference* (2007).

[31] Payne, B. D., Carbone, M., Sharif, M., and Lee, W. Lares: An Architecture for Secure Active Monitoring Using Virtualization. In *Proceedings of the 29th IEEE Symposium on Security and Privacy* (2008).

[32] Provos, N. Improving Host Security with System Call Policies. In *Proceedings of the 12th USENIX Security Symposium* (2003).

[33] Royal, P., Halpin, M., Dagon, D., Edmonds, R., and Lee, W. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. In *Proceedings of the 22nd Annual Computer Security Applications Conference* (2006).

[34] Sharif, M. I., Lee, W., Cui, W., and Lanzi, A. Secure In-VM Monitoring Using Hardware Virtualization. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (2009).

[35] Smith, J. M. A survey of process migration mechanisms. *ACM SIGOPS Operating Systems Review 22* (1988).

[36] Smith, J. M. The Design and Implementation of Berkeley Lab's Linux Checkpoint/Restart. *Berkeley Lab Technical Report* (2002).

[37] Srivastava, A., and Giffin, J. Tamper-Resistant, Application-Aware Blocking of Malicious Network Connections. In *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection* (2008).

[38] Srivastava, A., and Giffin, J. Efficient Monitoring of Untrusted Kernel-mode Execution. In *Proceedings of the 18th Annual Network and Distributed Systems Security Symposium* (2011).

[39] Ta-Min, R., Litty, L., and Lie, D. Splitting Interfaces: Making Trust between Applications and Operating Systems Configurable. In *Proceedings of the 7th Symposium on Operating Systems Design and Implementation* (2006).

[40] Wang, Z., and Jiang, X. HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity. *Proceedings of the 31st IEEE Symposium on Security and Privacy* (2010).