machine monitor. In *1st Workshop on Operating System and Architectural Support for the on demand IT InfraStructure (OASIS)*, pages 1–1, 2004.

[27] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: A virtual machine-based platform for trusted computing. In *ACM SIGOPS Operating Systems Review*, volume 37, pages 193–206. ACM, 2003.

[28] C. Gebtry, S. Halevi, and N. P. Smart. Homomorphic evaluation of the aes circuit. In *32nd International Cryptology Conference*, 2012.

[29] C. Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

[30] V. George, T. Piazza, and H. Jiang. Technology Insight: Intel© Next Generation Microarchitecture Codename Ivy Bridge, 2011. URL `www.intel.com/idf/library/pdf/sf_2011/SF11_SPCS005_101F.pdf`.

[31] O. S. Hofmann, S. Kim, A. M. Dunn, M. Z. Lee, and E. Witchel. InkTag: Secure Applications On An Untrusted Operating System. In *Proceedings of the eighteenth international conference on Architectural support for programming languages and operating systems, (ASPLOS)*, pages 265–278. ACM, 2013.

[32] V. P. Kemerlis, G. Portokalidis, and A. D. Keromytis. kguard: Lightweight kernel protection against return-to-user attacks. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, Berkeley, CA, USA, 2012. USENIX Association.

[33] V. P. Kemerlis, M. Polychronakis, and A. D. Keromytis. Ret2dir: Rethinking kernel isolation. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, 2014.

[34] C. Lattner and V. Adve. LLVM: A compilation framework for lifelong program analysis & transformation. In *Code Generation and Optimization, 2004. CGO 2004. International Symposium on*, pages 75–86. IEEE, 2004.

[35] D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell, and M. Horowitz. Architectural support for copy and tamper resistant software. *ACM SIGPLAN Notices*, 35 (11):168–177, 2000.

[36] J. M. McCune, Y. Li, N. Qu, Z. Zhou, A. Datta, V. Gligor, and A. Perrig. TrustVisor: Efficient TCB Reduction and Attestation. In *IEEE Symposium on Security and Privacy (SP)*, pages 143–158. IEEE, 2010.

[37] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar. Innovative instructions and software model for isolated execution. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, page 10. ACM, 2013.

[38] R. Nikolaev and G. Back. Virtuos: an operating system with kernel virtualization. In *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles (SOSP 2013)*, pages 116–132. ACM, 2013.

[39] K. Onarlioglu, C. Mulliner, W. Robertson, and E. Kirda. PRIVEXEC: Private Execution as an Operating System Service. In *IEEE Symposium on Security and Privacy*. IEEE, 2013.

[40] R. A. Popa, C. M. Redfield, N. Xeldovich, and H. Balakrishnan. Cryptdb: Protecting confidentiality with encrypted query processing. In *23rd ACM Symposium on Operating Systems Principles*, pages 85–100, 2011.

[41] M. Seaborn. Plash: tools for practical least privilege, 2008. URL `http://plash.beasts.org/index.html`.

[42] J. S. Shapiro, J. Vanderburgh, E. Northup, and D. Chizmadia. Design of the eros trusted window system. In *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13*, pages 12–12. USENIX Association, 2004.

[43] L. Soares and M. Stumm. Flexsc: flexible system call scheduling with exception-less system calls. In *Proceedings of the 9th USENIX conference on Operating systems design and implementation, OSDI*. ACM, 2010.

[44] R. Strackx and F. Piessens. Fides: Selectively hardening software application components against kernel-level or process-level malware. In *Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012)*, 2012.

[45] G. E. Suh, D. Clarke, B. Gassend, M. Van Dijk, and S. Devadas. AEGIS: architecture for tamper-evident and tamper-resistant processing. In *Proceedings of the 17th annual international conference on Supercomputing*, pages 160–171, 2003.

[46] S. D. Tetali, M. Lesani, R. Majumdar, and T. Millstein. Mrcrypt: static analysis for secure cloud computations. In *Proceedings of the 2013 ACM SIGPLAN international conference on Object oriented programming systems languages & applications*, pages 271–286. ACM, 2013.

[47] A. Virtualization. Secure Virtual Machine Architecture Reference Manual. *AMD Publication*, (33047), 2005.

[48] J. Yang and K. Shin. Using hypervisor to provide data secrecy for user applications on a per-page basis. In *Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments*, pages 71–80. ACM, 2008.

[49] M. Zhang and R. Sekar. Control flow integrity for cots binaries. In *Usenix Security*, pages 337–352, 2013.

[50] Z. Zhou, V. Gligor, J. Newsome, and J. McCune. Building verifiable trusted path on commodity x86 computers. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 616–630. IEEE, 2012.