2014. TaintDroid: an Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones. In *ACM Transactions on Computer Systems (TOCS)*.
[22] Derek R Hower and Mark D Hill. 2008. Rerun: Exploiting Episodes for Lightweight Memory Race Recording. In *ACM SIGARCH computer architecture news*.
[23] Intel. 2018. Intel XED. https://intelxed.github.io
[24] François Irigoin, Pierre Jouvelot, and Rémi Triolet. 2014. Semantical Interprocedural Parallelization: An overview of the PIPS project. In *ACM International Conference on Supercomputing 25th Anniversary Volume*.
[25] Anushri Jana and Ravindra Naik. 2012. Precise Detection of Uninitialized Variables Using Dynamic Analysis-Extending to Aggregate and Vector Types. In *Proceedings of the 19th Working Conference on Reverse Engineering*.
[26] Suman Jana and Vitaly Shmatikov. 2012. Abusing File Processing in Malware Detectors for Fun and Profit. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*.
[27] Rahul Jiresal, Adnan Contractor, and Ravindra Naik. 2011. Precise Detection of Un-initialized Variables in Large, Real-life COBOL Programs in Presence of Unrealizable Paths. (2011).
[28] Mateusz Jurczyk. 2017. Detecting Kernel Memory Disclosure with x86 Emulation and Taint Tracking. (2017).
[29] Timotej Kapus and Cristian Cadar. 2017. Automatic Testing of Symbolic Execution Engines via Program Generation and Differential Testing. In *Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering*.
[30] Wei Ming Khoo. 2018. Taintgrind: a Valgrind Taint Analysis Tool.
[31] Oren Laadan, Nicolas Viennot, and Jason Nieh. 2010. Transparent, Lightweight Application Execution Replay on Commodity Multiprocessor Operating Systems. In *ACM SIGMETRICS performance evaluation review*.
[32] Chris Lattner. 2018. Clang: a C language Family Frontend for LLVM. http://clang.llvm.org/index.html
[33] Yutao Liu, Tianyu Zhou, Kexin Chen, Haibo Chen, and Yubin Xia. 2015. Thwarting Memory Disclosure with Efficient Hypervisor-enforced Intra-domain Isolation. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*.
[34] Kangjie Lu, Chengyu Song, Taesoo Kim, and Wenke Lee. 2016. UniSan: Proactive Kernel Memory Initialization to Eliminate Data Leakages. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*.
[35] Kangjie Lu, Marie-Therese Walter, David Pfaff, Stefan Nürnberger, Wenke Lee, and Michael Backes. 2017. Unleashing Use-before-initialization Vulnerabilities in the Linux Kernel Using Targeted Stack Spraying. In *Proceedings of the 2017 Annual Network and Distributed System Security Symposium (NDSS)*.
[36] Chi-Keung Luk, Robert Cohn, Robert Muth, Harish Patil, Artur Klauser, Geoff Lowney, Steven Wallace, Vijay Janapa Reddi, and Kim Hazelwood. 2005. Pin: Building Customized Program Analysis Tools with Dynamic Instrumentation. In *Proceedings of the 2005 ACM SIGPLAN conference on Programming language design and implementation*.
[37] Manuel López-Ibáñez. 2007. Better Uninitialized Warnings. http://gcc.gnu.org/wiki/BetterUninitializedWarnings
[38] William M McKeeman. 1998. Differential Testing for Software. *Digital Technical Journal* (1998).
[39] Microsoft. 2018. Visual Studio.
[40] Alyssa Milburn, Herbert Bos, and Cristiano Giuffrida. 2017. Safeinit: Comprehensive and Practical Mitigation of Uninitialized Read Vulnerabilities. In *Proceedings of the 2017 Annual Network and Distributed System Security Symposium*.
[41] Jiang Ming, Dinghao Wu, Jun Wang, Gaoyao Xiao, and Peng Liu. 2016. StraightTaint: Decoupled Offline Symbolic Taint Analysis. In *Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering*.
[42] Jiang Ming, Dinghao Wu, Gaoyao Xiao, Jun Wang, and Peng Liu. 2015. TaintPipe: Pipelined Symbolic Taint Analysis. In *Proceedings of the 24th USENIX Security Symposium*.
[43] Pablo Montesinos, Luis Ceze, and Josep Torrellas. 2008. Delorean: Recording and Deterministically Replaying Shared-memory Multiprocessor Execution Efficiently. In *ACM SIGARCH Computer Architecture News*.
[44] Satish Narayanasamy, Cristiano Pereira, and Brad Calder. 2006. Recording Shared Memory Dependencies using Strata. *ACM SIGARCH Computer Architecture News* (2006).
[45] Nicholas Nethercote and Julian Seward. 2007. Valgrind: a Framework for Heavyweight Dynamic Binary Instrumentation. In *Proceedings of the 28th ACM SIGPLAN Conference on Programming Language Design and Implementation*.
[46] James Newsome and Dawn Song. 2005. Dynamic Taint Analysis: Automatic Detection, Analysis, and Signature Generation of Exploit Attacks on Commodity Software. In *Proceedings of the 12th Network and Distributed Systems Security Symposium*.
[47] Robert O'Callahan, Chris Jones, Nathan Froyd, Kyle Huey, Albert Noll, and Nimrod Partush. 2017. Engineering Record and Replay for Deployability. In *Proceedings of the 2017 USENIX Conference on Usenix Annual Technical Conference*.
[48] Jianfeng Pan, Guanglu Yan, and Xiaocao Fan. 2017. Digtool: A virtualization-based Framework for Detecting Kernel Vulnerabilities. In *Proceedings of the 26th USENIX Security Symposium*.
[49] Theofilos Petsios, Adrian Tang, Salvatore Stolfo, Angelos D Keromytis, and Suman Jana. 2017. Nezha: Efficient Domain-independent Differential Testing. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy*.
[50] Gilles Pokam, Klaus Danne, Cristiano Pereira, Rolf Kassa, Tim Kranich, Shiliang Hu, Justin Gottschlich, Nima Honarmand, Nathan Dautenhahn, Samuel T King, et al. 2013. QuickRec: Prototyping an Intel Architecture Extension for Record and Replay of Multithreaded Programs. *ACM SIGARCH Computer Architecture News* (2013).
[51] Nguyen Anh Quynh. 2014. Capstone: The Ultimate Disassembler.
[52] John Regehr, Yang Chen, Pascal Cuoq, Eric Eide, Chucky Ellison, and Xuejun Yang. 2012. Test-case Reduction for C Compiler Bugs. In *Proceedings of the 33rd ACM SIGPLAN Conference on Programming Language Design and Implementation*.
[53] Prof. John Regehr. 2011. Uninitialized Variables. http://blog.regehr.org/archives/519
[54] Michiel Ronsse and Koen De Bosschere. 1999. RecPlay: a Fully Integrated Practical Record/replay System. *ACM Transactions on Computer Systems (TOCS)* (1999).
[55] Yasushi Saito. 2005. Jockey: a User-space Library for Record-replay Debugging. In *Proceedings of the 6th international symposium on Automated analysis-driven debugging*.
[56] Sergej Schumilo, Cornelius Aschermann, Robert Gawlik, Sebastian Schinzel, and Thorsten Holz. 2017. KAFL: Hardware-assisted Feedback Fuzzing for OS Kernels. In *Proceedings of the 26th USENIX Security Symposium*.
[57] Edward J. Schwartz, Thanassis Avgerinos, and David Brumley. 2010. All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask). In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*.
[58] Julian Seward and Nicholas Nethercote. 2005. Using Valgrind to Detect Undefined Value Errors with Bit-Precision.. In *Proceedings of the annual conference on USENIX Annual Technical Conference*.
[59] Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. 2015. Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware. In *Proceedings of the 22nd Annual Network and Distributed System Security Symposium*.
[60] Suphannee Sivakorn, George Argyros, Kexin Pei, Angelos D Keromytis, and Suman Jana. 2017. HVLearn: Automated Black-box Analysis of Hostname Verification in SSL/TLS Implementations. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy*.
[61] Varun Srivastava, Michael D Bond, Kathryn S McKinley, and Vitaly Shmatikov. 2011. A Security Policy Oracle: Detecting Security Holes Using Multiple API Implementations. In *Proceedings of the 32nd ACM SIGPLAN Conference on Programming Language Design and Implementation*.
[62] Evgeniy Stepanov and Konstantin Serebryany. 2015. MemorySanitizer: Fast Detector of Uninitialized Memory Use in C++. In *Proceedings of the 13th Annual IEEE/ACM International Symposium on Code Generation and Optimization*.
[63] Xiajing Wang, Rui Ma, Bowen Dou, Zefeng Jian, and Hongzhou Chen. 2018. OFFDTAN: A New Approach of Offline Dynamic Taint Analysis for Binaries. In *Journal of Security and Communication Networks*.
[64] Min Xu, Rastislav Bodik, and Mark D Hill. 2003. A Flight Data Recorder for Enabling Full-system Multiprocessor Deterministic Replay. In *ACM SIGARCH Computer Architecture News*.
[65] Xuejun Yang, Yang Chen, Eric Eide, and John Regehr. 2011. Finding and Understanding Bugs in C Compilers. In *Proceedings of the 32nd ACM SIGPLAN Conference on Programming Language Design and Implementation*.
[66] Ding Ye, Yulei Sui, and Jingling Xue. 2014. Accelerating Dynamic Detection of Uses of Undefined Values with Static Value-flow Analysis. In *Proceedings of Annual IEEE/ACM International Symposium on Code Generation and Optimization*.
[67] Heng Yin and Dawn Song. 2010. Temu: Binary Code Analysis via Whole-system Layered Annotative Execution. *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2010-3* (2010).
[68] 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*.
[69] Michal Zalewski. 2018. American Fuzzy Lop: a Security-oriented Fuzzer. http://lcamtuf.coredump.cx/afl/
[70] Sebastian Österlund, Koen Koning, Pierre Olivier, Antonio Barbalace, Herbert Bos, and Cristiano Giuffrida. 2019. kMVX: Detecting Kernel Information Leaks with Multi-variant Execution. In *Proceedings of the 24th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*.