1/23 Optional: [Ern03]

1/28 [CPG$^+$04, NS05]

1/30 [SB09, BSB11] Historic: [Wal89] Optional: [BZL$^+$10, KMPS11, SAB10, RPB$^+$09]

2/4 [GKS05, CDE08] Historic: [Kin76, CE05, CGP$^+$06, SMA05]

2/6 [BCL$^+$07, CKC11] Optional: [GD07, BUZC11, BGM12]

2/11 [GKL08, MPFH11] Optional: [BMMS11, GL11, CARB12]

2/13 [Mye99, JW04]

2/18 [CLM$^+$07, MC12]

2/20 [Mal07, ME08] Historic: [Den82]

2/25 [NMS09, CCM08] Optional: [BKR09, YT10, PMTP12]

2/27 [WLAG93, MM06] Historic: [DG71]

3/4 [YSD$^+$09, SMB$^+$10]

3/6 [AMUE$^+$11, MTT$^+$12]

3/11 [ABUEL05, DDE$^+$12a] Optional: [ZTM11, WJ10]

3/13 [WMHL12, DKA06] Optional: [NLLcC06, ACR$^+$08]

3/25 [Sha07, MSMM09]

3/27 [LZX10, LAB11]

4/3 [GA03, CMS01]

4/8 [SHWK11, MPSW05] Optional: [KMO12]

4/10 [MNPS04, HEKM11] Optional: [SMBW12, HKE12]

4/15 [BGI$^+$01, MASB05]

4/17 [PLEB07, GLR09]

4/22 [JAB12, HDWY06] Optional: [BBC$^+$10, CKL$^+$12]

4/24 [KEH$^+$09, ULF06] Optional: [DDE$^+$12b]

4/29 [EGgC$^+$10, YY12] Optional: [EKKV11, EOMC11, OJM12]

5/1 [Chl10, PEGK11] Optional: [WS07, AKD$^+$08, SSS11, BCS09]

e01 [PLEB07, GLR09] Historic: [MFS90]

e02 [BS04, HJR10] Optional: [VC11]

e03 [GA03, SHWK11]

e04 [MPSW05, KMO12]

e05 [JAB12, HDWY06] Optional: [BBC$^+$10, CKL$^+$12]

e06 [KEH$^+$09, ULF06] Optional: [DDE$^+$12b]

1

e07 [LZX10, LAB11]

e08 [RP10, BKOB12] Optional: [GHH$^+$13]

e09 [MNPS04, HEKM11] Optional: [SMBW12, HKE12]

e10 [BGI$^+$01, MASB05]

e12 [WS07, AKD$^+$08, Chl10, PEGK11] Optional: [SSS11, BCS09]

e13 [EGgC$^+$10, EKKV11, EOMC11, YY12] Optional: [OJM12]

References

[ABUEL05] Martín Abadi, Mihai Budiu, Úlfar Erlingsson, and Jay Ligatti. Control-flow integrity. In *ACM Conference on Computer and Communications Security (CCS)*, pages 340–353, Alexandria, VA, USA, November 2005.

[ACR$^+$08] Periklis Akritidis, Cristian Cadar, Costin Raiciu, Manuel Costa, and Miguel Castro. Preventing memory error exploits with WIT. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 263–277, Oakland, CA, USA, May 2008.

[AKD$^+$08] Shay Artzi, Adam Kiezun, Julian Dolby, Frank Tip, Danny Dig, Amit M. Paradkar, and Michael D. Ernst. Finding bugs in dynamic web applications. In *International Symposium on Software Testing and Analysis (ISSTA)*, pages 261–272, Seattle, WA, USA, July 2008.

[AMUE$^+$11] Jason Ansel, Petr Marchenko, Úlfar Erlingsson, Elijah Taylor, Brad Chen, Derek L. Schuff, David Sehr, Cliff L. Biffle, and Bennet Yee. Language-independent sandboxing of just-in-time compilation and self-modifying code. In *Programming Language Design and Implementation (PLDI)*, pages 355–366, San Jose, CA, USA, June 2011.

[BBC$^+$10] Al Bessey, Ken Block, Benjamin Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, and Dawson R. Engler. A few billion lines of code later: using static analysis to find bugs in the real world. *Communications of the ACM*, 53(2):66–75, February 2010.

[BCL$^+$07] David Brumley, Juan Caballero, Zhenkai Liang, James Newsome, and Dawn Song. Towards automatic discovery of deviations in binary implementations with applications to error detection and fingerprint generation. In *USENIX Security Symposium*, pages 213–228, Boston, MA, USA, August 2007.

[BCS09] Adam Barth, Juan Caballero, and Dawn Song. Secure content sniffing for web browsers, or how to stop papers from reviewing themselves. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 360–371, Oakland, CA, USA, May 2009.

[BGI$^+$01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In *International Cryptology Conference (CRYPTO)*, pages 1–18, Santa Barbara, CA, USA, August 2001.

[BGM12] Ella Bounimova, Patrice Godefroid, and David Molnar. Billions and billions of constraints: Whitebox fuzz testing in production. Technical Report MSR-TR-2012-55, Microsoft Research, May 2012.

[BKOB12] Gilles Barthe, Boris Köpf, Federico Olmedo, and Santiago Zanella Béguelin. Probabilistic relational reasoning for differential privacy. In *Principles of Programming Languages (POPL)*, pages 97–110, Philadelphia, PA, USA, January 2012.

[BKR09]   Michael Backes, Boris Köpf, and Andrey Rybalchenko. Automatic discovery and quantification of information leaks. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 141–153, Oakland, CA, USA, May 2009.

[BMMS11]   Domagoj Babić, Lorenzo Martignoni, Stephen McCamant, and Dawn Song. Statically-directed dynamic automated test generation. In *International Symposium on Software Testing and Analysis (ISSTA)*, pages 12–22, Toronto, ON, Canada, July 2011.

[BS04]   David Brumley and Dawn Song. Privtrans: Automatically partitioning programs for privilege separation. In *USENIX Security Symposium*, pages 57–72, San Diego, CA, USA, August 2004.

[BSB11]   Erik Bosman, Asia Slowinska, and Herbert Bos. Minemu: The world's fastest taint tracker. In *Recent Advances in Intrusion Detection (RAID)*, pages 1–20, Menlo Park, CA, USA, September 2011.

[BUZC11]   Stefan Bucur, Vlad Ureche, Cristian Zamfir, and George Candea. Parallel symbolic execution for automated real-world software testing. In *ACM European Conference on Computer Systems (EuroSys)*, pages 183–198, Salzburg, Austria, April 2011.

[BZL$^+$10] Tao Bao, Yunhui Zheng, Zhiqiang Lin, Xiangyu Zhang, and Dongyan Xu. Strict control dependence and its effect on dynamic information flow analyses. In *International Symposium on Software Testing and Analysis (ISSTA)*, pages 13–24, Trento, Italy, July 2010.

[CARB12]   Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert, and David Brumley. Unleashing Mayhem on binary code. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 380–394, San Francisco, CA, USA, May 2012.

[CCM08]   Miguel Castro, Manuel Costa, and Jean-Philippe Martin. Better bug reporting with better privacy. In *Architectural Support for Programming Languages and Operating Systems (ASPLOS XIII)*, pages 319–328, Seattle, WA, USA, March 2008.

[CDE08]   Cristian Cadar, Daniel Dunbar, and Dawson Engler. KLEE: Unassisted and automatic generation of high-coverage tests for complex systems programs. In *Operating Systems Design and Implementation (OSDI)*, pages 209–223, San Diego, CA, USA, December 2008.

[CE05]   Cristian Cadar and Dawson R. Engler. Execution generated test cases: How to make systems code crash itself. In *SPIN Workshop on Model Checking Software*, pages 2–23, San Francisco, CA, USA, August 2005.

[CGP$^+$06] Cristian Cadar, Vijay Ganesh, Peter M. Pawlowski, David L. Dill, and Dawson R. Engler. EXE: automatically generating inputs of death. In *ACM Conference on Computer and Communications Security (CCS)*, pages 322–335, Alexandria, VA, USA, November 2006.

[Chl10]   Adam Chlipala. Static checking of dynamically-varying security policies in database-backed applications. In *Operating Systems Design and Implementation (OSDI)*, pages 105–118, Vancouver, BC, Canada, October 2010.

[CKC11]   Vitaly Chipounov, Volodymyr Kuznetsov, and George Candea. S2E: a platform for in-vivo multi-path analysis of software systems. In *Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pages 265–278, Newport Beach, CA, USA, March 2011.

[CKL$^+$12] Cristina Cifuentes, Nathan Keynes, Lian Li, Nathan Hawes, and Manuel Valdiviezo. Transitioning Parfait into a development tool. *IEEE Security & Privacy Magazine*, 10(3):16–23, May/June 2012.

[CLM+07]   Stephen Chong, Jed Liu, Andrew C. Myers, Xin Qi, K. Vikram, Lantian Zheng, and Xin Zheng. Secure web applications via automatic partitioning. In *Symposium on Operating Systems Principles (SOSP)*, pages 31–44, Stevenson, WA, USA, October 2007.

[CMS01]   Ajay Chander, John C. Mitchell, and Insik Shin. Mobile code security by Java bytecode instrumentation. In *DARPA Information Survivability Conference & Exposition (DISCEX)*, pages 27–40, Anaheim, CA, USA, June 2001.

[CPG+04]   Jim Chow, Ben Pfaff, Tal Garfinkel, Kevin Christopher, and Mendel Rosenblum. Understanding data lifetime via whole system simulation. In *USENIX Security Symposium*, pages 321–336, San Diego, CA, USA, August 2004.

[DDE+12a]   Lucas Davi, Alexandra Dmitrienko, Manuel Egele, Thomas Fischer, Thorsten Holz, Ralf Hund, Stefan Nürnberger, and Ahmad-Reza Sadeghi. MoCFI: A framework to mitigate control-flow attacks on smartphones. In *Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2012.

[DDE+12b]   Werner Dietl, Stephanie Dietzel, Michael D. Ernst, Nathaniel Mote, Brian Walker, Seth Cooper, Timothy Pavlik, and Zoran Popović. Verification games: making verification fun. In *Formal Techniques for Java-like Programs (FTfJP)*, pages 42–49, Beijing, China, June 2012.

[Den82]   Dorothy Elizabeth Robling Denning. *Cryptography and data security*. Addison-Wesley Longman Publishing, 1982.

[DG71]   Peter Deutsch and Charles A. Grant. A flexible measurement tool for software systems. In *IFIP Congress (1)*, pages 320–326, Ljubljana, Yugoslavia, August 1971.

[DKA06]   Dinakar Dhurjati, Sumant Kowshik, and Vikram Adve. SAFECode: enforcing alias analysis for weakly typed languages. In *Programming Language Design and Implementation (PLDI)*, pages 144–157, Ottawa, ON, CA, June 2006.

[EGgC+10]   William Enck, Peter Gilbert, Byung gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol Sheth. TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In *Operating Systems Design and Implementation (OSDI)*, pages 393–407, Vancouver, BC, Canada, October 2010.

[EKKV11]   Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. PiOS: Detecting privacy leaks in iOS applications. In *Network and Distributed System Security Symposium (NDSS)*, pages 473–487, San Diego, CA, USA, February 2011.

[EOMC11]   William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri. A study of Android application security. In *USENIX Security Symposium*, San Francisco, CA, USA, August 2011.

[Ern03]   Michael D. Ernst. Static and dynamic analysis: Synergy and duality. In *Workshop on Dynamic Analysis (WODA)*, pages 24–27, Portland, OR, USA, May 2003.

[GA03]   Sudhakar Govindavajhala and Andrew W. Appel. Using memory errors to attack a virtual machine. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 154–165, Oakland, CA, USA, May 2003.

[GD07]   Vijay Ganesh and David L. Dill. A decision procedure for bit-vectors and arrays. In *Computer Aided Verification (CAV)*, pages 519–531, Berlin, Germany, July 2007.

[GHH+13]   Marco Gaboardi, Andreas Haeberlen, Justin Hsu, Arjun Narayan, and Benjamin C. Pierce. Linear dependent types for differential privacy. In *Principles of Programming Languages (POPL)*, pages 357–370, Rome, Italy, January 2013.

[GKL08]   Patrice Godefroid, Adam Kiezun, and Michael Y. Levin. Grammar-based whitebox fuzzing. In *Programming Language Design and Implementation (PLDI)*, pages 206–215, Tucson, AZ, USA, June 2008.

[GKS05]   Patrice Godefroid, Nils Klarlund, and Koushik Sen. DART: directed automated random testing. In *Programming Language Design and Implementation (PLDI)*, pages 213–223, Chicago, IL, USA, June 2005.

[GL11]   Patrice Godefroid and Daniel Luchaup. Automatic partial loop summarization in dynamic test generation. In *International Symposium on Software Testing and Analysis (ISSTA)*, pages 23–33, Toronto, ON, Canada, July 2011.

[GLR09]   Vijay Ganesh, Tim Leek, and Martin C. Rinard. Taint-based directed whitebox fuzzing. In *International Conference on Software Engineering (ICSE)*, pages 474–484, Vancouver, BC, Canada, May 2009.

[HDWY06]   Brian Hackett, Manuvir Das, Daniel Wang, and Zhe Yang. Modular checking for buffer overflows in the large. In *International Conference on Software Engineering (ICSE)*, pages 232–241, Shanghai, China, May 2006.

[HEKM11]   Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In *USENIX Security Symposium*, San Francisco, CA, USA, August 2011.

[HJR10]   William R. Harris, Somesh Jha, and Thomas W. Reps. DIFC programs by automatic instrumentation. In *ACM Conference on Computer and Communications Security (CCS)*, pages 284–296, Chicago, IL, USA, October 2010.

[HKE12]   Yan Huang, Jonathan Katz, and David Evans. Quid-pro-quo-tocols: Strengthening semi-honest protocols with dual execution. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 272–284, San Francisco, CA, USA, May 2012.

[JAB12]   Jiyong Jang, Abeer Agrawal, and David Brumley. ReDeBug: Finding unpatched code clones in entire OS distributions. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 48–62, San Francisco, CA, USA, May 2012.

[JW04]   Rob Johnson and David Wagner. Finding user/kernel pointer bugs with type inference. In *USENIX Security Symposium*, pages 119–134, San Diego, CA, USA, August 2004.

[KEH+09]   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. seL4: formal verification of an OS kernel. In *Symposium on Operating Systems Principles (SOSP)*, pages 207–220, Big Sky, MT, USA, October 2009.

[Kin76]   James C. King. Symbolic execution and program testing. *Communications of the ACM*, 19(7):385–394, July 1976.

[KMO12]   Boris Köpf, Laurent Mauborgne, and Martín Ochoa. Automatic quantification of cache side-channels. In *Computer Aided Verification (CAV)*, pages 564–580, Berkeley, CA, USA, July 2012.

[KMPS11]   Min Gyung Kang, Stephen McCamant, Pongsin Poosankam, and Dawn Song. DTA++: Dynamic taint analysis with targeted control-flow propagation. In *Network and Distributed System Security Symposium (NDSS)*, pages 269–282, San Diego, CA, USA, February 2011.

[LAB11]   JongHyup Lee, Thanassis Avgerinos, and David Brumley. TIE: Principled reverse engineering of types in binary programs. In *Network and Distributed System Security Symposium (NDSS)*, pages 251–268, San Diego, CA, USA, February 2011.

[LZX10]   Zhiqiang Lin, Xiangyu Zhang, and Dongyan Xu. Automatic reverse engineering of data structures from binary execution. In *Network and Distributed System Security Symposium (NDSS)*, pages 409–426, San Diego, CA, USA, March 2010.

[Mal07]   Pasquale Malacaria. Assessing security threats of looping constructs. In *Principles of Programming Languages (POPL)*, pages 225–235, Nice, France, January 2007.

[MASB05]   Matias Madou, Bertrand Anckaert, Bjorn De Sutter, and Koen De Bosschere. Hybrid static-dynamic attacks against software protection mechanisms. In *Digital Rights Management Workshop (DRM)*, pages 75–82, Alexandria, VA, USA, November 2005.

[MC12]   Stefan Muller and Stephen Chong. Towards a practical secure concurrent language. In *Object Oriented Programming Systems Languages and Applications (OOPSLA)*, pages 57–74, Indianapolis, IN, USA, October 2012.

[ME08]   Stephen McCamant and Michael D. Ernst. Quantitative information flow as network flow capacity. In *Programming Language Design and Implementation (PLDI)*, pages 193–205, Tucson, AZ, USA, June 2008.

[MFS90]   Barton P. Miller, Lars Fredriksen, and Bryan So. An empirical study of the reliability of UNIX utilities. *Communications of the ACM*, 33(12):32–44, 1990.

[MM06]   Stephen McCamant and Greg Morrisett. Evaluating SFI for a CISC architecture. In *USENIX Security Symposium*, pages 209–224, Vancouver, BC, Canada, August 2006.

[MNPS04]   Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - secure two-party computation system. In *USENIX Security Symposium*, pages 287–302, San Diego, CA, USA, August 2004.

[MPFH11]   Kin-Keung Ma, Khoo Yit Phang, Jeffrey S. Foster, and Michael Hicks. Directed symbolic execution. In *Static Analysis Symposium (SAS)*, pages 95–111, Venice, Italy, September 2011.

[MPSW05]   David Molnar, Matt Piotrowski, David Schultz, and David Wagner. The program counter security model: Automatic detection and removal of control-flow side channel attacks. In *International Conference on Information Security and Cryptology (ICISC)*, pages 156–168, Seoul, Korea, December 2005.

[MSMM09]   Joshua Mason, Sam Small, Fabian Monrose, and Greg MacManus. English shellcode. In *ACM Conference on Computer and Communications Security (CCS)*, pages 524–533, Chicago, IL, USA, November 2009.

[MTT+12]   Greg Morrisett, Gang Tan, Joseph Tassarotti, Jean-Baptiste Tristan, and Edward Gan. RockSalt: better, faster, stronger SFI for the x86. In *Programming Language Design and Implementation (PLDI)*, pages 395–404, Beijing, China, June 2012.

[Mye99]   Andrew C. Myers. JFlow: practical mostly-static information flow control. In *Principles of Programming Languages (POPL)*, pages 228–241, San Antonio, TX, USA, January 1999.

[NLLcC06]   Susanta Nanda, Wei Li, Lap-Chung Lam, and Tzi cker Chiueh. BIRD: Binary interpretation using runtime disassembly. In *Code Generation and Optimization (CGO)*, pages 358–370, March 2006.

[NMS09]   James Newsome, Stephen McCamant, and Dawn Song. Measuring channel capacity to distinguish undue influence. In *Programming Languages and Analysis for Security (PLAS)*, pages 73–85, Dublin, Ireland, June 2009.

[NS05]   James Newsome and Dawn Song. Dynamic taint analysis: Automatic detection, analysis, and signature generation of exploit attacks on commodity software. In *Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, USA, February 2005.

[OJM12]   Damien Octeau, Somesh Jha, and Patrick McDaniel. Retargeting Android applications to Java bytecode. In *Foundations of Software Engineering (FSE)*, Cary, NC, USA, November 2012.

[PEGK11]   Joe Gibbs Politz, Spiridon Aristides Eliopoulos, Arjun Guha, and Shriram Krishnamurthi. ADsafety: Type-based verification of JavaScript sandboxing. In *USENIX Security Symposium*, San Francisco, CA, USA, August 2011.

[PLEB07]   Carlos Pacheco, Shuvendu K. Lahiri, Michael D. Ernst, and Thomas Ball. Feedback-directed random test generation. In *International Conference on Software Engineering (ICSE)*, pages 75–84, Minneapolis, MN, USA, May 2007.

[PMTP12]   Quoc-Sang Phan, Pasquale Malacaria, Oksana Tkachuk, and Corina Păsăreanu. Symbolic quantitative information flow. In *Java Pathfinder Workshop (JPF)*, Cary, NC, USA, November 2012.

[RP10]   Jason Reed and Benjamin C. Pierce. Distance makes the types grow stronger: a calculus for differential privacy. In *International Conference on Functional Programming (ICFP)*, pages 157–168, Baltimore, MD, USA, September 2010.

[RPB⁺09]   Indrajit Roy, Donald E. Porter, Michael D. Bond, Kathryn S. McKinley, and Emmett Witchel. Laminar: practical fine-grained decentralized information flow control. In *Programming Language Design and Implementation (PLDI)*, pages 63–74, Dublin, Ireland, June 2009.

[SAB10]   Edward J. Schwartz, Thanassis Avgerinos, and David Brumley. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask). In *IEEE Symposium on Security and Privacy "Oakland"*, pages 317–331, Oakland, CA, USA, May 2010.

[SB09]   Asia Slowinska and Herbert Bos. Pointless tainting?: evaluating the practicality of pointer tainting. In *ACM European Conference on Computer Systems (EuroSys)*, pages 61–74, Nuremberg, Germany, April 2009.

[Sha07]   Hovav Shacham. The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86). In *ACM Conference on Computer and Communications Security (CCS)*, pages 552–561, Alexandria, VA, USA, October 2007.

[SHWK11]   Cynthia Sturton, Matthew Hicks, David Wagner, and Samuel T. King. Defeating UCI: Building stealthy and malicious hardware. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 64–77, Oakland, CA, USA, May 2011.

[SMA05]   Koushik Sen, Darko Marinov, and Gul Agha. CUTE: a concolic unit testing engine for C. In *European Software Engineering Conference held jointly with Foundations of Software Engineering (ESEC/FSE)*, pages 263–272, Lisbon, Portugal, September 2005.

[SMB⁺10]   David Sehr, Robert Muth, Cliff Biffle, Victor Khimenko, Egor Pasko, Karl Schimpf, Bennet Yee, and Brad Chen. Adapting software fault isolation to contemporary CPU architectures. In *USENIX Security Symposium*, pages 1–12, Washington, DC, USA, August 2010.

[SMBW12]   Srinath Setty, Richard McPherson, Andrew J. Blumberg, and Michael Walfish. Making argument systems for outsourced computation practical (sometimes). In *Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2012.

[SSS11]   Mike Samuel, Prateek Saxena, and Dawn Song. Context-sensitive auto-sanitization in web templating languages using type qualifiers. In *ACM Conference on Computer and Communications Security (CCS)*, pages 587–600, Chicago, IL, USA, October 2011.

[ULF06]   Octavian Udrea, Cristian Lumezanu, and Jeffrey S. Foster. Rule-based static analysis of network protocol implementations. In *USENIX Security Symposium*, pages 193–208, Vancouver, BC, Canada, August 2006.

[VC11]   Jeffrey A. Vaughan and Stephen Chong. Inference of expressive declassification policies. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 180–195, Oakland, CA, USA, May 2011.

[Wal89]   Larry Wall. *perl — Practical Extraction and Report Language*, release 3.0 edition, October 1989.

[WJ10]   Zhi Wang and Xuxian Jiang. HyperSafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 380–395, Oakland, CA, USA, May 2010.

[WLAG93]   Robert Wahbe, Steven Lucco, Thomas E. Anderson, and Susan L. Graham. Efficient software-based fault isolation. In *Symposium on Operating Systems Principles (SOSP)*, pages 203–216, Asheville, NC, USA, December 1993.

[WMHL12]   Richard Wartell, Vishwath Mohan, Kevin W. Hamlen, and Zhiqiang Lin. Securing untrusted code via compiler-agnostic binary rewriting. In *Annual Computer Security Applications Conference (ACSAC)*, pages 299–308, Orlando, FL, USA, December 2012.

[WS07]   Gary Wassermann and Zhendong Su. Sound and precise analysis of web applications for injection vulnerabilities. In *Programming Language Design and Implementation (PLDI)*, pages 32–41, San Diego, CA, USA, June 2007.

[YSD+09]   Bennet Yee, David Sehr, Gregory Dardyk, J. Bradley Chen, Robert Muth, Tavis Ormandy, Shiki Okasaka, Neha Narula, and Nicholas Fullagar. Native Client: A sandbox for portable, untrusted x86 native code. In *IEEE Symposium on Security and Privacy "Oakland"*, pages 79–93, Oakland, CA, USA, May 2009.

[YT10]   Hirotoshi Yasuoka and Tachio Terauchi. Quantitative information flow — verification hardness and possibilities. In *Computer Security Foundations (CSF)*, pages 15–27, Edinburgh, UK, July 2010.

[YY12]   Lok Kwong Yan and Heng Yin. DroidScope: Seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis. In *USENIX Security Symposium*, Bellevue, WA, USA, August 2012.

[ZTM11]   Bin Zeng, Gang Tan, and Greg Morrisett. Combining control-flow integrity and static analysis for efficient and validated data sandboxing. In *ACM Conference on Computer and Communications Security (CCS)*, pages 29–40, Chicago, IL, USA, October 2011.