Themen

1. Buffer overflows [CWP+00]
2. Return-oriented Programming [BRSS08]
3. Sichere C-Implementierung [ABS94]
4. Eine sicherere C-Erweiterung [NMW02]
5. Command Injection Attacks [SW06]
6. Format-String Vulnerabilities, statische Erkennung [STFW01]
7. Code injection attacks und Tainting in PHP [PB06]
8. Tainting in PHP [NTGG+05]
9. Tainting in JavaScript [VNJ+07]
10. Tainting für Java [HCF05]
11. Positive Tainting [HOM06]
12. Information Flow Tracking [KHL+13]
13. Binary Rewriting, um Attacken zu erkennen [NS05]
14. Statische Analyse für PHP [JKK06]
15. Statische Analyse für Java [LL05]
16. Statische Erkennung von Buffer Overflows [LE01]
17. Singularity [HLA+05]
18. Sichere Programmdarstellung [ADvRF01]
19. Proof-Carrying Code [NL96]
20. Statische Analyse [CW02]
21. Security-Typed Languages [HAM06]
22. Side-Channel Attacks [CVBS09]

Literatur

[ABS94] Todd M. Austin, Scott E. Breach, and Gurindar S. Sohi. Efficient detection of all pointer and array access errors. In *Proceedings of the ACM SIGPLAN '94 Conference on Programming Language Design and Implementation*, pages 290–301, 1994.

[ADvRF01] Wolfram Amme, Niall Dalton, Jeffery von Ronne, and Michael Franz. Safetsa: A type safe and referentially secure mobile-code representation based on static single assignment form. In *SIGPLAN '01 Conference on Programming Language Design and Implementation*, pages 137–147, 2001.

[BRSS08] Erik Buchanan, Ryan Roemer, Hovav Shacham, and Stefan Savage. When good instructions go bad: generalizing return-oriented programming to RISC. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM Conference on Computer and Communications Security*, pages 27–38. ACM, 2008.

[CVBS09] Bart Coppens, Ingrid Verbauwhede, Koen De Bosschere, and Bjorn De Sutter. Practical mitigations for timing-based side-channel attacks on modern x86 processors. In *IEEE Symposium on Security and Privacy*, pages 45–60. IEEE Computer Society, 2009.

[CW02] Hao Chen and David Wagner. MOPS: an infrastructure for examining security properties of software. In Ravi Sandhu, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 235–244, Washington, DC, USA, November 2002. ACM Press.

[CWP+00] Crispin Cowan, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. Buffer overflows: Attacks and defenses for the vulnerability of the decade. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX 2000)*. IEEE Computer Society Press, January 2000.

[HAM06] Boniface Hicks, Kiyan Ahmadizadeh, and Patrick McDaniel. Understanding practical application development in security-typed languages. In *22nd Annual Computer Security Applications Conference*. ACM, December 2006.

[HCF05] Vivek Haldar, Deepak Chandra, and Michael Franz. Dynamic taint propagation for Java. In *21st Annual Computer Security Applications Conference*, pages 274–282. ACM, December 2005.

[HLA+05] Galen Hunt, James R. Larus, Martin Abadi, Mark Aiken, Paul Barham, Manuel Fahndrich, Chris Hawblitzel, Orion Hodson, Steven Levi, Nick Murphy, Bjarne Steensgaard, David Tarditi, Ted Wobber, and Brian D. Zill. An overview of the singularity project. Technical Report MSR-TR-2005-135, Microsoft Research (MSR), October 2005.

[HOM06] William G. J. Halfond, Alessandro Orso, and Panagiotis Manolios. Using positive tainting and syntax-aware evaluation to counter SQL injection attacks. In Michal Young and Premkumar T. Devanbu, editors, *Proceedings of the 14th ACM SIGSOFT International Symposium on Foundations of Software Engineering, FSE 2005, Portland, Oregon, USA, November 5-11, 2006*, pages 175–185. ACM, 2006.

[JKK06] Nenad Jovanovic, Christopher Krügel, and Engin Kirda. Pixy: A static analysis tool for detecting web application vulnerabilities (short paper). In *IEEE Symposium on Security and Privacy*, pages 258–263. IEEE Computer Society, 2006.

[KHL+13] Christoph Kerschbaumer, Eric Hennigan, Per Larsen, Stefan Brunthaler, and Michael Franz. Crowdflow: Efficient information flow security. In Yvo Desmedt, editor, *Information Security: 16th International Conference, ISC 2013*, pages 321–337, Cham, 2013. Springer LNCS 7807.

[LE01] David Larochelle and David Evans. Statically detecting likely buffer overflow vulnerabilities. In USENIX, editor, *Proceedings of the Tenth USENIX Security Symposium, August 13–17, 2001, Washington, DC, USA*, pages ??–??, pub-USENIX:adr, 2001. USENIX.

[LL05] V. Benjamin Livshits and Monica S. Lam. Finding security vulnerabilities in Java applications using static analysis. In *Proceedings of the 14th USENIX Security Symposium*, August 2005.

[NL96] George C. Necula and Peter Lee. Safe kernel extensions without run-time checking. In *Proceedings of the Second Symposium on Operating System Design and Implementation*, Seattle, WA, USA, October 1996.

[NMW02] George C. Necula, Scott McPeak, and Westley Weimer. CCured: Type-safe retrofitting of legacy code. In *Conference Record of POPL'02: The 29th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 128–139, Portland, Oregon, January 16–18, 2002.

[NS05] James Newsome and Dawn Xiaodong Song. Dynamic taint analysis for automatic detection, analysis, and signaturegeneration of exploits on commodity software. In *NDSS*. The Internet Society, 2005.

[NTGG+05] Anh Nguyen-Tuong, Salvatore Guarnieri, Doug Greene, Jeff Shirley, and David Evans. Automatically hardening web applications using precise tainting. In Ryôichi Sasaki, Sihan Qing, Eiji Okamoto, and Hiroshi Yoshiura, editors, *Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11 20th International Conference on Information Security (SEC 2005), May 30 - June 1, 2005, Chiba, Japan*, pages 295–308. Springer, 2005.

[PB06] Tadeusz Pietraszek and Chris Vanden Berghe. Defending against injection attacks through context-sensitive string evaluation? In *Recent Advances in Intrusion Detection — Proceedings of the 8th International Symposium (RAID 2005)*, volume 3858 of *Lecture Notes in Computer Science*, pages 124–145. Springer-Verlag, Berlin Germany, September 2006.

[STFW01] Umesh Shankar, Kunal Talwar, Jeffrey S. Foster, and David Wagner. Detecting format string vulnerabilities with type qualifiers. In USENIX, editor, *Proceedings of the Tenth USENIX Security Symposium, August 13–17, 2001, Washington, DC, USA*, pages ??–??, pub-USENIX:adr, 2001. USENIX.

[SW06] Zhendong Su and Gary Wassermann. The essence of command injection attacks in web applications. In J. Gregory Morrisett and Simon L. Peyton Jones, editors, *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2006, Charleston, South Carolina, USA, January 11-13, 2006*, pages 372–382. ACM, 2006.

[VNJ+07] Philipp Vogt, Florian Nentwich, Nenad Jovanovic, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. Cross site scripting prevention with dynamic data tainting and static analysis. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2007)*, San Diego, CA, February 2007. Internet Society.