1/27 [RTSS09]

1/29 [SS13] Background: [GO96]

2/3 [KAC12] Background: [Nak08]

2/5 [MGGR13]

2/10 [ZS13] Background: [ABUEL05]

2/12 [PPK13] Background: [Sha07]

2/17 [FHE+12] Optional related: [NZD+14]

2/19 [NE13]

NS [UDWH13]

2/24 [HSF+13]

2/26 [GDNP12]

NS [SSS11, HNS+12]

3/3 [FNB13]

3/5 [WWGH11]

NS [DCRS13, WPF13]

3/10 [BPW13] Background: [DMS04]

3/12 [JTJS14]

NS [NDW10, JWJ+13]

3/24 [RAW+13]

3/26 [GBC+12]

NS [DGZ13, PJM+14]

3/31 [EBFK13]

4/2 [DH14]

NS [WCGB13, BBC+10]

4/7 [McS09]

4/9 [Mir12]

NS [CSS10, LQS+13]

4/14 [GHR+11]

4/16 [BBE+13]

NS [HHBR+08, Cul12, KCC+13]

4/21 [CMK+11]

5/7 [LWS08]

NS [BDG+10, FHJ+13]

NS [Whe05, IEGT13, BRPB13] Background: [Tho84]

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.

[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.

[BBE+13] Josh Benaloh, Michael D. Byrne, Bryce Eakin, Philip Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, Dan S. Wallach, Gail Fisher, Julian Montoya, Michelle Parker, and Michael Winn. STAR-Vote: A secure, transparent, auditable, and reliable voting system. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, Washington, DC, USA, August 2013.

[BDG+10] Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, and Caroline Sporleder. Acoustic side-channel attacks on printers. In *USENIX Security Symposium*, pages 307–322, Washington, DC, USA, August 2010.

[BPW13] Alex Biryukov, Ivan Pustogarov, and Ralf-Philipp Weinmann. Trawling for Tor hidden services: Detection, measurement, deanonymization. In *IEEE Symposium on Security and Privacy ("Oakland")*, pages 80–94, San Francisco, CA, USA, May 2013.

[BRPB13] Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans. In *Cryptographic Hardware and Embedded Systems (CHES)*, pages 197–214, Santa Barbara, CA, USA, August 2013.

[CMK+11] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, San Francisco, CA, USA, August 2011.

[CSS10] T.-H. Hubert Chan, Elaine Shi, and Dawn Song. Private and continual release of statistics. In *International Collquium on Automata, Languages and Programming (ICALP)*, pages 405–417, Bordeaux, France, June 2010.

[Cul12] Chris Culnane. A hybrid touch interface for Prêt à Voter. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, Bellevue, WA, USA, August 2012.

[DCRS13] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. Protocol misidentification made easy with format-transforming encryption. In *ACM Conference on Computer and Communications Security (CCS)*, pages 61–72, Berlin, Germany, November 2013.

[DGZ13] Vacha Dave, Saikat Guha, and Yin Zhang. ViceROI: Catching click-spam in search ad networks. In *ACM Conference on Computer and Communications Security*, pages 765–776, Berlin, Germany, November 2013.

[DH14] Johannes Dahse and Thorsten Holz. Simulation of built-in PHP features for precise static code analysis. In *Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, USA, February 2014.

[DMS04] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303–320, San Diego, CA, USA, August 2004.

[EBFK13] Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. An empirical study of cryptographic misuse in Android applications. In *ACM Conference on Computer and Communications Security*, pages 73–84, Berlin, Germany, November 2013.

[FHE+12] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: user attention, comprehension, and behavior. In *Symposium On Usable Privacy and Security (SOUPS)*, Washington, DC, USA, July 2012.

[FHJ+13] Mario Frank, Tiffany Hwu, Sakshi Jain, Robert Knight, Ivan Martinovic, Prateek Mittal, Daniele Perito, and Dawn Song. Subliminal probing for private information via EEG-based BCI devices. *arXiv.org Cryptography and Security (cs.CR)*, 1312.6052, December 2013.

[FNB13] David Fifield, Gabi Nakibly, and Dan Boneh. OSS: Using online scanning services for censorship circumvention. In *Privacy Enhancing Technologies (PET)*, pages 185–204, Bloomington, IN, USA, July 2013.

[GBC+12] Chris Grier, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, Niels Provos, M. Zubair Rafique, Moheeb Abu Rajab, Christian Rossow, Kurt Thomas, Vern Paxson, Stefan Savage, and Geoffrey M. Voelker. Manufacturing compromise: the emergence of exploit-as-a-service. In *ACM Conference on Computer and Communications Security*, pages 821–832, Raleigh, NC, USA, November 2012.

[GDNP12] Willem De Groef, Dominique Devriese, Nick Nikiforakis, and Frank Piessens. FlowFox: a web browser with flexible and precise information flow control. In *ACM Conference on Computer and Communications Security*, pages 748–759, Raleigh, NC, USA, November 2012.

[GHR+11] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. In *ACM SIGCOMM*, pages 2–13, Toronto, ON, Canada, August 2011.

[GO96] Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on oblivious RAMs. *J. ACM*, 43(3):431–473, May 1996.

[HHBR+08] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security and Privacy ("Oakland")*, pages 129–142, Oakland, CA, USA, May 2008.

[HNS+12] Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, and Jörg Schwenk. Scriptless attacks: stealing the pie without touching the sill. In *ACM Conference on Computer and Communications Security*, pages 760–771, Raleigh, NC, USA, November 2012.

[HSF+13] Mario Heiderich, Jörg Schwenk, Tilman Frosch, Jonas Magazinius, and Edward Z. Yang. mXSS attacks: attacking well-secured web-applications by using innerHTML mutations. In *ACM Conference on Computer and Communications Security*, pages 777–788, Berlin, Germany, November 2013.

[IEGT13] Frank Imeson, Ariq Emtenan, Siddharth Garg, and Mahesh V. Tripunitara. Securing computer hardware using 3D integrated circuit (IC) technology and split manufacturing for obfuscation. In *USENIX Security Symposium*, Washington, DC, USA, August 2013.

[JTJS14] Rob Jansen, Florian Tschorsch, Aaron Johnson, and Björn Scheuermann. The sniper attack: Anonymously deanonymizing and disabling the Tor network. In *Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, USA, February 2014.

[JWJ+13] Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, and Paul F. Syverson. Users get routed: traffic correlation on Tor by realistic adversaries. In *ACM Conference on Computer and Communications Security (CCS)*, pages 337–348, Berlin, Germany, November 2013.

[KAC12] Ghassan Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in Bitcoin. In *ACM Conference on Computer and Communications Security (CCS)*, pages 906–917, Raleigh, NC, USA, November 2012.

[KCC+13] Eric Kim, Nicholas Carlini, Andrew Chang, George Yiu, Kai Wang, and David Wagner. Improved support for machine-assisted ballot-level audits. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, Washington, DC, USA, August 2013.

[LQS+13] Ninghui Li, Wahbeh Qardaji, Dong Su, Yi Wu, and Weining Yang. Membership privacy: a unifying framework for privacy definitions. In *ACM Conference on Computer and Communications Security*, pages 889–900, Berlin, Germany, November 2013.

[LWS08] Benjamin Laxton, Kai Wang, and Stefan Savage. Reconsidering physical key secrecy: Teleduplication via optical decoding. In *ACM Conference on Computer and Communications Security (CCS)*, pages 469–478, Alexandria, VA, USA, November 2008.

[McS09] Frank McSherry. Privacy integrated queries: An extensible platform for privacy-preserving data analysis. In *SIGMOD International Conference on Management of Data*, pages 19–30, Providence, RI, USA, June 2009.

[MGGR13] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin. In *IEEE Symposium on Security and Privacy ("Oakland")*, pages 397–411, San Francisco, CA, USA, May 2013.

[Mir12] Ilya Mironov. On significance of the least significant bits for differential privacy. In *ACM Conference on Computer and Communications Security*, pages 650–661, Raleigh, NC, USA, November 2012.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `http://www.bitcoin.org/bitcoin.pdf`, October 2008.

[NDW10] Tsuen-Wan Ngan, Roger Dingledine, and Dan S. Wallach. Building incentives into Tor. In *Financial Cryptography and Data Security (FC)*, pages 238–256, Tenerife, Canary Islands, January 2010.

[NE13] Adwait Nadkarni and William Enck. Preventing accidental data disclosure in modern operating systems. In *ACM Conference on Computer and Communications Security (CCS)*, pages 1029–1042, Berlin, Germany, November 2013.

[NZD+14] Muhammad Naveed, Xiaoyong Zhou, Soteris Demetriou, XiaoFeng Wang, and Carl A Gunter. Inside job: Understanding and mitigating the threat of external device mis-bonding on Android. In *Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, USA, February 2014.

[PJM+14] Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, and Markus Jakobsson. Scambaiter: Understanding targeted Nigerian scams on Craigslist. In *Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, USA, February 2014.

[PPK13] Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis. Transparent ROP exploit mitigation using indirect branch tracing. In *USENIX Security Symposium*, Washington, DC, USA, August 2013.

[RAW+13] Christian Rossow, Dennis Andriesse, Tillmann Werner, Brett Stone-Gross, Daniel Plohmann, Christian J. Dietrich, and Herbert Bos. SoK: P2PWNED — modeling and evaluating the resilience of peer-to-peer botnets. In *IEEE Symposium on Security and Privacy ("Oakland")*, pages 97–111, San Francisco, CA, USA, May 2013.

[RTSS09] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *ACM Conference on Computer and Communications Security (CCS)*, pages 199–212, Chicago, IL, USA, November 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.

[SS13] Emil Stefanov and Elaine Shi. Multi-cloud oblivious storage. In *ACM Conference on Computer and Communications Security (CCS)*, pages 247–258, Berlin, Germany, November 2013.

[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*, pages 587–600, Chicago, IL, USA, October 2011.

[Tho84] Ken Thompson. Reflections on trusting trust. *Commun. ACM*, 27(8):761–763, 1984.

[UDWH13] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the security of graphical passwords: the case of Android unlock patterns. In *ACM Conference on Computer and Communications Security (CCS)*, pages 161–172, Berlin, Germany, November 2013.

[WCGB13] Maverick Woo, Sang Kil Cha, Samantha Gottlieb, and David Brumley. Scheduling black-box mutational fuzzing. In *ACM Conference on Computer and Communications Security*, pages 511–522, Berlin, Germany, November 2013.

[Whe05] David Wheeler. Countering trusting trust through diverse double-compiling. In *Annual Computer Security Applications Conference (ACSAC)*, pages 33–48, Tucson, AZ, USA, December 2005.

[WPF13] Philipp Winter, Tobias Pulls, and Jürgen Fuß. ScrambleSuit: a polymorphic network protocol to circumvent censorship. In *Workshop on Privacy in the Electronic Society (WPES)*, pages 213–224, Berlin, Germany, November 2013.

[WWGH11] Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. Alex Halderman. Telex: Anticensorship in the network infrastructure. In *USENIX Security Symposium*, San Francisco, CA, USA, August 2011.

[ZS13] Mingwei Zhang and R. Sekar. Control flow integrity for COTS binaries. In *USENIX Security Symposium*, Washington, DC, USA, August 2013.