References Cited

[1] M. Alam, H. A. Khan, M. Dey, N. Sinha, R. Callan, A. Zajic, and M. Prvulovic. One&Done: A Single-Decryption EM-Based Attack on OpenSSL's Constant-Time Blinded RSA. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 585–602, Baltimore, MD, 2018. USENIX Association.

[2] M. Alam, B. Yilmaz, F. Werner, N. Samwel, A. Zajic, D. Genkin, Y. Yarom, and M. Prvulovic. Nonce@Once: A Single-Trace EM Side Channel Attack on Several Constant-Time Elliptic Curve Implementations in Mobile Platforms. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 507–522, 2021.

[3] A. Althoff, J. McMahan, L. Vega, S. Davidson, T. Sherwood, M. B. Taylor, and R. Kastner. Hiding intermittent information leakage with architectural support for blinking. In *Proceedings of the 45th Annual International Symposium on Computer Architecture*, ISCA '18, pages 638–649, Piscataway, NJ, USA, 2018. IEEE Press.

[4] M. Andrysco, A. Nötzli, F. Brown, R. Jhala, and D. Stefan. Towards verified, constant-time floating point operations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 1369–1382, New York, NY, USA, 2018. ACM.

[5] E. K. Ardestani and J. Renau. Esesc: A fast multicore simulator using time-based sampling. In *Proceedings of the 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA)*, HPCA '13, pages 448–459, Washington, DC, USA, 2013. IEEE Computer Society.

[6] E. K. Ardestani and J. Renau. ESESC: A Fast Multicore Simulator Using Time-Based Sampling. In *19th International Conference on High Performance Computer Architecture (HPCA)*, Feb 2013.

[7] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder. Acoustic side-channel attacks on printers. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security'10, pages 20–20, Berkeley, CA, USA, 2010. USENIX Association.

[8] J. Balasch, B. Gierlichs, O. Reparaz, and I. Verbauwhede. DPA, Bitslicing and Masking at 1 GHz. *IACR Cryptology ePrint Archive*, 2015:727, 2015.

[9] A. Barenghi and G. Pelosi. Side-channel security of superscalar cpus: Evaluating the impact of micro-architectural features. In *Proceedings of the 55th Annual Design Automation Conference*, DAC '18, pages 120:1–120:6, New York, NY, USA, 2018. ACM.

[10] M. F. Bergamini, A. L. Santos, N. R. Stradiotto, and M. V. B. Zanoni. A disposable electrochemical sensor for the rapid determination of levodopa. *Journal of Pharmaceutical and Biomedical Analysis*, 39(1):54–59, 2005.

[11] D. J. Bernstein, J. Breitner, D. Genkin, L. Groot Bruinderink, N. Heninger, T. Lange, C. van Vreden-daal, and Y. Yarom. Sliding right into disaster: Left-to-right sliding windows leak. In W. Fischer and N. Homma, editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, pages 555–576, Cham, 2017. Springer International Publishing.

[12] N. Binkert, B. Beckmann, G. Black, S. K. Reinhardt, A. Saidi, A. Basu, J. Hestness, D. R. Hower, T. Krishna, S. Sardashti, R. Sen, K. Sewell, M. Shoaib, N. Vaish, M. D. Hill, and D. A. Wood. The Gem5 Simulator. *ACM SIGARCH Computer Architecture News*, 39(2):1–7, Aug. 2011.

[13] N. Bleier, , F. Rodriguez, A. Sou, S. White, and R. Kumar. Exploiting short application lifetimes for low cost hardware encryption in flexible electronics. In *Proceedings of the 2023 Conference & Exhibition on Design, Automation & Test in Europe*, DATE '23, New York, NY, USA. Association for Computing Machinery.

[14] N. Bleier, M. H. Mubarik, F. Rasheed, J. Aghassi-Hagmann, M. B. Tahoori, and R. Kumar. Printed microprocessors. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)*, pages 213–226, 2020.

[15] N. Bleier, J. Sartori, and R. Kumar. Property-driven automatic generation of reduced-isa hardware. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, pages 349–354, 2021.

[16] J. Brouchier, T. Kean, C. Marsh, and D. Naccache. Temperature attacks. *IEEE Security Privacy*, 7(2):79–82, March 2009.

[17] R. Callan, F. Behrang, A. Zajic, M. Prvulovic, and A. Orso. Zero-overhead profiling via EM emanations. In *Proceedings of the 25th International Symposium on Software Testing and Analysis, ISSTA 2016, Saarbrücken, Germany, July 18-20, 2016*, pages 401–412, 2016.

[18] R. Callan, A. Zajić, and M. Prvulovic. A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events. In *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO-47, pages 242–254, Washington, DC, USA, 2014. IEEE Computer Society.

[19] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 163–177, New York, NY, USA, 2018. ACM.

[20] T. E. Carlson, W. Heirman, S. Eyerman, I. Hur, and L. Eeckhout. An evaluation of high-level mechanistic core models. *ACM Transactions on Architecture and Code Optimization (TACO)*, 2014.

[21] S. Chari, J. R. Rao, and P. Rohatgi. Template attacks. In *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, pages 13–28, London, UK, UK, 2003. Springer-Verlag.

[22] J. Chen, Y. Feng, and I. Dillig. Precise detection of side-channel vulnerabilities using quantitative cartesian hoare logic. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 875–890, New York, NY, USA, 2017. ACM.

[23] Y. Chen, G. Fu, Y. Zilberman, W. Ruan, S. K. Ameri, E. Miller, and S. Sonkusale. Disposable colorimetric geometric barcode sensor for food quality monitoring. In *2017 19th International Conference on Solid-State Sensors, Actuators and Microsystems (TRANSDUCERS)*, pages 1422–1424, 2017.

[24] C.-L. Cheng and A. Zajic. Characterization of propagation phenomena relevant for 300 ghz wireless data center links. *IEEE Transactions on Antennas and Propagation*, 68(2):1074–1087, 2020.

[25] H. Cherupalli, H. Duwe, W. Ye, R. Kumar, and J. Sartori. Bespoke processors for applications with ultra-low area and power constraints. In *Proceedings of the 44th Annual International Symposium on Computer Architecture*, ISCA '17, page 41–54, New York, NY, USA, 2017. Association for Computing Machinery.

[26] H. Cherupalli, H. Duwe, W. Ye, R. Kumar, and J. Sartori. Software-based gate-level information flow security for iot systems. In *Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO-50 '17, page 328–340, New York, NY, USA, 2017. Association for Computing Machinery.

[27] L. Conrad. Ece outreach:@ georgia tech. `https://www.www-new.ece.gatech.edu/outreach`.

[28] J. Demme, M. Maycock, J. Schmitz, A. Tang, A. Waksman, S. Sethumadhavan, and S. Stolfo. On the feasibility of online malware detection with performance counters. In *Proceedings of the 40th Annual International Symposium on Computer Architecture*, ISCA '13, pages 559–570, New York, NY, USA, 2013. ACM.

[29] H. Derakhshandeh, S. S. Kashaf, F. Aghabaglou, I. O. Ghanavati, and A. Tamayol. Smart bandages: The future of wound care. *Trends in Biotechnology*, 36(12):1259–1274, 2018.

[30] M. Dey, A. Nazari, A. Zajic, and M. Prvulovic. Emprof: Memory profiling via em-emanation in iot and hand-held devices. In *2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 881–893, 2018.

[31] M. Dey, B. B. Yilmaz, M. Prvulovic, and A. Zajic. Primer: Profiling interrupts using electromagnetic side-channel for embedded devices. *IEEE Transactions on Computers*, pages 1–1, 2021.

[32] T. Elfaramawy, C. L. Fall, S. Arab, M. Morissette, F. Lellouche, and B. Gosselin. A wireless respiratory monitoring system using a wearable patch sensor network. *IEEE Sensors Journal*, 19(2):650–657, 2019.

[33] J. Fu, P. Juyal, and A. Zajic. Thz channel characterization of chip-to-chip communication in desktop size metal enclosure. *IEEE Transactions on Antennas and Propagation*, 67(12):7550–7560, 2019.

[34] J. Fu, P. Juyal, and A. Zajic. Modeling of 300 ghz chip-to-chip wireless channels in metal enclosures. *IEEE Transactions on Wireless Communications*, 19(5):3214–3227, 2020.

[35] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer. Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation. In T. Güneysu and H. Handschuh, editors, *Cryptographic Hardware and Embedded Systems – CHES 2015*, pages 207–228, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[36] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom. Ecdsa key extraction from mobile devices via nonintrusive physical side channels. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1626–1638, New York, NY, USA, 2016. ACM.

[37] D. T. Gethin, E. H. Jewell, and T. C. Claypole. Printed silver circuits for fmcg packaging. *Circuit World*, 2013.

[38] D. I. Gorman, M. R. Guthaus, and J. Renau. Architectural opportunities for novel dynamic emi shifting (demis). In *Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO-50 '17, pages 774–785, New York, NY, USA, 2017. ACM.

[39] Z. Hadjilambrou, S. Das, M. A. Antoniades, and Y. Sazeides. Leveraging cpu electromagnetic emanations for voltage noise characterization. In *2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 573–585, Oct 2018.

[40] Y. Han, S. Etigowni, H. Liu, S. Zonouz, and A. Petropulu. Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 1095–1108, New York, NY, USA, 2017. ACM.

[41] D. J. Hand. Statistical concepts: A second course, fourth edition by richard g. lomax, debbie l. hahs-vaughn. *International Statistical Review*, 80(3):491–491, 2012.

[42] Z. He and R. B. Lee. How secure is your cache against side-channel attacks? In *Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO-50 '17, pages 341–353, New York, NY, USA, 2017. ACM.

[43] E. Jorgensen, A. Kacmarcik, M. Prvulovic, and A. Zajic. Novel feature selection for non-destructive detection of hardware trojans using hyperspectral scanning. *J Hardware and Systems Security*, 6:32–46, 2022.

[44] S. Kim and A. Zajic. Characterization of 300-ghz wireless channel on a computer motherboard. *IEEE Transactions on Antennas and Propagation*, 64(12):5411–5423, 2016.

[45] S. Kim and A. Zajic. Statistical modeling and simulation of short-range device-to-device communication channels at sub-thz frequencies. *IEEE Transactions on Wireless Communications*, 15(9):6423–6433, 2016.

[46] S. Li, J. H. Ahn, R. D. Strong, J. B. Brockman, D. M. Tullsen, and N. P. Jouppi. Mcpat: An integrated power, area, and timing modeling framework for multicore and manycore architectures. In *Proceedings of the 42Nd Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO 42, pages 469–480, New York, NY, USA, 2009. ACM.

[47] S. Li, K. Chen, J. H. Ahn, J. B. Brockman, and N. P. Jouppi. Cacti-p: Architecture-level modeling for sram-based structures with advanced leakage reduction techniques. In *Proceedings of the International Conference on Computer-Aided Design*, ICCAD '11, pages 694–701, Piscataway, NJ, USA, 2011. IEEE Press.

[48] C. Liu, A. Harris, M. Maas, M. Hicks, M. Tiwari, and E. Shi. Ghostrider: A hardware-software system for memory trace oblivious computation. In *Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '15, pages 87–101, New York, NY, USA, 2015. ACM.

[49] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, and Q. Xu. On code execution tracking via power side-channel. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1019–1031, New York, NY, USA, 2016. ACM.

[50] G. Marrazza, I. Chianella, and M. Mascini. Disposable dna electrochemical biosensors for environmental monitoring. *Analytica Chimica Acta*, 387(3):297–307, 1999.

[51] D. McCann, E. Oswald, and C. Whitnall. Towards practical tools for side channel aware software engineering: Grey box' modelling for instruction leakages. In *Proceedings of the 26th USENIX Conference on Security Symposium*, SEC'17, pages 199–216, Berkeley, CA, USA, 2017. USENIX Association.

[52] J. K. Millen. Covert channel capacity. In *Security and Privacy, 1987 IEEE Symposium on*, pages 60–60, April 1987.

[53] M. H. Mubarik, D. D. Weller, N. Bleier, M. Tomei, J. Aghassi-Hagmann, M. B. Tahoori, and R. Kumar. Printed machine learning classifiers. In *2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 73–87, 2020.

[54] K. Nayak, C. W. Fletcher, L. Ren, N. Chandran, S. V. Lokam, E. Shi, and V. Goyal. Hop: Hardware makes obfuscation practical. In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, NDSS '17, 2017.

[55] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic. Eddie: Em-based detection of deviations in program execution. In *Proceedings of the 44th Annual International Symposium on Computer Architecture*, ISCA '17, pages 333–346, New York, NY, USA, 2017. ACM.

[56] L. Nguyen, C.-L. Cheng, M. Prvulovic, and A. Zajic. Creating a backscattering side channel to enable detection of dormant hardware trojans. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2019.

[57] L. N. Nguyen, B. B. Yilmaz, M. Prvulovic, and A. Zajic. A novel golden-chip-free clustering technique using backscattering side channel for hardware trojan detection. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 1–12, 2020.

[58] A. Patel, F. Afram, S. Chen, and K. Ghose. Marss: A full system simulator for multicore x86 cpus. In *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1050–1055, June 2011.

[59] A. Rane, C. Lin, and M. Tiwari. Raccoon: Closing digital side-channels through obfuscated execution. In *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC'15, pages 431–446, Berkeley, CA, USA, 2015. USENIX Association.

[60] A. Rane, C. Lin, and M. Tiwari. Secure, precise, and fast floating-point operations on x86 processors. In *Proceedings of the 25th USENIX Conference on Security Symposium*, SEC'16, pages 71–86, Berkeley, CA, USA, 2016. USENIX Association.

[61] T. Rappaport, K. Remley, C. Gentle, A. Molisch, and A. Zajic. *Radio propagation measurements and channel modeling: best practices for millimeter-wave and sub-terahertz frequencies*. Cambridge University Press, 2022.

[62] J. Renau, B. Fraguela, J. Tuck, W. Liu, M. Prvulovic, L. Ceze, S. Sarangi, P. Sack, K. Strauss, and P. Montesinos. SESC simulator, January 2005. http://sesc.sourceforge.net.

[63] A. Rinaldi, C. Becchimanzi, and F. Tosi. Wearable devices and smart garments for stress management. In S. Bagnara, R. Tartaglia, S. Albolino, T. Alexander, and Y. Fujita, editors, *Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018)*, pages 898–907, Cham, 2019. Springer International Publishing.

[64] R. Rutledge, S. Park, H. Khan, A. Orso, M. Prvulovic, and A. Zajic. Zero-overhead path prediction with progressive symbolic execution. In *2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)*, pages 234–245, 2019.

[65] N. Sehatbakhsh, A. Nazari, A. Zajic, and M. Prvulovic. Spectral profiling: Observer-effect-free profiling by monitoring em emanations. In *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 1–11, Oct 2016.

[66] N. Sehatbakhsh, A. Nazari, A. Zajic, and M. Prvulovic. Spectral profiling: Observer-effect-free profiling by monitoring em emanations. In *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 1–11, 2016.

[67] N. Sehatbakhsh, B. B. Yilmaz, A. Zajic, and M. Prvulovic. Emsim: A microarchitecture-level simulation tool for modeling electromagnetic side-channel signals. In *2020 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, pages 71–85, 2020.

[68] T. Syrový, R. Vik, S. Pretl, L. Syrová, J. Čengery, A. Hamáček, L. Kubáč, and L. Menšík. Fully printed disposable iot soil moisture sensors for precision agriculture. *Chemosensors*, 8(4), 2020.

[69] M. Taha and P. Schaumont. Key updating for leakage resiliency with application to aes modes of operation. *IEEE Transactions on Information Forensics and Security*, 10(3):519–528, March 2015.

[70] M. Taram, A. Venkat, and D. Tullsen. Mobilizing the micro-ops: Exploiting context sensitive decoding for security and energy efficiency. In *2018 ACM/IEEE 45th Annual International Symposium on Computer Architecture (ISCA)*, pages 624–637, June 2018.

[71] E. M. Ugurlu, B. B. Yilmaz, A. Zajic, and M. Prvulovic. Pitem: Permutations-based instruction tracking via electromagnetic side-channel signal analysis. *IEEE Transactions on Computers*, pages 1–1, 2021.

[72] W. van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers and Security*, 4(4):269 – 286, 1985.

[73] J. Wichelmann, A. Moghimi, T. Eisenbarth, and B. Sunar. Microwalk: A framework for finding side channels in binaries. In *Proceedings of the 34th Annual Computer Security Applications Conference*, ACSAC '18, pages 161–173, New York, NY, USA, 2018. ACM.

[74] S. J. E. Wilton and N. P. Jouppi. Cacti: an enhanced cache access and cycle time model. *IEEE Journal of Solid-State Circuits*, 31(5):677–688, May 1996.

[75] M. Wu, S. Guo, P. Schaumont, and C. Wang. Eliminating timing side-channel leaks using program repair. In *Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis*, ISSTA 2018, pages 15–26, New York, NY, USA, 2018. ACM.

[76] B. Yilmaz, A. Zajic, and M. Prvulovic. Modelling jitter in wireless channel created by processor-memory activity. In *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2018*, pages 2037–2041, 04 2018.

[77] B. B. Yilmaz, R. Callan, A. Zajic, and M. Prvulovic. Capacity of the em covert/side-channel created by the execution of instructions in a processor. *IEEE Transactions on Information Forensics and Security*, 13(3):605–620, 2018.

[78] B. B. Yilmaz, R. L. Callan, M. Prvulovic, and A. Zajić. Capacity of the em covert/side-channel created by the execution of instructions in a processor. *IEEE Transactions on Information Forensics and Security*, 13(3):605–620, 2017.

[79] B. B. Yilmaz, M. Prvulovic, and A. Zajic. Capacity of deliberate side channels created by software activities. In *Military Communications Conference (MILCOM), MILCOM 2018-2018 IEEE*. IEEE, 2018.

[80] B. B. Yilmaz, M. Prvulovic, and A. Zajic. Electromagnetic side channel information leakage created by execution of series of instructions in a computer processor. *IEEE Transactions on Information Forensics and Security*, 15:776–789, 2020.

[81] J. Yu, L. Hsiung, M. E. Hajj, and C. W. Fletcher. Data oblivious isa extensions for side channel-resistant and high performance computing. In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, NDSS '19, 2019. `https://eprint.iacr.org/2018/808`.

[82] A. Zajić and M. Prvulovic. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *IEEE Transactions on Electromagnetic Compatibility*, 56(4):885–893, Aug 2014.