Seer: A Lightweight Online Failure Prediction Approach

Burcu Ozcelik
Barcelona Supercomputing Center
08034 Barcelona, Spain
Email: burcu.mutlu@bsc.es

Cemal Yilmaz
Faculty of Engineering and Natural Sciences
Sabanci University
34956 Istanbul, Turkey
Email: cyilmaz@sabanciuniv.edu

***Abstract*—In [1], we present a lightweight online failure prediction approach, called *Seer*, to predict the manifestation of failures at runtime, i.e., while the system is running and before the failures occur, so that preventive and/or protective measures can proactively be taken to improve software reliability. One way Seer differs from the other related approaches is that it collects information from inside program executions, from which the existing approaches generally refrain themselves due to the typically excessive runtime overheads incurred. Seer overcomes this issue by pushing the substantial parts of the data collection task onto the hardware with the help of hardware performance counters (HPCs) – CPU resident counters that record various low level events occurring on a CPU, such as the number of instructions executed and the number of branches taken. At a very high level, Seer operates as follows: functions, called seer functions, that can reliably distinguish failing executions from passing executions are determined; these functions are then instrumented in such a way that after every invocation of a seer function, a binary prediction (i.e., passing or failing) about the future of the execution is made; the instrumented system is deployed and the sequence of predictions made by the seer functions are analyzed at runtime using fixed-length sliding windows to predict the manifestation of failures. We have evaluated Seer by conducting a series of experiments on three software systems in the presence of both single and multiple defects. At the lowest level of runtime overheads, Seer predicted the failures about 54% way through the executions (when the duration of an execution is measured as the number of function calls made in the execution) with an F-measure of 0.77 (computed by giving equal importance to precision and recall) and a runtime overhead of 1.98%, on average. At the highest level of prediction accuracies, Seer predicted the failures about 56% way through the executions with an F-measure of 0.88 and a runtime overhead of 2.67%, on average. Furthermore, Seer performed significantly better than the other online failure prediction approaches used in the empirical studies.**

One way we have been extending this line of work is by combining the low-level internal execution data collected by HPCs with the high-level external data, which is collected directly from outside executions, such as the number of processes and the CPU, memory, and network utilization, to further improve the quality of predictions. Another avenue we have been extensively investigating is using HPC-collected data in a related domain to detect the presence of ongoing side-channel attacks [2], [3], [4], [5] against software implementations of cryptographic applications at runtime. One type of attack we are currently interested in, is the cache-based attacks where a *spy* process discovers a secret key processed by a cryptographic application via creating intentional contentions in a cache memory with the victim [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]. One approach that we have had great success with, monitors the contentions in shared resources by using HPCs and issues warnings whenever the extent to which the victim process suffers from these contentions reaches a suspicious level.

Acknowledgments

This research was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme (FP7-PEOPLE-IRG-2008), and by the Scientific and Technological Research Council of Turkey (109E182).

References

[1] B. Ozcelik and C. Yilmaz, "Seer: A lightweight online failure prediction approach," *IEEE Transactions on Software Engineering*, vol. 42(1), pp. 26–46, Jan 2016. doi:10.1109/TSE.2015.2442577.

[2] A. C. Atici, C. Yilmaz, and E. Savas, "An approach for isolating the sources of information leakage exploited in cache-based side-channel attacks," in *Seventh International Conference on Software Security and Reliability, SERE 2012, Gaithersburg, Maryland, USA, 18-20 June 2013 - Companion Volume*, pp. 74–83, IEEE, 2013.

[3] M. Chiappetta, E. Savas, and C. Yilmaz, "Real time detection of cache-based side-channel attacks using hardware performance counters," *Applied Soft Computing*, vol. 49, pp. 1162 – 1174, 2016.

[4] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Proceedings of Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996* (N. Koblitz, ed.), vol. 1109 of *Lecture Notes in Computer Science*, pp. 104–113, Springer, 1996.

[5] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO* (M. J. Wiener, ed.), vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397, Springer, 1999.

0730-3157/17 $31.00 © 2017 IEEE
DOI 10.1109/COMPSAC.2017.210

[6] D. Page, "Theoretical use of cache memory as a cryptanalytic side-channel," *IACR Cryptology ePrint Archive*, vol. 2002, p. 169, 2002.

[7] Y. Tsunoo, T. Saito, T. Suzaki, M. Shigeri, and H. Miyauchi, "Cryptanalysis of DES implemented on computers with cache," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003* (C. D. Walter, Ç. K. Koç, and C. Paar, eds.), vol. 2779 of *Lecture Notes in Computer Science*, pp. 62–76, Springer, 2003.

[8] D. J. Bernstein, "Cache-timing attacks on AES," tech. rep., 2005.

[9] G. Bertoni, V. Zaccaria, L. Breveglieri, M. Monchiero, and G. Palermo, "AES power attack based on induced cache miss and countermeasure," in *International Symposium on Information Technology: Coding and Computing (ITCC 2005), Volume 1, 4-6 April 2005, Las Vegas, Nevada, USA*, pp. 586–591, IEEE Computer Society, 2005.

[10] O. Aciiçmez and Çetin Kaya Koç, "Trace-Driven Cache Attacks on AES (Short Paper)," in *ICICS* (P. Ning, S. Qing, and N. Li, eds.), vol. 4307 of *Lecture Notes in Computer Science*, pp. 112–121, Springer, 2006.

[11] M. Neve, J.-P. Seifert, and Z. Wang, "A refined look at Bernstein's AES side-channel analysis," in *ASIACCS* (F.-C. Lin, D.-T. Lee, B.-S. P. Lin, S. Shieh, and S. Jajodia, eds.), p. 369, ACM, 2006.

[12] J. Bonneau and I. Mironov, "Cache-collision timing attacks against AES," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006* (L. Goubin and M. Matsui, eds.), vol. 4249 of *Lecture Notes in Computer Science*, pp. 201–215, Springer, 2006.

[13] O. Aciiçmez, W. Schindler, and Çetin Kaya Koç, "Cache based remote timing attack on the AES," in *CT-RSA* (M. Abe, ed.), vol. 4377 of *Lecture Notes in Computer Science*, pp. 271–286, Springer, 2007.

[14] O. Aciiçmez, "Yet another microarchitectural attack: Exploiting i-cache," *IACR Cryptology ePrint Archive*, vol. 2007, p. 164, 2007.

[15] O. Aciiçmez and W. Schindler, "A vulnerability in RSA implementations due to instruction cache analysis and its demonstration on openssl," in *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008. Proceedings* (T. Malkin, ed.), vol. 4964 of *Lecture Notes in Computer Science*, pp. 256–273, Springer, 2008.

[16] O. Aciiçmez, B. B. Brumley, and P. Grabher, "New results on instruction cache attacks," in *CHES* (S. Mangard and F.-X. Standaert, eds.), vol. 6225 of *Lecture Notes in Computer Science*, pp. 110–124, Springer, 2010.

[17] E. Tromer, D. A. Osvik, and A. Shamir, "Efficient cache attacks on aes, and countermeasures," *J. Cryptology*, vol. 23, no. 1, pp. 37–71, 2010.

[18] Y. Yarom and K. Falkner, "FLUSH+RELOAD: A high resolution, low noise, L3 cache side-channel attack," in *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*. (K. Fu and J. Jung, eds.), pp. 719–732, USENIX Association, 2014.

[19] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side channel cryptanalysis of product ciphers," in *Proceedings of Computer Security - ESORICS 98, 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, September 16-18, 1998* (J. Quisquater, Y. Deswarte, C. A. Meadows, and D. Gollmann, eds.), vol. 1485 of *Lecture Notes in Computer Science*, pp. 97–110, Springer, 1998.

[20] G. I. Apecechea, M. S. Inci, T. Eisenbarth, and B. Sunar, "Wait a minute! A fast, cross-vm attack on AES," in *Proceedings of Research in Attacks, Intrusions and Defenses - 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014*. (A. Stavrou, H. Bos, and G. Portokalidis, eds.), vol. 8688 of *Lecture Notes in Computer Science*, pp. 299–319, Springer, 2014.

[21] Y. Yarom and N. Benger, "Recovering openssl ECDSA nonces using the FLUSH+RELOAD cache side-channel attack," *IACR Cryptology ePrint Archive*, vol. 2014, p. 140, 2014.