ECE511 - Assignment 01

Stewart Schuler

September 27, 2024

1 Assignment 1

Task 1.1

The following list of papers were pulled from *IEEE Xplore*

[1] F. Behnia et al., "Code-Bridged Classifier (CBC): A Low or Negative Overhead Defense for Making a CNN Classifier Robust Against Adversarial Attacks," 2020 21st International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 2020, pp. 27-32, doi: 10.1109/ISQED48828.2020.9136987.

[2] N. Nazari et al., "SpecScope: Automating Discovery of Exploitable Spectre Gadgets on Black-Box Microarchitectures," 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE), Valencia, Spain, 2024, pp. 1-6, doi: 10.23919/DATE58400.2024.10546869.

[3] H. M. Makrani et al., "Cloak & Co-locate: Adversarial Railroading of Resource Sharing-based Attacks on the Cloud," 2021 International Symposium on Secure and Private Execution Environment Design (SEED), Washington, DC, USA, 2021, pp. 1-13, doi: 10.1109/SEED51797.2021.00011.

Task 1.2

This following paper was pulled from *ACM Digital Library*. Combined with the papers from *IEEE Explore*, the three authors, *Khasawneh*, *Homayoun*, and *Sasan* collaborated on four different papers.

[4] Neha Nagarkar, Khaled Khasawneh, Setareh Rafatirad, Avesta Sasan, Houman Homayoun, and Sai Manoj Pudukotai Dinakarrao. 2021. Energy-Efficient and Adversarially Robust Machine Learning with Selective Dynamic Band Filtering. In Proceedings of the 2021 Great Lakes Symposium on VLSI (GLSVLSI '21). Association for Computing Machinery, New York, NY, USA, 195–200. https://doi.org/10.1145/3453688.3461756

Task 2

It would appear the *MSAR* ranking is either depreciated or no longer support as Microsoft Academic redirects to the microsoft home page. Instead the limited *MSAR* rankings were pulled from the conference ranks website. Since many of the papers we presented at the same conference, I ranked the conferences rather than duplicating the ranking for each paper.

Symposium	ERA	Qualis	MSAR
S&P	A	A1	N/A
NDSS	A	A1	N/A
MICRO	N/A	A1	87
RAID	B	A2	N/A
ISQED	N/A	B1	N/A
GLSVLSI	N/A	B1	25
HOST	N/A	B3	N/A

Task 3

Paper	Year	Citations
Ensemble Learning for Low-level Hardware-supported Malware Detection	2015	125
Constructing and Characterizing Covert Channels on GPGPUs	2017	74
RHMD: Evasion-Resilient Hardware Malware Detectors	2017	81
LATCH: Locality Aware Taint CHecker	2019	8
SPECCFI: Mitigating Spectre Attacks using CFI informed Speculation	2020	95
Code-Bridged Classifier (CBC): A Low or Negative Overhead Defense for Making a CNN Classifier Robust Against Adversarial Attacks	2020	21
A Review of In-Memory Computing Architecture for Machine Learning Applications	2020	64
Evolution of Defenses against Transient-Execution Attacks	2020	34
The Evolution of Transient-Execution Attacks	2020	26
MonotonicHMDs: Exploiting Monotonic Features to Defend Against Evasive Malware	2021	9
Cloak & Co-locate: Adversarial Railroading of Resource Sharing-based Attacks on the Cloud	2021	27
Energy-Efficient and Adversarially Robust Machine Learning with Selective Dynamic Band Filtering	2021	1
REPTTACK: Exploiting Cloud Schedulers to Guide Co-Location Attacks	2022	15
HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity	2023	4
Vpp: Privacy Preserving Machine Learning via Undervolting	2023	5
A Brain-inspired Approach for Malware Detection using Sub-semantic Hardware Features	2023	4
Hardware Support for Trustworthy Machine Learning: A Survey	2024	0

Task 4

Task 4.1

10 influential papers.

360 Citations
[1] Wang, Zhenghong, and Ruby B. Lee. "A novel cache architecture with enhanced performance and security." 2008 41st IEEE/ACM International Symposium on Microarchitecture. IEEE, 2008.

324 Citations
[2] Liu, Fangfei, and Ruby B. Lee. "Random fill cache architecture." 2014 47th Annual IEEE/ACM International Symposium on Microarchitecture. IEEE, 2014.

427 Citations
[3] Zhang, Chuanjun, Frank Vahid, and Walid Najjar. "A highly configurable cache architecture for embedded systems." Proceedings of the 30th annual international symposium on Computer architecture. 2003.

343 Citations
[4] Malik, Afzal, Bill Moyer, and Dan Cermak. "A low power unified cache architecture providing power and performance flexibility." Proceedings of the 2000 international symposium on Low power electronics and design. 2000.

538 Citations
[5] Sun, Guangyu, et al. "A novel architecture of the 3D stacked MRAM L2 cache for CMPs." 2009 IEEE 15th International Symposium on High Performance Computer Architecture. IEEE, 2009.

442 Citations
[6] Hagersten, Erik, Anders Landin, and Seif Haridi. "DDM-a cache-only memory architecture." Computer 25.9 (1992): 44-54.

226 Citations
[7] Agarwal, Amit, et al. "A process-tolerant cache architecture for improved yield in nanoscale technologies." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 13.1 (2005): 27-38.

325 Citations
[8] Rodriguez, Pablo, Christian Spanner, and Ernst W. Biersack. "Analysis of web caching architectures: Hierarchical and distributed caching." IEEE/ACM Transactions On Networking 9.4 (2001): 404-418.

283 Citations

[9] Mancuso, Renato, et al. "Real-time cache management framework for multi-core architectures." 2013 IEEE 19th Real-Time and Embedded Technology and Applications Symposium (RTAS). IEEE, 2013.

800 Citations
[10] Kim, Seongbeom, Dhruba Chandra, and Yan Solihin. "Fair cache sharing and partitioning in a chip multiprocessor architecture." Proceedings. 13th International Conference on Parallel Architecture and Compilation Techniques, 2004. PACT 2004.. IEEE, 2004.

Task 4.2

Influential authors in the field of *Cache Architecture*.

Author	Citations	H-index	i10-index	Publications
Anoop Gupta	54069	109	391	1382
Yuan Xie	43567	103	557	944
Yuan Xie	43567	103	557	944
Yiran Chen	32262	89	405	783
Lixin Zhang	23836	71	322	566
Ruby B. Lee	17583	64	195	410