M. Caner Tol

[janner tol]

Phone: +1 774 253 5691
Email: mtol@wpi.edu
Website: canertol.com
LinkedIn: canertol

Education

Worcester Polytechnic Institute — Worcester, MA
Ph.D. in Electrical and Computer Engineering — 2019–**December 2024**
Advisor: Prof. Berk Sunar

M.S. in Electrical and Computer Engineering — 2019–2022

Middle East Technical University — Ankara, TR
B.S. in Electrical and Electronics Engineering — 2014–2019

Professional Experience

Hardware Security Intern — Remote - Santa Clara, CA
NVIDIA — May 2022 - Aug 2022, **May 2024**

- Developed a ML-based tool for automatic detection of side-channel leakage on CUDA libraries using GPU hardware performance counters.

Research and Teaching Assistant — Worcester, MA
Vernam Lab, Worcester Polytechnic Institute — 2019 - Current

- Research on Microarchitectural side-channel, fault injection attacks, and the applications of Transformer models, generative AI, and reinforcement learning on discovery, detection, and mitigation of these attacks.

Part Time Security Engineer — Ankara, TR
Network Security Team, Aselsan — Nov 2018 - Mar 2019

- Assisted on network security management, malware detection using YARA rules in the Network Security Team of Aselsan (Military Electronic Industries) which is the top company in the defense industry in Turkey.

Student Computer Assistant — Ankara, TR
Middle East Technical University — Sep 2016 - Nov 2018

- Operated local IT office in the Faculty of Economics and Administrative Sciences.

Engineering Intern — Istanbul, TR
Voltage Performance and Standby Lab, Arçelik A.Ş. — Jul 2017 - Sep 2017

- Developed a MATLAB GUI to automate voltage performance test procedure using image processing.

Skills

Programming:	C/C++, ARM/x86 Assembly, Python, CUDA, Bash
Tools:	Intel Pin, Ghidra, LaTeX, Git
Libraries:	PyTorch, TensorFlow, Keras

Languages

English:	Fluent
Turkish:	Native speaker
Italian:	Elementary

Research

M. C. Tol, K. Derya, and B. Sunar, "Reinforcement Learning-based Discovery of Microarchitectural Vulnerabilities", *[Ongoing Work].*

K. Derya, **M. C. Tol**, and B. Sunar, "Fault+Probe: A Generic Rowhammer-based Bit Recovery Attack", 2024 *[Under Review].*

A. J. Adiletta, **M. C. Tol**, and B. Sunar, "LeapFrog: The Rowhammer Instruction Skip Attack", *hardwear.io USA, Santa Clara, CA, 2024.*

M. C. Tol, and B. Sunar, "ZeroLeak: Automated Side-Channel Patching in Source Code Using LLMs", *Real World Crypto, Toronto, Canada, 2024.*

A. J. Adiletta*, **M. C. Tol***, Y. Doroz, and B. Sunar, "Mayhem: Targeted Corruption of Register and Stack Variables", in *Proceedings of the 2024 ACM Asia CCS, Singapore, 2024.* 3rd place in poster competition @NEHWS23.

M. C. Tol, S. Islam, A. J. Adiletta, B. Sunar, and Z. Zhang, "Don't Knock! Rowhammer at the Backdoor of DNN Models", in *Proceedings of the 2023 IEEE/IFIP International Conference on Dependable Systems and Network, Porto, Portugal, 2023.* 1st place in poster competition @NEHWS22.

K. Mus, Y. Doroz, **M. C. Tol**, K. Rahman, and B. Sunar, "Jolt: Recovering TLS Signing Keys via Faults", in *Proceedings of the 2023 IEEE Symposium on Security and Privacy, San Francisco, CA, 2023.*

M. C. Tol, B. Gulmezoglu, K. Yurtseven, and B. Sunar, "FastSpec: Scalable Generation and Detection of Spectre Gadgets Using Neural Embeddings", in *Proceedings of the 2021 IEEE European Symposium on Security and Privacy, Vienna, Austria, 2021.*

L. Amorós, S. M. Hafiz, K. Lee, and **M. C. Tol**, "Gimme That Model!: A Trusted ML Model Trading Protocol", *Protecting Privacy through Homomorphic Encryption, 2021.*

B. Gulmezoglu, A. Zankl, **M. C. Tol**, S. Islam, T. Eisenbarth, and B. Sunar, "Undermining User Privacy on Mobile Devices Using AI", in *Proceedings of the 2019 ACM Asia CCS, Auckland, New Zealand, 2019.*

Services

Artifact Evaluation Committee Member **ACM CCS**	May 2024
Reviewer at **IEEE Transactions on Information Forensics and Security**	December 2024
Reviewer at **IEEE Transactions on Emerging Topics in Computing**	October 2023
Reviewer at **The Computer Journal, Oxford University Press**	May 2023

ACHIEVEMENTS

Student Travel Grant — Jun 2021, May 2023
IEEE Symposium on Security and Privacy

Best Poster Award — Apr 2022
New England Hardware Security Day

Microsoft Private AI Bootcamp — Dec 2019
Microsoft Research, Privacy Preserving Machine Learning

IoT Application Award — Jun 2019
The Senior Engineering Design Course Committee, METU EE

Honor Student — Jun 2019
Middle East Technical University

569th place in 1.9 Million in General University Exam — Jun 2013
Council of Higher Education, Republic of Turkey