Mahmood Sharif

Senior Lecturer

Tel Aviv University

mahmoods@tauex.tau.ac.il | https://mahmoods01.github.io/

Education

Carnegie Mellon University

Ph.D. in Electrical and Computer Engineering — *Sep/2014 - Nov/2019*

- Dissertation: "Practical Inference-Time Attacks Against Machine-Learning Systems and a Defense Against Them."
- Committee: Lujo Bauer (co-chair), Nicolas Christin (co-chair), Matt Fredrikson, and Michael K. Reiter.

University of Haifa

M.Sc. in Computer Science — *Oct/2010 - Nov/2013*

- Graduated *summa cum laude*.
- Dissertation: "Privacy Preserving Key Generation and Authentication from Face Images."
- Committee: Margarita Osadchy (chair), Orr Dunkelman, and Moni Naor.

University of Haifa

B.Sc. in Computer Science — *Feb/2007 - Sep/2010*

- Via the "Etgar" program, a prestigious program for high-school students, offering a university degree one year after graduating from high-school. Headed by Gad Landau.

Professional Experience

2021-pres.	**Senior Lecturer**, School of Computer Science, Tel Aviv University.
2020-pres.	**Adjunct Faculty Member**, Software and Societal Systems Department (S3D), Carnegie Mellon University.
2020-2021	**Postdoctoral Researcher**, VMware Research Group.
2020-2021	**Visiting Lecturer**, School of Computer Science, Tel Aviv University.
2020-2021	**Adjunct Research Fellow**, CyLab Security and Privacy Institute, Carnegie Mellon University.
2019-2020	**Principal Research Engineer**, NortonLifeLock Research Group (previously Symantec Research Labs).
2018	**Research Intern**, Symantec Research Labs.

Honors and Awards

2023	**Intel Rising Star Award for Early-Career Faculty Members**, Intel
2021	**Israeli Council for Higher Education's (CHE) Maof prize for excellent young faculty**, CHE
2018	**CyLab Presidential Fellowship at Carnegie Mellon University**, Carnegie Mellon University
2018	**Student travel grant to join CVPRW**, CVPR
2018	**Symantec Research Labs Fellowship**, Symantec
2018	**Student travel grant to join NDSS**, NDSS
2017	**Student travel grant to join the C3E Workshop**, C3E
2017	**Selected to join the French-American Doctoral Exchange program**, French Embassy
2017	**Finalist of the Qualcomm Innovation Fellowship**, Qualcomm
2017	**Finalist of Symantec Research Labs Fellowship**, Symantec
2016	**CyLab Presidential Fellowship at Carnegie Mellon University**, Carnegie Mellon University
2016	**Student travel grant to join ACM CCS**, CCS
2014	**Carnegie Institute of Technology Dean's Tuition Fellowship**, Carnegie Mellon University
2014	**Recipient of the Uri N. Peled memorial prize**, University of Haifa
2013	**First place in Startup Weekend**, Startup Weekend, Haifa
2011	**Recipient of the Akavia scholarship**, University of Haifa
2011	**Recipient of the Graduate Studies Authority's scholarship**, Graduate Studies Authority

Publications

Refereed Conference Publications

Y. Sawaya, S. Lu, T. Isohara, **M. Sharif**. "A High Coverage Cybersecurity Scale Predictive of User Behavior." USENIX Security Symposium. 2024. Acceptance rate: TBA. To appear.

W. Lin, K. Lucas, N. Eyal, L. Bauer, M. K. Reiter, **M. Sharif**. "Group-based Robustness: A General Framework for Customized Robustness in the Real World." Network and Distributed System Security Symposium (NDSS). 2024. Acceptance rate: TBA. To appear.

A. Cohen, **M. Sharif**. "Accessorize in the Dark: A Security Analysis of Near-Infrared Face Recognition." European Symposium on Research in Computer Security (ESORICS). 2023. Acceptance rate: 18.5%.

K. Lucas, W. Lin, S. Pai, L. Bauer, M. K. Reiter, **M. Sharif**. "Adversarial Training for Raw-Binary Malware Classifier." USENIX Security Symposium. 2023. Acceptance rate: 29.2%

H. Wu, C. Barrett, **M. Sharif**, N. Narodytska, G. Singh. "Scalable Verification of GNN-based Job Schedulers." International Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA). 2022. Acceptance rate: 31%. Also appeared at Workshop on Formal Methods for ML-Enabled Autonomous Systems (FoMLAS). 2022.

D. Kats, **M. Sharif**. "I Have No Idea What a Social Bot Is: On Users' Perceptions of Social Bots and Ability to Detect Them." International Conference on Human-Agent Interaction (HAI). 2022. Acceptance rate: 39%.

W. Lin, K. Lucas, L. Bauer, M. K. Reiter, **M. Sharif**. "Constrained Gradient Descent: Building Strong Adversarial Attacks Against Neural Networks." International Conference on Machine Learning (ICML). 2022. Acceptance rate: 22%.

K. Lucas, **M. Sharif**, L. Bauer, M. K. Reiter, S. Shintre. "Malware Makeover: Breaking ML-based Static Analysis by Modifying Executable Bytes." Asia Conference on Computer and Communications Security (AsiaCCS). 2021. Acceptance rate: 19%.

C. Cobb, M. Surbatovich, A. Kawakami, **M. Sharif**, L. Bauer, A. Das, L. Jia. "How Risky Are Real Users' IFTTT Applets?" Symposium on Usable Privacy and Security (SOUPS). 2020. Acceptance rate: 20%.

M. Sharif, K. A. Roundy, M. Dell'Amico, C. Gates, D. Kats, L. Bauer, N. Christin. "A Field Study of Computer-Security Perceptions Using Anti-Virus Customer-Support Chats." CHI Conference on Human Factors in Computing Systems (CHI). 2019. Acceptance rate: 24%.

M. Sharif, J. Urakawa, N. Christin, A. Kubota, A. Yamada. "Predicting Impending Exposure to Malicious Content from User Behavior." Conference on Computer and Communications Security (CCS). 2018. Acceptance rate: 17%.

W. Melicher, A. Das, **M. Sharif**, L. Bauer, L. Jia. "Riding out DOMsday: Toward Detecting and Preventing DOM Cross-Site Scripting." Network and Distributed System Security Symposium (NDSS). 2018. Acceptance rate: 22%.

Y. Sawaya, **M. Sharif**, N. Christin, A. Kubota, A. Nakarai, A. Yamada. "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior." CHI Conference on Human Factors in Computing Systems (CHI). 2017. Acceptance rate: 25%. Equal contribution by the first two authors.

Z. Weinberg, **M. Sharif**, J. Szurdi, N. Christin. "Topics of Controversy: An Empirical Analysis of Web Censorship Lists." Privacy Enhancing Technologies (PETS). 2017. Acceptance rate: 23%.

M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter. "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition." Conference on Computer and Communications Security (CCS). 2016. Acceptance rate: 17%.

W. Melicher, **M. Sharif**, J. Tan, L. Bauer, M. Christodorescu, P. G. Leon. "Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking." Privacy Enhancing Technologies (PETS). 2016. Acceptance rate: 24%.

Refereed Journal Publications

M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter. "A General Framework for Adversarial Examples with Objectives." ACM Transactions on Security and Privacy (TOPS). 2019. Impact factor: 3.0.

Refereed Workshop Publications

A. Chakravarthy, N. Narodytska, A. Rathis, M. Vilcu, **M. Sharif**, G. Singh. "Property-Driven Evaluation of RL-Controllers in Self-Driving Datacenters." Workshop on Challenges in Deploying and monitoring Machine Learning Systems (DMML@NeurIPS). 2022.

M. Davies, D. Marino, A. Nash, K. A. Roundy, **M. Sharif**, A. Tamersoy. "Training Older Adults to Resist Scams with Fraud Bingo and Scam-Detection Challenges." CHI Workshop on Designing Interactions for the Ageing Populations (CHI EA). 2020.

J. Tan, M. Sharif, S. Bhagavatula, M. Beckerle, L. Bauer, M. Mazurek. "Comparing Hypothetical and Realistic Privacy Valuations." Workshop on Privacy in the Electronic Society (WPES). 2018. Acceptance rate: 29%.

M. Sharif, L. Bauer, M. K. Reiter. "On the Suitability of L_p-norms for Creating and Preventing Adversarial Examples." Computer Vision and Patter Recognition Workshop (CVPRW). 2018.

Books and Book Chapters

K. Lucas, M. Sharif, L. Bauer, M. K. Reiter, S. Shintre. "Deceiving ML-Based Friend-or-Foe Identification for Executables." Cyber Deception: Techniques, Strategies, and Human Aspects (217-249). 2022.

Pre-prints

M. Sharif, L. Bauer, M. K. Reiter. "n-ML: Mitigating Adversarial Examples via Ensembles of Topologically Manipulated Classifiers." arXiv:1912.09059, 2019.

Posters

Y. Sawaya, T. Isohara, **M. Sharif**. "Toward Accurate Prediction of Security Behavior via Comprehensive Scales." Symposium on Usable Privacy and Security (SOUPS). 2022.

Y. Sawaya, **M. Sharif**, N. Christin, A. Kubota, A. Nakarai, A. Yamada. "Toward a Security Behavior Scale Robust to Linguistic Differences." Symposium on Usable Privacy and Security (SOUPS). 2016.

O. Dunkelman, M. Osadchy, **M. Sharif**. "Secure Authentication from Facial Attributes with No Privacy Loss." Conference on Computer and Communications Security (CCS). 2013.

Patents

Approved

M. Sharif, V. Ganti. "Distributed Representations of Computing Processes and Events." US Patent 17375702. 2023.

Y. Ben-Itzhak, S. Vargaftik, N. Narodytska, **M. Sharif**. "Efficient Federated Learning of Deep Neural Networks (DNNs) Using Approximation Layers." US Patent 17492457. 2023.

M. Sharif, S. Bhatkar, K. A. Roundy, S. Shintre. "Systems and Methods for Training Malware Classifiers." US Patent 11210397. 2021.

K. A. Roundy, **M. Sharif**, M. Dell'Amico, C. Gates, D. Kats, D. Chung. "Discovery of Computer System Incidents to Be Remediated Based on Correlation Between Support Interaction Data and Computer System Telemetry Data." US Patent 11163875. 2021.

K. A. Roundy, **M. Sharif**, A. Tamersoy. "Systems and Methods for Real-Time Scam Protection on Phones." US Patent 10455085. 2019.

Pending

M. Sharif, P. Kotzias, K. A. Roundy. "A Recommender System to Protect Users from Potentially Unwanted Programs." 2020.

Teaching and Instructing Experience

S24	**Software Project**, Instructor	*TAU*
S24, S23, S22	**Trustworthy Machine Learning**, Instructor	*TAU*
F23, S23, S22	**Workshop on Usable Security and Privacy**, Instructor	*TAU*
S17	**Network Security**, Teaching Assistant	*CMU*
S16	**Secure Software Systems**, Teaching Assistant	*CMU*
F15	**Introduction to Information Security**, Teaching Assistant	*CMU*
F14, F11	**Introduction to Computer Science**, Teaching Assistant	*UHaifa*
F12, S12, F11	**Introduction to Computer Science**, Lab Instructor	*UHaifa*

Mentoring

Current Students

2023	**Ido Abelman**, B.Sc., SCS	*TAU*
2023	**Matan Ben-Tov**, M.Sc., SCS	*TAU*
2023	**Sagi Polaczek**, B.Sc., SCS (Joint with Eyal Ronen)	*TAU*
2023	**Zebin Yun**, M.Sc., SCS (Joint with Eyal Ronen)	*TAU*
2022	**Nadav Gat**, M.Sc., SCS	*TAU*
2022	**Tsufit Ronen**, M.Sc., SCS	*TAU*
2022	**Ben Shapira**, M.Sc., SCS	*TAU*
2021	**Achi-Or Weingarten**, M.Sc., SCS (Joint with Eyal Ronen)	*WIS*

Past Students

2023	**Amit Cohen**, M.Sc., SCS	*TAU*
2023	**Alon Leshem**, Undergraduate summer intern from UPitt	*TAU*
2023	**Jiahao Yu**, Undergraduate summer intern from Bristol University	*TAU*
2022	**Sarah Lu**, Undergraduate summer intern from MIT	*TAU*
2022	**Zebin Yun**, Undergraduate summer intern from SUSTech	*TAU*
2021	**Nimrod de la Vega**, B.Sc., SCS (Joint with Eyal Ronen)	*TAU*

Theses Committees

2023	**Ofir Bar Tal**, M.Sc., SCS	*TAU*
2023	**Adi Kaufman**, M.Sc., SCS	*TAU*
2022	**Aviv Engelberg**, M.Eng., EE	*TAU*
2022	**Maor Ivgi**, Ph.D., SCS	*TAU*
2022	**Elad Segal**, M.Sc., SCS	*TAU*
2022	**Uri Shaham**, Ph.D., SCS	*TAU*

Past Mentoring

2019	**Max Wolff**, High school student (Paper accepted at ICLR TML workshop, 2020)	*CMU*
2019	**Anna Kawakami**, Participant in the REUSE program, ISR	*CMU*
2018	**Jihye Choi**, M.Sc., ECE	*CMU*
2017	**Siyao Meng**, M.Sc., INI	*CMU*
2017	**Alessio Buraggina**, Participant in the REUSE program, ISR	*CMU*
2017	**Andrew Zhang**, Participant in the REUSE program, ISR	*CMU*
2016	**Truth Iyiewuare**, Participant in the REUSE program, ISR	*CMU*
2011	**Said Agha**, B.Sc., SCS	*UHaifa*

Service

Conference and Workshop Program Committees

2024	**IEEE Symposium on Security and Privacy (S&P)**
2024	**IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)**
2023, 2022	**USENIX Security Symposium**
2023-2021	**Privacy Enhancing Technologies Symposium (PETS)**
2022	**International Conference on Machine Learning (ICML)**
2022	**Financial Cryptography and Data Security (FC)**
2020	**Workshop on Towards Trustworthy ML (co-located with ICLR)**
2019	**Workshop on Cyber Security Experimentation and Test (co-located with USENIX Security)**
2019, 2018	**European Workshop on Usable Security (co-located with IEEE EuroS&P)**
2019, 2018	**Workshop on NLP for Internet Freedom (co-located with COLING)**
2018	**Workshop on Privacy in the Electronic Society (co-located with CCS)**
2018	**IEEE Symposium on Security and Privacy (S&P) Student PC**

Invited External Reviewing

2024	**ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS)**
2023	**Conference on Neural Information Processing Systems (NeurIPS)**
2023, 2022	**IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI)**
2022	**AAAS Science Advances**
2021	**ACM CHI Conference on Human Factors in Computing Systems (CHI)**
2021-2018	**ACM Transactions on Privacy and Security (TOPS)**
2021, 2019-2016	**IEEE Symposium on Security and Privacy (S&P)**
2020, 2019, 2016, 2015	**Privacy Enhancing Technologies (PETS)**
2020, 2019	**IEEE Transactions on Dependable and Secure Computing (TDSC)**
2020, 2018, 2017	**USENIX Security Symposium**
2019, 2017, 2016	**ACM Conference on Communication and Computer Security (CCS)**
2019	**IEEE European Symposium on Security and Privacy (EuroS&P)**
2019-2016	**Network and Distributed System Security Symposium (NDSS)**
2018	**ACM CHI Conference on Human Factors in Computing Systems (CHI) Late-Breaking Track**
2018	**International World Wide Web Conference (WWW)**
2018	**Symposium on Usable Privacy and Security (SOUPS)**
2015	**International Journal on Machine Vision and Applications (MVAP)**
2014, 2013	**IEEE Conference on Computer Vision and Pattern Recognition (CVPR)**

Talks

"Assessing and Enhancing ML Systems' Adversarial Robustness in the Real World." Machine-Learning Seminar. Weizmann Institute of Science. June/2023.

"On Machine-Learning Integrity and Threats to Autonomous Transportation." The Shmeltzer Institute for Smart Transportation. Tel Aviv University. Apr/2023.

"Assessing Biometric Systems in Adversarial Settings: Limitations and Opportunities." The Center for Cyber Law & Policy. University of Haifa. Mar/2023.

Invited panelist to "Cybersecurity Education in Israel." Federmann Cyber Security Research Center. Hebrew University of Jerusalem. Jun/2022.

"Toward Robust Malware Detection and Faithfully Evaluating the Robustness of Neural Networks." Learning Club Seminar. Bar-Ilan University. Jun/2022.

"Introduction to Adversarial Machine Learning." Cloud InnovWave Overseas Workshop. Huawei. Jun/2022.

"Introduction to Adversarial Machine Learning." Security Business Unit's Seminar. VMware. Jun/2022.

Invited panelist in "Annual Privacy Workshop." Faculty of Law. Tel Aviv University. May/2022.

"Physical-World Attacks on Biometric Systems." Joint Biometric Seminar Series. Michigan State University and University of Haifa. Apr/2022.

"Physical-World Attacks on Machine Learning." Principles and Tools for Computer Security. Guest lecture. Technion. Jan/2021.

"The Security of Machine Learning in the Real World." Deep Learning Seminar. Interdisciplinary Center Herzliya. Sep/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." Computer Science Department. University of Haifa. Jul/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." School of Computer Science and Engineering. Hebrew University of Jerusalem. Jul/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." Faculty of Electrical Engineering. Technion. Jul/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." School of Computer Science. Tel Aviv University. Jul/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." VMware Research Group. Herzliya and Palo Alto. Jul/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." Department of Industrial Engineering. Tel Aviv University. Jul/2020.

"The Security of Machine Learning in the Real World and Machine Learning for Personalized Security." Computer Science Department. Bar-Ilan University. Jun/2020.

"Physical-World Attacks on Machine Learning." Security and Fairness of Deep Learning. Guest lecture. Carnegie Mellon University. Apr/2020.

"Comparing Hypothetical and Realistic Privacy Valuations." Federal Trade Commission's PrivacyCon. Washington DC. Jun/2019.

"A Field Study of Computer-Security Perceptions Using Anti-Virus Customer-Support Chats." CHI Conference on Human Factors in Computing Systems. Glasgow. May/2019.

"Physical-World Attacks on Machine Learning." Security and Fairness of Deep Learning. Guest lecture. Carnegie Mellon University. Apr/2019.

"Physical-World Attacks on Machine Learning." Ethics and Policy Issues in Computing. Guest lecture. Carnegie Mellon University. Feb/2019.

"Physical-World Attacks on Machine Learning." Privacy, Policy, Law, and Technology. Guest lecture. Carnegie Mellon University. Nov/2018.

"Predicting Impending Exposure to Malicious Content from User Behavior." Conference on Computer and Communications Security (CCS). Toronto. Oct/2018.

Invited panelist in "The Hugh Thompson Show: Artificial Intelligence APJ Style." RSA Asia Pacific & Japan. Singapore. Jul/2018.

"On the Suitability of L_p-norms for Creating and Preventing Adversarial Examples." Computer Vision and Pattern Recognition Workshop (CVPRW). Salt Lake City. Jun/2018.

"Predicting Impending Exposure to Malicious Content from User Behavior." CyLab Partners Conference. Carnegie Mellon University. Oct/2018.

"Physical-World Attacks on Machine Learning." Symantec Research Labs. Symantec. Mountain View. May/2018.

"Predicting Impending Exposure to Malicious Content from User Behavior." Network Security. Guest lecture. Carnegie Mellon University. Apr/2018.

"Physical-World Attacks on Machine Learning." Introduction to Information Security. Guest lecture. Carnegie Mellon University. Nov/2017.

"Physical-World Attacks on Machine Learning." Privacy, Policy, Law, and Technology. Guest lecture. Carnegie Mellon University. Nov/2017.

"Physical-World Attacks on Machine Learning." CyLab Partners Conference. Carnegie Mellon University. Oct/2017.

"Physical-World Attacks on Machine Learning." The French-American Doctoral Exchange (FADEx) Program. French Institute for Research in Computer Science and Automation (INRIA). Jun/2017.

"Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior." CHI Conference on Human Factors in Computing Systems. Denver. May/2017.

"Special Topic: Adversarial Machine Learning." Network Security. Guest lecture. Carnegie Mellon University. Apr/2017.

"(Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking." Federal Trade Commission's PrivacyCon. Washington DC. Jan/2017.

"Privacy in the Age of Face and Speech Recognition." Privacy, Policy, Law, and Technology. Guest lecture. Carnegie Mellon University. Dec/2016.