Mahmood Sharif Ph.D.

Education

Sep/2014 – Nov/2019
Ph.D. in Electrical and Computer Engineering, Carnegie Mellon University.
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.

Oct/2010 – Nov/2013
M.Sc. in Computer Science, *summa cum laude*, University of Haifa.
Dissertation: "Privacy Preserving Key Generation and Authentication from Face Images."
Committee: Margarita Osadchy (chair), Orr Dunkelman, and Moni Naor.

Feb/2007 – Sep/2010
B.Sc. in Computer Science, University of Haifa.
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

Oct/2021 – present
Senior Lecturer at School of Computer Science, Tel Aviv University.

Jul/2020 – present
Adjunct Faculty Member at Institute of Software Research, Carnegie Mellon University.

Sep/2020 – Sep/2021
Postdoctoral Researcher at VMware Research Group.

Sep/2020 – Sep/2021
Visiting Lecturer at School of Computer Science, Tel Aviv University.

Jul/2020 – Jun/2021
Adjunct Research Fellow at CyLab Security and Privacy Institute, Carnegie Mellon University.

Nov/2019 – Aug/2020
Principal Research Engineer at NortonLifeLock Research Group (previously Symantec Research Labs).

May/2018 – Aug/2018
Research Intern at Symantec Research Labs.

Honors and Awards

- Israeli Council for Higher Education's Maof prize for excellent young faculty, May/2021.
- CyLab Presidential Fellowship at Carnegie Mellon University, 2018/19.
- Student travel grant to join CVPRW, Jun/2018.
- Symantec Research Labs Fellowship, 2018/19.
- Student travel grant to join NDSS, Feb/2018.
- Student travel grant to join the C3E Workshop, Oct/2017.
- Funding to join the French-American Doctoral Exchange (FADEx) program, Jun/2017.

- Finalist, Qualcomm Innovation Fellowship, 2017/18.
- Finalist, Symantec Research Labs Fellowship, 2017/18.
- CyLab Presidential Fellowship at Carnegie Mellon University, 2016/17.
- Student travel grant to join ACM CCS, Oct/2016.
- Carnegie Institute of Technology Dean's Tuition Fellowship, Sep/2014.
- Recipient of the Uri N. Peled memorial prize, Jun/2014.
- First place in Startup Weekend, Haifa, Mar/2013.
- Recipient of the Akavia scholarship, 2011/12.
- Recipient of the Graduate Studies Authority's scholarship, 2011/12.

Refereed Conference Publications

1. 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%.
2. 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%.
3. 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%.
4. 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%.
5. 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%.
6. 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.*
7. 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%.
8. M. Sharif, S. Bhagavatula, L. Bauer, M. 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%.
9. 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 Articles

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

Refereed Workshop Publications

1. 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.

2. 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%.
3. M. Sharif, L. Bauer, M. Reiter. "On the Suitability of L_p-norms for Creating and Preventing Adversarial Examples." Computer Vision and Patter Recognition Workshop (CVPRW), 2018.

Preprints and Working Papers

1. W. Lin, K. Lucas, L. Bauer, M. K. Reiter, M. Sharif. "Constrained Gradient Descent: Building Strong Adversarial Attacks Against Neural Networks." arXiv:2112.14232, 2021.
2. M. Sharif, L. Bauer, M. K. Reiter. "n-ML: Mitigating Adversarial Examples via Ensembles of Topologically Manipulated Classifiers." arXiv:1912.09059, 2019.

Posters

1. 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.
2. O. Dunkelman, M. Osadchy, M. Sharif. "Secure Authentication from Facial Attributes with No Privacy Loss." Conference on Computer and Communications Security (CCS), 2013.

Approved Patents

1. M. Sharif, S. Bhatkar, K. A. Roundy, S. Shintre. "Systems and Methods for Training Malware Classifiers." US Patent 11210397 , 2021.
2. 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.
3. K. A. Roundy, M. Sharif, A. Tamersoy. "Systems and Methods for Real-Time Scam Protection on Phones." US Patent 10455085, 2019.

Pending Patents

1. M. Sharif, V. Ganti. "Distributed Representations of Computing Processes and Events." 2021.
2. M. Sharif, P. Kotzias, K. A. Roundy. "A Recommender System to Protect Users from Potentially Unwanted Programs." 2020.

Teaching and Instructing Experience

- Instructor. Trustworthy Machine Learning (TAU). S22.
- Instructor. Workshop on Usable Security and Privacy (TAU). S22.
- Teaching Assistant. Network Security (CMU). S17.
- Teaching Assistant. Secure Software Systems (CMU). S16.
- Teaching Assistant. Intro to Information Security (CMU). F15.
- Teaching Assistant. Intro to Computer Science (University of Haifa). F11, S14.
- Lab Instructor. Intro to Computer Science (University of Haifa). F11, S12, F12.

Present Students

- Amit Cohen. M.Sc., SCS, TAU.
- Tsufit Ronen. M.Sc., SCS, TAU.
- Achi-Or Weingarten. M.Sc., CS, Weizmann.
  (Joint with Eyal Ronen.)
- Naama Yochai. M.Sc., SCS, TAU.

Past Students

- Nimrod de la Vega. B.Sc., SCS, TAU. 2021.
  (Joint with Eyal Ronen.)

Past Mentoring

- Max Wolff. High school student. 2019.
  (Paper accepted at ICLR TML workshop, 2020.)
- Anna Kawakami. Participant in the REUSE program. ISR, CMU. 2019.
  (Paper accepted at SOUPS, 2020.)
- Jihye Choi. Master's student in ECE, CMU. 2018.
- Siyao Meng. Master's student in INI, CMU. 2017.
- Alessio Buraggina. Participant in the REUSE program. ISR, CMU. 2017.
- Andrew Zhang. Participant in the REUSE program. ISR, CMU. 2017.
- Truth Iyiewuare. Participant in the REUSE program. ISR, CMU. 2016.
- Said Agha. Freshman at University of Haifa, 2010/11.

Conference and Workshop Program Committees

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

Invited External Reviewing

- AAAS Science Advances. 2022.
- ACM Conference on Communication and Computer Security (CCS). 2016, 2017, 2019.
- ACM CHI Conference on Human Factors in Computing Systems (CHI). 2021.
- ACM CHI Conference on Human Factors in Computing Systems (CHI) Late-Breaking Track. 2018.
- ACM Transactions on Privacy and Security (TOPS). 2018, 2019, 2020, 2021.
- IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2013, 2014.
- IEEE European Symposium on Security and Privacy (EuroS&P). 2019.
- IEEE Symposium on Security and Privacy (S&P). 2016, 2017, 2018, 2019, 2021.
- IEEE Transactions on Dependable and Secure Computing. 2019, 2020.
- International Conference on Machine Learning. 2022.
- International Journal on Machine Vision and Applications (MVAP). 2015.
- International World Wide Web Conference (WWW). 2018.

- Network and Distributed System Security Symposium (NDSS). 2016, 2017, 2018, 2019.
- Privacy Enhancing Technologies (PETS). 2015, 2016, 2019, 2020.
  Symposium on Usable Privacy and Security (SOUPS), 2018.
- USENIX Security Symposium. 2017, 2018, 2020.

Talks

1. "The Security of Machine Learning in the Real World"
   - Deep Learning Seminar. Interdisciplinary Center Herzliya, Sep/2020.
2. "The Security of Machine Learning in the Real World and Machine Learning for Personalized Security."
   - Computer Science Department. Bar-Ilan University, Jun/2020.
   - School of Computer Science and Engineering. Hebrew University of Jerusalem, Jun/2020.
   - Faculty of Electrical Engineering. Technion, Jun/2020.
   - School of Computer Science. Tel Aviv University, Jun/2020.
   - VMware Research Group. Herzliya and Palo Alto, Jun/2020.
   - Department of Industrial Engineering. Tel Aviv University, June/2020.
   - Computer Science Department. University of Haifa, July/2020.
3. "Comparing Hypothetical and Realistic Privacy Valuations."
   - Federal Trade Commission's PrivacyCon. Washington DC, Jun/2019.
4. "A Field Study of Computer-Security Perceptions Using Anti-Virus Customer-Support Chats."
   - CHI Conference on Human Factors in Computing Systems. Glasgow, May/2019.
5. Invited panelist to "The Hugh Thompson Show: Artificial Intelligence APJ Style."
   - RSA Asia Pacific & Japan. Singapore, Jul/2018.
6. "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.
7. "Predicting Impending Exposure to Malicious Content from User Behavior."
   - Conference on Computer and Communications Security (CCS). Toronto, Oct/2018.
   - CyLab Partners Conference. Carnegie Mellon University, Oct/2018.
   - Network Security. Guest lecture. Carnegie Mellon University, Apr/2018.
8. "Physical-World Attacks on Machine Learning."
   - Principles and Tools for Computer Security. Guest lecture. Technion, Jan/2021.
   - Security and Fairness of Deep Learning. Guest lecture. Carnegie Mellon University, Apr/2019, Apr/2020.
   - Ethics and Policy Issues in Computing. Guest lecture. Carnegie Mellon University, Feb/2019.
   - Symantec Research Labs. Mountain View, Jun/2018.
   - Introduction to Information Security. Guest lecture. Carnegie Mellon University, Nov/2017.
   - Privacy, Policy, Law, and Technology. Guest lecture. Carnegie Mellon University, Nov/2017, Nov/2018.
   - CyLab Partners Conference. Carnegie Mellon University, Oct/2017.
   - The French-American Doctoral Exchange (FADEx) Program. French Institute for Research in Computer Science and Automation (INRIA), Jun/2017.
9. "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior."
   - CHI Conference on Human Factors in Computing Systems. Denver, May/2017.
10. "Special Topic: Adversarial Machine Learning."
    - Network Security. Guest lecture. Carnegie Mellon University, Apr/2017.
11. "(Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking."
    - Federal Trade Commission's PrivacyCon. Washington DC, Jan/2017.

12. “Privacy in the Age of Face and Speech Recognition.”
    - Privacy, Policy, Law, and Technology. Guest lecture. Carnegie Mellon University, Dec/2016.
13. “Accessorize to a Crime: Real and Stealthy Attacks on State-Of-The-Art Face Recognition.”
    - Conference on Computer and Communications Security (CCS). Vienna, Oct/2016.
14. “Biometric Authentication and Key-Derivation: Closing the Gap between Theory and Practice.”
    - Privacy Enhancing Technologies for Biometric Data Workshop. University of Haifa, Jan/2016.
15. “Privacy-Preserving Key Generation and Authentication from Face Images.”
    - Doctoral Symposium, IEEE Conference on Software Science, Technology, and Engineering. Bar-Ilan University, Jun/2014.
    - Computer-Science Day. University of Haifa, Jun/2014.