Curriculum Vitae of Avishai Wool

Jan 2023

Office Address
School of Electrical Engineering,
Tel Aviv University, Tel Aviv 69978, Israel.
Phone: +972-3-640-6316 Mobile: +972-52-3330052
E-mail: yash@eng.tau.ac.il
Web: http://www.eng.tau.ac.il/~yash

Home Address
26 Ha'Aviv St., Neve Oz,
Petah Tikva 49213, Israel
Phone: +972-3-924 6473

Personal Data

Date and Place of birth: 17 July 1963, Petah Tikva, Israel
Citizenship: Israeli

Education

TEL AVIV UNIVERSITY — Ramat Aviv, Israel
1986–1989
B.Sc. in Mathematics and Computer Science. Graduated with honors.

WEIZMANN INSTITUTE OF SCIENCE — Rehovot, Israel
1991–1992
M.Sc. in Computer Science.
Thesis Title: "Approximating bounded 0-1 integer linear programs".
Advisor: Prof. David Peleg.

WEIZMANN INSTITUTE OF SCIENCE — Rehovot, Israel
1993–1997
Ph.D. in Computer Science.
Thesis title: "Quorum Systems for Distributed Control Protocols".
Advisors: Profs. David Peleg and Moni Naor.

Academic Appointments

CESDIS, NASA GODDARD SPACE FLIGHT CENTER — Greenbelt, MD, USA
Oct.–Nov. 1995
Visiting research scholar (student).

BELL LABS RESEARCH, LUCENT TECHNOLOGIES — Murray Hill, NJ, USA
Oct. 1996–Mar. 2000
Member of technical staff in the Secure Systems Research Department.

SCHOOL OF ELECTRICAL ENGINEERING, TEL AVIV UNIVERSITY — Tel Aviv, Israel
Jan. 2002–present
Full Professor since Mar 2018. Head of department since 2022.

INTERDISCIPLINARY CYBER RESEARCH CENTER AT TAU — Tel Aviv, Israel
May 2014–present
Deputy Director.

Industrial Appointments

ISRAEL DEFENSE FORCE
1981–1986
Last position: head of an IBM mainframe programming section with staff of 13. Rank of captain (discharged).

ELRON ELECTRONIC INDUSTRIES LTD. Or-Yehuda, Israel
1986–1990
Last position: Senior software engineer, team lead with staff of 4.

LUCENT NEW VENTURES GROUP Murray Hill, NJ, USA
Apr. 2000–Sep. 2000
Co-founder of an internal Lucent startup company, It was incorporated as Lumeta Corporation in Oct. 2000.

LUMETA CORP. Somerset, NJ, USA
2000–2003
Chief Scientist and co-founder.

ALGOSEC INC. Ridgefield Park, NJ, USA
2003–Present
Chief Technical Officer and co-founder. Creator of the Firewall Analyzer.

Areas of Research

My research is in the areas of computer and network security, and networking in general. Recently I have been focusing on:

- Computer and network security
- Industrial control systems security
- Secure hardware, side-channel cryptography
- In-car vehicle control networks
- Wireless security (WiFi, Bluetooth, RFID)

My Ph.D. work was in the field of distributed computing, and centered around quorum systems.

Academic and Professional Awards

- Dean's honors list (for B.Sc. students), School of Mathematics and Computer Science, Tel Aviv University, 1987, 1989.
- Israeli ministry of communication scholarship for Ph.D. students, 1992.
- Wolf distinction fellowship — Weizmann Institute of Science award for excellence in Ph.D., 1996.
- Rothschild postdoctoral fellowship, 1996 (declined).
- Best Case Study prize, 17th Annual Computer Security Applications Conference, New Orleans, LA, December 2001.
- Senior Member of the IEEE, 2003.
- Winner of the Thomas Edison Patent Award competition, for US patent 6,839,436 "A Method for providing long-lived broadcast encryption."

- Rector's Teaching award - Top 3 teachers at School of Electrical Engineering, Tel Aviv University, 2013, 2021.
- Member of "100-club" — Best 100 teachers at Tel Aviv University, 2012, 2013, 2014, 2017, 2018, 2019, 2021, 2022
- Outstanding Teacher award, School of Electrical Engineering, Tel Aviv University, 2004, 2006, 2011, 2013, 2016, 2017.

Professional Societies

I am an IEEE Senior Member, and a member of the ACM and USENIX. I am the campus liason for USENIX at Tel Aviv University. I was the treasurer of IEEE Israel Section, Jan/2004–Dec/2005.

Professional Activities

Editorial activities:

- Associate Editor, *ACM Transactions on Information and System Security*, 2003–2009.
- Member of the Editorial and Advisory Board, *International Journal of Information and Computer Security*.
- Member of the Editorial Board, *The Handbook of Information Security*, John Wiley & Sons.
- Member of the Editorial Board, *ACM/Springer Wireless Networks* until 9/2005.

Grant proposal & Academic program reviews (since 2013):

- Grant selection committee member: Ministry of Science, Cyber-security program, 2013
- Reviewer for proposed new M.Sc. degree in Cyber Space Security at Ben Gurion University, 2014
- Grant selection committee: Interdisciplinary Cyber Research Center at TAU, 2015
- Grant selection committee: Italy-Israel Scientific and Technological Cooperation, 2015
- Grant selection committee: Interdisciplinary Cyber Research Center at TAU, 2016
- Grant selection committee: Japan-Israel Scientific Research Cooperation, 2016
- Grant selection committee: Technion Cyber Research Center, 2017
- Grant selection committee: Interdisciplinary Cyber Research Center at TAU, 2017
- Chair, grant selection committee: TCS-iCRC, 2018
- Grant selection committee: Interdisciplinary Cyber Research Center at TAU, 2019

Member of the program committee (last 5 years):

- *International Symposium on Cyber Security, Cryptography and Machine Learning* (CSCML'17)
- *3rd ACM workshop on Cyber-Physical Systems Security & Privacy* (ACM CPS-SPC'17)
- *4th ACM workshop on Cyber-Physical Systems Security & Privacy* (ACM CPS-SPC'18)
- *Program Committee Co-Chair, 5th ACM workshop on Cyber-Physical Systems Security & Privacy* (ACM CPS-SPC'19)
- *1st Joint Workshop on CPS & IoT Security and Privacy* (CPSIoTSec'20)
- *26th European Symposium on Research in Computer Security* (ESORICS'21)
- *2nd Joint Workshop on CPS & IoT Security and Privacy* (CPSIoTSec'21)
- *24th Information Security Conference* (ISC'21)

- *27th European Symposium on Research in Computer Security* (ESORICS'22)

Teaching - Graduate Courses:

- Cryptography and Computer Security: Spring 2002, Spring 2003, Spring 2004, Spring 2006, Fall 2008, Fall 2010.
- Coordinator for department and student seminars, 2003.
- SecurityTheater advanced seminar, Annual 2010–2012.
- Topics in multiprocessing, Spring 2021.
- Topics in Information Security, Spring 2005, Spring 2007, Fall 2009, Fall 2011, Fall 2012, Fall 2013, Spring 2016, Spring 2018, Spring 2020, Spring 2022.

Teaching - Undergraduate Courses:

- Faculty of Engineering coordinator - C programming course, 2002–2006.
- Faculty of Engineering coordinator - programming prep course, summer 2005.
- Digital Logic Systems, Spring 2007
- Data Structures and Algorithms, 2009–2013.
- Computer Organization, Spring 2014.
- Programming 2 — C language: 2015–2018.
- Introduction to Information Security (MOOC): developing an online course, 2018-2019.
- Introduction to Systems Programming, 2002–2006, 2008–2021.
- Introduction to Information Security: 2013–2014, 2016–2022.

Student Supervision

Ph.D. students:

1. Mira Gonen. Ph.D., 2008.
   Thesis: Internet Topology and Communication Networks.
   Lecturer at the University or Ariel.
2. Yossi Oren. Ph.D., 2014.
   Thesis: Secure Hardware – Physical Attacks and Countermeasures.
   Senior Lecturer (Assistant Professor) at Ben Gurion University.
3. Amit Kleinman. Ph.D., 2017.
   Thesis: Network Intrusion Detection for Supervisory Control And Data Acquisition (SCADA) Systems.
4. Tsvika Dagan. Ph.D., 2020.
   Thesis: Active Defense Systems for Vehicle Cyber Security.
5. Liron David. Ph.D., 2021.
   Thesis: Estimating the Security Level of Cryptographic Keys Against Side-Channel Attacks and Using it to Estimate a Password Strength.

Current Ph.D. students:

6. Lior Shafir, Joint with Prof. Raja Giryes. Topic: network attack classification. Started 2022.

M.Sc. students (with thesis):

1. Noam Kogan. M.Sc., 2004. Joint with Prof. Yuval Shavitt. Thesis: "A practical revocation scheme for broadcast encryption using smart cards."
2. Danny Nebenzahl (Computer Science). M.Sc., 2005. Thesis: "Install-time vaccination of Windows executables to defend against stack smashing attacks."
3. Dmitry Rovniagin. M.Sc., 2005. Thesis: "The geometric efficient matching algorithm for firewalls."
4. Gonen Sagie (Computer Science). M.Sc., 2005. Thesis: "A clustering approach for exploring the Internet structure."
5. Ophir Levy. M.Sc., 2005. Thesis: "A Uniform Framework for Cryptanalysis of the Bluetooth E_0 Cipher".
6. Amir Shenhav. M.Sc., 2006. Thesis: "Practical One-Time Signatures with Applications to Secure Untrusted Storage".
7. Yaniv Shaked. M.Sc., 2006. Thesis: "Cracking the Bluetooth PIN".
8. Noa Bar-Yosef (Computer Science). M.Sc., 2006. Thesis: "Remote Algorithmic Complexity Attacks Against Randomized Hash Tables."
9. Yigael Berger (Computer Science). M.Sc., 2006. Thesis: "Dictionary Attacks Using Keyboard Acoustic Emanations".
10. Ziv Kfir. M.Sc., 2007. Thesis: "Picking Virtual Pockets using Relay attacks on Contactless Smartcard Systems"
11. Erel Geron. M.Sc., 2007. Thesis: "CRUST: Cryptographic Remote Untrusted Storage without Public Keys".
12. Ilan Kirschenbaum. M.Sc., 2008. Thesis: "How to build a low-cost, extended-range RFID skimmer."
13. Ehud Doron. M.Sc., 2008. Thesis: "WDA: A Web Farm Distributed Denial Of Service Attack Attenuator."
14. Ohad Ben-Cohen. M.Sc., 2008. Thesis: "Korset: Automated, zero false-alarm intrusion detection for Linux."
15. Idan Sheetrit. M.Sc., 2011. Thesis: "Cryptanalysis of KeeLoq code-hopping using a Single FPGA".
16. Eyal Ronen. M.Sc., 2011. Thesis: "Security Applications for Hardware Performance Counters".
17. Ory Samorodnitzky (Computer Science). M.Sc., 2013. Thesis: "Analyzing unique-bid auction sites for fun and profit."
18. Niv Goldenberg. M.Sc., 2013. Thesis: "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems."
19. Dvir Schirman. M.Sc., 2013. Thesis: "Range extension attacks on contactless smart cards."
20. Asaf Tzur. M.Sc., 2014. Thesis: "Direction Finding of RogueWi-Fi Access Points Using an Off-the-Shelf MIMO-OFDM Receiver."

21. Ofir Weisse (Computer Science). M.Sc., 2014. Thesis: "New Methods for Side Channel Cryptanalysis."
22. Noam Erez. M.Sc., 2015. Thesis: "Control Variable Classification, Modeling and Anomaly Detection in Modbus/TCP SCADA Networks."
23. Moti Markovitz. M.Sc., 2016. Thesis: "Field Classification, Modeling and Anomaly Detection in Unknown CAN Bus Networks"
24. Eyal Itkin (Computer Science). M.Sc., 2016. Thesis: "A Security Analysis and Revised Security Extension for the Precision Time Protocol."
25. Uri Kanonov (Computer Science). M.Sc., 2016. Thesis: Secure Containers in Android: the Samsung KNOX Case Study.
26. Elad Carmon. M.Sc., 2016. Theis: "Photonic Side Channel Attacks."
27. Itamar Pipman. Joint with with Prof. Eran Tromer. M.Sc., 2018. Theis: "Physical Side-Channel Attacks on PC-class Devices."
28. Dor Fledel. M.Sc., 2018. Thesis: "Sliding-Window Correlation Attacks Against Encryption Devices with an Unstable Clock."
29. Ben Lapid. M.Sc., 2018. Thesis: "Navigating the Samsung TrustZone with applications to Cache-Attacks on AES-256/GCM in the Keymaster Trustlet."
30. Chen Markman. M.Sc., 2019. Thesis: "A new Burst-DFA model for SCADA Anomaly Detection and Traffic Phase Detection."
31. Uriel Malin (Computer Science). M.Sc., 2019. Thesis: "Security assessment of Siemens S7-1500 Communication Protocol P3."
32. Nimrod Gilboa Markevich. M.Sc., 2020. Thesis: "Hardware Fingerprinting for the ARINC 429 Avionic Bus."
33. Eldad Zuberi. M.Sc., 2021. Thesis: "Characterizing GPU Overclocking Faults."
34. Aviv Engelberg (Computer Science). M.Sc, 2022. Thesis: Classification of Encrypted IoT Traffic Despite Padding and Shaping.
35. Alon Shakevsky (Computer Science). M.Sc, 2022. Joint with with Eyal Ronen. Thesis: Trust Dies in Darkness: Shedding Light on Samsung's TrustZone Cryptographic Design.

Current M.Sc. students:

36. Tomer Avrahami. Joint with with Ofer Amrani. Started 2020. Topic: WiFi security.
37. Reuven Yakar (Computer Science). Joint with with Eyal Ronen. Started 2021. Topic: GPU Security.
38. Sharon Vaisman. Started 2022. Topic: Vehicular radars security.
39. Dror Peri. Started 2022. Topic: Vehicular camera security.

M.Sc. project students:

1. Kfir Israel. M.Sc., 2004. Project: "Network re-engineering with Citrix: measurements and simulation."

2. Oren Malerevich. M.Sc., 2004. Project: "A fast hardware implementation of the Rijndael Advanced Encryption Standard using field programmable gate arrays."
3. Michael Rafael. M.Sc., 2005. Project: Security issues in IEEE 802.11 Wireless LANs.
4. Erez Meirovich. M.Sc., 2005. Topic: Implementation of AES on FPGA.
5. Alex Arbit. M.Sc., 2011. Project: "Toward practical public key anti-counterfeiting for low-cost EPC tags."
6. Yoel Livne. M.Sc., 2013. Project: "A Full Implementation of WIPR in Hardware".
7. Daniel Aviram, M.Sc., 2016. Project: "Backdoor Access Framework using HAL integration".
8. Ori Amichay, M.Sc., 2017. Project: "TAU ICS Attack Tool (TIAT)".

Undergaduate project students:

1. Project 10-1-1-86: Amit Erez, Shay Cohen, Doron Shutzberg, 2011. "WIPR Software software Environment".
2. Summer Student project: Ariel Levy, 2012. RFID signal generation lab testbench.
3. Summer Student project: Gal Lerman, 2013. SCADA Intrudion Detection - Database Performance improvements.