Curriculum Vitae of Avishai Wool

March 2012

Associate Professor
School of Electrical Engineering,
Tel Aviv University, Tel Aviv 69978, Israel.
Phone: +972-3-640-6316 Fax: +972-3-640-7095
E-mail: yash@eng.tau.ac.il
Web: http://www.eng.tau.ac.il/~yash

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.

Grants

- "Key Management for Smart-card Based Broadcast Encryption". Giesecke & Devrient GmbH, 1/2002–12/2003, €170,000. Yuval Shavitt and Avishai Wool.
- "A Security Analysis of Contactless Smartcards' Communication Protocols". Giesecke & Devrient GmbH, 1/2004–12/2006, €150,525. Avishai Wool.
- "Security Issues in Storage Networking". IBM Faculty Award, 10/2004–9/2005, $7,500. Avishai Wool.
- "A Security Analysis of the Bluetooth System". Intel Communication Research Grant, 10/2004–9/2005, $18,000. Avishai Wool.
- "A Cryptographic Network Storage System". IBM Faculty Award, 12/2005–11/2006, $10,000. Avishai Wool.
- "Ultra-long fiber Lasers – A new concept for secure key distribution". Advanced Communication Center – Tel Aviv University, 1/2007–12/2007, $15,000. Koby Scheuer and Avishai Wool.
- "Security Issues with RFID Proximity Cards". Israel Ministry of Defense, 9/2007–8/2008, $20,000. Avishai Wool.
- "Lasers for Secure Communications". Israel Ministry of Defense, 2008–2009, $50,000. Koby Scheuer and Avishai Wool.
- "Security Issues with RFID Proximity Cards - extension". Israel Ministry of Defense, 12/2008–12/2009, $24,000. Avishai Wool.
- "Protecting Privacy in Webmail with Secret Sharing". Microsoft Israel R&D, 6/2009–5/2010, $15,000. Avishai Wool.

- "Low Cost RFID Public Key Cryptography for Anti Counterfeiting". Giesecke & Devrient GmbH, 1/2010–12/2011, €75,000. Avishai Wool.
- "Security Implications of Extended-Range RFID access". Giesecke & Devrient GmbH, 3/2012–12/2012, €55,100. Avishai Wool.

Awards and Prizes

- Member of "100-club" - Best 100 teachers at Tel Aviv University, 2012.
- Outstanding Teacher award, School of Electrical Engineering, Tel Aviv University, 2011, 2006, 2004.
- Winner of the Thomas Edison Patent Award competition, for US patent 6,839,436 "A Method for providing long-lived broadcast encryption."
- Outstanding Teacher award, School of Electrical Engineering, Tel Aviv University, 2006.
- Outstanding Teacher award, School of Electrical Engineering, Tel Aviv University, 2004.
- Senior Member of the IEEE, 2003.
- Best Case Study prize, 17th Annual Computer Security Applications Conference, New Orleans, LA, December 2001.
- Rothschild postdoctoral fellowship, 1996 (declined).
- Wolf distinction fellowship, 1996.
- Israeli ministry of communication scholarship, 1992.
- Dean's honors list, Tel Aviv University, 1987, 1989.

Research Experience

SCHOOL OF ELECTRICAL ENGINEERING, TEL AVIV UNIVERSITY — Tel Aviv, Israel
Jan. 2002–present
Associate Professor since 2006.

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

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

Students

Current Ph.D. students:

[1] Yossi Oren. Topic: RFID systems and side-channel attacks on Secure Hardware.

Current M.Sc. students:

[1] Dvir Schirman. Started 2009. Topic: RFID relay attacks system.
[2] Niv Goldenberg. Started 2010. Topic: Security of SCADA systems.
[3] Ory Smorodinsky (Computer Science). Started 2010. Topic: Attacking Online Auctions
[4] Idan Ganot. Started 2011. Topic: Security of car control networks.
[5] Dmitry Boyarer. Project started 2010. Topic: Side Channel attacks
[6] Yoel Livne. Project started 2010. Topic: FPGA implementation of WIPR.

Graduated Ph.D. students:

[1] Mira Gonen. Ph.D., 2008. Thesis: "Internet Topology and Communication Networks."

Graduated M.Sc. students:

[1] Noam Kogan. M.Sc., 2004. Joint with Dr. 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.”

[14] Idan Sheetrit. M.Sc., 2011. Thesis: “Cryptanalysis of KeeLoq code-hopping using a single FPGA.”

[15] Eyal Ronen. M.Sc., 2011 Thesis: “Security Applications for Hardware Performance Counters: Software Attestation and Random Generation”. M.Sc., 2012

M.Sc. Projects:

[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. Project: Implementation of AES on FPGA.

[5] Alex Arbit. M.Sc., 2011. Project: “Toward practical public key anti-counterfeiting for low-cost EPC tags.”

Industrial Experience

ALGORITHMIC SECURITY INC. (FORMERLY LUMETA CORP.) Reston, VA, USA
Oct. 2000–Present
Chief Technical Officer and co-founder. Creator of the Firewall Analyzer.

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.

ELRON ELECTRONIC INDUSTRIES LTD. Or-Yehuda, Israel
1986–1990
Last position: senior software engineer, head of the PC department, with staff of 4.

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

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. Published in 2006.
- Member of the Editorial Board, *ACM/Springer Wireless Networks* until 9/2005.

Member of the program committee:

- *7th Workshop on Systematic Approaches to Digital Forensic Engineering* (SADFE'12)
- *10th International Conference on Applied Cryptography and Network Security* (ACNS'12)
- *7th Workshop on RFID Security* (RFIDsec'11)
- *6th Workshop on Systematic Approaches to Digital Forensic Engineering* (SADFE'11)
- *6th Workshop on RFID Security* (RFIDsec'10)
- *6th International Conference on Security and Privacy for Emerging Areas in Communication Networks* (SecureComm'10)
- *5th Workshop on Systematic Approaches to Digital Forensic Engineering* (SADFE'10)
- *5th International Conference on Security and Privacy for Emerging Areas in Communication Networks* (SecureComm'09)
- *4th Workshop on Systematic Approaches to Digital Forensic Engineering* (SADFE'09)
- *7th International Conference on Applied Cryptography and Network Security* (ACNS'09)
- *13th European Symposium on Research in Computer Security* (ESORICS'08)
- *6th International Conference on Applied Cryptography and Network Security* (ACNS'08)
- *12th European Symposium on Research in Computer Security* (ESORICS'07)
- *5th International Conference on Applied Cryptography and Network Security* (ACNS'07)
- *ACM Workshop on Wireless Security* (WiSe 2006)
- *2nd International Conference on Security and Privacy for Emerging Areas in Communication Networks* (SecureComm'06)

- *IEEE Network Security and Information Assurance Symposium* (at ICC'06)
- *1st International Conference on Security and Privacy for Emerging Areas in Communication Networks* (SecureComm'05)
- *25th International Conference on Distributed Computing Systems* (ICDCS'05).
- *2004 Workshop on Information Security Applications* (WISA'04).
- *2004 IEEE Symposium on Security and Privacy* (Oakland'04).
- *10th ACM Conference on Computer and Communication Security* (CCS'2003).
- *32nd International Conference on Parallel Processing, Network Security Track* (ICPP'03).
- *9th ACM Conference on Computer and Communication Security* (CCS'2002).
- *2002 IEEE Symposium on Security and Privacy* (Oakland'02).
- *2001 IEEE Symposium on Security and Privacy* (Oakland'01).
- *7th ACM Conference on Computer and Communication Security* (CCS'2000).
- *19th International Conference on Distributed Computing Systems* (ICDCS'99).

Proposal reviewer for the Israel Science Foundation, Bi-National Science Foundation and the Netherlands Organisation for Scientific Research (NWO).

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