Avi Rubin's Vita

Academic Degrees

- 1994, Ph.D., Computer Science and Engineering, University of Michigan, Ann Arbor
- 1991, M.S.E., Computer Science and Engineering, University of Michigan, Ann Arbor
- 1989, B.S., Computer Science (Honors), University of Michigan, Ann Arbor

Academic Appointments

- April, 2004 - present
  Professor, Johns Hopkins University

- August, 2010 - July, 2011
  Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel

- January, 2003 - April, 2004
  Associate Professor, Johns Hopkins University

- January, 2003 - present
  Technical Director, Johns Hopkins University Information Security Institute

- 2006 - 2010
  Director and Principal Investigator (PI), National Science Foundation's ACCURATE Center

- 1995 - 1999
  Adjunct Professor, New York University
  - *Internet and Web Security* Spring, 1999 (with Dave Kormann)
  - *Privacy in Networks: Attacks and Defenses* Spring, 1998 (with Dave Kormann and Mike Reiter)
  - *Design and Analysis of Cryptographic Protocols* Fall, 1996 & Spring, 1997 (with Matt Franklin)
  - *Cryptography and Computer Security* Fall, 1995 & Spring, 1996

- Summer, 1999
  Visiting Professor, École Normale Supérieure, Paris, France

- 1988 - 1993
  Teaching Assistant, University of Michigan
  - 1993 *Intro. to Cryptography*
  - 1992 *Assembler Language Programming*
  - 1991 *Software Engineering*
  - 1990 *IVHS Seminar*
  - 1989-1990 **Head TA**, *Intro. to Computer Science*
  - 1988-1989 *Intro. to Computer Science*

- **Doctoral Committees**
  - **Doctoral Thesis Advisor:** Ayo Akinyele, JHU
  - **Doctoral Thesis Advisor:** Christina Garman, JHU
  - **Doctoral Thesis Advisor:** Paul Martin, JHU
  - **Doctoral Thesis Advisor:** Matthew Pagano, JHU
  - **Doctoral Thesis Advisor:** Michael Rushanan, JHU
  - **Doctoral Thesis Advisor:** Ryan Gardner, JHU (August, 2009)
  - **Doctoral Thesis Advisor:** Sam Small, JHU (May, 2009)
  - **Doctoral Thesis Advisor:** Sujata Doshi, JHU (May, 2009)
  - **Doctoral Thesis Advisor:** Joshua Mason, JHU (June, 2009)
  - **Dissertation Committee:** J. Alex Halderman, Princeton University (May, 2009)
  - **Dissertation Committee:** Sophie Qiu (May, 2007).
  - **Doctoral Thesis Advisor:** Adam Stubblefield (April, 2005).
  - **Dissertation Committee:** Kevin FU, MIT (February, 2005).
  - **Dissertation Committee:** Robert Fischer, Harvard University (June, 2003).
  - **Dissertation Committee:** Marc Waldman, New York University, (April, 2003).
  - **Dissertation Committee:** Patrick McDaniel, University of Michigan (September, 2001).
  - **Doctoral Thesis Advisor:** Fabian Monrose, New York University (April, 1999).
  - **Dissertation Committee:** Mike Just, Carleton University (November, 1998).
  - **Dissertation Committee:** Trent Jaeger, University of Michigan (October, 1996).

Industry Experience

- 1997 - 2002
  AT&T Labs - Research , Secure Systems Research Department
- 1994 - 1996
  Bellcore, Cryptography and Network Security Research Group
- Summer, 1990
  Great Lakes Software Co., *Programmer*, Howell, MI
- Summer, 1989
  IBM, *Programmer*, Meyers Corners Lab, Poughkeepsie, NY

Books

- Aviel D. Rubin, *Brave New Ballot*, Random House, (September, 2006).
- William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2e)*, Addison Wesley Publishing Company, Inc., (February, 2003).
- **Chapter 4**, *Communications Policy and Information Technology: Promises, Problems, Prospects*, MIT Press, Lorrie Faith Cranor and Shane Mitchell Greenstein, eds., (2002).
- Aviel D. Rubin, *White-hat Security Arsenal*, Addison Wesley Publishing Company, Inc., (June, 2001).
- **Chapter 8**, *Publius* and **Chapter 14**, *Trust in Distributed Systems*, Marc Waldman, Lorrie Faith Cranor, and Aviel D. Rubin, *Peer-to-Peer*, O'Reilly & Associates, Inc., (February, 2001).
- Aviel D. Rubin, Daniel Geer, Marcus J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, Inc , (June, 1997).
- **Ph.D. dissertation:** *Nonmonotonic Cryptographic Protocols* (ps.gz, pdf), University of Michigan, Ann Arbor (April, 1994).

Refereed Journal Publications

- Ayo Akinyele, Christina Garman, Matthew D. Green, Ian Miers, Matthew Pagano, Aviel D. Rubin, Michael Rushanan, *Charm: A Framework for Rapidly Prototyping Cryptosystems,* Journal of Cryptographic Engineering (JCEN), (January, 2013).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *Detecting Code Alteration by Creating a Temporary Memory Bottleneck*, IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, (December, 2009).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin, *Anonymity in Wireless Broadcast Networks*, International Journal of Network Security (IJNS), (January, 2008).
- Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green, *Security Through Legality*, Communications of the ACM (June, 2006).
- Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security*, Electronic Commerce Research Journal, February, 2005.
- David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *Analyzing Internet Voting Security*, Communications of the ACM (October, 2004).

- Simon Byers, Aviel D. Rubin, and David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Transactions on Internet Technology (TOIT), August, 2004.
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)* (pdf), ACM Transactions on Information and System Security, May, 2004.
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, Communications of the ACM (December, 2002).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *The Architecture of Robust Publishing Systems*, ACM Transactions on Internet Technology (TOIT), (November, 2001).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Signon Protocol,* Computer Networks, (July, 2000).
- Christian Gilmore, David P. Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, IEEE Network, (November, 1999).
- Fabian Monrose and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, (pdf) Future Generation Computer Systems, (March, 2000).
- Michael K. Reiter and Aviel D. Rubin, *Anonymity Loves Company: Anonymous Web Transactions with Crowds* (ps.gz, pdf) Communications of the ACM (February, 1999).
- Aviel D. Rubin and Daniel E. Geer, Jr., *Mobile Code Security* (ps.gz, pdf), IEEE Internet Computing (November/December, 1998).
- Aviel D. Rubin and Daniel E. Geer, Jr., *A Survey of Web Security*, IEEE Computer, (September, 1998).
- Michael K. Reiter and Aviel D. Rubin, *Crowds: Anonymity for Web Transactions* (ps.gz, pdf), ACM Transactions on Information and System Security, (June, 1998).
- Aviel D. Rubin, *An Experience Teaching a Graduate Course in Cryptography* (ps, pdf), Cryptologia (April, 1997).
- Aviel D. Rubin, *Extending NCP for public Key Protocols*, Mobile Networks and Applications (ACM/Balzer), 2(3) (April, 1997).
- Aviel D. Rubin, *Independent One-Time Passwords*, (ps.gz, pdf) USENIX Journal of Computer Systems (February, 1996).
- Aviel D. Rubin, *Secure Distribution of Documents in a Hostile Environment*, Computer Communications (June, 1995).

Refereed Conference Publications

- Paul Martin, Avi Rubin and Rafae Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control,* Health Informatics Symposium at the ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics, (September, 2013).
- Ian M. Miers, Christina Garman, Matthew D. Green, Aviel D. Rubin, *Zerocoin: Anonymous Distributed e-Cash from Bitcoin*, Proc. IEEE Symposium on Security and Privacy (May, 2013).
- Ian M. Miers, Matthew D. Green, Christoph U. Lehmann, Aviel D. Rubin, *Vis-à-Vis Cryptography: Private and Trustworthy In-Person Certifications*, In Proceedings of the 3rd USENIX/HealthSec Workshop, (August, 2012).

- Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N. J. Peterson and Aviel D. Rubin, *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, (October, 2011).
- Matthew D. Green, Aviel D. Rubin, *A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report - 4 page Extended Abstract*, In Proceedings of the 2nd USENIX/HealthSec Workshop, (August, 2011).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Designing for Audit: A Voting Machine with a Tiny TCB*, Financial Cryptography Conference, (January , 2010).
- Ryan Gardner, Sujata Garera, Matthew W. Pagano, Matthew D. Green, Aviel D. Rubin, *Securing Medical Records on Smart Phones, Workshop on Security and Privacy in Medical and Home-Care Systems*, (November, 2009).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Coercion Resistant End-to-end Voting*, Financial Cryptography Conference, (February, 2009).
- Ryan Gardner, Sujata Garera, Anand Rajan, Carols Rozas, Aviel D. Rubin, Manoj Sastry, *Protecting Patient Records from Unwarranted Access*, Future of Trust in Computing, (July, 2008).
- Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, 5th ACM Workshop on Recurring Malcode (WORM 2007), (November, 2007).
- Sujata Garera and Aviel D. Rubin, *An Independent Audit Framework for Software Dependent Voting Systems*, 14th ACM Conference on Computer and Communications Security, (November, 2007).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *On the Difficulty of Validating Voting Machine Software with Software*, In Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), (August, 2007).
- Sujata Doshi, Fabian Monrose, and Aviel D. Rubin, *Efficient Memory Bound Puzzles using Pattern Databases*, 4th International Conference on Applied Cryptography and Network Security (ACNS'06), (June, 2006).
- Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Avi Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, (June 2006).
- Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Aviel D. Rubin, *Secure Deletion for a Versioning Filesystem* , Proc. USENIX Conference on File and Storage Technologies (FAST '05), (December, 2005).
- Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, *Security Analysis of a Cryptographically-Enabled RFID Device* 14th USENIX Security Symposium, (August, 2005).
- Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004).
- Nathanael Paul, David Evans, Aviel D. Rubin and Dan Wallach, *Authentication for Remote Voting*, ACM Workshop on Human-Computer Interaction and Security Systems (April, 2003).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Aviel Rubin, *Protocols for Anonymity in Wireless Networks,* Proc. 11th International Workshop on Security

Protocols (April, 2003).
- Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing* , Proc. ISOC Symposium on Network and Distributed System Security (February, 2003).
- Simon Byers, Aviel D. Rubin, David Kormann, *Defending Against an Internet-based Attack on the Physical World* (pdf), ACM Workshop on Privacy in the Electronic Society (November, 2002).
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2002).
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), (October, 2001).
- Aviel D. Rubin and Rebecca N. Wright, *Off-line generation of limited-use credit card numbers*, (ps.gz, pdf) Financial Cryptography Conference, (February, 2001).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *Publius, A robust, tamper-evident and censorship-resistant web publishing system*, 9th USENIX Security Symposium, (August, 2000).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Signon Protocol*, 9th International World Wide Web Conference, (May, 2000).
- Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, (ps.gz, pdf), Financial Cryptography Conference, (February, 2000).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device* (ps.gz, pdf), 6th ACM Conference on Computer and Communications Security, (November, 1999).
- Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords* (ps.gz, pdf) 8th USENIX Security Symposium, (August, 1999).
- Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, (ps.gz, pdf), Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Fabian Monrose, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit* (ps.gz, pdf), Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground* (ps, pdf) Proc. IEEE Symposium on Security and Privacy (May, 1998).
- Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread E-mail in an Untrusted Network* (ps.gz, pdf), Second Australasian Conference on Information Security and Privacy (July, 1997).
- Fabian Monrose and Aviel D. Rubin, *Authentication via Keystroke Dynamics* (ps, pdf), 4th ACM Conference on Computer and Communications Security (April, 1997).
- David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall* (ps, pdf), Proc. ISOC Symposium on Network and Distributed System

Security (February, 1997).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content*, Proc. 6th USENIX Security Symposium (July, 1996).
- Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, (ps, pdf), Proc. of Eurocrypt '96 (May, 1996).
- Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
- Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
- Aviel D. Rubin, *Pseudo-Random Functions for One-Time Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
- Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).
- Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
- Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

- Steven M. Bellovin, Thomas J. Killian, Bruce LaRose, Aviel D. Rubin, Norman L. Schryer, Method and apparatus for connection to virtual private networks for secure transactions, **US Patent Number 8,239,531**, (August 7, 2012).
- Christian A. Gilmore, David P. Kormann, and Aviel D. Rubin, Method and apparatus for secure remote access to an internal web server, **US Patent Number 7,334,126**, (February 19, 2008).
- Aviel D. Rubin, "Method for secure remote backup", **US Patent Number 7,222,233**, (May 22, 2007).
- Frederick Douglis, Michael Rabinovich, Aviel D. Rubin, and Oliver Spatscheck, "Method for content distribution in a network supporting a security protocol", **US Patent Number 7,149,803**, (December 12, 2006).
- William A. Aiello, Steven M. Bellovin, Charles Robert Kalmanek, Jr., William T Marshal, and Aviel D. Rubin, "Method and apparatus for enhanced security in a broadband telephony network", **US Patent Number 7,035,410**, (April 25, 2006).
- Aviel D. Rubin, "Broadband Certified Mail", **US Patent Number 6,990,581**, (January 24, 2006).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, "Using smartcards to enable probabilistic transaction on an untrusted device", **US Patent Number 6,496,808**, (December 17, 2002).
- Aviel D. Rubin and Victor J. Shoup, "Session Key Distribution Using Smart Cards", **US Patent Number 5,809,140**, (September 15, 1998).
- Aviel D. Rubin, "Method for the Secure Distribution of Electronic Files in a Distributed Environment", **US Patent Number 5,638,446**, (June 10, 1997).

Professional Activities

- **Board of Directors**
  - Director, USENIX Organization, elected by popular vote (2000 - 2004).

- **Editorial and Committees**
  - **Associate Editor:** IEEE Transactions on Information Forensics and Security (2009-2011).
  - **Associate Editor**: Communications of the ACM (CACM), 2009 - present.
  - **Guest Co-Editor:** IEEE Transactions on Information Forensics and Security: *Special Issue on Electronic Voting*, December 1, 2009.
  - **Guest Co-Editor:** IEEE Security & Privacy Magazine, *Special Issue on Electronic Voting*, October/November, 2007.
  - **Associate Editor:** IEEE Transactions on Software Engineering (2005-2006).
  - **Editorial and Advisory Board:** International Journal of Information and Computer Security (IJICS) (2004-2006).
  - **Guest Co-Editor:** IEEE Computer Networks, *Special Issue on Web Security*, January, 2005.
  - **Editorial Board:** Journal of Privacy Technology (2004-2006).
  - **Guest Co-Editor:** IEEE Security & Privacy Magazine, *Special Issue on Electronic Voting Security*, January/February, 2004.
  - **Member:** Security Peer Review Group (SPRG) of the Federal Voting Assistance Program's (FVAP) Secure Electronic Registration and Voting Experiment (SERVE) Project, 2003-2004.
  - **Member:** DARPA Information Science And Technology Study Group (2003-2006).
  - **Associate Editor:** IEEE Security & Privacy Magazine (2003-present).
  - **Guest Editor:** Communications of the ACM, *Special Issue on Wireless Networking Security*, May, 2003.
  - **Associate Editor:** ACM Transactions on Internet Technology (2002-2005).
  - **Executive Committee Member:** DIMACS Workshop Series with Special Focus on Network Security (2002-2004).
  - **Advisory Board Member:** Information Security and Cryptography Book Series, Springer, 2001-2006.
  - **Member:** Steering Group, ISOC Symposium on Network and Distributed System Security, 2001-2004.
  - **Member:** Government Infosec Science and Technology Study Group on malicious code, 1999 - 2000.
  - **Member:** *AT&T Internet Intellectual Property Review Team*, 1999 - 2001.
  - **Associate Editor:** *Electronic Commerce Research Journal*, Baltzer Science Publishers, 1999 - 2002.
  - **Co-Editor:** Electronic Newsletter of the IEEE Technical Committee on Security & Privacy, with Paul Syverson, 1998.
  - **Editorial Board:** Bellcore Security Update Newsletter, 1995-1996.

- **Conference Committees**
  - Program Committee member: 2nd USENIX Workshop on Health Security and Privacy

(HealthSec '11), August 9, 2011.
- **Program Co-chair:** (w/Kevin Fu & Yoshi Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
- Program Committee member: First Security and Privacy in Medical and Home-Care Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.
- Invited Talks Co-Coordinator: 17th USENIX Security Symposium, San Jose, CA, July 28 - August 1, 2008.
- **Program Co-chair:** (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 18-22, 2008.
- **Program Co-chair:** (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
- Program Committee member: IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.
- Program Committee member: Financial Cryptography '04 Key West, Florida, February 9-12, 2004.
- Program Committee member: 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
- Program Committee member: 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
- Program Committee member: 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
- **Program Vice Chair:** Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 20-24, 2003.
- Program Committee member: IEEE Symposium on Security and Privacy, Oakland, California, May 11-14, 2003.
- Program Committee member: Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
- Program Committee member: 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRDL), Singapore December 9-12, 2002.
- Program Committee member: ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
- Program Committee member: 9th ACM Conference on Computer and Communications Security, Washington D.C., November 17-21, 2002.
- Program Committee member: 5th International Conference on Electronic Commerce Research (ICECR-5), Montreal, Canada, October 23-27, 2002.
- Program Committee member: 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 14-15, 2002.
- Program Committee member: 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 14-16, 2002.
- Program Committee member: 11th USENIX Security Symposium, San Francisco, Ca, August 5-9, 2002.
- Program Committee member: International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 21-24, 2002.

- Program Committee member: 11th International World Wide Web Conference Honolulu, Hawaii, May 7-11, 2002.
- Program Committee member: 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 14-15, 2002.
- Program Committee member: The 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 7-8, 2002.
- Program Committee member: The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001.
- Program Committee member: 10th USENIX Security Symposium, Washington D.C., August 13-17, 2001.
- Program Committee member: Financial Cryptography '01 Grand Cayman, Cayman Islands, BWI, February, 2001.
- **Program Co-chair:** (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 7-9, 2001.
- Program Committee member: The 3rd International Conference on Telecommunications and Electronic Commerce Dallas, TX, November 16-19, 2000.
- Program Committee member: 9th USENIX Security Symposium, Denver, Colorado, August 14-17, 2000.
- Program Committee member: Workshop on Design Issues in Anonymity and Unobservability Berkeley, California, July 25-26, 2000.
- Program Committee member: Performance and Architecture of Web Servers (PAWS), Santa Clara, CA, June 18, 2000.
- **Program Co-chair:** (w/Gene Tsudik): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 2-4, 2000.
- Program Committee member: 1999 International Information Security Workshop (ISW'99), Kuala Lumpur, Malaysia, November 6-7, 1999.
- Program Committee member: 2nd Int'l. Conference on Telecommunications and Electronic Commerce, Nashville, TN, October 6-8, 1999.
- Invited Talks coordinator: 8th USENIX Security Symposium, Washington D.C., August, 1999.
- **Program Chair:** 24th USENIX Annual Technical Conference, Monterey, CA, June 7-11, 1999.
- Program Committee member: 8th International World Wide Web Conference , Toronto, Canada, May 11-14, 1999.
- Program Committee member: 3rd USENIX workshop on Electronic Commerce , Boston, MA, August 31 - September 3, 1998.
- Program Committee member: 5th ACM Conference on Computer and Communications Security, San Francisco, CA, November 3-5, 1998.
- **Program Chair:** 7th USENIX Security Symposium, San Antonio, TX, Jan. 26-29, 1998.
- Program Committee member: 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 2-4, 1997.
- Program Committee member: 6th USENIX Security Symposium, San Jose, CA, July 22-25, 1996.
- Program Committee member: ISOC Symposium on Network and Distributed System

Security, San Diego, CA, February 22-23, 1996.

- Panels

- **Panelist:** Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
- **Panelist:** Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).
- **Panelist:** Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
- **Panelist:** First Security and Privacy in Medical and Home-Care Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
- **Panelist:** Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
- **Panelist:** Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel May 18, 2009.
- **Panelist:** RSA Conference, Exploiting Online Games, San Francisco, CA April 23, 2009.
- **Panelist:** American Association for the Advancement of Science, *Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel*, Washington DC, (November 27, 2006).
- **Panelist:** California Secretary of State's Voting System Testing Summit, *Security Panel*, Sacramento, CA, (November 28-29, 2005).
- **Panelist:** NIST Symposium on Voting System Threats, *Configuration and Usability Threats*, Gaithersburg, MD, (October 7, 2005).
- **Panelist:** Conference of State Supreme Court Chief Justices, *Voting Technologies*, Charleston, SC (August 1, 2005).
- **Panelist:** *Workshop on observation of automated elections*, The Carter Center, Atlanta, GA (March 18, 2005).
- **Panelist:** The Carter Center Venezuela Virtual Panel, (November, 2004).
- **Panelist:** Workshop on Voting, *Vote Capture and Vote Counting*, Harvard Kennedy School of Government, The Technologies of Voting, Cambridge, MA (June 1, 2004).
- **Panelist:** Computer Science and Telecommunications Board of The National Academy of Science *Workshop on Dependable Software Systems*, Case Study: Electronic Voting Washington D.C. (April 20, 2004).
- **Panelist:** USENIX Security 2003, *Electronic Voting*, Washington D.C. (August 6, 2003).
- **Panelist:** Democracy Now, 2003, *Voter-Verifiable Elections: How Do We Get There?*, Washington D.C. (November 23, 2003).
- **Panelist:** USENIX Security 2003, *Electronic Voting*, Washington D.C. (August 6, 2003).
- **Panelist:** IEEE Infocom 2002, *Securing Wireless and Mobile Networks - Is It Possible?*, New York City (June 25, 2002).
- **Participant:** 2002 Security Visionary Roundtable: *A Roadmap for a Safer Wireless World*, Washington D.C., (May 5-7,2002).
- **Panelist:** Computers Freedom and Privacy 2002, *Who Goes There? Privacy in*

Identity and Location Services, San Francisco (April 18, 2002).
- **Panel moderator:** Conference on Democracy and the Internet in an Enlarging Europe *Overview of On-Line Voting: Systems and Issues*, New York, NY (March, 2001).
- **Panelist:** Financial Cryptography 2001, *The Business of Electronic Voting*, Grand Cayman (February, 2001).
- **Panelist:** National Science Foundation *E-voting workshop*, Washington, D.C., (October, 2000).
- **Panelist:** 5th ACM Conference on Computer and Communications Security, Anonymity on the Internet, San Francisco, CA, (November 1998).
- **Panelist:** Open Systems Security and ISSA Annual Conference, *Securing the Web*, Orlando, FL (March, 1998).
- **Panel organizer and moderator:** *Implementation Issues for Electronic Commerce: What Every Developer Should Know*. ISOC Symposium on Network and Distributed System Security, (March, 1998).
- **Panel organizer and moderator:** *Downloadable Executable Content - Past, Present and Future*. ISOC Symposium on Network and Distributed System Security (February, 1997).
- **Panelist:** DIMACS Workshop on Network Threats, Web/Java Security Issues, New Brunswick, NJ (December 5, 1996).

- Tutorials Taught

- The Mathematics of Information Technology and Complex Systems Network (MITACS), *Network Security*, (May 8, 2003).
- IEEE Infocom 2002, *End to End Web Security and E-commerce*, (June 23, 2002).
- 2002 USENIX Annual Technical Conference, *Introduction to Computer Security*, (June 10, 2002).
- LISA 2001, 15th Systems Administration Conference, *Introduction to Computer Security*, (December, 2001).
- 8th & 9th USENIX Security Symposia, *Cryptography - From the Basics Through PKI in 23,400 Seconds*, (August, 2000) & (August 1999), with Dan Geer.
- 9th International World Wide Web Conference, *Security on the World Wide Web*, (May, 2000).
- ISOC Symposium on Network and Distributed System Security, *Cryptography 101*, (February, 2000).

Testimony

Before Legislative Bodies

- United Stated House Committee on Oversight and Government Reform, *hearing on electronic voting*, Washington, D.C., (April 18, 2007).
- United Stated House Committee on Appropriations, *hearing on ensuring the integrity of elections*, Washington, D.C., (March 7, 2007).
- Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, *Hearing on Senate Bill 392 for Voter-Verified Records in Voting Systems*,

Annapolis, MD, (February 22, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, *Hearing on House Bill 18 for improving voting systems in Maryland*, Annapolis, MD, (February 1, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, *Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland*, Annapolis, MD, (February 1, 2006).
- United States Election Assistance Commission, *Hearing on Voluntary Voting Systems Guidelines*, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).
- Senate hearing: *Voting in 2004: A Report to the Nation on America's Election Process*, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
- United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, *Public Hearings on Computer Security and Transparency*, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).
- United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, *Hearing on Electronic Voting*, Washington, D.C. (July 20, 2004).
- United States House Committee on House Administration, Expert Testimony, *Hearing on Security of Electronic Voting*, Washington, D.C. (July 7, 2004).
- United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
- United States Election Assistance Commission, Expert Testimony, *Hearing on Electronic Voting Security*, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

- Juniper vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR, United States District Court, District of Delaware.
  -Expert Testimony at deposition, Baltimore, MD (June, 2013).
- Intellectual Ventures vs. Symantec and Trend, Case # 12-CV-1581-LPS, United States District Court, District of Delaware.
  -Expert Testimony at deposition, Baltimore, MD (May, 2013).
- Prism Technologies. v. Adobe Systems Inc., Case # 8:10-cv-00220-LES-TDT, United States District Court, District of Nebraska.
  -Expert Testimony at deposition, Baltimore, MD (August, 2012).
- Finjan Inc. vs. McAfee, Inc., Case # 10-593 (GSM), United States District Court, District of Delaware.
  -Expert Testimony at deposition, Washington, DC (June, 2012).
- Avaya Inc. vs. Telecom Labs Inc,. TeamTLI.com Corp., and Continuant Technologies, Case # 3:06-cv-02490 (GEB), United States District Court, District of New Jersey.
  - Expert Testimony at deposition, Newark, NJ (August, 2011).
- Lear Automotive vs. Johnson Controls Inc (JCI), Case # 04-CV-73461, United States District Court, Eastern District of Michigan.

    - Expert Testimony at trial, Detroit, MI (February, 2011).
    - Expert Testimony at deposition, Baltimore, MD (December, 2005).
- TecSec Inc vs. International Business Machines Corporation, Case # 1:10-CV 115 LMB/TCB, United States District Court, Eastern District of Virginia.
    - Expert Testimony at deposition, Newark, NJ (November, 2010).
- Echostar Satellite Corporation vs. NDS Group, Case # SA CV 03-950 DOC(JTL), United States District Court, Central District of California.
    - Expert Testimony at trial, Santa Ana, CA (April, 2008).
    - Expert Testimony at deposition, Santa Ana, CA (April, 2008).
    - Expert Testimony at deposition, Baltimore, MD (October, 2007).
- Web.com Inc vs. The Go Daddy Group Inc., Case # CV07-01552-PHX-MHM, United States District Court, Arizona.
    - Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
    - Expert Testimony at deposition, Baltimore, MD (May, 2008).
- z4 Technologies vs. Microsoft & Autodesk, Case # 2:04-CV-00335-LED, United States District Court, Eastern District of Texas.
    - Expert Testimony at trial, Tyler, TX, (April, 2006).
    - Expert Testimony at deposition, Washington DC (January, 2006).
- Linda Schade vs. Linda Lamone et. al., *Trial on the Legality of Paperless Voting Machines in Maryland*.
    - Expert Testimony at trial, Annapolis, MD (August 25, 2004).

Awards

- **Fulbright Scholar** in Israel at Tel Aviv University, academic year 2010-2011.
- 2009, **Google Research Award**, *Securing Medical Records on Smartphones.*
- Chosen as one of **54 favorite people, places and things in Jewish Baltimore**, Baltimore Jewish Times, February 22, 2008.
- 2007 Award for Outstanding Research in Privacy Enhancing Technologies, for *Security Analysis of a Cryptographically-Enabled RFID Device* (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2005 **Best Student Paper Award** at the 14th USENIX Security Symposium, *Security Analysis of a Cryptographically-Enabled RFID Device* (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2004 **Electronic Frontiers Foundation** *Pioneer Award*.
- **Baltimorean of the Year**, Baltimore Magazine, January, 2004.
- 2001 **Index on Censorship** *Freedom of Expression Award* for the Best Circumvention of Censorship for the Publius project.
- 2000 **Best Paper Award** at the 9th USENIX Security Symposium, *A robust, tamper-evident and censorship-resistant web publishing system* (with Marc Waldman and Lorrie Cranor).
- 1999 **Best Paper Award & Best Student Paper Award** at the 8th USENIX Security Symposium, *The Design and Analysis of Graphical Passwords* (with Ian Jermyn, Alain Mayer, Fabian Monrose, and Michael K. Reiter).
- 1996 Co-author of **Best Student Paper**, *Building Systems that Flexibly Control Downloaded Executable Content*, at the 6th USENIX UNIX Security Symposium. Student:

Trent Jaeger.
- 1992 National Science Foundation Fellowship - Summer Institute in Japan
- 1986 Branstrom Prize, University of Michigan

Technical Advisory Boards

Current Positions

- Oculis Labs
    - Provide security from the computer screen to the user's eyes by tracking their eye movements with a camera.
- Riskive
    - Provide security for social networking

Past Successful Technical Advisory Board Positions

- Arbor Networks
    - Acquired by Danaher, August, 2010.
- Authentica
    - Acquired by EMC Corporation, March, 2006.
- Fortify Software
    - Acquired by Hewlett Packard, September 2010.
- Gilian Technologies
    - Acquired by Breach Security, Inc, July, 2004.
- Hx Technologies
    - Acquired by MEDecision, May, 2009.
- Indigo Security
    - Acquired by Tablus, February, 2005.
- NeoPath Networks
    - Acquired by Cisco, April, 2007.
- Netscaler
    - Acquired Citrix Systems, August, 2005.
- SiteAdvisor
    - Acquired by McAfee, April, 2006.
- Tablus
    - Acquired by EMC Corporation, August, 2007.