

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:** Ian Miers, JHU
- **Doctoral Thesis Advisor:** Gary Truslow, JHU
- **Doctoral Thesis Advisor:** Christina Garman, JHU
- **Doctoral Thesis Advisor:** Paul Martin, JHU
- **Doctoral Thesis Advisor:** Michael Rushanan, JHU
- **Doctoral Thesis Advisor:** Ayo Akinyele, JHU (December, 2013)
- **Doctoral Thesis Advisor:** Matthew Pagano, JHU (August, 2013)
- **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 Monroe, New York University (April, 1999).
- **Dissertation Committee:** Mike Just, Carleton University (November, 1998)

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*

- 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

- Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy - SoK Track (May, 2014).
- Christina Garman, Matthew Green, Ian Miers, Aviel D. Rubin, *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity*, 1st Workshop on Bitcoin Research (March, 2014).
- 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).

- 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).

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.