Dr. Matthew Green

Summary

Assistant Professor of computer science and author of numerous peer-reviewed conference papers and journal articles. Recognized internationally as an expert in the fields of cryptography and computer security. Expertise and experience includes virtual machines, computer backup, disaster recovery, and distributed storage. Experienced as a testifying expert witness and litigation consultant includes court cases involving issues ranging from patent infringement and validity to mobile devices and operating system software including theft of copyrighted source code to computer security, interception of encrypted signals, virtual machines, and backup technology.

Work Experience

Johns Hopkins University, *Assistant Professor*, July 2015 – present; *Assistant Research Professor*, Sep 2010 – June 2015; *Instructor*, Spring 2009

Grant. PI. Google ATAP. Secure cryptographic co-processor. Amount: $108,000.

Grant. Co-PI. Mozilla. Analysis of Cryptographic Protocols. Amount: $68,000, .

Grant. Co-PI. Mozilla. Scientific Analysis of the TLS protocol. Amount: $74,000, .

Grant. Co-PI, National Science Foundation award CNS-1010928, "Self Protecting Electronic Medical Records". Amount: $1,733,881.

Grant. Investigator, Office of Naval Research, $680,000. Automating the development of cryptographic protocols.

Grant. Co-PI, DARPA PROgramming Computation on EncryptEd Data (PROCEED). Amount: $344,000.

Grant. Senior Personnel, Department of Health and Human Services Strategic Healthcare Information Technology Advanced Research Projects on Security (SHARPS), Research Focus Area: Security of Health Information Technology. Amount: $1,600,399.

Instructor for Practical Cryptographic Systems (Spring 2009, 2010, 2011, 2012, 2013, 2014), which examines the issues surrounding the design and evaluation of industrial cryptographic products, and the ways that these systems fail in practice

Cryptography Engineering, *Owner*, Jan 2012-present

Scientific consulting work, largely related to data security and encryption

Cryptography Engineering Current Client List

- Akamai
- CipherCloud Inc.

- Content Guard v. Samsung
- Dunbar
- Microstrategy Inc.
- PNC Bank
- Stach & Liu
- Knobbe Martens
- Venable LLP
- Blackberry
- US Federal Reserve Bank of New York
- Xsette

Barr Group, *Consulting Chief Scientist,* Feb 2012-present

Technical consultant to embedded systems developers and attorneys

Barr Group Client List

- Acacia Research Group
- Advanced Auctions v. Ebay
- Appistry
- Brainscope
- CCE Consolidated Cases
- Edward Selmani and Nevila Celaj
- Evolutionary Intelligence
- Ford
- Hagens Berman Sobol Shapiro LLP
- Knology
- Mederi
- Rembrandt IP Management
- Smartphone LLC
- Symantec

Zeutro LLC, *Founder,* July 2010 – present

Functional encryption technology development

Harbor Edge Group, *Partner,* Jan 2010 – Jan 2012

Expert witness and litigation support.

Harbor Edge Group Client List

- Aristocrat
- Bell ExpressVu
- McAfee

Independent Security Evaluators (ISE), *CTO,* Apr 2005 – Sep 2011

White hat hacking and independent evaluation of cryptography-based digital security systems

Partial ISE Client List

- Adobe Systems
- Barnes & Noble
- Bell ExpressVu
- Brother Industries
- Dunbar
- MediData Solutions
- Motorola
- Qualcomm
- Riverbed Technologies
- Samsung
- SecurityFirst Corporation
- Symbol Technologies
- Walt Disney Publishing
- Symbol Technologies

AT&T Labs, *Senior Technical Staff Member*, Jun 1999 – Jun 2003; *Contractor,* Summer 1998 – May 1999

Advanced research in telecommunications, IP-based telephony, distributed storage, and virtual machines including development of software for desktop and mobile devices, a secure text messaging system for mobile devices, and AT&T's Interactive Voice Response (IVR) system, and researching technology transfer for audio coding, secure content delivery, and content distribution network

Advisory Board Experience

Open Crypto Audit Project, *Co-Founder and Board of Directors***,** October 2013-present

CipherCloud, *Technical Advisory Board*, June 2015-present

Linux Foundation Core Infrastructure Initiative, *Technical Advisory Board*, June 2014-present

Mozilla Cybersecurity Delphi, *Technical Advisory Board,* June 2014-present

Expert Witness Engagements

Multiple current engagements involving patent litigation and related to Android, iOS, WiFi hotspots, and other mobile devices/technologies. A sample of public engagements includes those below:

Testimony at Trial

Videotron, et.al. v. **Bell ExpressVu** (security of satellite TV), Quebec Superior Court, 13-14 Dec 2011

Testimony at Deposition

Keith Dunbar v. Google, Inc. (class action), U.S. District Court for the Eastern District of Texas. Case #5:10CV00194

Keith Dunbar v. Google, Inc. (class action), U.S. District Court for the Northern District of California. Case $5:12-cv-003305-LHK.

SmartPhone Technologies LLC v. HTC Co., Ltd.., U.S. District Court for the Eastern District of Texas. Case # 6:10-cv-00580-LED.

SmartPhone Technologies LLC v. Huawei Technologies Co., Ltd.., U.S. District Court for the Eastern District of Texas. Case #6:12-cv-00245

SmartPhone Technologies LLC v. ZTE USA, U.S. District Court for the Eastern District of Texas. Case #6:12-cv-00245

Michael Houlf v. Toyota Motor North America, Inc. et al, California Central District Court. Case # 2:2012cv04054

Veeam v. **Symantec,** Inter Partes Review IPR2013-00150 (3 separate depositions)

Evolutionary Intelligence v. Apple et al., Inter Partes Review.

Moore v. Apple Inc., California Northern District Court, Case No. 5:14-cv-02269-LHK

Consulting

No Magic, Inc. v. Thales e-Security, Inc., Texas Eastern District Court, Case No. 2:15-cv-00945

Farstone Technology, Inc. v. Apple Inc., Central District of California, Case No. 8:13-cv-01537

HID Global Corporation Assa Abloy AB v. Kwikset Corporation, U.S. District Court for the Central District of California, Case No. 8:14-cv-00947-CJC-DFM

MyFord Touch Consumer Litigation, U.S. District Court, Northern District of California. Case # CV 13-3072-**EMC**

MAZ vs. **Blackberry Inc.** U.S. District Court, District of Delaware. Case #1:13-cv-00304.

Advanced Auctions LLC v. eBay Inc., California Southern District Court. 3:2013cv00360

Edward Selmani and Nevila Celaj v. Toyota Motor Corp. et al. Ontario Superior Court of Justice.

Appistry, Inc. v. Amazon.com, Inc. et al., Missouri Eastern District Court. Case # 4:2013cv02547

Evolutionary Intelligence v. Apple et al., Inter Partes Review.

ContentGuard Holdings v Amazon.com et al (**Samsung),** Texas Eastern District Court. Case # 2:2013cv01112

Symbol Technologies, et. al. v. Aruba Networks, U.S. District Court for the District of Delaware. Case #07-519-JJFF

DataSci v. **Medidata Solutions,** U.S. District Court for the District of Delaware. Case #09-cv-01611-MJG

TecSec v. International Business Machines Corp. (IBM), U.S. District Court for the Eastern District of Virginia, Alexandria Division. Case #1:10-CV 115

PACid Group v. 2Wire, **Brother Industries, et. al.,** U.S. District Court for the Eastern District of Texas. Case #6:08-cv-00498

Manard, et.al. v. **Knology**, U.S. District Court for the Middle District of Georgia. Case #4:10-CV-15

SmartPhone Technologies LLC v. Apple, U.S. District Court for the Eastern District of Texas. Case #6:10-cv-00074

Smartphone Technologies LLC v. Huawei Technologies Co., Ltd., U.S. District Court for the Eastern District of Texas, Tyler Division. Case #6:12-cv-00245

Smartphone Technologies LLC v. ZTE Corporation, U.S. District Court for the Eastern District of Texas, Tyler Division. Case #6:12-cv-350

Rembrandt IP Management v. Facebook and AddThis

Dunbar v. Google (class action), U.S. District Court for Eastern Texas

IGT v. **Aristocrat**, Case No. SACV10-1748JVS (MLGX), C.D. California

Finjan Inc. vs. **McAfee, Inc**. et al., Case No. 10-593 (GMS), D. Delaware.

Patents

Issued

Method and Apparatus for Limiting Access to Sensitive Data. U.S. Patent No. 7,840,795

Method for Content-Aware Redirection and Content Renaming. U.S. Patent No. 6,954,456

Method for Content-Aware Redirection and Content Renaming. U.S. Patent No. 8,306,022

Unidirectional Proxy Re-encryption. U.S. Patent No. 8,094,810

Systems and Methods for Secure Workgroup Management and Communication. U.S. Patent No. 8,656,167

Pending

Outsourcing the Decryption of Functional Encryption Ciphertexts. U.S. Patent Pub. No. 2012/0300936

Degrees

Computer Science

Ph.D. in Computer Science, *Johns Hopkins University*, Nov 2008
Cryptography for Secure and Private Databases: Enabling Practical Data Access without Compromising Privacy
Advisor: Susan Hohenberger, Ph.D.

Master of Science in Computer Science. *Johns Hopkins University*, Dec 2005

Bachelor of Arts in Computer Science. *Oberlin College*, May 1998

Music

Bachelors of Music: Technology in Music and Related Arts. *Oberlin Conservatory of Music*, May 1999

Awards

Award for Outstanding Research in Privacy Enhancing Technologies (PET Award), 2007

Publications

Conference Papers

Matthew Green, Ian Miers. "Forward Secure Asynchronous Messaging from Puncturable Encryption". To appear in *IEEE Symposium on Security and Privacy (Oakland) 2015*.

Eli Ben-Sasson, Allesandro Chiesa, Matthew Green, Eran Tromer, Madars Virza. "Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs". In *IEEE Symposium on Security and Privacy (Oakland) 2015.*

Eli Ben-Sasson, Allesandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza. "Zerocash: Practical Decentralized Anonymous E-Cash from Bitcoin". In *IEEE Symposium on Security and Privacy (Oakland) 2014.*

S. Checkoway, M. Fredrikson, R. Niederhagen, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskeiwicz, H. Shacham. "On the Practical Exploitability of Dual EC in TLS Implementations". In Usenix Security 2014.

Christina Garman, Matthew Green, Ian Miers. "Decentralized Anonymous Credentials". In *Network and Distributed Systems Symposium (NDSS '14).*

Christina Garman, Matthew Green, Ian Miers, Avi Rubin. "Rational Zero: Economic Security for Zerocoin with everlasting anonymity". To appear in *Bitcoin Workshop 2014*.

J. Ayo Akinyele, Matthew Green, Susan Hohenberger. "Using SMT Solvers to Automate Design Tasks for Encryption and Signature Schemes". In *ACM Conference on Computer and Communications Security (CCS '13)*.

Ian Miers, Christina Garman, Matthew Green, Avi Rubin. "Zerocoin: Anonymous Distributed e-Cash from Bitcoin". In *IEEE Symposium on Security and Privacy (Oakland) 2013.*

J. Ayo Akinyele, Matthew Green, Susan Hohenberger, Matthew Pagano. "Machine-Generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature. Schemes". In *ACM Conference on Computer and Communications Security (CCS '12).*

Ian Miers, Matthew Green, Chris Lehman, Avi Rubin. "Vis-a-Vis Cryptography: Private and Trustworthy In-Person Certifications". In *ACM Conference on Computer and Communications Security (CCS '12).*

David Cash, Matthew Green, Susan Hohenberger. ”New Definitions and Separations for Circular Security“. In *15th International Conference on Practice and Theory of Public Key Cryptography (PKC '12)*. Springer, 2012.

J. A. Akinyele, M. W. Pagano, M. Green, C. Lehmann, Z. Peterson, and A. Rubin. "Securing electronic medical records using attribute-based encryption on mobile devices." In *1st ACM CCS-SPSM*, 2011.

Matthew Green, Susan Hohenberger, and Brent Waters. "Outsourcing the decryption of ABE cipher-texts." In *Proceedings of the 20th USENIX conference on Security (SEC'11)*, pages 34–34, Berkeley, CA, USA, 2011. USENIX Association.

Matthew D. Green and Aviel D. Rubin. "A research roadmap for healthcare IT security inspired by the PCAST health information technology report." In *Proceedings of the 2nd USENIX conference on Health security and privacy (HealthSec '11)*, Berkeley, CA, USA, 2011. USENIX Association.

Matthew Green and Susan Hohenberger. "Oblivious transfer from simple assumptions." In *Theory of Cryptography Conference (TCC '11)*. Springer, 2011.

Matthew Green. "Secure blind decryption." In *14th International Conference on Practice and Theory of Public Key Cryptography (PKC '11)*. Springer, 2011.

Jae Hyun Ahn, Matthew Green, and Susan Hohenberger. "Synchronized aggregate signatures." In *ACM Conference on Computer and Communications Security (CCS '10)*. ACM Press, 2010.

Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, and Michael Østergaard Pedersen. "Practical short signature batch verification." In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009: CT-RSA 2009*, volume 5473 of LNCS, pages 309–324. Springer, 2009.

Scott Coull, Matthew Green, and Susan Hohenberger. "Controlling access to an oblivious database using stateful anonymous credentials." In *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography (PKC 2009)*, volume 5443 of LNCS, pages 501– 520. Springer, 2009.

Matthew Green and Susan Hohenberger. "Universally composable adaptive oblivious transfer." In *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '08),* volume 5350 of LNCS. Springer, 2008.

Matthew Green and Susan Hohenberger. "Blind identity-based encryption and simulatable oblivious transfer." In *Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '07)*, volume 4833 of LNCS, pages 265–282. Springer, 2007.

Matthew Green and Giuseppe Ateniese. "Identity-based proxy re-encryption." In *Proceedings of the 5th International Conference on Applied Cryptography and Network Security (ACNS '07)*, volume 4521 of LNCS, pages 288–306, 2007.

Stephen Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel Rubin, and Michael Szydlo. "Security analysis of a cryptographically-enabled RFID device." In *Proceedings of USENIX Security '05*. USENIX Association, 2005. Winner of Best Student Paper Award.

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. "Improved proxy re-encryption schemes with applications to secure distributed storage." In *The 12th Annual Network and Distributed System Security Symposium (NDSS '05)*. The Internet Society, 2005.

Andrea Basso, Charles D. Cranor, Raman Gopalakrishnan, Matthew Green, Charles R. Kalmanek, David Shur, Sandeep Sibal, Cormac J. Sreenan, and Jacobus E. van der Merwe. "PRISM, an IP-based architecture for broadband access to TV and other streaming media." In *IEEE International Workshop on Network and Operating System Support for Digital Audio and Video*, 2000.

Journal Papers

J. Ayo Akinyele, Matthew Green, Susan Hohenberger, Matthew Pagano. "Machine-Generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature. Schemes". To appear in *Journal of Computer Security.*

Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, Aviel D. Rubin. "Charm: a framework for rapidly prototyping cryptosystems". In *Journal of Cryptographic Engineering.* June 2013, Volume 3, Issue 2, pp 111-128.

Matthew Green. "The Threat in the Cloud". In *IEEE Security & Privacy Magazine (Spring 2013)*.

Scott Coull, Matthew Green, Susan Hohenberger. "Access Controls for Oblivious and Anonymous Systems". In *ACM Transactions on Information and System Security (TISSEC)*.

Scott Coull, Matthew Green, and Susan Hohenberger. "Controlling access to an oblivious database using stateful anonymous credentials." *ACM Transactions on Information and System Security (TISSEC)*, 2011.

Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green. "Security through legality." *Communications of the ACM*, 49(6):41–43, 2006.

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. "Improved proxy re-encryption schemes with applications to secure distributed storage." *ACM Transactions on Information and System Security (TISSEC)*, 9(1), February 2006.

Charles D. Cranor, Matthew Green, Chuck Kalmanek, David Shur, Sandeep Sibal, Jacobus E. Van der Merwe, and Cormac J. Sreenan. "Enhanced streaming services in a content distribution network." *IEEE Internet Computing*, 05(4):66–75, 2001.

Media Pieces

Matthew Green, Blog: *A Few Thoughts on Cryptographic Engineering*. Blog Archive available at http://blog.cryptographyengineering.com/. Sep 2011 – present

Matthew Green, The Daunting Challenge of Secure E-mail, *The New Yorker*, November 2013. Archive available at: http://www.newyorker.com/tech/elements/the-daunting-challenge-of-secure-e-mail

Matthew Green, Is Apple Picking a Fight with the U.S. Government?, Slate, September 2014. Archive available at http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html