DAVID WAGNER
Associate Professor of Computer Science
University of California, Berkeley

Education

Ph.D. in Computer Science. U.C. Berkeley, 2000. Advisor: Professor Eric A. Brewer.
Dissertation title: *Static analysis and computer security: New techniques for software assurance.*

M.S. in Computer Science. U.C. Berkeley, 1999. Advisor: Professor Eric A. Brewer.
Thesis title: *Janus: an approach for confinement of untrusted applications.*

A.B. in Mathematics. Princeton University, 1995. Magna cum laude, 3.8 GPA.
Undergraduate thesis title: *The security of MacGuffin.*

Employment

Associate professor (2006–). U.C. Berkeley, EECS Department. Advising nine Ph.D. students, teaching undergraduate and graduate classes, serving as PI and co-PI on several grants.

Assistant professor (2000–2006). U.C. Berkeley, EECS Department. Founded several research groups.

Graduate student researcher (1995–2000). U.C. Berkeley, EECS Department. Co-founder of U.C. Berkeley's ISAAC security research group, which has made substantial contributions in computer, network, and wireless security and in online privacy.

Consultant (1995–). Occasional independent security consulting. My reviews have helped change a million-dollar design decision in a cellphone standards committee, influenced a Fortune 500 company's data security architecture, uncovered serious vulnerabilities in commercial webservers intended for secure e-commerce, and helped transfer my software security research into shipping products.

Honors and awards

Recent awards:
2002: ACM Dissertation Award (Honorary Mention)
2002: Computer Science Division Information Technology Faculty Award
2002: CRA Digital Government Fellow
2002: Named one of Popular Science's Brilliant 10
2003: Alfred P. Sloan Research Fellow
2003: Named Information Security Magazine's Best Academic Researcher
2004: Diane S. McEntyre Award for Excellence in Teaching
2006: U.C. Berkeley Distinguished Teaching Award

Recent fellowships:
2000: Okawa Foundation Research Grant
2001: NSF CAREER
2002: Microsoft CITRIS Research Grant
2003: Microsoft CITRIS Research Grant
2004: Microsoft CITRIS Research Grant
2005: IBM Faculty Award

Teaching

Fall 1998:
CS261: Security in Computer Systems (co-taught with Ian Goldberg and Prof. Eric Brewer)
(with major curriculum revisions; class projects led to publications at Mobicom '99 and NDSS 2000)

Fall 2000:
CS261: Security in Computer Systems
(with major curriculum updates; class projects led to papers at Mobicom 2001, Usenix Security 2001, & ICICS 2001)

Spring 2001:
CS70: Discrete Mathematics (co-taught with Prof. Manuel Blum)

Fall 2001:
CS70: Discrete Mathematics

Spring 2002:
CS276: Cryptography (co-taught with Prof. Luca Trevisan)
CS294-5: Analysis and Design of Cryptographic Primitives
CS298-36: Digital Defense: Issues in Security, Privacy and Critical Infrastructure Protection
(co-organized with Dr. Darlene Fisher, Dr. Vern Paxson, Prof. Shankar Sastry)

Fall 2002:
CS261: Security in Computer Systems
(class projects led to a publication at Usenix Security 2003)

Spring 2003:
CS170: Efficient Algorithms and Intractable Problems

Fall 2003:
CS70: Discrete Mathematics

Spring 2004:
CS276: Cryptography

Fall 2004:
CS261: Computer Security

Spring 2005:
CS70: Discrete Mathematics (co-taught with Prof. Mike Clancy)

Fall 2005:
CS161: Computer Security (co-taught with Profs. Anthony Joseph, Doug Tygar, Umesh Vazirani)

Spring 2006:
CS276: Cryptography

Presentations and talks

Conference talks:
Full-length presentations at NDSS '96, USENIX Electronic Commerce '96, COMPCON '97, CRYPTO '97, FSE '98 (three talks), FSE '99, CRYPTO '99, AES '99, NDSS 2000, EUROCRYPT 2000, ASIACRYPT 2000 (two talks), IEEE S&P 2001, CRYPTO 2002, ACM CCS 2002, ISC 2003, FSE 2004, TACAS 2004, CCS 2004, SASN 2004, SPIN 2005, SecCo 2005, SECURECOMM 2005, and PLAS 2006.
Also numerous other short work-in-progress and rump session talks.

Invited lectures:
Nov 1998: CTIA Wireless Security Conference
Jul 1999: Intl. Workshop on Cryptographic Techniques and E-Commerce, Hong Kong (CryptTEC '99)
Sep 1999: Xerox PARC Forum
Jul 2001: Static Analysis Symposium (SAS 2001)
Jan 2002: IPAM Contemporary Methods in Cryptography
Feb 2002: UC Berkeley seminar on Digital Defense
Apr 2002: Federal Communications Commission, Engineering and Technology Tutorial
Apr 2002: The National Academies' Workshop on the Mathematical Sciences' Role in Homeland Security
Aug 2002: Selected Areas in Cryptography (SAC 2002)
Mar 2003: Berkeley in Silicon Valley Symposium
Mar 2003: UC Berkeley's EECS Colloqium, Distinguished Lecture Series
Jun 2003: Software Security Workshop
Sep 2003: NAE Symposium on Frontiers of Engineering
Oct 2003: ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2003)
Nov 2003: Technology and Policy (UCB Law275T)
Feb 2004: Fast Software Encryption (FSE 2004)
Aug 2005: SPIN 2005 and SecCo 2005
Sep 2005: SECURECOMM 2005
Feb 2006: Berkeley EECS Annual Research Symposium (BEARS 2006)
Jun 2006: ACM Workshop on Programming Languages and Analysis for Security (PLAS 2006)
Aug 2006: CRYPTO 2006

Invited panel presentations:
Nov 1998: ACM Computer & Communications Security (CCS '98)
Jun 2001: Computer Security Foundations Workshop (CSFW 2001)
Oct 2001: Special Computing Workshop: Computing and Security
Jun 2002: ACM Symposium on Access Control Models and Technologies (SACMAT 2002)
Jun 2002: IEEE INFOCOM 2002
Oct 2003: Information Security Conference (ISC 2003)
Apr 2004: Computers, Freedom, and Privacy (CFP 2004)
Mar 2005: Pervasive Computing (Percom 2005)
May 2005: IEEE Security & Privacy 2005

Service

Program committee chaired:
Program co-chair, IEEE Security & Privacy 2003
Program co-chair, IEEE Security & Privacy 2004

Program committee memberships:
Usenix Security 1998
NDSS 2000
CRYPTO 2000
NDSS 2001
IEEE S&P 2001
EUROCRYPT 2001
Usenix Security 2001
RAID 2002
FSE 2003
Usenix Security 2003
ACM SASN 2003

Usenix Security 2004
CRYPTO 2004
OSDI 2004
ACM CCS 2005
Usenix Security 2006
IEEE S&P 2006
Electronic Voting Technology Workshop 2006

Journal positions:
Editorial Board, ACM Transactions on Information and System Security (TISSEC), 2005–2006

Other miscellaneous refereeing (journals):
Journal of Cryptology
IEEE Internet Computing
IEEE Transactions on Information Theory
IEEE Transactions on Computers
IEEE Transactions on Dependable and Secure Computing
Information Processing Letters
International Journal of Information Security
Journal of Computer Systems Science and Engineering
British Telecom Technical Journal

Other miscellaneous refereeing (conferences):
SOSP 1999
FSE 2001
FSE 2002
IFIP TCS 2002
OSDI 2002
EUROCRYPT 2002
Usenix Security 2002
SOSP 2003
IEEE IT 2003
ACM Sensys 2003
ACISP 2004
SIGGRAPH 2004
USENIX 2005
Usenix Security 2005

Other refereeing (miscellaneous):
Panelist, NSF ITR 2002 competition, evaluating grant proposals
Panelist, NSF CyberTrust 2004 competition, evaluating grant proposals
Panelist, NSF CAREER 2005 competition, evaluating grant proposals

Steering committees:
2001–2005: ISOC Symposium on Network & Distributed System Security (NDSS)
2003: DIMACS Workshop on Software Security
2003–2004: DIMACS Workshop on Mobile and Wireless Security
2003–2006: DIMACS Special Focus on Security

Advisory:
2004: Member, Security Peer Review Group, Federal Voting Assistance Program (FVAP)
2004: Technical advisor, ACLU Touchscreen Voting Committee
2004–now: Member, California Secretary of State's Voting Systems Technology Assessment Advisory Board
2005: Member, USACM Voter Registration Database Study
2005: Member, Alameda County's Equipment Advisory Board
2005–now: Member, Alameda County's Election Advisory Committee

2007–now: Technical and Security Advisor, Overseas Vote Foundation

Other service to the research community:
Participant, NSF, DARPA, and ISAT study groups
Expert witness; declarations submitted to state and federal courts and governmental agencies on the impact of law and policy on cryptography and academic freedom
Participant, IETF, NIST, and IEEE standards efforts (IPSec, TLS, AES, 802.11, and CFRG)

UC Berkeley committees:
Jan 1999: Student member, EECS Graduate admissions committee
Jan 2001: EECS Graduate admissions committee
Mar 2001: EECS Prelims examiner in Operating Systems
Nov 2001: EECS Prelims examiner in Operating Systems
Jan 2002: EECS Graduate admissions committee
Sep 2002: EECS Prelims examiner in Operating Systems
Jan 2003: EECS Graduate admissions committee
Jan 2004: EECS Graduate admissions committee
Sep 2004: EECS Prelims examiner in Operating Systems
Jan 2005: EECS Graduate admissions committee
Sep 2005: EECS Prelims examiner in Operating Systems
Feb 2006: EECS Prelims examiner in Operating Systems
2002–2005: UC Berkeley Committee on Academic Freedom

Advising

Current Ph.D. students:
Karl Chen
Arel Cordero
Robert Johnson
Chris Karlof
Adrian Mettler
David Molnar
Naveen Sastry
Umesh Shankar
Ka-Ping Yee

Ph.D. dissertations supervised:
2004: Hao Chen (Asst. Prof., U.C. Davis). "Lightweight Model Checking for Improving Software Security."

M.S. theses supervised:
2004: Jason Waddle (developer, Google): "Formalizing Secure Computation for Embedded Systems."
2005: Ben Schwarz, "Model Checking An Entire Linux Distribution for Security Violations."

Past undergraduate research advising:
1997–1998: Michael Kaminsky (Ph.D., MIT; now at Intel Research)
2001: Mark Goodman
1999–2001: Tal Garfinkel (Ph.D. student, Stanford; won honorable mention, CRA Outstanding Undergraduate)
2000–2001: Thu Trinh
2001–2002: Michael Manapat
2001–2002: Lea Kissner (Ph.D. student, CMU)
2001–2002: Paolo Soto (developer, Secure Software)
2001–2002: James Donald (Ph.D. student, Princeton)
2002–2003: David Schultz (Ph.D. student, MIT; won honorable mention, CRA Outstanding Undergraduate)

2003–2004: Geoff Morrison (developer, Fortify Software)
2003–2004: Jacob West (developer, Fortify Software)
2003–2004: Jeremy Lin
2004–2005: Wei Tu (won honorable mention, CRA Outstanding Undergraduate)
2004–2006: Chris Crutchfield (Ph.D. student, MIT)
2004–2006: David Turner (Ph.D. student, U.C¿ Berkeley)

Publications

The text of all papers listed below may be found online at http://www.cs.berkeley.edu/~daw/papers/.

Books

"System Security: A Management Perspective." David L. Oppenheimer, David Wagner, and Michele D. Crabb. Booklet #3 from the SAGE Short Topics in System Administration Series. USENIX Association, ISBN 1-880446-85-5, March 1997, 91 pages.

"The Twofish Encryption Algorithm: A 128-Bit Block Cipher." Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. John Wiley & Sons, ISBN 0-471353-81-7, April 1999, 186 pages.

Refereed Archival Journal Publications

"TAZ Servers and the Rewebber Network: Enabling Anonymous Publishing on the World Wide Web." Ian Goldberg and David Wagner. First Monday, vol. 3 no. 4, April 1998.

"Side Channel Cryptanalysis of Product Ciphers." John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Journal of Computer Security, vol 8, no 2–3, pp. 141–158, 2000.

"On The Structure of Skipjack." Lars R. Knudsen and David Wagner. Discrete Applied Mathematics, volume 111, issue 1–2, 15 July 2001, pp.103–116, special issue on coding theory and cryptology, C. Carlet (ed.).

"Security flaws in 802.11 data link protocols." Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. *Communications of the ACM, vol. 46 no. 5, May 2003, special issue on wireless networking security.*

"Secure Routing in Sensor Networks: Attacks and Countermeasures." Chris Karlof and David Wagner. Ad Hoc Networks, vol. 1 no. 2–3, September 2003, special issue on sensor network applications and protocols.

"Secure Verification of Location Claims." Naveen Sastry, Umesh Shankar, and David Wagner. CryptoBytes volume 6, no 1, Spring 2004, RSA Labs.

"Security in wireless sensor networks." *Adrian Perrig, John Stankovic, and David Wagner. Communications of the* ACM, 47(6), June 2004, Special Issue: Wireless sensor networks, pp.53–57.

"Analyzing internet voting security." David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. Communications of the ACM, 47(10), October 2004, Special issue: The problems and potentials of voting systems, pp.59–64.

"A class of polynomially solvable range constraints for interval analysis without widenings." Zhendong Su and David Wagner. Theoretical Computer Science, November 21, 2005, pp.122–138.

"Security considerations for incremental hash functions based on pair block chaining." Raphael C.-W. Phan and David Wagner. Computers & Security, 25(2), 2006, pp.131–136.

Refereed Conference Publications

"A "bump in the stack" encryptor for MS-DOS systems." David Wagner and Steven M. Bellovin. 3rd ISOC Symposium on Network & Distributed System Security (NDSS '96), February 23, 1996.

"A secure environment for untrusted helper applications: confining the wily hacker." Ian Goldberg, David Wagner, Randi Thomas, and Eric A. Brewer. 6th USENIX Security Symposium, July 24, 1996. Received **best paper** award.

"Analysis of the SSL 3.0 protocol." David Wagner and Bruce Schneier. 2nd USENIX Workshop on Electronic Commerce, November 19, 1996. Received **best student paper** award.

"Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, GOST, RC4, SAFER, and Triple-DES." John Kelsey, Bruce Schneier, and David Wagner. Advances in Cryptology—CRYPTO '96, August 20, 1996.

"Cryptanalysis of the Cellular Message Encryption Algorithm." David Wagner, Bruce Schneier, and John Kelsey. Advances in Cryptology—CRYPTO '97, August 21, 1997.

"Secure Applications of Low-Entropy Keys." John Kelsey, Bruce Schneier, and David Wagner. 1st Information Security Workshop (ISW '97), September 18, 1997.

"Privacy-enhancing technologies for the Internet." Ian Goldberg, David Wagner, and Eric A. Brewer. IEEE COMPCON '97, February 1997.

"Protocol Interactions and the Chosen Protocol Attack." John Kelsey, Bruce Schneier, and David Wagner. 5th International Security Protocols Workshop, April 8, 1997.

"Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA." John Kelsey, Bruce Schneier, and David Wagner. 1st International Conference on Information and Communications Security (ICICS '97), November 13, 1997.

"Cryptanalytic Attacks on Pseudorandom Number Generators." John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. 5th Fast Software Encryption Workshop (FSE '98), February 24, 1998.

"Cryptanalysis of some recently-proposed multiple modes of operation." David Wagner. 5th Fast Software Encryption Workshop (FSE '98), February 25, 1998.

"Differential cryptanalysis of KHF." David Wagner. 5th Fast Software Encryption Workshop (FSE '98), February 25, 1998.

"Cryptanalysis of TWOPRIME." Don Coppersmith, David Wagner, Bruce Schneier, and John Kelsey. 5th Fast Software Encryption Workshop (FSE '98), February 23, 1998.

"Side Channel Cryptanalysis of Product Ciphers." John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. 5th European Symposium on Research in Computer Security (ESORICS '98), September 16, 1998.

"Cryptanalysis of SPEED (extended abstract)." Chris Hall, John Kelsey, Bruce Schneier, and David Wagner. 2nd Financial Cryptography Conference (FC '98), February 25, 1998.

"Cryptanalysis of SPEED." Chris Hall, John Kelsey, Vincent Rijmen, Bruce Schneier, and David Wagner. 5th Workshop on Selected Areas in Cryptography (SAC '98), August 18, 1998.

"Cryptanalysis of ORYX." D. Wagner, L. Simpson, E. Dawson, John Kelsey, W. Millan, and B. Schneier. 5th Workshop on Selected Areas in Cryptography (SAC '98), August 18, 1998.

"On the Twofish Key Schedule." Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. 5th Workshop on Selected Areas in Cryptography (SAC '98), August 17, 1998.

"Building PRFs from PRPs." Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Advances in Cryptology—CRYPTO '98, August 26, 1998.

"Cryptanalysis of FROG." David Wagner, Niels Ferguson, and Bruce Schneier. 2nd Advanced Encryption Standard conference (AES '99), March 23, 1999.

"Key Schedule Weaknesses in SAFER+." John Kelsey, Bruce Schneier, and David Wagner. 2nd Advanced Encryption Standard conference (AES '99), March 23, 1999.

"Performance Comparison of the AES Submissions.." Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. 2nd Advanced Encryption Standard conference (AES '99), March 22, 1999.

"New Results on the Twofish Encryption Algorithm." Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. 2nd Advanced Encryption Standard conference (AES '99), March 23, 1999.

"Mod n Cryptanalysis, with Applications Against RC5P and M6." John Kelsey, Bruce Schneier, and David Wagner. 6th Fast Software Encryption Workshop (FSE '99), March 26, 1999.

"Slide attacks." Alex Biryukov and David Wagner. 6th Fast Software Encryption Workshop (FSE '99), March 26, 1999.

"The boomerang attack." David Wagner. 6th Fast Software Encryption Workshop (FSE '99), March 26, 1999.

"Truncated Differentials and Skipjack." Lars R. Knudsen, M.J.B. Robshaw, and David Wagner. Advances in Cryptology—CRYPTO'99, August 16, 1999.

"Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)." Bruce Schneier, Mudge, and David Wagner. Secure Networking—CQRE [Secure] '99, Dusseldorf, October 1999, Springer-Verlag LNCS 1740.

"The Ninja Jukebox." Ian Goldberg, Steven D. Gribble, David Wagner, and Eric Brewer. 2nd USENIX Symposium on Internet Technologies & Systems (USITS '99), October 12, 1999.

"Improved Cryptanalysis of Rijndael." Niels Ferguson, John Kelsey, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting. 7th Fast Software Encryption Workshop (FSE 2000), April 10, 2000.

"Real Time Cryptanalysis of A5/1 on a PC." Alex Biryukov, Adi Shamir, and David Wagner. 7th Fast Software Encryption Workshop (FSE 2000), April 10, 2000.

"A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities." David Wagner, Jeffrey S. Foster, Eric A. Brewer, and Alexander Aiken. 7th ISOC Symposium on Network & Distributed System Security (NDSS 2000), February 3, 2000.

"Practical Techniques for Searches on Encrypted Data." Dawn Song, David Wagner, and Adrian Perrig. 2000 IEEE Symposium on Security and Privacy, May 14, 2000.

"Advanced Slide Attacks." Alex Biryukov and David Wagner. Advances in Cryptology—EUROCRYPT 2000, May 18, 2000.

"Security Weaknesses in Maurer-Like Randomized Stream Ciphers." Niels Ferguson, Bruce Schneier, and David Wagner. 5th Australasian Conference on Information Security and Privacy (ACISP 2000), July 10, 2000.

"Proofs of security for the Unix password hashing algorithm." David Wagner and Ian Goldberg. Advances in Cryptology—ASIACRYPT 2000, December 6, 2000.

"Cryptanalysis of the Yi-Lam hash." David Wagner. Advances in Cryptology—ASIACRYPT 2000, December 6, 2000.

"Intrusion Detection via Static Analysis." David Wagner and Drew Dean. 2001 IEEE Symposium on Security and Privacy, May 13, 2001.

"Intercepting Mobile Communications: The Insecurity of 802.11." Nikita Borisov, Ian Goldberg, and David Wagner. 7th ACM Conference on Mobile Computing and Networking (MOBICOM 2001), July 16, 2001.

"Timing Analysis of Keystrokes and Timing Attacks on SSH." Dawn Xiaodong Song, David Wagner, and Xuqing Tian. 10th USENIX Security Symposium, August 17, 2001.

"Detecting Format String Vulnerabilities With Type Qualifiers." Umesh Shankar, Kunal Talwar, Jeffrey S. Foster, and David Wagner. 10th USENIX Security Symposium, August 16, 2001.

"A Cryptanalysis of the High-Bandwidth Digital Content Protection System." Scott Crosby, Ian Goldberg, Robert Johnson, Dawn Song, and David Wagner. Security and Privacy in Digital Rights Management, November 5, 2001.

"Integral Cryptanalysis (Extended abstract)." Lars Knudsen and David Wagner. 9th Fast Software Encryption Workshop (FSE 2002), February 4, 2002.

"Multiplicative Differentials." Nikita Borisov, Monica Chew, Rob Johnson, and David Wagner. 9th Fast Software Encryption Workshop (FSE 2002), February 4, 2002.

"Homomorphic Signature Schemes." Robert Johnson, David Molnar, Dawn Song, and David Wagner. Topics in Cryptology—CT-RSA 2002, LNCS 2271, Springer-Verlag, February 18, 2002.

"Insecurity in ATM-based passive optical networks." Stephen Thomas and David Wagner. IEEE International Conference on Communications (ICC 2002), Optical Networking Symposium, April 29, 2002.

"Setuid Demystified." Hao Chen, David Wagner, and Drew Dean. 11th USENIX Security Symposium, August 8, 2002.

"Markov Truncated Differential Cryptanalysis of Skipjack." Ben W. Reichardt and David Wagner. Selected Areas in Cryptography: SAC 2002, August 16, 2002.

"A Generalized Birthday Problem (extended abstract)." David Wagner. Advances in Cryptology—CRYPTO 2002, August 21, 2002.

"Tweakable Block Ciphers." Moses Liskov, Ronald L. Rivest, and David Wagner. Advances in Cryptology—CRYPTO 2002, August 19, 2002.

"MOPS: An Infrastructure for Examining Security Properties of Software." Hao Chen and David Wagner. ACM Computer & Communications Security (CCS 2002), November 18, 2002.

"Mimicry Attacks on Host-Based Intrusion Detection Systems." David Wagner and Paolo Soto. ACM Computer & Communications Security (CCS 2002), November 18, 2002.

"Secure Routing in Sensor Networks: Attacks and Countermeasures." Chris Karlof and David Wagner. First IEEE International Workshop on Sensor Network Protocols and Applications (SNPA 2003), May 11, 2003.

"Private Circuits: Securing Hardware against Probing Attacks." Yuval Ishai, Amit Sahai, and David Wagner. Advances in Cryptology—CRYPTO 2003, August 20, 2003.

"Hidden Markov Model Cryptanalysis." Chris Karlof and David Wagner. Fifth Workshop on Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS 2779, September 2003.

"Secure Verification of Location Claims." Naveen Sastry, Umesh Shankar, and David Wagner. ACM Workshop on Wireless Security (WiSe 2003), September 19, 2003.

"Cryptanalysis of an Algebraic Privacy Homomorphism." David Wagner. 6th Information Security Conference (ISC 2003), October 2, 2003.

"Model Checking One Million Lines of C Code." Hao Chen, Drew Dean, and David Wagner. 11th Annual Symposium on Network & Distributed System Security (NDSS 2004), February 2004.

"The EAX Mode of Operation: A Two-Pass Authenticated-Encryption Scheme Optimized for Simplicity and Efficiency." Mihir Bellare, Phillip Rogaway, and David Wagner. 11th Fast Software Encryption (FSE 2004), February 7, 2004.

"On Compressing Encrypted Data Without the Encryption Key." Mark Johnson, David Wagner, and Kannan Ramchandran. Theory of Cryptography Conference (TCC 2004), February 21, 2004.

"A Class of Polynomially Solvable Range Constraints for Interval Analysis without Widenings and Narrowings." Zhendong Su and David Wagner. Tenth International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2004), March 31, 2004.

"Towards Efficient Second-Order Power Analysis." Jason Waddle and David Wagner. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), August 11, 2004. Received **best paper** award.

"Finding User/Kernel Pointer Bugs With Type Inference." Rob Johnson and David Wagner. 13th USENIX Security Symposium, August 12, 2004.

"Security Considerations for IEEE 802.15.4 Networks." Naveen Sastry and David Wagner. ACM Workshop on Wireless Security (WiSe 2004), October 1, 2004. Received **best student paper** award.

"Privacy and Security in Library RFID: Issues, Practices, and Architectures." David Molnar and David Wagner. ACM Computer & Communications Security (CCS 2004), October 2004.

"Cryptanalysis of a Provably Secure CRT-RSA Algorithm." David Wagner. ACM Computer & Communications Security (CCS 2004), October 20, 2004.

"Resilient Aggregation in Sensor Networks." David Wagner. 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004), October 25, 2004.

"Radio Frequency Id and Privacy with Information Goods." Nathan Good, David Molnar, Jennifer M. Urban, Deirdre Mulligan, Elizabeth Miles, Laura Quilter, and David Wagner. 2004 ACM Workshop on Privacy in the Electronic Society (WPES 2004), October 28, 2004.

"TinySec: A Link Layer Security Architecture for Wireless Sensor Networks." Chris Karlof, Naveen Sastry, and David Wagner. 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), November 4, 2004.

"An Analysis of PMF Based Tests for Detection of Least Significant Bit Image Steganography." Stark Draper, Prakash Ishwar, David Molnar, Vinod Prabhakaran, Kannan Ramchandran, Daniel Schonberg, and David Wagner. Information Hiding Workshop, June 8, 2005.

"Cryptographic Voting Protocols: A Systems Perspective." Chris Karlof, Naveen Sastry, and David Wagner. 14th USENIX Security Symposium, August 3, 2005.

"Fixing Races for Fun and Profit: How to abuse atime." Nikita Borisov, Rob Johnson, Naveen Sastry, and David Wagner. 14th USENIX Security Symposium, August 5, 2005.

"A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags." David Molnar, Andrea Soppera, and David Wagner. Selected Areas in Cryptography: SAC 2005, August 11-12, 2005.

"Security and Privacy Issues in E-passports." Ari Juels, David Molnar, and David Wagner. SECURECOMM 2005, September 6, 2005.

"Privacy for RFID through Trusted Computing (Short Paper)." David Molnar, Andrea Soppera, and David Wagner. WPES 2005, November 7, 2005.

"The Program Counter Security Model: Automatic Detection and Removal of Control-Flow Side Channel Attacks." David Molnar, Matt Piotrowski, David Schultz, and David Wagner. ICISC 2005, December 1, 2005.

"Model Checking An Entire Linux Distribution for Security Violations." Benjamin Schwarz, Hao Chen, David Wagner, Geoff Morrison, Jacob West, Jeremy Lin, and Wei Tu. ACSAC 2005, December 6, 2005.

"Fault Attacks on Dual-Rail Encoded Systems." Jason Waddle and David Wagner. ACSAC 2005, December 8, 2005.

"Generic On-line/Off-line Threshold Signatures." Chris Crutchfield, David Molnar, David Turner, and David Wagner. Public Key Cryptography (PKC) 2006, April 24, 2006.

"Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Mach David Molnar, Tadayoshi Kohno, Naveen Sastry, and David Wagner. 2006 IEEE Symposium on Security and Privacy, May 24, 2006.

"Private Circuits II: Keeping Secrets in Tamperable Circuits." Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Advances in Cryptology—EUROCRYPT 2006, May 31, 2006.

"Preventing Secret Leakage from fork(): Securing Privilege-Separated Applications." Umesh Shankar and David Wagner. 2006 IEEE International Conference on Communications (Network Security and Information Assurance Symposium at ICC 2006), June 13, 2006.

"The Role of Dice in Election Audits—Extended Abstract." Arel Cordero, David Wagner, and David Dill. IAVoSS Workshop On Trustworthy Elections (WOTE 2006), June 29, 2006.

"Prerendered User Interfaces for Higher-Assurance Electronic Voting." Ka-Ping Yee, David Wagner, Marti Hearst, and Steven M. Bellovin. USENIX/ACCURATE Electronic Voting Technology Workshop, August 1, 2006.

"Designing voting machines for verification." Naveen Sastry, Tadayoshi Kohno, and David Wagner. Usenix Security 2006, August 4, 2006.

Technical Reports

"Time-lock puzzles and timed-release Crypto." Ronald Rivest, Adi Shamir, and David Wagner. MIT technical report MIT/LCS/TR-684, February 21, 1996.

"Empirical Verification of Twofish Key Uniqueness Properties." Doug Whiting and David Wagner. Counterpane technical report (Twofish #2), September 22, 1998.

"Further Observations on the Key Schedule of Twofish." Doug Whiting, John Kelsey, Bruce Schneier, David Wagner, Niels Ferguson, and Chris Hall. Counterpane technical report (Twofish #4), March 16, 1999.

Non-Refereed Conference Publications

"Twofish: a 128-bit block cipher." Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. 1st AES Candidate Conference (AES '98), August 22, 1998.

"Comments to NIST Concerning AES-modes of Operations: CTR-mode Encryption." Helger Lipmaa, Phillip Rogaway, and David Wagner. 1st NIST Modes of Operation Workshop, October 20, 2000.

"Towards a unifying view of block cipher cryptanalysis." David Wagner. 11th Fast Software Encryption (FSE 2004), February 7, 2004.

"Towards a Privacy Measurement Criterion for Voting Systems." Lillie Coney, Joseph L. Hall, Poorvi L. Vora, David Wagner. Poster Paper, National Conference on Digital Government Research (dg.o2005), May 16, 2005.

Articles in Non-Archival Magazines/Journals

"Randomness and the Netscape Browser." Ian Goldberg and David Wagner. Dr. Dobb's Journal, January 1996.

Other Publications

"A programmable plaintext recognizer." David Wagner and Steven M. Bellovin. Unpublished, September 1994.

"Architectural considerations for cryptanalytic hardware." Ian Goldberg and David Wagner. Chapter 10 of Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design, O'Reilly, July 1998.

"A Note on NSA's Dual Counter Mode of Encryption." Pompiliu Donescu, Virgil D. Gligor, and David Wagner. Formal contribution to the NIST Advanced Encryption Standard standardization process, September 28, 2001.

"Comments on RMAC." David Wagner. Formal contribution to the NIST Advanced Encryption Standard modes of operation standardization process, December 5, 2002.

"A Critique of CCM." Phillip Rogaway and David Wagner. Cryptology ePrint Archive, Report 2003/070. February 2, 2003.

"A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)." David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. Public report for Department of Defense's FVAP (Federal Voting Assistance Program), January 21, 2004.

"Killing, Recoding, and Beyond." David Molnar, Ross Stapleton-Gray, and David Wagner. Chapter 23 of RFID Applications, Security and Privacy, Addison Wesley Professional, July 6, 2005.

"Analysis of Volume Testing of the AccuVote TSx/AccuView." Matt Bishop, Loretta Guarino, David Jefferson, and David Wagner. Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), October 11, 2005.

"Security Analysis of the Diebold AccuBasic Interpreter." David Wagner, David Jefferson, Matt Bishop, Chris Karlof, and Naveen Sastry. Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), February 14, 2006.

"Statewide Databases of Registered Voters: Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues." Paula Hawthorn, Barbara Simons, Chris Clifton, David Wagner, Steven M. Bellovin, Rebecca N. Wright, Arnon Rosenthal, Ralph Spencer Poore, Lillie Coney, Robert Gellman, and Harry Hochheiser. Study commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery, February 16, 2006.

"Cryptanalysis of a Cognitive Authentication Scheme." Philippe Golle and David Wagner. IACR ePrint Archive, Report 2006/258, July 31, 2006.

Theses

"The security of MacGuffin." David Wagner. Princeton University undergraduate thesis, April 19, 1995.

"Janus: an approach for confinement of untrusted applications." David A. Wagner. Master's thesis, August 12, 1999.

"Static analysis and computer security: New techniques for software assurance." David Wagner. Ph.D. dissertation, University of California at Berkeley, December 2000.