Dr. Fred Cohen
PO Box 811 – Pebble Beach CA 93953
http: //all.net/ - US+925-454-0171

Education:

Ph.D. Electrical Engineering - University of Southern California, 1986
M.S. Information Science - University of Pittsburgh, 1980
B.S. Electrical Engineering - Carnegie-Mellon University, 1977

Positions (* current):

* CEO, Management Analytics, 2012-07 - present
* CEO, Fred Cohen & Associates, 1986-03 – present
* Acting Laboratory Director, Webster University Cyber Lab, 2013-11 – present
* Member. Fearless Security, LLC 2014-08 - present
President, California Sciences Institute, 2007-11 - 2012-12
Community Faculty Member, Metropolitan State University, 04/08-01/09
Adjunct Professor, University of San Francisco, 08/07-08/08
Research Professor, University of New Haven, 09/02-08/08
Chairman, Security Posture, 10/02-09/06
Principal Analyst, Burton Group, 04/03-04/06
Principal Member of Technical Staff, Sandia National Laboratories, 10/97-11/02
Chief Computer Forensic Scientist/Investigator, TAL Global, 09/01-11/02
Senior Member Technical Staff, Sandia National Laboratories, 7/96-9/97
Practitioner in Residence, University of New Haven, 06/98-09/02
Senior Scientist, SAIC, Inc., 7/93-6/95
Chairman, AllThings Incorporated, 1/95-1/96
Board Member, AllThings Incorporated, 6/94-1/96
Professor, Queensland University of Technology (visiting), 7/92-12/92
President, The Radon Project, Inc. 3/87-10/89
Asst. Professor, University of Cincinnati, 9/87-12/88
Asst. Professor, Lehigh University, 1/86-8/87
Lecturer, Lehigh University, 1/85-12/85

Editorial Boards, Program Committees:

2013-present, International Conference on Digital Forensics & Cyber Crime
2011-present, Journal of Digital Forensics, Security, and Law (Topic editor: Science)
2010-present, Board of Referees for the journal Digital Investigation
2009-present, IFIP WG 11.10 Program Committee (reviewer)
2008-present, IFIP WG 11.9 Program Committee (reviewer)
2007-present, EDP Audit, Control, and Security (EDPACS)
2005-present, Journal of Computer Virology
1987-present, IFIP TC-11 journal Computers and Security
2007-2011, MiniMetriCon Program Committee (and founding chair)
2010-2011, IEEE Security & Privacy, Beyond the Horizon (co-editor)
1995-2002, Network Security Magazine
1990-1993, ACM/SigSAC Annual Student Paper Review Board
1989-1991, DPMA, IEEE, and ACM Computer Virus and Security Conference
1989-1991, Computer Virus Bulletin

Honors and Awards:

2011: Honorary Doctorate (Honoris causa) Computer Science, University of Pretoria, South Africa
2011: International Information Systems Security Certification Consortium – Fellow of the $(ISC)^2$
2004: Burton Group Best Award
2002: Sandia Certificate of Appreciation (CCD Program)
2002: Techno-Security Industry Professional of the Year

2001: Sandia Employee Recognition Award (College Cyber Defenders)
2000: Sandia Meritorious Achievement Award (Security Immersion Program)
2000: Sandia Award for Excellence (Cyber Security / Surety)
1999: Sandia Exceptional Service Award (Security Awareness Work)
1998: Sandia Exceptional Service Award (Red Team Work)
1989: UK IT Auditors: Information Technology Award

Professional Societies

International Information Systems Security Certification Consortium – Fellow of the $(ISC)^2$
IEEE - Senior member

Books and Book Chapters not otherwise listed:

F. Cohen, “Protection and Engineering Design Issues in Critical Infrastructures”, pp67-153 in Thomas A. Johnson Ed. “CyberSecurity – Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, 2015, CRC Press, ISBN 978-1-4822- 3922-5.
F. Cohen, “Challenges to Digital Forensic Evidence in the Cloud”, in “Cybercrime and Cloud Forensics: Applications for Investigation Processes”, K. Ruan, Ed. 978-1-4666-2662-1, 2013.
F. Cohen, ”Digital Forensic Evidence Examination”, ASP Press, 2nd ed., 2010, 3rd ed.. 2011, 4th ed, 2012
F. Cohen, “Fundamentals of Digital Forensic Evidence”, (chapter in Handbook of Information and Communications Security, Springer, 2010, pp 789-808, Mark Stamp and Peter Stavroulakis, Ed.).
F. Cohen, ”Digital Forensic Evidence Examination”, ASP Press, 2009
F. Cohen, ”Enterprise Information Protection Architecture”, ASP Press, 2008
F. Cohen, “Challenges to Digital Forensic Evidence”, ASP Press, 2008
F. Cohen, “A Framework for Deception”, (chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007.
F. Cohen, “Critical Infrastructure Protection: Issues and Answers”, (one chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007. (in press).
F. Cohen, “Information Warfare, Netwar, and Cyber Intelligence.”, (chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007.
F. Cohen, "Challenges to Digital Forensic Evidence", (chapter in "Forensic Computer Crime Investigation", Thomas A. Johnson, Ed. Taylor & Francis, 2006
F. Cohen, “Security Decisions”, ASP Press, 2006
F. Cohen, “IT Security Governance Guidebook with Security Program Metrics on CD-ROM.” , Taylor & Francis/CRC Press, 2006
F. Cohen, “The Use of Deception Techniques: Honeypots and Decoys”, (chapter in Handbook of Information Security), V3, p646. Wiley and Sons, 2006.
World War 3 ... Information Warfare Basics , ASP Press, 2006
Information Security Awareness Basics , ASP Press, 2006
Frauds, Spies, and Lies - and how to defeat them , ASP Press, 2005
The CISO ToolKit: Security Checklists - Governance , ASP Press, 2005
The CISO ToolKit: Security Metrics , ASP Press, 2005
The CISO ToolKit: Governance Guidebook , ASP Press, 2005
Protection and Security on the Information Superhighway , John Wiley and Sons (1995)
F. Cohen, “It's Alive!!!”, John Wiley and Sons (1994)
F. Cohen, “A Short Course in Computer Viruses (2nd edition)”, John Wiley and Sons (1994)
F. Cohen, “A Short Course on Systems Administration and Security Under Unix”, ASP Press, (1992)
F. Cohen, “Payback - Automated Bill Collection System”, ASP Press (1992)
F. Cohen, “A Short Course in Computer Viruses”, ASP Press (1991)
F. Cohen, “The ASP Integrity Toolkit”, ASP Press (1990)
F. Cohen, “Introductory Information Protection”, ASP Press (1987)
F. Cohen, “Computer Viruses”, ASP Press, (1985)

Patents:

F. Cohen, “Detecting Inconsistencies in Data”, (pending) 61/531,609
F. Cohen, “Detecting Inconsistencies Consistent With Subversion of Normal Operations in an Operating Environment ” (pending) 61/531,609
F. Cohen, “Depiction of Digital Data for Forensic Purposes”, (pending)
F. Cohen, “Method and/or System for Providing and/or Analyzing and/or Presenting Decision Strategies“, 60/957,455 (pending)
F. Cohen, “Method and/or System for Providing and/or Analyzing Influence Strategies“, US Pat. 8,095,492.
F. Cohen, “Method and Apparatus for Invisible Network Responder” 20040148521 (pending) 20040162994 (pending)
F. Cohen, “Method and Apparatus for Specifying Communication Indication Matching and/or Responses” 20040153574 (pending)
F. Cohen, D Koike, V. Nagaeu, “Method and Apparatus Providing Deception and/or Altered Operation in an Information System Operating System”, US Pat. 7,437,766 10/679,186
F. Cohen, “Method and Apparatus for Configurable Communication Network Defenses”
F. Cohen, “Method and Apparatus for Network Deception/Emulation”, US Pat. 7,107,347.
F. Cohen, “Method and Apparatus for Providing Deception and/or Altered Execution of Logic in an Information System US Pat. 7,296,274.

Refereed journal articles:

F. Cohen, “Digital diplomatics and forensics: Going forward on a global basis”, Records Management Journal, 2015-03
Cohen F, Cohen D, “Time and space interval record schedule consistency analysis for atomic items without interactions in open spaces with stationary locations”, Computers & Security (2014), http://dx.doi.org/10.1016/ j.cose.2014.03.002
F. Cohen, "Identifying and Attributing Similar Traces with Greatest Common Factor Analysis", J. of Digital Forensics, Security, and Law, V7#2, 2012.
F. Cohen, "A Case Study in Forensic Analysis of Control", Journal of Digital Forensics, Security, and Law., V6#1, 2011.
F. Cohen, "A Method for Forensic Analysis of Control", IFIP TC11, Computers & Security, V29#8, pp 891-902, Nov., 2010, doi: 10.1016/j.cose.2010.05.003
F. Cohen, et. al. "Leading Attackers Through Attack Graphs with Deceptions", IFIP-TC11, `Computers and Security', V22#5, July 2003, pp. 402-411(10)
F. Cohen, et. al. "A Mathematical Structure of Simple Defensive Network Deceptions", IFIP-TC11, `Computers and Security', Volume 19, Number 6, 1 October 2000, pp. 520-528(9)
Cohen F.; Phillips C.; Swiler L.P.; Gaylor T.; Leary P.; Rupley F.; Isler R., “A Cause and Effect Model of Attacks on Information Systems. Some Analysis Based on That Model, and The Application of that Model for CyberWarfare in CID”, IFIP-TC11 Computers and Security, V17#3, 1998 pp. 211-221 (11)
F. Cohen, "Providing for Responsibility in a Global Information Infrastructure ", IFIP-TC11, `Computers and Security', 1997.
F. Cohen, "Simulating Cyber Attacks, Defenses, and Consequences", IFIP-TC11, `Computers and Security', 1999, vol. 18, no. 6, pp. 479-518(40)
F. Cohen, et. al. "Intrusion Detection and Response", IFIP-TC11, `Computers and Security', V16,#6, 1997, pp. 516-516(1) (also appearing below under National Info-Sec Technical Baseline studies from Dec, 1996)
F. Cohen, "A Note on the Role of Deception in Information Protection", IFIP-TC11, Computers and Security, 1998, vol. 17, no. 6, pp. 483-506(24)
F. Cohen, “Information System Defences: A Preliminary Classification Scheme”, IFIP TC-11, Computers and Security, V16,#2, 1997, pp. 94-114(21)
F. Cohen, "A Note on Distributed Coordinated Attacks", IFIP-TC11, `Computers and Security', Volume 15, Number 2, 1996, pp. 103-121(19), also appearing as an invited paper in 4th

Computer Misuse and Anomaly Detection Workshop, Monterey, 1996 (referenced below).
F. Cohen, "A Secure World-Wide-Web daemon", IFIP-TC11, `Computers and Security', V15#8, 1996, pp. 707-724(18)
F. Cohen, "Operating Systems Protection Through Program Evolution", IFIP-TC11 `Computers and Security' (1993) V12#6 (Oct. 1993) pp.565 - 584
J. Voas, J. Payne, F. Cohen "A Model for Detecting the Existence of Software Corruption in Real-Time", IFIP-TC11 "Computers and Security", V12#3 May, 1993 pp. 275-283.
F. Cohen, "A Formal Definition of Computer Worms and Some Related Results", IFIP-TC11 "Computers and Security" V11#7, November, 1992, pp. 641-652.
F. Cohen, "Defense-In-Depth Against Computer Viruses", IFIP-TC11 "Computers and Security", V11#6, 1992 pp. 563-579.
F. Cohen, "A DOS Based POset Implementation", IFIP-TC11 "Computers and Security", V10#6, October 1991.
F. Cohen, "A Note On High Integrity PC Bootstrapping", IFIP-TC11 "Computers and Security", V10#6, October 1991.
F. Cohen, "A Cost Analysis of Typical Computer Viruses and Defenses", IFIP-TC11 "Computers and Security", V10#3, May, 1991 (also appearing in 4th DPMA, IEEE, ACM Computer Virus and Security Conference, 1991)
F. Cohen, "Automated Integrity Maintenance for Viral Defense", IFIP-TC11 "Computers and Security", 1990
F. Cohen, "Computational Aspects of Computer Viruses", IFIP-TC11, "Computers and Security", V8 pp325-344, 1989.
Y. J. Huang and F. Cohen, "Some Weak Points of One Fast Cryptographic Checksum Algorithm and its Improvement", IFIP-TC11 "Computers and Security", V8#1, February, 1989
B. Cohen and F. Cohen, "Error Prevention at a Radon Measurement Service Laboratory", Radiation Protection Management, V6#1, pp43-47, Jan. 1989
F. Cohen, "Models of Practical Defenses Against Computer Viruses", IFIP-TC11, "Computers and Security", V8#2, April, 1989 pp149-160.
F. Cohen, "Two Secure Network File Servers", IFIP-TC11, "Computers and Security", V7#4, August, 1988.
F. Cohen, "Designing Provably Correct Information Networks with Digital Diodes", IFIP-TC11, "Computers and Security", V7#3, June, 1988.
F. Cohen, "On the Implications of Computer Viruses and Methods of Defense", Invited Paper, IFIP-TC11, "Computers and Security", V7#2, April, 1988,
F. Cohen, "Maintaining a Poor Person's Information Integrity", IFIP-TC11, "Computers and Security", V7#1, Feb 1988.
F. Cohen, "A Cryptographic Checksum for Integrity Protection", IFIP-TC11 "Computers and Security", V6#6 (Dec. 1987), pp 505-810.
F. Cohen, "Design and Protection of an Information Network Under a Partial Ordering: A Case Study", IFIP-TC11, "Computers and Security", V6#4 (Aug. 1987) pp 332-338.
F. Cohen, "Design and Administration of Distributed and Hierarchical Information Networks Under Partial Orderings", IFIP-TC11, "Computers and Security", V6#3 (June 1987), pp 219-228.
F. Cohen, "Protection and Administration of Information Networks with Partial Orderings", IFIP-TC11, "Computers and Security", V6#2 (April 1987) pp 118-128.
F. Cohen, "Computer Viruses - Theory and Experiments", DOD/NBS 7th Conference on Computer Security, originally appearing in IFIP-sec 84, also appearing as invited paper in IFIP-TC11, "Computers and Security", V6#1 (Jan. 1987), pp 22-35 and other publications in several languages.
F. Cohen, "A Secure Computer Network Design", IFIP-TC11, "Computers and Security", V4#3, (Sept. 1985), pp 189-205, also appearing in AFCEA Symp. and Expo. on Physical and Electronic Security, Aug. 1985.
F. Cohen, "Algorithmic Authentication of Identification", Information Age, V7#1 (Jan. 1985), pp 35-41.

Invited Papers and Keynotes with Published Papers:

F. Cohen, “The Future of Digital Forensics” - 2012-09-21. 1st Chinese Conference on Digital Forensics, Keynote Address and Paper.
F. Cohen, "What Makes Critical Infrastructures Critical?", International Journal of Critical Infrastructure Protection(2010), doi: 10.1016/j.ijcip.2010.06.002.
F. Cohen, "The Smarter Grid", IEEE Security and Privacy - On the Horizon, 2010, V8#1, January/February, 2010.
F. Cohen, "Toward a Science of Digital Forensic Evidence Examination", IFIP TC11.8 International Conference on Digital Forensics", Hong Kong, China, Jan 4, 2010 (Keynote), Published in Advances in Digital Forensics VI, pp17-36, Springer, ISBN#3-642-15505-7, 2010.
F. Cohen, "The past and future history of computer viruses", EICAR annual conference, Berlin, Germany, May 11-12, 2009.
F. Cohen, "30 Lies About Secure Electronic Commerce: The Truth Exposed", Institute for International Research Electronic Commerce Conference, Feb. 1999.
F. Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart "A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model", Encyclopedia of Computer Science, 1999.
F. Cohen, "National Info-Sec Technical Baseline - Intrusion Detection and Response" National InfoSec Research Council, Dec, 1996. (also appearing above in Computers and Security, 1997).
F. Cohen, "A Note on Distributed Coordinated Attacks", 4th Computer Misuse and Anomaly Detection Workshop, Monterey, 1996 (also appearing above in Computers and Security, 1996).
F. Cohen, "The Internet, ..., and Information Security", Computer Society of South Africa, 7th Annual Conference, August, 1995, South Africa.
F. Cohen, "The Internet, Corporate Networks, and Firewalls", Computer Society of South Africa, 7th Annual Conference, August, 1995, South Africa.
F. Cohen, "Information Assurance", IFIP TC-11 World Congress, May, 1995, Cape Town, South Africa.
F. Cohen, "`Information Warfare Considerations", Norwegian Academy of Sciences, September, 1993.
F. Cohen, "Computer Viruses", (one chapter in "The Computer Security Reference Book", Butterworth/Heinemann, Oxford, England, 2004.
F. Cohen, "Fault Tolerant Software for Computer Virus Defense", November, 1991.
F. Cohen, "Some Applications of Benevolent Viruses in Networked Computing Environments", `DPMA, IEEE, ACM Computer Virus and Security Conference', March 1993
F. Cohen and S. Mishra, "Some Initial Results From the QUT Virus Research Network", `The Virus Bulletin Conference', Edinburgh, Scotland, July, 1992 (keynote).
F. Cohen, "Computer Viruses", (one chapter in "The Computer Security Reference Book" Butterworth/Heinemann (1992), Oxford, England
F. Cohen, "Current Trends in Computer Viruses", Invited Paper, International Symposium on Information Security, Oct. 17-18, 1991, Tokyo, Japan
F. Cohen, "Current Best Practice Against Computer Viruses", Invited Paper, 1991, 25th IEEE International Carnahan Conference on Security Technology, Oct. 1-3, 1991, Taiwan ROC.
F. Cohen, "Exploiting Defense-In-Depth Against Computer Viruses", Invited Paper, The Oxbridge Sessions, Sept. 3-5, 1991, The Netherlands.
F. Cohen, "Computers Under Attack" (one paper), ACM/Addison Wesley (1990)
F. Cohen, "A Summary of Results on Computer Viruses and Defenses", Invited Paper, 1990 NIST/DOD Conference on Computer Security.
F. Cohen, "Integrity Maintenance in Untrusted Computing Environments", Invited Paper, IBC Computer Virus Conference, London, 1990.
F. Cohen, "Information Systems as a Competitive Weapon", Keynote Address, Utah State School of Business, Annual Computer Conference, March 1-2, 1990.
F. Cohen, "Recent Advances in Integrity Maintenance in Untrusted Systems", Invited Paper, The

Netherlands Computer Security Seminar, April 10-12, 1990.
F. Cohen, "A Note on the use of Pattern Matching in Computer Virus Detection", Invited Paper, Computer Security Conference, London, England, Oct 11-13, 1989, also appearing in DPMA, IEEE, ACM Computer Virus Clinic, 1990.
F. Cohen, "Computer Viruses - Attacks and Defensive Measures", London Corporate Computer Security Conference - Keynote Address, London, England, Feb. 14, 1989.
F. Cohen, "Current Trends in Computer Virus Research", 2nd Annual Invited Symp. on Computer Viruses - Keynote Address, Oct. 10, 1988. New York, NY
F. Cohen, "Recovery Techniques in Computer Virus Attack", Invited Paper, Invitational Conference on Computer Viruses, 1988.

Peer Reviewed Conference and Other Papers:

F. Cohen, “A Tale of Two Traces - Archives, Diplomatics, and Digital Forensic”, IFIP Tenth annual IFIP WG 11.9 International Conference on Digital Forensics, 2015-01-26-8, also to be published as a chapter in in “Advances in Digital Forensics X”.
F. Cohen, “As the consequences rise, where is the risk management?”, EDPACS: The EDP Audit, Control, and Security Newsletter, V41# 4, (2013), DOI:10.1080/07366981.2013.775779, reprint from analyst report.
F. Cohen, “The Bottom Ten List—Information Security Worst Practices”, EDPACS: The EDP Audit, Control, and Security Newsletter, V41#1, (2012), DOI:10.1080/07366981003634460, reprint from analyst report.
F. Cohen, “F. Cohen, “The Physics of Digital Information – Part 2”, JDFSL v7#1”, July, 2012 (editorial column)
F. Cohen, “Forensic Methods for Detecting Insider Turning Behaviors”, IEEE Workshop on Research for Insider Threat, 2012-05-25, with the IEEE Oakland Conference, IEEE Computer Society Press.
F. Cohen, “Update on the State of the Science of Digital Evidence Examination”, Conference on Digital Forensics, Security, and Law, May 29-31, 2012 – pending publication.
F. Cohen, “Consistency under deception implies integrity”, ICSJWG Quarterly Newsletter. Republished from 2011-09 Short Analyst Reports.
F. Cohen, “F. Cohen, “The Physics of Digital Information”, Journal of Digital Forensics, Security, and Law, V6#3, October, 2011 (editorial column)
F. Cohen, “Progress and evolution of critical infrastructure protection over the last 10 years?”, The CIP Report, Center for Infrastructure Protection and Homeland Security, V10#3, 2011-09, Republished from 2011-08 Short Analyst Reports.
F. Cohen, “Putting the Science in Digital Forensics” Journal of Digital Forensics, Security, and Law, V6#1, July, 2011 (editorial column)
F. Cohen, “How Do We Measure Security?”, Insight, V14#2, 2011-07, pp 30-32, International Council on Systems Engineering.
F. Cohen, "Change your passwords how often?”, EDPACS 44(4), April, 2010. (Reprinted from Analyst Newsletter)
F. Cohen, J. Lowrie, C. Preston, “The State of the Science of Digital Evidence Examination”, IFIP Seventh annual IFIP WG 11.9 International Conference on Digital Forensics, 2011/01/30, also published as a chapter in in “Advances in Digital Forensics VII”.
F. Cohen, “Digital Forensic Evidence Examination - The State of the Science - and Where to Go From Here”, NeFX Workshop, Sep 14, 2010.
F. Cohen, "Fonts for Forensics", IEEE SADFE (in conjunction with the IEEE Oakland Conference), 2010-05-19, Oakland, CA.
F. Cohen, "The Bottom Ten List - Information Security Worst Practices”, EDPACS 41(1), January, 2010. (Reprinted from Analyst Newsletter)
F. Cohen, "Attribution of messages to sources in digital forensics cases", HICSS-43, Jan 7, 2010.
F. Cohen, "Analysis of redundant traces for consistency", IEEE International Workshop on Computer Forensics in Software Engineering (CFSE 09), Seattle, Washington, USA, July 20-24, 2009

F. Cohen, "Two models of digital forensic examination", IEEE SADFE (in conjunction with the IEEE Oakland Conference), 2009-05-21, Oakland, CA
F. Cohen, "Issues and a case study in bulk email forensics", Fifth annual IFIP WG 11.9 International Conference on Digital Forensics, 2009/01/27, published as "Bulk Email Forensics" in the conference publication.
F. Cohen and T. Johnson, "A Ph.D. Curriculum for Digital Forensics", HICSS-42, Jan 7, 2009.
F. Cohen, "Information Assurance Architectural Models", HICSS-42 Product and Process Assurance Symposium Position Paper, Jan 5, 2009,
F. Cohen, "Social tension and separation of duties", EDPACS 38(5) (2009). (Reprinted from Analyst Newsletter).
F. Cohen, "Control Requirements for Control Systems... Matching Surety to Risk", EDPACS, 2008
F. Cohen, "Making Compliance Simple – Not", EDPACS, March 2008, V37#3. (Reprinted from Analyst Newsletter)
F. Cohen and C. Preston, "A Method for Recovering Data From Failing Floppy Disks with a Practical Example", Fourth annual IFIP WG 11.9 International Conference on Digital Forensics, 2008/01/27 to 30. Published in "Advances in Digital Forensics IV", Springer, ISBN 978-0-387-84926-3, pp29-42, 2008.
F. Cohen, "Fault Modeling and Root Cause Analysis for Information Security Governance", Computers and Security, 2007.
Cohen, "A Note on Detecting Tampering with Audit Trails"', 1995. Available at http://all.net/books/audit/audmod.html
F. Cohen and D. Koike, "Misleading attackers with deception", Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC
Publication Date: 10-11 June 2004: pp. 30- 37
F. Cohen, "Airbag Inflator Inspection System", LumenX Corporation, November, 1994.
F. Cohen, R. Knecht, C. Preston, et. al., "Planning Considerations for Defensive Information Warfare - Information Assurance", Contract DCA 100-90-C-0058 T.O. 90-SAIC-019, November, 1993.
F. Cohen, "Threats and Defenses for WCCS", US Air Force, Wing Command and Control System, August, 1993.
F. Cohen, "Information Warfare Considerations", National Academy of Sciences - National Research Council, September, 1993.
F. Cohen, "A Case for Benevolent Viruses" DPMA, IEEE, ACM Computer Virus and Security Conference, March 1992
F. Cohen, "Current Best Practice Against Computer Viruses with Examples from the DOS Operating System", DPMA, IEEE, ACM Computer Virus and Security Conference, March 1992
F. Cohen, "A Roving Emulator", Conference on Modeling and Simulation, April, 1987.
F. Cohen, "Information Protection", Curriculum Module for the graduate degree in Software Engineering, The Software Engineering Institute, June, 1986, also appearing in ACM SIGSAC in abbreviated form.
F. Cohen, "A Complexity Based Integrity Maintenance Mechanism", Conference on Information Sciences and Systems, Princeton University, March 1986.
F. Cohen, "Recent Results in Computer Viruses", Conference on Information Sciences and Systems, Johns Hopkins University, March 1985.
F. Cohen, "The HAD Cryptosystem", IACR Crypto84 rump session, Aug. 1984.
F. Cohen, "Computer Security Methods and Systems", Conference on Information Sciences and Systems, Princeton University, March 1984.
F. Cohen, "Learning Networks for Database Access", Yale Conference on Adaptive Systems Theory, New Haven, CT, June, 1983.
M.A. Breuer, F. Cohen, and A.A. Ismaeel, "Roving Emulation", Built-In Self-Test Conference, March 1983.
F. Cohen, "The Delta-Net Model of Computation", Conference on Information Sciences and Systems, Johns Hopkins University, March 1983.
F. Cohen, "The U.S.C. Roving Emulator", U.S.C. DISC Report #82-8, Dept of Electrical

Engineering, University Park, LA, Ca. 90089-0781, Dec. 1982.
M.A. Breuer, F. Cohen, A.A. Ismaeel, "Roving Emulation as Applied to a (255,223) RS-encoder System", U.S.C. DISC Report #82-6, Dec. 1982.

Burton Group Reports:

F. Cohen, "Outsourcing, Offshoring, and Security: What's the Difference?" 28 Jun 2006
F. Cohen, "IT Risk Management and COSO" 24 May 2006
F. Cohen, "Defending Against the Evil Insider" 16 Nov 2005
F. Cohen, "Raising the Bar: Solving Medium-Risk Problems with Medium-Surety Solutions" 27 Sep 2005
P. Schacter and F. Cohen, "Enterprise Strategies for Defending Against Spyware" 23 Aug 2005
F. Cohen, "Security Metrics: Horses for Courses" 24 Jun 2005
F. Cohen, "Security Governance for the Enterprise" 31 Mar 2005
F. Cohen, "Business Continuity Planning for IT" 24 Mar 2005
D. Blum and F. Cohen, "A Systematic, Comprehensive Approach to Information Security" 24 Feb 2005
F. Cohen, "Security Awareness, Training, and Education Programs for the Enterprise" 17 Jan 2005
F. Cohen, "Change Management for the Enterprise" 17 Jan 2005
D. Blum and F. Cohen, "Concepts and Definitions" 17 Jan 2005
F. Cohen, "Database Security: Protecting the Critical Content of the Enterprise" 28 Oct 2004
F. Cohen, "Building Secure Applications: How secure do you want to be today?" 09 Sep 2004
F. Cohen, "Risk Aggregation: The Unintended Consequence", 27 Apr 2004
F. Cohen, "Auditing and Audit Trails", 18 Mar 2004
F. Cohen, "Patch Management", 2003
F. Cohen, "The Evolving Role of Firewalls", 2003
F. Cohen, "Linux Security Features", 2003 (unpublished)
F. Cohen, "Intrusion Detection and Response Systems", October, 2003
F. Cohen, "Analysis of Information-Related Threats to Enterprises", 18 Sep 2003
F. Cohen, "Risk Management: Concepts and Frameworks", 18 July, 2003
F. Cohen, "Policy-Based Security and Enterprise Policy Management", 9 Dec 2003

Special Cyber Terrorism Studies:

The Provisional Irish Republican Army - 2000
The Animal Liberation Front (ALF) - 2000
Revolutionary Armed Forces of Colombia (FARC) - 2000
National Liberation Army (ELN)--Colombia - 2000
Issues in Cyber-Terrorism – 2000

Short Analyst Reports and Other Substantial Collections:

2015-09: Why can't we make any of the systems we use secure from remote attack?
2015-07: Who's to blame?
2015-06: Reducing the effects of malicious insiders non-technologically
2015-05: Iran(t) on merchantability for software
2015-04: Fishing and phishing
2015-03 B: Error-induced misoperation - rowhammer
2015-03 Temporal microzones and end-user workstations
2015-02 Input checking
2015-01 The year of the Trojans (and their unintended side effects)
2014-12 Stupid security getting even stupider
2014-11-B Eat your own dog food deal about big data loss (actually theft)?
2014-10 Cyber (whatever that is) insurance yet again?
2014-09 2-factor this into your thinking
2014-08-B A touch of the Ebola

2014-08 Aurora and why it doesn't really matter
2014-07 Encrypt it all!!!
2014-06 Is it secure?
2014-05 May Day - attack mechanisms revisited - were you surprised by the NSA's activities?
2014-04 The RSA: Science Fiction and Humor
2014-03-B The Snowden virus - disrupting the secret world by exploiting their policies
2014-03 The four tactical situations of cyber conflict
2014-02 Countering hardware storage device Trojans
2014-01-B After the Red Team
2014-01 Why we need better reporters to solve our security problems
2013-12 Return of the telnet return
2013-11-B Transparency - a different protection objective
2013-11 Demystifying control architecture
2013-10-B The "big deal" approach to risk management
2013-10 Trust and worthiness
2013-09 The surveillance society: pros, cons, alternatives, and my view.
2013-08 50 Ways to respond to "Computer Repair..."
2013-08 Three words you should never use in security and risk management
2013-07-B How to justify (security) metrics and what to measure
2013-07 Mobility and industrial control systems
2013-06 Separation of Duties and RFPs
2013-05-B The harder problems
2013-05 Write lock the past, access control the present, anticipate the future
2013-04-B Actionable metrics (Guest Editor)
2013-04 Managing Oops
2013-03-C Limiting Insider Effects Through Micro-Zoning
2013-03-B Welcome to the Information Age - a 1-page primer
2013-03 Security Heroes
2013-02-B Stupid Security Winner for 2012
2013-02 Thinking more clearly
2013-01 Raising all boats - by improving the average
2012-12 Enterprise Security Architecture Options and Basis
2012-12 Ten Bad Assumptions
2012-11 The Design Basis Threat
2012-10 Changing the leverage
2012-10 Industrial Control System Security Decisions and Architecture
2012-09 Eventually, you are going to make a mistake
2012-08 As the consequences rise, where is the risk management?
2012-07-01B The Facebook debacle and what it says about the other providers
2012-07-01 - Open CyberWar - Early Release
2012-06-01 - Question everything
2012-05-01 - The threat reduction approach - Point – Counterpoint
2012-04-01 - The insider turned bad
2012-03-01 - Three emerging technologies
2012-02-01 - Ethics in security research
2012-01-31 - Influence Operations
2012-01-01 - The security squeeze
2011-12-01 - Can we attribute authorship or human characteristics by automated inspection?
2011-11-03 - Saving SMBs from data leakage
2011-11-01 - Webification and Authentication Insanity
2011-10-01 - Consistency Under Deception Implies Integrity - ICSJWG version
2011-10-01 - Security vs. Convenience - The Cloud - Mobile Devices - and Synchronization
2011-09-11 - CIP version of "Progress and evolution of critical infrastructure protection over the last 10 years?"

2011-09 - Consistency under deception implies integrity
2011-08 - Progress and evolution of critical infrastructure protection over the last 10 years?
2011-07 - The structure of risk and reward
2011-06 - Security Metrics - A Matter of Type
2011-05 - The "R" word
2011-04 - Change your passwords how often?
2011-03 - Any is not All
2011-02 - Why are we so concerned about governments getting our data?
2011-01b - The Bottom Ten List - Information Security Worst Practices - Getting Even Worse
2011-01 - Risk aggregation - again and again and again...
2010-12b - Code book cryptography may be nearly dead
2010-12 - Changes to the Federal Rules of Evidence - Rule 26
2010-11 - How do we measure "security"?
2010-10 - Moving target defenses with and without cover deception
2010-09 - User Platform Selection Revisited
2010-08 – The DMCA Still Restricts Forensics
2010-07 - Mediated Investigative Electronic Discovery
2010-06 - The difference between responsibility and control
2010-05 - The Virtualization Solution
2010-04 - Attacks on information systems - a bedtime story
2010-03 - The attacker only has to be right once - another information protection fallacy
2010-02b - Another ridiculous cyber warfare game to scare deciders into action
2010-02 - Developing the science of information protection
2010-01 - The Bottom Ten List - Information Security Worst Practices
2009-12-B - COFEE and the state of digital forensics
2009-12 - Using the right words
2009-11 - Passwords again - why we can't leave well enough alone
2009-10 - Partitioning and virtualization - a strategic approach
2009-09 - Forensics: The limits of my tools, my techniques, and myself
2009-08 - Virtualization and the cloud - Risks and Rewards
2009-07 - The speed of light, it's easy to forge, email is always fast, and more
2009-06 - Security Decisions: Deception - When and where to use it
2009-05-B - Culture clash: Cloud computing and digital forensics
2009-05 - Protection testing: What protection testing should we do?
2009-04-B - Proposed Cyber-Security Law: What's the problem?
2009-04 - Risk management: There are no black swans
2009-03 - How spam vigilantes are wrecking email and encourage violations of law
2009-02-B Digital forensics must come of age
2009-02 - A structure for addressing digital forensics
2009-01 - Change management: How should I handle it?
2008-12-B - Short Note: Twittering away your privacy
2008-12 - Digital Forensic Evidence: A Wave Starting to Break
2008-11 - Security Decision: Zoning your network
2008-10 - Social tension and separation of duties
2008-09 - Default deny is best practice? Not anymore!
2008-08 - Control architecture: Access controls
2008-07 - Fault modeling, the scientific method, and thinking out of the box
2008-06 - Inventory Revisited - How to reduce security losses by 70%?
2008-05 - Control Requirements for Control Systems... Matching Surety to Risk
2008-04 - The Botnets have come - The Botnets have come...
2008-03 - Enterprise Information Protection - It's About the Business
2008-02 - The Digital Forensics World
2008-02 - Who Should Do Your Digital Forensics?
2008-01 - Unintended Consequences

2008-01 - Accidental Security
2007-12 - Security, justice, and the future
2007-12 - Security End-of-year
2007-11 - Security by Psychology
2007-11 - Covert Awareness
2007-10 - Making compliance simple - not
2007-10 - Measuring Compliance
2007-09 - Identity Assurance and Risk Aggregation
2007-09 - Identity Assurance
2007-08 - The ethical challenge
2007-08 - Conflicts of Interest
2007-07 - Security Decision Support
2007-07 - Making Better Security Decisions
2007-06 - User platform selection
2007-06 - Which User Platform
2007-05 - Risk Management
2007-05 - Managing Risks
2007-04 - Security Ethics and the Professional Societies
2007-04 - Information Content Inventory
2007-03 - Emerging Risk Management Space
2007-03 - Sensible Security - You Wouldn't?
2007-02 - Emerging Market Presence
2007-02 - Measuring Security
2007-01 - Market Maturity and Adoption Analysis Summary
2007-01 - Closing the Gap
2007-00 - Analysis Framework
2006-12 - The Security Schedule
2006-11 - The Holidays Bring the Fraudsters
2006-10 - Physical/Logical Convergence??
2006-09 - How can I Show I am Me in Email?
2006-08 - Service Oriented Architecture Security Elements
2006-07 - The Life Expectancy of Defenses
2006-07 - BONUS ISSUE: The End of the World as we Know it
2006-06 - Why the CISO should work for the CEO - Three Case Studies

Professional magazine articles:

F. Cohen, "Managing Network Security" Nov. 2002, Breaking In... to test security?
F. Cohen, "Managing Network Security" Oct., 2002 - Reworking Your Firewalls
F. Cohen, "Managing Network Security" Sept, 2002 - Deception Rising
F. Cohen, "Managing Network Security" Aug, 2002 - You're in a Bind!
F. Cohen, "Managing Network Security" July, 2002 - Smashed Again by Stupid Security (appears in Computer Frauds and Security Bulletin)
F. Cohen, "Managing Network Security" July, 2002 - Is Open Source More or Less Secure?
F. Cohen, "Managing Network Security" June, 2002 - Academia's Vital Role in Information Protection
F. Cohen, "Managing Network Security" May, 2002 - Terrorism and Cyberspace
F. Cohen, "Managing Network Security" April, 2002 - Misimpressions We Need to Extinguish
F. Cohen, "Managing Network Security" March, 2002 - Embedded Security
F. Cohen, "Managing Network Security" February, 2002 - How to Get Around Your ISP
F. Cohen, "Managing Network Security" January, 2002 - The End of the Internet as we Know it
F. Cohen, " 2001: Red Teaming Experiments with Deception Technologies"
F. Cohen, " 2001: A Framework for Deception"
F. Cohen, "Managing Network Security - The World Doesn't Want to be Fixed", Network Security, Dec., 2001.

F. Cohen, "Managing Network Security: The Deception Defense", Network Security, Nov., 2001.
F. Cohen, "Managing Network Security: The DMCA ", Network Security, Oct., 2001.
F. Cohen, "Managing Network Security: The Best Security Book Ever Written ", Network Security, Sep., 2001.
F. Cohen, "Managing Network Security: Special Issue - The Balancing Act ", Network Security, Sep., 2001.
F. Cohen, "Managing Network Security: Bootable CDs", Network Security, Aug., 2001.
F. Cohen, "Managing Network Security: A Matter of Power", Network Security, Jul., 2001.
F. Cohen, "Managing Network Security: The Wireless Revolution", Network Security, Jun., 2001.
F. Cohen, "Managing Network Security: The New Cyber Gang - A Real Threat Profile ", Network Security, May., 2001.
F. Cohen, "Managing Network Security: To Prosecute or Not to Prosecute", Network Security, Apr., 2001.
F. Cohen, "Managing Network Security: Corporate Security Intelligence", Network Security, Mar., 2001.
F. Cohen, "Managing Network Security: Testing Your Security by Breaking In - NOT ", Network Security, Feb., 2001.
F. Cohen, "Managing Network Security: Marketing Hyperbole at its Finest", Network Security, Jan., 2001.
F. Cohen, "Managing Network Security: The Millennium Article - Yet Again! - The Bots are Coming!!! The Bots are Coming!!!", Network Security, Dec., 2000.
F. Cohen, "Managing Network Security: Why Everything Keeps Failing", Network Security, Nov., 2000.
F. Cohen, "Managing Network Security: The Threat", Network Security, Oct., 2000.
F. Cohen, "Managing Network Security: Chipping ", Network Security, Sep., 2000.
F. Cohen, "Managing Network Security: Understanding Viruses Bio-logically", Network Security, Aug., 2000.
F. Cohen, "Managing Network Security: What does it do behind your back?", Network Security, Jul., 2000.
F. Cohen, "Managing Network Security: Why Can't We Do DNS Right?", Network Security, June, 2000.
F. Cohen, "Managing Network Security: Eliminating IP Address Forgery - 5 Years Old and Going Strong ", Network Security, May, 2000.
F. Cohen, "Managing Network Security: Countering DCAs", Network Security, Apr., 2000.
F. Cohen, "Managing Network Security: Collaborative Defense", Network Security, Mar., 2000.
F. Cohen, "Managing Network Security: Worker Monitoring ", Network Security, Feb., 2000.
F. Cohen, "Managing Network Security: Digital Forensics ", Network Security, Jan., 2000.
F. Cohen, "Managing Network Security: Why it was done that way", Network Security, Dec., 1999.
F. Cohen, " So Much Evidence... So Little Time", Information Security Magazine, November. 1999. Special issue with articles by "The 20 Most Influential Figures in Information Security Today."
F. Cohen, "50 Ways to Defeat Your PKI and Other Cryptosystems", The 50 Ways Series at all.net. (/journal/50/index.html)
F. Cohen, "50 Ways to Defeat Your Firewall", The 50 Ways Series at all.net. (/journal/50/index.html)
F. Cohen, "Managing Network Security: The Limits of Cryptography", Network Security, Nov., 1999.
F. Cohen, "Managing Network Security: Security Education in the Information Age", Network Security, Oct., 1999.
F. Cohen, "Managing Network Security: In Your Face Information Warfare", Network Security, Sep., 1999.
F. Cohen, "Managing Network Security: What's Happening Out There", Network Security, Aug., 1999.
F. Cohen, "Managing Network Security: Attack and Defense Strategies", Network Security, July,

1999.
F. Cohen, "Managing Network Security: The Limits of Awareness", Network Security, June, 1999.
F. Cohen, "Managing Network Security: Watching the World ", Network Security, May, 1999.
F. Cohen, "Managing Network Security: Simulating Network Security ", Network Security, Apr., 1999.
F. Cohen, "Managing Network Security: The Millisecond Fantasy", Network Security, Mar., 1999.
F. Cohen, Eli Dart "DARE: Distributed Analysis and REsponse", SANS conference, San Diego, 1999.
F. Cohen, "Managing Network Security: Returning Fire", Network Security, Feb., 1999.
F. Cohen, "Managing Network Security: Anatomy of a Successful Sophisticated Attack", Network Security, Jan., 1999.
F. Cohen, "Managing Network Security: Balancing Risk", Network Security, Dec., 1998.
F. Cohen, "Managing Network Security: The Real Y2K Issue?", Network Security, Nov., 1998.
F. Cohen, "Managing Network Security: Time-Based Security?", Network Security, Oct., 1998.
F. Cohen, "Managing Network Security: What Should I Report to Whom?", Network Security, Sep., 1998.
F. Cohen, "Managing Network Security: Third Anniversary Article - The Seedy Side of Security", Network Security, Aug., 1998.
F. Cohen, "Managing Network Security: How Does a Typical IT Audit Work?", Network Security, Jul., 1998.
F. Cohen, "Managing Network Security: Technical Protection for the Joint Venture", Network Security, Jun., 1998.
F. Cohen, "Managing Network Security: Risk Staging", Network Security, May., 1998.
F. Cohen, "Managing Network Security: The Unpredictability Defense", Network Security, Apr., 1998.
F. Cohen, "Managing Network Security: Red Teaming", Network Security, Mar., 1998.
F. Cohen, "Managing Network Security: The Management of Fear", Network Security, Feb., 1998.
F. Cohen, "Managing Network Security: Y2K - Alternative Solutions", Network Security, Jan., 1998.
F. Cohen, "Managing Network Security: 50 Ways to Defeat Your Intrusion Detection System", Network Security, Dec., 1997.
F. Cohen, "Managing Network Security: To Outsource or Not to Outsource - That is the Question.", Network Security, Nov., 1997.
F. Cohen, "Managing Network Security: The Network Security Game", Network Security, Oct., 1997.
F. Cohen, "Managing Network Security: Change Your Password - Doe See Doe", Network Security, Sep., 1997.
F. Cohen, "Managing Network Security: Penetration Testing?", Network Security, Aug., 1997.
F. Cohen, "Managing Network Security: Relativistic Risk Analysis", Network Security, Jun., 1997.
F. Cohen, "Managing Network Security: Prevent, Detect, and React", Network Security, May., 1997.
F. Cohen, "Managing Network Security: Would you like to play a game?", Network Security, Apr., 1997.
F. Cohen, "Protection Issues in ASCII Red Based on a Limited Unclassified Briefing" (C).
F. Cohen, "Managing Network Security: Risk Management or Risk Analysis?", Network Security, Mar., 1997.
F. Cohen, "Managing Network Security: Network Security as a Control Issue?", Network Security, Feb., 1997.
F. Cohen, "Managing Network Security: Integrity First - Usually", Network Security, Jan., 1997.
F. Cohen, S. Cooper, et. al. "Intrusion Detection and Response", National InfoSec Technical Baseline, October, 1996. (Also appearing in SecureNet 97, March, 1997 and Computers and Security as cited above)
F. Cohen, "Managing Network Security: Where Should We Concentrate Protection?", Network Security, Dec., 1996.

F. Cohen, "Managing Network Security: How Good Do You Have to Be?", Network Security, Nov., 1996.
F. Cohen, "Managing Network Security: Why Bother?", Network Security, Oct., 1996.
F. Cohen, "Internet Holes - The SYN Flood", Network Security, Sep., 1996.
F. Cohen, "Internet Holes - Internet Incident Response", Network Security, Aug., 1996.
F. Cohen, "Internet Holes - Internet Lightning Rods", Network Security, July, 1996.
F. Cohen, "Internet Holes - UDP Viruses", Network Security, June, 1996.
F. Cohen, "Internet Holes - Eliminating IP Address Forgery", Network Security, May, 1996.
F. Cohen, "Internet Holes - Spam", Network Security,April , 1996.
F. Cohen, "Internet Holes - The Human Element", Network Security, March, 1996.
F. Cohen, "Internet Holes - Automated Attack and Defense", Network Security, February, 1996.
F. Cohen, "Internet Holes - 50 Ways to Attack Your World Wide Web Systems", Network Security, December, 1995 - January, 1996.
F. Cohen, "Internet Holes - Network News Transfer Protocol ", Network Security, November, 1995.
F. Cohen, "Internet Holes - Sendmail Attacks", Network Security, October, 1995.
F. Cohen, "Internet Holes - Packet Fragmentation Attacks", Network Security, September, 1995.
F. Cohen, "Internet Holes - Internet Control Message Protocol", Network Security, August, 1995.

Software products developed:

F. Cohen - Forensic Fonts, 2009
F. Cohen - Decider, 2007
F. Cohen - JDM, 2006
F. Cohen - Security Decisions, 2006
F. Cohen - Surveyor, 2006
F. Cohen - Influence, 2006
F. Cohen and Garrett Gee, 2002 - White Glove Bootable Linux CD
F. Cohen, 2002 - Responder - large-scale network deception system
F. Cohen and Garrett Gee, 2002 - White Glove developer platform
F. Cohen, Darrian Hale, et. al., 2002 - Resilience - Resilient network infrastructure
F. Cohen, Anthony Carathemus, et. al. 2001 - Secure DNS Server
F. Cohen, Anthony Carathemus, et. al. 2001 - Partition Dump
F. Cohen, Eric Thomas, and Anthony Carathemus, 2001 - Invisible Router
F. Cohen, 2000 - D-Wall - Large-scale high fidelity deception system
F. Cohen, 1999 – ForensiX – Digital Forensics ToolKit for Linux and Unix
F. Cohen, 1999 - Network Security Simulator
F. Cohen and E. Dart, 1998 - DARE - Distributed Analysis and Response
F. Cohen, 1998 - Deception Toolkit
F. Cohen, 1998 - The Security Maze
F. Cohen, 1997 - The Cracking Game
F. Cohen, 1997 - Automated Threat, Attack, and Defense Analysis Tool
F. Cohen, 1996 - CID Database Analysis Tool
F. Cohen, 1995 - Auditor - Internal Audit Tool
F. Cohen, 1995 - Analyzer - Network Audit Tool
F. Cohen, 1995 - Trivial HTTP Daemon - provably secure web server
F. Cohen, 1995 - Secure Gopher Server - provably secure gopher server
F. Cohen, 1993 - Calendar Supplement
F. Cohen, 1992 - PayBack Automated Bill Collection Software
F. Cohen, 1989 - Integrity ToolKit - Integrity Shell and Access Control System
F. Cohen, 1988 - Advanced Software Protection Scanner - Virus Scanner
F. Cohen, 1987 - Advanced Software Protection - Crypto-Checksum Integrity Checker
F. Cohen, 1987 - TRP - Small business office software
F. Cohen, 1986 - VCE - Viral Computing Environment
F. Cohen, 1985 - Legal Assistant - Law Office Software