Computer Security Bibliography

Authors : René Rydhof Hansen
Date : July 5, 2001
Number : SECSAFE-DAIMI-003-1.1
Classification : Public; Pre-Existing Know How;
This work is funded totally by sources outside the SecSafe project.

[1] Martín Abadi. Secrecy by Typing in Security Protocols. In Martín Abadi and Takayasu Ito, editors, *Proc. of Theoretical Aspects of Computer Software*, volume 1281 of *Lecture Notes in Computer Science*, pages 611–638, Sendai, Japan, September 1997. Springer Verlag.

[2] Martín Abadi. Protection in Programming-Language Translations. SRC Research Report 154, Digital Systems Research Center, April 1998.

[3] Martín Abadi. Two Facets of Authentication. In *Proc. of the 11th IEEE Computer Security Foundations Workshop*, pages 27–32. IEEE Computer Society, June 1998. Also appeared as SRC Technical Note 1998-007.

[4] Martín Abadi. Security Protocols and Specifications. In Wolfgang Thomas, editor, *Proc. of Foundations of Software Science and Computational Structures, FoSSaCS'99*, volume 1578 of *Lecture Notes in Computer Science*, pages 1–13, Amsterdam, The Netherlands, March 1999. Springer Verlag. Held as Part of the Joint European Conferences on Theory and Practice of Software (ETAPS'99).

[5] Martín Abadi, Michael Burrows, Charles Kaufman, and Butler Lampson. Authentication and Delegation with Smart-cards. SRC Research Report 67, Digital Systems Research Center, October 1990. Revised Jul. 1992.

[6] Martín Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A Calculus for Access Control in Distributed Systems. SRC Research Report 70, Digital Systems Research Center, February 1991. Revised Aug. 1991.

[7] Martín Abadi and Andrew D. Gordon. A Calculus for Cryptographic Protocols The Spi Calculus. In *Proc. of the 4th ACM Conference on Computer and Communications Security*, pages 36–47. ACM Press, April 1997.

[8] Martín Abadi and Andrew D. Gordon. Reasoning about Cryptographic Protocols in the Spi Calculus. In *Proc. of conference on Concurrency Theory, CONCUR'97*, volume 1243 of *Lecture Notes in Computer Science*, pages 59–73. Springer Verlag, July 1997.

[9] Martín Abadi and Andrew D. Gordon. A Bisimulation Method for Cryptographic Protocols. In *Proc. ESOP'98*, Lecture Notes in Computer Science. Springer Verlag, 1998. Full version appears in Nordic Journal of Computing 5(1998):267–303.

[10] Martín Abadi and Andrew D. Gordon. A Calculus for Cryptographic Protocols: The Spi calculus. SRC Research Report 149, Digital Research, January 1998.

[11] Martín Abadi, Mark A. Lomas, and Roger Needham. Strengthening Passwords. SRC Technical Note 1997-033, Digital Systems Research Center, September 1997. Revised Dec. 1997.

[12] Martín Abadi and Roger Needham. Prudent Engineering Practice for Cryptographic Protocols. SRC Research Report 125, Digital Systems Research Center, June 1994.

[13] Johan Agat. Transforming out Timing Leaks. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, POPL'00*, Boston, Massachusetts, January 2000. ACM Press.

[14] Ross Anderson. How to Cheat at the Lottery (or, Massively Parallel Requirements Engineering). In *Computer Security Applications Conference, ACSAC'99*, pages xix–xxvii, Phoenix, Arizona, USA, December 1999. IEEE Computer Society.

[15] Ross Anderson and Markus Kuhn. Tamper Resistance - a Cautionary Note. In *Proc. Second USENIX Workshop on Electronic Commerce*, pages 1–11, Oakland, California, USA, November 1996.

[16] Ross Anderson and Roger Needham. Programming Satan's Computer. In J. van Leeuwen, editor, *Computer Science Today. Recent Trends and Developments*, volume 1000 of *Lecture Notes in Computer Science*, pages 426–440. Springer Verlag, 1995.

[17] Ross Anderson and Roger Needham. Robustness principles for public key protocols. In Don Coppersmith, editor, *Advances in Cryptology — CRYPTO'95*, volume 963 of *Lecture Notes in Computer Science*, pages 236–247, Santa Barbara, California, USA, August 1995. Springer Verlag.

[18] Ross Anderson, Serge Vaudenay, Bart Preneel, and Kaisa Nyberg. The Newton Channel. In *Proc. of the International Workshop on Information Hiding, IH'96*, 1996.

[19] Ross J. Anderson. Liability and Computer Security: Nine Principles. In *ESORICS*, 1994.

[20] Ross J. Anderson. Why Cryptosystems Fail. *Communications of the ACM*, 37(11):32–40, November 1994.

[21] Ross J. Anderson. A Security Policy Model for Clinical Information Systems. In *Proc. of the IEEE Symposium on Security and Privacy 1996*. IEEE Computer Society, 1996.

[22] Ross J. Anderson. The Eternity Service. In *Proc. of the 1st International Conference on the Theory and Applications of Cryptology, PRAGOCRYPT'96*, Prague, Czech Republic, 1996.

[23] Ross J. Anderson and S. Johann Bezuidenhoudt. On the Reliability of Electronic Payment Systems. *IEEE Transactions on Software Engineering*, May 1996. Earlier version appeared in 1995 IEEE Symposium on Security and Privacy.

[24] Ross J. Anderson, Václav Matyáš Jr., and Fabien A. Petitcolas. The eternal resource locator: an alternative means of establishing trust on the world wide wib. In *Proc. Third USENIX Workshop on Electronic Commerce*, pages 141–153, Boston, Massachusetts, USA, August/September 1998. USENIX.

[25] Ross J. Anderson, Václav Matyáš Jr., Fabien A. Petitcolas, Iain E. Buchan, and Rudolf Hanka. Secure Books: Protecting the Distribution of Knowledge. In *Security Protocol Workshop'97*, Paris, France, April 1997.

[26] Ross J. Anderson and Jong-Hyeon Lee. Jikzi: A New Framework for secure publishing. In *Proc. of the 7th International Workshop on Security Protocols*, 1999.

[27] Ross J. Anderson, Roger Needham, and Adi Shamir. The Steganographic File System. In David Aucsmith, editor, *Proc. of the International Workshop on Information Hiding, IH'98*, volume 1525 of *Lecture Notes in Computer Science*, pages 73–82, Portland, Oregon, USA, April 1998. Springer Verlag.

[28] Gregory R. Andrews and Richard P. Reitman. An Axiomatic Approach to Information Flow in Programs. *ACM Transactions on Programming Languages and Systems*, 2(1):56–76, 1980.

[29] William A. Arbaugh, David J. Farber, and Jonathan M. Smith. A Secure and Reliable Bootstrap Architecture. In *Proc. of the IEEE Symposium on Security and Privacy 1997*, pages 65–81, Oakland, California, USA, May 1997. IEEE Computer Society.

[30] Taimur Aslam. A taxonomy of security faults in the unix operating system. Master's thesis, Department of Computer Science, Purdue University, 1995.

[31] Taimur Aslam, Ivan Krsul, and Eugene H. Spafford. Use of A Taxonomy of Security Faults. Technical Report TR-96-051, COAST Laboratory, Department of Computer Science, Purdue University, 1996. Also presented at 19th National Information Systems Security Conference, October 22–25, 1996, Baltimore, Maryland, USA.

[32] Lee Badger, Daniel F. Sterne, David L. Sherman, Kenneth M. Walker, and Sheila A. Haghighat. Practical Domain and Type Enforcement for UNIX. In *Proc. of the IEEE Symposium on Security and Privacy 1995*. IEEE Computer Society, 1995.

[33] Robert Bagwill, John Barkley (ed), Lisa Carnahan, Shu jen Chang, Richard Kuhn, Paul Markovitz, Anastase Nakassis, Karen Olsen, Michael Ransom, and John Wack. *Security in Open Systems*. National Institute of Standards and Technology. NIST Special Publication 800-7.

[34] Fuat Baran, Howard Kaye, and Margarita Suarez. Security Breaches: Five Recent Incidents at Columbia University. In *Proc. of USENIX Second Security Workshop Program*, pages 151–171. USENIX, August 1990.

[35] Friedrich L. Bauer. *Decrypted Secrets*. Springer Verlag, 1997.

[36] D. Elliot Bell and Leonard J. LaPadula. Secure Computer Systems: Mathematical Foundations. Technical Report ESD-TR-73-278, ESD/AFSC, Hanscom AFB, Bedford, Mass., November 1973. Also appears as MTR-2547, vol. 1, Mitre Corp., Bedford Mass. Digitally reconstructed in 1996.

[37] D. Elliott Bell and Leonard J. LaPadula. Secure Computer Systems: A Mathematical Model. MITRE Technical Report 2547, Vol. 2, MITRE Corporation, May 1973. Digitally recontructed in 1996.

[38] Steven M. Bellovin. Security Problems in the TCP/IP Protocol Suite. *Computer Communications Review*, 19(2):32–48, April 1989.

[39] Steven M. Bellovin. There Be Dragons. In *Proc. of the Third USENIX UNIX Security Symposium*, pages 1–16, Baltimore, September 1992.

[40] Shimshon Berkovits, Joshua D. Guttman, and Vipin Swarup. Authentication for Mobile Agents. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 114–136. Springer Verlag, 1998.

[41] Matt Blaze. A Cryptographic File System for Unix. Preprint of a paper presented at the First ACM Conference on Communications and Computing Security, 1993.

[42] Matt Blaze. Key Management in an Encrypting File System. Preprint of a paper appearing in Proc. Summer 1994 USENIX Technical Conference, Boston, MA, USA, June 1994., 1994.

[43] Matt Blaze. Protocol Failure in the Escrowed Encryption Standard. In *Proc. of the Second ACM Conference on Computer and Communications Security*. ACM Press, November 1994.

[44] Chiara Bodei, Pierpaolo Degano, Flemming Nielson, and Hanne Riis Nielson. Control Flow Analysis for the π-calculus. In D. Sangiorgi and R. de Simone, editors, *Proc. of conference on Concurrency Theory, CONCUR'98*, volume 1466 of *Lecture Notes in Computer Science*, pages 84–98, Nice, France, September 1998. Springer Verlag.

[45] Chiara Bodei, Pierpaolo Degano, Flemming Nielson, and Hanne Riis Nielson. Static Analysis of Processes for No Read-Up and No Write-Down. In Wolfgang Thomas, editor, *Proc. of Foundations of Software Science and Computational Structures, FoSSaCS'99*, volume 1578 of *Lecture Notes in Computer Science*, pages 120–134, Amsterdam, The Netherlands, March 1999. Springer Verlag. Held as Part of the Joint European Conferences on Theory and Practice of Software (ETAPS'99).

[46] Chiara Bodei, Pierpaolo Degano, Flemming Nielson, and Hanne Riis Nielson. Security Analysis using Flow Logics. *EATCS Bulletin*, 70:112–129, 2000.

[47] D. Bolignano. An approach to the formal verification of cryptographic protocols. In *Proc. 3rd ACM Conf. on Computer and Communications Security*, pages 106–118. ACM Press, 1996.

[48] Dan Boneh, Ricahrd A. DeMillo, and Richard J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *Advances in Cryptology — EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer Verlag, 1997.

[49] Colin Boyd and Wenbo Mao. On a Limitation of BAN Logic. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 240–247, Lofthus, Norway, May 1993. Springer Verlag.

[50] David F. C. Brewer and Michael J. Nash. The Chinese Wall Security Policy. In *Proc. of the IEEE Symposium on Security and Privacy 1989*, pages 206–214. IEEE Computer Society, 1989.

[51] Michael Burrows, Martín Abadi, and Roger Needham. A Logic of Authentication. SRC Research Report 39 (revised), Digital Research, December 1989.

[52] Michael Burrows, Martín Abadi, and Roger Needham. A Logic of Authentication. *ACM Transactions on Computer Systems (TOCS)*, 8(1):18–36, February 1990. An abridged version of SRC Research Report 39 ([51]).

[53] Michael Burrows, Martín Abadi, and Roger M. Needham. A Logic of Authentication. In *Proc. of The Royal Society of London A*, volume 426, pages 233–271, 1989.

[54] Iliano Cervesato, Nancy Durgin, Pat Lincoln, John Mitchell, and Andre Scedrov. A Meta-notation for Protocol Analysis. In *Proc of the 12th IEEE Computer Security Foundations Workshop*, Mordano, Italy, June 28–30 1999. IEEE Computer Society.

[55] D. Brent Chapman. Network (In)Security Through IP Packet Filtering. In *Proc. of the Third USENIX UNIX Security Symposium*, Baltimore, MD, USA, September 1992. USENIX.

[56] David M. Chess. Security Issues in Mobile Code Systems. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 1–14. Springer Verlag, 1998.

[57] Bill Cheswick. The Design of a Secure Internet Gateway. In *Proc. of the USENIX Summer 1990 Conference*, pages 233–237, Anaheim, California, USA, June 1990. USENIX.

[58] Bill Cheswick. An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied. In *USENIX Conference Proceedings*, pages 163–174. USENIX, 1992.

[59] David D. Clark and David R. Wilson. A Comparison of Commercial and Military Computer Security Policies. In *Proc. of the IEEE Symposium on Security and Privacy 1987*, pages 184–194. IEEE Computer Society, 1987.

[60] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model*, August 1999. Version 2.1. Also appears as International Standard ISO/IEC 15408:1999. Available for download at `http://cs-www.ncsl.nist.gov/cc/`.

[61] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements*, August 1999. Version 2.1. Also appears as International Standard ISO/IEC 15408:1999. See also Parts 1[60] and 3[62].

[62] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements*, August 1999. Version 2.1. Also appears as International Standard ISO/IEC 15408:1999. See also Parts 1[60] and 2[61].

[63] Oliver Costich, John McLean, and John McDermott. Confidentiality in a Replicated Architecture Trusted Database System: A Formal Model. In *Proc. of the 7th IEEE Computer Security Foundations Workshop*, pages 60–65. IEEE Computer Society, 1994.

[64] David A. Curry. Improving the Security of your UNIX System. Technical Report IT STD-721-FR-90-21, SRI International, April 1990.

[65] Dorothy Denning. *Secure Information Flow in Computer Systems*. PhD thesis, Purdue University, 1975.

[66] Dorothy Denning. A Lattice Model of Secure Information Flow. *Communications of the ACM*, 19(5):236–242, 1976.

[67] Dorothy Denning. *Cryptography and Data Security*. Addison Wesley, 1982.

[68] Dorothy Denning and Peter Denning. Certification of Programs for Secure Information Flow. *Communications of the ACM*, 20(7):504–513, 1977.

[69] Dorothy E. Denning. Secure Personal Computing in an Insecure Network. *Communications of the ACM*, 22(8):476–482, August 1979.

[70] Dorothy E. Denning and Peter J. Denning. Research in Secure Computing. Technical Report CSD-TR-349, Computer Science Department, Purdue University, West Lafayette, Indiana 47907, August 1980.

[71] Dorothy E. Denning and Giovanni M. Sacco. Timestamps in Key Distribution Protocols. *Communications of the ACM*, 24(8):533–536, August 1981.

[72] Department of Defense. *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985. DOD 5200.28-STD. Also known as "The Orange Book" and/or TCSEC. Obsoleted by [60, 61, 62].

[73] Danny Dolev and Andrew C. Yao. On the Security of Public Key Protocols. In *Proc. of the 22nd annual IEEE Symposium on the Foundations of Computer Science*, pages 350–357, October 1981.

[74] Wenliang Du and Aditya P. Mathur. Categorization of Software Errors that led to Security Breaches. In *21st National Information Systems Security Conference*, Crystal City, VA, USA, 1998. Also appears as COAST TR-97-09, 1997.

[75] Mark W. Eichin and Jon A. Rochlis. With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988. In *Proc. of the IEEE Symposium on Security and Privacy 1989*. IEEE Computer Society, 1989.

[76] Taher ElGamal. A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. In G.R. Blakley and David Chaum, editors, *Advances in Cryptology — CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18, Santa Barbara, USA, August 1984. Springer Verlag.

[77] F. Javier Thayer Fábrega, Jonathan C. Herzog, and Joshua D. Guttman. Strand Spaces: Why is a Security Protocol Correct? In *Proc. of the IEEE Symposium on Security and Privacy 1998*, pages 160–171, Oakland, California, USA, May 1998. IEEE Computer Society.

[78] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Web Spoofing: An Internet Con Game. Technical Report 540-96, Department of Computer Science, Princeton University, 1996. Revised Feb. 1997.

[79] Riccardo Focardi, Anna Ghelli, and Roberto Gorrieri. Using Non Interference for the Analysis of Security Protocols. In *Proc. of DIMACS Workshop on Design and Formal Verification of Security Protocols*, DIMACS Center, Rutgers University, September 1997.

[80] Riccardo Focardi and Roberto Gorrieri. A Classification of Security Properties for Process Algebras. *Journal of Computer Security*, 3(1):5–33, 1995.

[81] Riccardo Focardi and Roberto Gorrieri. Non Interference: Past, Present and Future. In *Proc. of DARPA Workshop on Foundations for Secure Mobile Code*, Monterey, California, USA, March 1997.

[82] Joseph A. Goguen and José Meseguer. Security Policies and Security Models. In *Proc. of the IEEE Symposium on Security and Privacy 1982*, pages 11–20, Oakland, California, USA, April 1982.

[83] Joseph A. Goguen and José Meseguer. Unwinding and Inference Control. In *Proc. of the IEEE Symposium on Security and Privacy 1984*, pages 75–86, 1984.

[84] Dieter Gollmann. What do we mean by Entity Authentication? In *Proc. of the IEEE Symposium on Security and Privacy 1996*. IEEE Computer Society, 1996.

[85] Dieter Gollmann. Insider Fraud. In Bruce Christianson, Bruno Crispo, William S. Harbinson, and Michael Roe, editors, *Proc. of the 6th International Workshop on Security Protocols*, volume 1550 of *Lecture Notes in Computer Science*, pages 213–219, Cambridge, UK, April 1998. Springer Verlag.

[86] Dieter Gollmann. *Computer Security*. Wiley Press, 1999.

[87] Li Gong and Roland Schemers. Signing, Sealing, and Guarding Java Objects. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 206–216. Springer Verlag, 1998.

[88] Nevin Heintze and Jon G. Riecke. The SLam calculus: Programming with Secrecy and Integrity. In *Conference Record of the Twenty-Fifth Annual ACM Symposium on Principles of Programming Languages*, pages 365–377. ACM Press, 1998.

[89] Nevin Heintze and J.D. Tygar. A Model for Secure Protocols and Their Compositions. *IEEE Transactions on Software Engineering*, 22(1):16–30, 1996.

[90] Fritz Hohl. Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*. Springer Verlag, 1998.

[91] David K. Hsiao, Douglas S. Kerr, and Stuart E. Madnick. *Computer Security*. ACM Monograph Series. Academic Press, 1979.

[92] Thomas Jensen, Daniel Le Métayer, and Tommy Thorn. Security and Dynamic Class Loading in Java: A Formalisation. In *Proc. IEEE International Conference on Computer Languages*, pages 4–15, Chicago, Illinois, USA, May 1998. IEEE Computer Society. Preliminary version appears as IRISA Technical Report 1137.

[93] Thomas Jensen, Daniel Le Métayer, and Tommy Thorn. Verification of control flow based security properties. In *Proc. of the IEEE Symposium on Security and Privacy 1999*, Oakland, California, USA, May 1999. IEEE Computer Society. Also appears as IRISA Research Report 1210.

[94] David Kahn. *The Codebreakers*. McMillan, 1967.

[95] Richard Y. Kain and Carl E. Landwehr. On Access Checking in Capability-Based Systems. In *Proc. of the IEEE Symposium on Security and Privacy 1986*. IEEE Computer Society, 1986.

[96] Myong H. Kang, Judith N. Froscher, John McDermott, Oliver Costich, and Rodney Peyton. Achieving Database Security Through Data Replication: The SINTRA Prototype. In *Proc. 17th National Computer Security Conference*, pages 77–87, Baltimore, MD, USA, September 1994.

[97] Marc Kekicheff, Forough Kashef, and David Brewer. Open Platform Security. In Isabelle Attali and Thomas Jensen, editors, *Java Card Workshop, JCW'2000*, Cannes, France, September 2000. Proceedings available as an INRIA technical report.

[98] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113, Santa Barbara, California, USA, August 1996. Springer Verlag.

[99] Ivan Victor Krsul. *Software Vulnerability Analysis*. PhD thesis, Purdue University, May 1998.

[100] Charlie Lai, Li Gong, Larry Koved, Anthony Nadalin, and Roland Schemers. User Authentication and Authorization in the Java Platform. In *Computer Security Applications Conference, ACSAC'99*, pages 285–290, Phoenix, Arizona, USA, December 1999. IEEE Computer Society.

[101] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in Distributed Systems: Theory and Practice. SRC Research Report 83, Digital Systems Research Center, 1992. Preliminary version appeared in Proc. of the Thirteenth ACM Symposium on Operating Systems Principles.

[102] Butler W. Lampson. A Note on the Confinement Problem. *Communications of the ACM*, 16(10):613–615, October 1973.

[103] Christopher Landauer and Stephen Crocker. Precise Information Flow Analysis by Program Verification. In *Proc. of the IEEE Symposium on Security and Privacy 1982*. IEEE Computer Society, 1982.

[104] Carl E. Landwehr. Formal Models for Computer Security. *ACM Computing Surveys*, 13(3):247–278, September 1981.

[105] Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi. A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys*, 26(3):211–254, September 1994.

[106] K. Rustan M. Leino and Rajeev Joshi. A Semantic Approach to Secure Information Flow. SRC Technical Note 1997-032, Digital Systems Research Center, December 1997. Also appears in Proc. of Mathematics of Program Construction, Sweden, Lecture Notes in Computer Science 1422, 1998, pages 254–271.

[107] Xavier Leroy and François Rouaix. Security properties of typed applets. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, POPL'98*, pages 391–403, San Diego, CA, USA, 1998. ACM, ACM Press.

[108] Raph Levien and Alexander Aiken. Attack-resistant truct metrics for public key certification. In *Proc. of the 7th USENIX Security Symposium*, pages 229–241, San Antonio, Texas, USA, January 1998. USENIX.

[109] Ulf Lindqvist and Erland Jonsson. How to Systematically Classify Computer Security Intrusions. In *Proc. of the IEEE Symposium on Security and Privacy 1997*, pages 154–163, Oakland, CA, USA, May 1997. IEEE Computer Society.

[110] Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, and John F. Farrell. The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. In *Proc. 21st National Information Systems Security Conference*, pages 303–314, October 1998.

[111] Gavin Lowe. An Attack on the Needham-Schroeder Public-Key Authentication Protocol. *Information Processing Letters*, 56(3):131–133, 1995.

[112] Gavin Lowe. Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR. In Margaria and Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 1055 of *Lecture Notes in Computer Science*, pages 147–166. Springer Verlag, 1996.

[113] Gavin Lowe. Some New Attacks upon Security Protocols. In *Proc. of the 9th IEEE Computer Security Foundations Workshop*, 1996.

[114] Gavin Lowe. A Family of Attacks upon Authentication Protocols. Technical Report 1997/5, Department of Matematics and Computer Science, University of Leicester, January 1997.

[115] Gavin Lowe. A Hierarchy of Authentication Specifications. In *Proc. of the 10th IEEE Computer Security Foundations Workshop*, 1997.

[116] Gavin Lowe. Casper: A Compiler for the Analysis of Security Protocols. In *Proc. of the 10th IEEE Computer Security Foundations Workshop*, pages 18–30. IEEE Computer Society, 1997.

[117] Gavin Lowe. Towards a Completeness Result for Model Checking of Security Protocols. In *Proc. of 11th IEEE Computer Security Foundations Workshop*, pages 96–105, 1998.

[118] Gavin Lowe. Defining Information Flow. Technical Report 1999/3, Department of Mathematics and Computer Science, University of Leicester, 1999.

[119] Daryl McCullough. Noninterference and the Composability of Security Properties. In *Proc. of the IEEE Symposium on Security and Privacy 1988.* IEEE Computer Society, 1988.

[120] Andrew D. McDonald and Markus G. Kuhn. StegFS: A Steganographic File System for Linux. In *Proc. of the International Workshop on Information Hiding, IH'99*, volume 1768 of *Lecture Notes in Computer Science*, pages 463–477, Dresden, Germany, September/October 1999. Springer Verlag.

[121] John McLean. A Comment on the "Basic Security Theorem" of Bell and LaPadula. *Information Procesing Letters*, 20(2):67–70, February 1985.

[122] John McLean. Security Models and Information Flow. In *Proc. of the IEEE Symposium on Security and Privacy 1990.* IEEE Computer Society, 1990.

[123] John McLean. The Specification and Modeling of Computer Security. *Computer*, 23(1), January 1990.

[124] John McLean. Proving Noninterference and Functional Correctness Using Traces. *Journal of Computer Security*, 1(1), 1992.

[125] John McLean. A General Theory of Composition for Trace Sets Closed Under Selective Interleaving Functions. In *Proc. of the IEEE Symposium on Security and Privacy 1994.* IEEE Computer Society, 1994.

[126] John McLean. Security Models. In John Marciniak, editor, *Encyclopedia of Software Engineering*. Wiley Press, 1994.

[127] Catherine Meadows. Using Narrowing in the Analysis of Key Management Protocols. In *Proc. of the IEEE Symposium on Security and Privacy 1989*, pages 138–147. IEEE Computer Society, 1989.

[128] Catherine Meadows. Extending the Brewer-Nash Model to a Multilevel Context. In *Proc. of the IEEE Symposium on Security and Privacy 1990*. IEEE Computer Society, 1990.

[129] Catherine Meadows. A Formal Framework and Evaluation Method for Network Denial of Service. In *Proc. of the 12th IEEE Computer Security Foundations Workshop*. IEEE Computer Society, 1999.

[130] Catherine Meadows. Analysis of the Internet Key Exchange Protocol Using the NRL Protocol Analyzer. In *Proc. of the IEEE Symposium on Security and Privacy 1999*. IEEE Computer Society, 1999.

[131] Alfred Menezes, Paul van Oorschot, and Scott Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. Freely available (for personal use) at `http://www.cacr.math.uwaterloo.ca/hac/index.html`.

[132] Barton P. Miller, Lars Fredriksen, and Bryan So. An Emprirical Study of the Reliability of UNIX Utilities. *Communications of the ACM*, 12(33):32–44, December 1990.

[133] Barton P. Miller, David Koski, Cjin Pheow Lee, Vivekananda Maganty, Ravi Murthy, Ajitkumar Natarajan, and Jeff Steidl. Fuzz Revisited: A Reexamination of the Reliability of UNIX Utilities and Services. Technical report, University of Wisconsin-Madison, 1995.

[134] Masaaki Mizuno and David Schmidt. A Security Flow Control Algorithm and its Denotational Semantics-Based Correctness Proof. *Formal Aspects of Computing*, 4(6A):727–754, 1992.

[135] David Monniaux. Abstracting Cryptographic Protocols with Tree Automata. In Agostino Cortesi and Gilberto Filé, editors, *Proc. Static Analysis Symposium, SAS'99*, volume 1694 of *Lecture Notes in Computer Science*, pages 149–163, Venice, Italy, September 1999. Springer Verlag.

[136] Mark Moriconi, Xiaolei Qian, R. A. Riemenschneider, and Li Gong. Secure Software Architectures. In *Proc. of the IEEE Symposium on Security and Privacy 1997*, pages 84–93, Oakland, CA, USA, May 1997. IEEE Computer Society.

[137] Andrew C. Myers. JFlow: Practical Mostly-Static Information Flow Control. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, POPL'99*, pages 228–241, San Antonio, Texas, USA, January 1999. ACM, ACM Press.

[138] Andrew C. Myers. *Mostly-Static Decentralized Information Flow Control*. PhD thesis, Massachusetts Institute of Technology, January 1999.

[139] Andrew C. Myers and Barbara Liskov. A Decentralized Model for Information Flow Control. In *Proc. of the 16th ACM Symposium on Operating Systems Principles*, Saint-Malo, France, October 1997.

[140] Andrew C. Myers and Barbara Liskov. Complete, Safe Information Flow with Decentralized Labels. In *Proc. of the IEEE Symposium on Security and Privacy 1998*, Oakland, California, USA, May 1998. IEEE Computer Society.

[141] National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* NIST Special Publication 800-12.

[142] George C. Necula. Proof-Carrying Code. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, POPL'97*, pages 106–119, Paris, France, January 1997. ACM, ACM Press.

[143] George C. Necula and Peter Lee. Safe, Untrusted Agents Using Proof-Carrying Code. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 61–91. Springer Verlag, 1998.

[144] Roger M. Needham. Denial of Service: an Example. *Communications of the ACM*, 37(11):42–46, November 1994.

[145] Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978.

[146] Dan M. Nessett. A Critique of Burrows, Abadi, and Needham Logic. *Operating Systems Review*, 24(2):35–38, April 1990. A rejoinder from Burrows, Abadi, and Needham follows on page 39.

[147] Flemming Nielson, Hanne Riis Nielson, René R. Hansen, and Jacob G. Jensen. Validating Firewalls in Mobile Ambients. In *Proc. of conference on Concurrency Theory, CONCUR'99*, volume 1664 of *Lecture Notes in Computer Science*, pages 463–477. Springer Verlag, August 1999.

[148] Flemming Nielson, Hanne Riis Nielson, and René Rydhof Hansen. Validating Firewalls using Flow Logics. To appear. Extended version of [147]., 2001.

[149] Marcus Oestreicher. Transactions in Java Card. In *Computer Security Applications Conference, ACSAC'99*, pages 291–298, Phoenix, Arizona, USA, December 1999. IEEE Computer Society.

[150] Peter Ørbæk and Jens Palsberg. Trust in the λ-calculus. *Journal of Functional Programming*, 3(2):75–85, 1997.

[151] Flavio De Paoli, Andre L. Dos Santos, and Richard A. Kemmerer. Web Browsers and Security. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 235–256. Springer Verlag, 1998.

[152] Lawrence C. Paulson. Proving Properties of Security Protocols by Induction. Technical Report TR409, Computer Laboratory, University of Cambridge, December 1996. Extended version of [154].

[153] Lawrence C. Paulson. Mechanized Proofs for a Recursive Authentication Protocol. In *Proc. of the 10th IEEE Computer Security Foundations Workshop*, pages 84–94. IEEE Computer Society, 1997.

[154] Lawrence C. Paulson. Proving Properties of Security Protocols by Induction. In *Proc. of the 10th IEEE Computer Security Foundations Workshop*, pages 70–83. IEEE Computer Society, 1997.

[155] Lawrence C. Paulson. The Inductive Approach to Verifying Cryptographic Protocols. *Journal of Computer Security*, 6:85–128, 1998.

[156] Birgit Pfitzmann and Michael Waidner. How to Break and Repair a "Provably Secure" Untraceable Payment System. In *Advances in Cryptology — CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 338–350, Santa Barbara, USA, 1991. Springer Verlag.

[157] Birgit Pfitzmann and Michael Waidner. A General Framework for Formal Notions of "Secure" Systems. Hildesheimer Informatikberichte 11/94, Universität Hildesheim, Institut für Informatik, April 1994.

[158] Sylvan Pinsky. Absorbing Covers and Intransitive Non-Interference. In *Proc. of the IEEE Symposium on Security and Privacy 1995*, pages 102–113. IEEE Computer Society, 1995.

[159] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communication*, 1998. Special Issue on Copyright and Privacy Protection.

[160] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[161] A. W. Roscoe and M. H. Goldsmith. What is intransitive noninterference? In *Proc. of the 12th IEEE Computer Security Foundations Workshop*, 1999.

[162] John Rushby. Noninterference, Transitivity, and Channel-Control Security Policies. Technical Report CSL-92-02, SRI International, December 1992.

[163] P. Y. A. Ryan and S. A. Schneider. Process algebra and Non-interference. In *Proc of the 12th IEEE Computer Security Foundations Workshop*. IEEE Computer Society, 1999.

[164] Tomas Sander and Christian F. Tschudin. Protecting Mobile Agents Against Malicious Hosts. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 44–60. Springer Verlag, 1998.

[165] Tomas Sander and Christian F. Tschudin. Towards Mobile Cryptography. In *Proc. of the IEEE Symposium on Security and Privacy 1998*, pages 215–224, Oakland, California, USA, May 1998. IEEE Computer Society.

[166] Ravi S. Sandhu. On Five Definitions of Data Integrity. In *Proc. of the IFIP WG11.3 Workshop on Database Security*, Lake Guntersville, Alabama, USA, September 1993.

[167] Steve Schneider. Security properties and CSP. In *Proc. of the IEEE Symposium on Security and Privacy 1996*. IEEE Computer Society, 1996.

[168] Bruce Schneier. *Applied Cryptography*. Wiley Press, second edition, 1996.

[169] Cristoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni. Analysis of a Denial of Service Attack on TCP. In *Proc. of the IEEE Symposium on Security and Privacy 1997*, pages 208–223, Oakland, CA, USA, May 1997. IEEE Computer Society. Also appears as COAST Technical Report TR 97-06.

[170] Senior Officials Group - Information Systems Security (SOG-IS). *Information Technology Security Evaluation Criteria*, June 1991. The European "Orange Book" and/or ITSEC. Obsoleted by [60, 61, 62].

[171] Geoffrey Smith and Dennis Volpano. Secure Information Flow in a Multi-threaded Imperative Language. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, POPL'98*, pages 355–364, San Diego, CA, USA, January 1998. ACM, ACM Press.

[172] Dawn Xiaodong Song. Athena: a New Efficient Automatic Checker for Security Protocol Analysis. In *Proc of the 12th IEEE Computer Security Foundations Workshop*, Mordano, Italy, June 28–30 1999. IEEE Computer Society.

[173] Eugene H. Spafford. The Internet Worm Program: An Analysis. Purdue Technical Report CSD-TR-823, Department of Computer Science, Purdue University, 1988.

[174] Eugene H. Spafford. The Internet Worm Incident. Technical Report CSD-TR-933, Computer Science Department, Purdue University, West Lafayette, IN USA 47907-2004, September 1991. Also appeared in the Proc. of the 1989 European Software Engineering Conference (ESEC'89), LNCS 87.

[175] Frank Stajano and Ross Anderson. The Cocaine Auction Protocol: On The Power Of Anonymous Broadcast. In A. Pfitzmann, editor, *Proc. of the International Workshop on Information Hiding, IH'99*, Lecture Notes in Computer Science, Dresden, Germany, 1999. Springer Verlag.

[176] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In Bruce Christianson, Bruno Crispo, and Michael Roe, editors, *Proc. of the 7th International Workshop on Security Protocols*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–182, Cambridge, UK, April 1999. Springer Verlag.

[177] William Stallings. *Cryptology and Network Security.* Prentice Hall International, second edition, 1998.

[178] Adam B. Stubblefield and Dan S. Wallach. A Security Analysis of My.MP3.com and the Beam-it Protocol. Technical Report TR-00-353, Department of Commmputer Science, Rice University, February 2000.

[179] Marianne Swanson and Barbara Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* National Institute of Standards and Technology, September 1996. NIST Special Publication 800-14.

[180] Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr. Towards an Analysis of Onion Routing Security. In *Proc. Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, USA, July 2000.

[181] Paul F. Syverson, Michael G. Reed, and David M. Goldschlag. Onion Routing Access Configurations. In *Proc. of the DARPA Information Survivability Conference and Exposition, DISCEX'2000*, pages 34–40. IEEE Computer Society Press, January 2000.

[182] Ken Thompson. Reflections on Trusting Trust. *Communications of the ACM*, 27(8):761–763, August 1984. Turing Award Lecture.

[183] Paul C. van Oorschot. An Alternate Explanation of two BAN-logic "failures". In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 443–447, Lofthus, Norway, May 1993. Springer Verlag.

[184] Giovanni Vigna. Cryptographic Traces for Mobile Agents. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 137–153. Springer Verlag, 1998.

[185] Visa International. *Open Platform Card Protection Profile*, May 2000. Version 0.5.0.1.

[186] Dennis Volpano. Provably-Secure Programming Languages for Remote Evaluation. *SIGPLAN Notices*, 32(1):117–119, January 1997.

[187] Dennis Volpano. Safety versus Secrecy. In Agostino Cortesi and Gilberto Filé, editors, *Proc. Static Analysis Symposium, SAS'99*, volume 1694 of *Lecture Notes in Computer Science*, pages 303–311, Venice, Italy, September 1999. Springer Verlag. Invited talk.

[188] Dennis Volpano. Secure Introduction of One-way Functions. In *Proc. of the 13th IEEE Computer Security Foundations Workshop*, Cambridge, England, July 2000.

[189] Dennis Volpano and Geoffrey Smith. Language Issues in Mobile Program Security. In Giovanni Vigna, editor, *Mobile Agents and Security*, volume 1419 of *Lecture Notes in Computer Science*, pages 44–60. Springer Verlag, 1998.

[190] Dennis Volpano and Geoffrey Smith. Probabilistic Noninterference in a Concurrent Language. In *Proc. of the 11th IEEE Computer Security Foundations Workshop*, Rockport, Massachusetts, USA, June 1998. IEEE Computer Society.

[191] Dennis Volpano and Geoffrey Smith. Verifying Secrets and Relative Secrecy. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, POPL'00*, Boston, MA, USA, January 2000. ACM, ACM Press.

[192] Dennis Volpano, Geoffrey Smith, and Cynthia Irvine. A Sound Type System for Secure Flow Analysis. *Journal of Computer Security*, 4(3):167–187, December 1996.

[193] John P. Wack and Lisa J. Carnahan. *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls.* National Institute of Standards and Technology. NIST Special Publication 800-10.

[194] David Wagner, Jeffrey S. Foster, Eric A. Brewer, and Alexander Aiken. A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities. In *Proc. of the 2000 Network and Distributed Systems Security Conference*, 2000. To appear.

[195] Adam Young and Moti Yung. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 89–103, Santa Barbara, California, USA, August 1996. Springer Verlag.

[196] Che-Fn Yu and Virgil D. Gligor. A Formal Specification and Verification Method for the Prevention of Denial of Service. In *Proc. of the IEEE Symposium on Security and Privacy 1988.* IEEE Computer Society, 1988.