R E S U M E

RICHARD ALLEN KEMMERER

EDUCATION

Ph.D. Computer Science, University of California, Los Angeles, California, 1979

M.S. Computer Science, University of California, Los Angeles, California, 1976

B.S. Mathematics, Pennsylvania State University University Park, Pennsylvania, 1966

RESEARCH INTERESTS

Specification and verification of systems
Computer system security and reliability
Programming and specification language design
Software engineering
Secure Mobile Computing

PROFESSIONAL EXPERIENCE

7/93 - 6/97: Chair, Department of Computer Science, University of California, Santa Barbara

7/89 - Present: Professor, Department of Computer Science, University of California, Santa Barbara

7/85 - 6/89: Associate Professor, Department of Computer Science, University of California, Santa Barbara

9/85 - 5/86: Visiting Scientist, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts

7/79 - 6/85: Assistant Professor, Department of Computer Science, University of California, Santa Barbara

7/79 - Present: System security specification and verification consultant.

Consulting on enhancements to formal verification tools and the specification and verification of secure systems.

2/77 - 6/79: Computer Science Department, UCLA

Research Assistant sponsored by the Advanced Research Projects Agency of the Department of Defense, with the Computer Science Department. This research was concerned with the formal verification of the UCLA Secure Unix Operating System and formed the basis of my dissertation.

11/74 - 1/77: Computer Science Department, UCLA

Programmer for the Department of Computer Science at UCLA. Responsibilities included the design, implementation, checkout, and documentation of computer network simulators to test various network topologies and queuing systems.

1/70 - 9/72: Institute of Transportation and Traffic Engineering, UCLA

Computer Services Manager for ITTE at UCLA. Supervised the programming staff of approximately twenty people. Responsibilities were outlining the general nature of tasks to be performed by the programming staff, planning of programming systems, and assisting in proposal preparations in the areas of computer use and programming requirements.

1/67 - 1/70: Autonetics, Division of Rockwell International, Anaheim, California

Lead Engineer for Minuteman II and Minuteman III inertial navigation computer programs. Responsibilities were generating computer program requirements, and designing, implementing, and documenting computer routines. Additional software experience included using machine and assembly level languages for real-time, online, and scientific applications.

MEMBERSHIPS

ACM Association for Computing Machinery
IEEE Institute of Electrical and Electronics Engineers
IEEE/CS Computer Society of IEEE
IEEE Technical Committee on Security and Privacy, Vice Chairman, 1983-84
IEEE Technical Committee on Security and Privacy, Chairman, 1985-87
IACR International Association of Cryptologic Research
IFIP Working Group 11.3 on Database Security

HONORARIES AND FELLOWSHIPS

Alpha Phi Omega: National Honorary Mathematics Society
Upsilon Pi Epsilon: Computer Science National Honor Society
IBM Predoctoral Fellowship
Outstanding Professor, Department of Computer Science 1981-1982
Outstanding Professor, University of California, Santa Barbara 1983-1984
Speaker, Naval Postgraduate School Distinguished Speaker Series 1990
Speaker, University of California, San Diego Distinguished Lecture Series 1991
Fellow, IEEE Institute of Electrical and Electronics Engineers 1995
Fellow, Association for Computing Machinery 1997
Keynote speaker, First IEEE International Conference on Formal Engineering Methods 1997
Speaker, FAA Software Engineering Distinguished Lecture Series 1998
Keynote speaker, Fourth International Conference on Achieving Quality in Software 1998
Keynote speaker, System Design and Management (SD&M) Internet Conference 1999
IEEE/CS Meritorious Service Award 2001
Speaker, University of Massachusetts Amherst, Distinguished Lecture Series 2002
Speaker, Georgia Tech Information Security Center, Distinguished Lecture Series 2002
IEEE Golden Core Award 2002
Speaker, Michigan State University Computer Science and Engineering, Distinguished Lecture Series 2003
Speaker, University of California, Irvine, Institute for Software Research, Distinguished Lecture Series 2003
Keynote speaker, International Conference on Information Technology 2004
Keynote speaker, NATO Symposium on Adaptive Defence in Unclassified Networks 2004
Speaker, University of Illinois at Urbana-Champaign Information Trust Institute Distinguished Seminar Series 2005
Speaker, University of California, Irvine, Bren School of ICS, Ted and Janice Smith Distinguished Lecture Series 2005
Keynote speaker, Fifth Brazilian Symposium on Information and Computer System Security, Florianopolis, Brazil, 2005
Keynote speaker, 20th IEEE/ACM International Conference on Automated Software Engineering, Long Beach, CA, 2005
Keynote speaker, International Conference on Emerging Trends in Information and Communication Security, Freiburg, Germany, 2006

NATIONAL AND INTERNATIONAL SERVICE

Organization Committee, IEEE Workshop on Communications Security, sponsored by the Data and Communications Committees of the IEEE Communications Society, Santa Barbara, California, August 1981.

Western Area Committee of IEEE Computer Society, 1981-86, Vice Chairman Technical Activities, 1983/84.

Program Committee, Workshop on Effectiveness of Testing and Proving Methods, sponsored by the IEEE Computer Society, Avalon, California, May 1982.

Organization Committee, Workshop on the Theory and Application of Cryptographic Techniques, sponsored by the IEEE Information Theory Group and the IEEE Communications Society, Santa Barbara, California, August 1982.

Invited full-time participant at the National Academy of Science Air Force Studies Board Summer Study Session on Multi-Level Secure Database Management Systems, 1982 (final report "Multilevel Data Management Security," National Academy Press, 1983).

Program Committee, Seventh International Conference on Software Engineering, sponsored by Sigsoft ACM, National Bureau of Standards and IEEE Computer Society, Orlando, Florida, March 1984.

Organization Committee, CRYPTO 84, Workshop on Cryptographic Techniques, sponsored by the International Association for Cryptologic Research, Santa Barbara, California, August 1984.

DoD Task Force on Secure Ada, 1984.

Organization Committee, Third Workshop on Formal Verification, February 1985.

Advisory Board for the ACM's Special Interest Group on Security, Audit, and Control, September 1985 through January, 1992.

National Computer Security Center Formal Verification Working Group (formerly the Formal Verification Panel), since February 1986.

Invited participant at the Office of Technology Assessment workshop on SDI Software, January 1987.

Member of the National Academy of Science National Research Council Committee on Computer Security in the DOE, January 1987 through June 1988 (final report "Computer Security in the Department of Energy's Classified Environment," National Academy Press, 1988).

Invited Participant in the Computer Security Curricula Workshop sponsored by the National Computer Security Center, June 1987.

Member National Institute of Standards and Technology (formerly NBS) Computer and Telecommunications Council since December 1987.

Program Committee, 1988 IEEE Symposium on Security and Privacy, Oakland, California, April 1988.

Member of the DOE/Los Alamos National Laboratory Integrated Computing Network Study Team June 1988 through July 1989.

Invited Participant in the SDI Software Testing and Evaluation Workshop sponsored by the Institute for Defense Analysis, September 1988.

Program Committee, Eleventh National Computer Security Conference, Baltimore, Maryland, October 1988.

Program Committee, Eleventh International Conference on Software Engineering, Pittsburgh, Pennsylvania, March 1989.

Program Committee, 1989 IEEE Symposium on Security and Privacy, Oakland, California, May 1989.

Member of the Editorial Board of the IEEE Transactions on Software Engineering, February 1989 through December 1999.

Member of the National Academy of Science Computer Science and Technology Board's System Security Study Committee, from February 1989 through June 1991 (final report "Computers at Risk: Safe Computing in the Information Age," National Academy Press 1991).

Invited Participant in the Formal Methods Workshop, FM89, sponsored by the U.S., Canadian, and United Kingdom governments, Halifax, Nova Scotia, July 1989.

Invited Participant in the Workshop on Directions in Software Analysis and Testing sponsored by the Office of Naval Research, August 1989.

Invited participant in the Formal Methods and Software Engineering Workshop sponsored by the National Computer Security Center, Linthicum, Maryland, October 1989.

Program Chair, TAV3/SIGSOFT89 -- Testing, Analysis, and Verification Symposium, Key West, Florida, December 1989.

Invited Participant in the DARPA Formal Methods Transition Workshop sponsored by the Defense Advanced Research Projects Agency, Arlington, Virginia, February 1990.

Program Committee, Twelfth International Conference on Software Engineering, Nice, France, March 1990.

Invited Participant at the Mathematical Concepts of Dependable Systems meeting sponsored by the Mathematisches Forschunginstitut Oberwolfach, Oberwolfach, Germany, April 1990.

NSF Formal Methods in Software Engineering Review Panel, Reston, Virginia, May 1990.

Program Committee, European Symposium on Research in Computer Security, ESORICS 90, Toulouse, France, October 1990.

Member of review panel for the Department of Interior's Natural Resources Damage Assessment Model, Washington, D.C., February 1991.

Member of the External Core Review Panel for the Naval Research Laboratory's Basic Research Program, Washington, D.C., February 1991.

Program Committee, Thirteenth International Conference on Software Engineering, Austin, Texas, May 1991.

Program Committee, 1991 IEEE Symposium on Research in Security and Privacy, Oakland, California, May 1991.

Program Committee, Fifth International Conference on the Technology of Object-Oriented Languages and Systems, Santa Barbara, California, August 1991.

Invited Participant in the Formal Methods Workshop, FM91, sponsored by the U.S., Canadian, and United Kingdom governments, Drymen, Scotland, September 1991.

Member of the National Academy of Science Aeronautical and Space Engineering Board's Committee for Review of Oversight Mechanisms for Space Shuttle Flight Software Processes, January 1992 through October 1993 (final report "An Assessment of Space Shuttle Flight Software Development Process," National Academy Press 1993).

Program Co-Chair, 1992 IEEE Symposium on Research in Security and Privacy, Oakland, California, May 1992.

Program Committee, Fourteenth International Conference on Software Engineering, Melbourne, Australia, May 1992.

Member of the Editorial Board of ACM Computing Surveys, July 1992 through April 1996.

Program Committee, Third IFIP Working Conference on Dependable Computing for Critical Applications, Mondello, Sicily, Italy, September 1992.

Program Committee, 15th National Computer Security Conference, Baltimore, Maryland, October 1992.

Program Committee, Eighth Annual Computer Security Applications Conference, San Antonio, Texas, December 1992.

Expert Consultant for the Nuclear Regulatory Commission's Advisory Committee on Nuclear Reactor Safety February 1993 through February 1995.

NSF National Young Investigator Review Panel, Washington, DC, April 1993.

Program Co-Chair, 1993 IEEE Symposium on Research in Security and Privacy, Oakland, California, May 1993.

Member of the BMD Trusted Software Methodology Peer Review Panel, Vero Beach, Florida, October 1993.

Invited Participant, Security Architecture and Separation Kernels Workshop, sponsored by the National Security Agency, Fort Meade, Maryland, March 1994.

Program Committee, Sixteenth International Conference on Software Engineering, Sorrento, Italy, May 1994.

Program Committee, Features Interaction Workshop, Amsterdam, the Netherlands, May 1994.

Program Committee, International Symposium on Software Testing and Analysis, Seattle, Washington, August 1994.

Program Committee, Fifth European Software Engineering Conference, Barcelona Spain, September 1995.

Program Committee, Third International Workshop on Feature Interactions in Telecommunications Software Systems, Kyoto, Japan, October 1995.

Member of the National Academy of Science Computer Science Telecommunications Board's Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, September 1995 through December 1996 (final report "For the Record: Protecting Electronic Health Information," National Academy Press, 1997).

Editor-in-Chief, IEEE Transactions on Software Engineering, January 1996 through December 1999.

Invited Participant, Isaac Newton Institute Research Programm on Computer Security, Cryptology and Coding Theory, Cambridge University, Cambridge, England, April through May 1996.

Program Committee, ICSE 97 International Conference on Software Engineering, Boston, Massachusetts, May 1997.

Member of the National Academy of Science Computer Science Telecommunications Board's Committee on the Review of Programs for Command, Control, Communication, Computers, and Intelligence (C4I) in the Department of Defense, June 1997 through February 2000 (final report "Realizing the Potential of C4I: Fundamental Challenges," National Academy Press, 1999).

Program Committee, Sixth European Software Engineering Conference, Zurich, Switzerland, September 1997.

Program Co-chair, ICSE 98 International Conference on Software Engineering, Kyoto, Japan, April 1998.

Member, IEEE/CS Fellow Evaluation Committee, 1999.

Program Committee, ICSE 00 International Conference on Software Engineering, Limerick, Ireland, June 2000.

Member, IEEE/CS Fellow Evaluation Committee, 2000.

Program Committee, ICSE 01 International Conference on Software Engineering, Toronto, Ontario, Canada, May 2001.

Member, IEEE Computer Society Board of Governors, 2001-2003.

Member, IEEE Computer Society Audit Committee, 2001.

Member, IEEE/CS Fellow Evaluation Committee, 2001.

Program Committee, International Symposium on Recent Advances in Intrusion Detection (RAID 2001), Davis, California, September 2001.

Member, NSF/CISE Advisory Board, 2002-2004.

Vice Chair, IEEE Computer Society Publications Board, 2002.

Program Committee, International Symposium on Recent Advances in Intrusion Detection (RAID 2002), Zurich, Switzerland, September 2002.

Program Committee, 9th ACM Conference on Computer and Communications Security (CCS02), November 2002.

Member, Microsoft Trustworthy Computing Academic Advisory Board, since 2002.

Member, DARPA Independent Assessment Team for DARPA Dem/Val project, September 2002 through December 2004.

Program Committee, Twenty Fifth International Conference on Software Engineering (ICSE03), Portland, Oregon, May 2003.

Program Committee, 2003 IEEE Symposium on Research in Security and Privacy, Oakland, California, May 2003.

Member, IEEE/CS Fellow Evaluation Committee, 2003.

Program Committee, 2003 USENIX Security Symposium, August 2003.

Program Committee, International Symposium on Recent Advances in Intrusion Detection (RAID 2003), Pittsburgh, Pennsylvania, September 2003.

Vice President, IEEE Computer Society, 2004.

Chair, IEEE Computer Society Chapter Activity Board, 2004.

Program Committee, 2004 IEEE Symposium on Research in Security and Privacy, Oakland, California, May 2004.

Program Committee, AusCERT2004 Asia Pacific Information Technology Security Conference, Gold Coast, Australia, May 2004.

Member, IEEE Computer Society Board of Governors, 2005-2007.

Member, IEEE/CS Nominations Committee, 2005.

Program Committee, Twenty Seventh International Conference on Software Engineering (ICSE05), Saint Louis, Missouri, May 2005.

Program Committee, Software Engineering for Secure Systems (SESS05), Saint Louis, Missouri, May 2005.

Program Committee, AusCERT2005 Asia Pacific Information Technology Security Conference, Gold Coast, Australia, May 2005.

Program Committee, Twenty Eighth International Conference on Software Engineering (ICSE06), Shanghai, China, May 2006.

Program Committee, 2006 IEEE Symposium on Research in Security and Privacy, Oakland, California, May 2006.

Program Committee, Fourteenth Annual Network & Distributed System Security Symposium, San Diego, California, February 2007.

Program Committee, Twenty Ninth International Conference on Software Engineering (ICSE07), Minneapolis, Minnesota, May 2007.

PUBLICATIONS

"Assignments and Predicates in KalKan," *Fourth International Conference on the Implementation of Algorithmic Languages,* Courant Institute of New York University, New York, N.Y., June 1976 (with P. Eggert, M. Hall and R. Uzgalis).

"A SIMULA 67 Debugging System," *Fourth International Conference on the Implementation of Algorithmic Languages,* Courant Institute of New York University, New York, N.Y., June 1976.

"An Experience in Group Structured and Modular Programming: Conclusions and Recommendations," *International Symposium on Methodologies for the Design and Construction of Software and Hardware Systems,* Pontifica Universidade Catolica do Rio de Janeiro, Rio de Janeiro, Brazil, July 1976 (with D.M. Berry, I.M. Campos, R.P. Hooper, M.A. Kampe and M.L. Rhodes).

"The Need for a Dynamic MIL," *Tenth Annual Hawaii International Conference on System Sciences,* Honolulu, Hawaii, January 1977.

"Formal Verification of the UCLA Security Kernel: Abstract Model, Mapping Functions, Theorem Generation, and Proofs," Ph.D. Dissertation, UCLA, Los Angeles, California, June 1979.

"Towards Modular Verifiable Exception Handling," *Journal of Computer Languages,* Vol. 5, pp. 77-101, Pergamon Press, Ltd., 1980 (with D.M. Berry, A. von Staa and S. Yemini).

"Specification and Verification of the UCLA Security Kernel," Presented at the *7th Symposium on Operating Systems Principles,* December 1979; *Communications of the ACM,* Vol. 23, No. 2, February 1980 (with B. Walker and G.J. Popek).

"Retrospective: Verification Experiences with the UCLA Operating System Kernel," position paper at the Workshop on Formal Verification, SRI, Menlo Park, California, April 1980 (with B.J. Walker and G.J. Popek). Also appeared in *Software Engineering Notes,* Vol. 5, No. 3, July 1980.

"Applications of SDC's Formal Development Methodology," position paper at the Workshop on Formal Verification, SRI, Menlo Park, California, April 1980 (with M. Schaefer). Also appeared in *Software Engineering Notes,* Vol. 5, No. 3, July 1980.

"FDM - A Specification and Verification Methodology," *Third Seminar on the Department of Defense Security Initiative,* National Bureau of Standards, Gaithersburg, Maryland, November 1980.

"Status Report on SDC's Formal Development Methodology," position paper at the Second Workshop on Formal Verification, National Bureau of Standards, Gaithersburg, Maryland, April 1981. Also appeared in *Software Engineering Notes,* Vol. 6, No. 3, July 1981.

"A Practical Approach to Identifying Storage and Timing Channels," *IEEE Symposium on Security and Privacy,* Oakland, California, April 1982.

"Finding Errors Using Formal Specification and Verification," Workshop on the Effectiveness of Testing and Proving Methods, Avalon, California, May 1982.

"Testing Formal Specifications", Fourth Convention on Quality Assurance, Herzlia, Israel, October 1982.

"SDC Secure Release Terminal Project," *IEEE Symposium on Security and Privacy,* Oakland, California, April 1983 (with T. Hinke and J. Althouse).

"Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels", *ACM Transactions on Computer Systems,* Vol. 1, No. 3, August 1983.

"Testing Formal Specifications to Detect Design Errors," *IEEE Transactions on Software Engineering,* Vol. SE-11, No. 1, January 1985.

"INATEST: an Interactive Environment for Testing Formal Specifications," Third Workshop on Formal Verification, Pajaro Dunes, California, February 1985 (with S. Eckmann). Also appeared in *Software Engineering Notes,* Vol. 10, No. 4, August 1985.

"UNISEX: A UNIx-based Symbolic EXecutor for Pascal," *Software Practice and Experience,* Vol. 15, No. 5, May 1985 (with S. Eckmann).

"Complexity Measures for Assembly Language Programs," *The Journal of Systems and Software,* Vol. 5, No. 3, August 1985 (with D. Blaine).

"Procedural and Nonprocedural Semantics of the ASLAN Formal Specification Language," *Nineteenth Annual Hawaii International Conference on System Sciences,* Honolulu, Hawaii, January 1986 (with B. Auernheimer).

"Analyzing Encryption Protocols Using Formal Verification Techniques," *Eurocrypt 86,* Linkoping, Sweden, May 1986.

"Testing Formal Specifications and the Inatest System," Software Testing Systems Workshop, University of Bremen, Bremen Germany, also appeared in *Softwaretechnik Trends*, June 1986.

"RT-ASLAN: A Specification Language for Real-Time Systems," *IEEE Transactions on Software Engineering,* Vol. SE-12, No. 9, September 1986 (with B. Auernheimer).

"A Brief Summary of a Verification Assessment Study," *Ninth National Computer Security Conference,* Gaithersburg, Maryland, September 1986.

"An Overview of Computer Security," invited paper at *IMA Conference on Cryptography and Coding*, Cirencester, England, December 1986, also included in *Cryptography and Coding*, edited by Henry J. Beker and F.C. Piper, Oxford University Press, 1989.

"An Experience Using Two Covert Channel Analysis Techniques on a Real System Design," *Proceedings of the IEEE Symposium on Security and Privacy,* Oakland, California, April 1986, also appeared in *IEEE Transactions on Software Engineering,* Vol. SE-13, No. 2, February 1987 (with J. Haigh, J. McHugh, and B. Young).

"Using Formal Verification Techniques to Analyze Encryption Protocols," *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, April 1987.

"Analyzing Encryption Protocols Using Formal Verification Techniques," *CRYPTO 87, Workshop on Cryptographic Techniques*, sponsored by the International Association for Cryptologic Research, Santa Barbara, California, August 1987.

"Formal Specification and Verification Techniques for Secure Database Management Systems," *Proceedings of the IFIP WG 11.3 Workshop on Database Security,* Annapolis, Maryland, October 1987, also appeared in *Database Security: Status and Prospects,* edited by C.E. Landwehr, North Holland Publishing Company, Amsterdam, 1988.

"An Interleaving Symbolic Execution Approach for the Formal Verification of Ada Programs with Tasking," *Third International IEEE Conference on Ada Applications and Environments,* Manchester, New Hampshire, May 1988 (with L.J. Harrison).

"An Experience with Two Symbolic Execution Approaches to Formal Verification of Ada Tasking Programs," *Second Workshop on Software Testing, Verification, and Analysis,* Banff, Alberta, Canada, July 1988 (with L. Dillon and L.J. Harrison).

"Critical Gaps in Formal Verification Technology - A Position Paper," SDI Software Testing and Evaluation Workshop, Alexandria, Virginia, September 1988.

"How Soon for Code Level Verification - A Position Paper," *Eleventh National Computer Security Conference,* Baltimore, Maryland, October 1988.

"Completely Validated Software - A Position Paper," *Eleventh International Conference on Software Engineering,* Pittsburgh, Pennsylvania, May 1989.

"Analyzing Encryption Protocols Using Formal Verification Techniques," *IEEE Journal on Selected Areas in Communications,* Vol. 7, No. 4, May 1989.

"The Integration of Formal Specification and Verification Techniques into the Software Engineering Process" - position paper, ONR/ONT Workshop on Directions in Software Testing and Analysis, San Diego, California, August 1989.

"Formal Specification of a Mental Health Delivery System," *Proceedings of the Third IFIP WG 11.3 Working Conference on Database Security,* Monterey, California, September 1989, also appeared in *Database Security III: Status and Prospects,* edited by D. Spooner and C.E. Landwehr, North Holland Publishing Company, Amsterdam, 1990.

"The Need for Formal Specification and Verification Techniques in the Software Engineering Process" - position paper, Formal Methods and Software Engineering Workshop, sponsored by the National Computer Security Center, Linthicum, Maryland, October 1989.

"Integrating Formal Methods into the Development Process," *IEEE Software,* September 1990.

"A Multi-level Formal Specification of a Mental Health Care Database," *Proceedings of the Fourth IFIP WG 11.3 Working Conference on Database Security,* Halifax, England, September 1990, also appeared in *Database Security IV: Status and Prospects,* edited by S. Jajodia and C.E. Landwehr, North Holland Publishing Company, Amsterdam, 1991.

"Covert Flow Trees: A Technique for Identifying and Analyzing Covert Storage Channels," *Proceedings of the IEEE Symposium on Research in Security and Privacy,* Oakland, California, May 1991 (with P. Porras).

"Executing Formal Specifications: the ASTRAL to TRIO Translation Approach," *Proceedings of TAV4: the Symposium on Testing, Analysis, and Verification,* Victoria, B.C., Canada, October 1991 (with C. Ghezzi).

"ASTRAL: An Assertion Language for Specifying Realtime Systems," *Proceedings of the Third European Software Engineering Conference,* Milano, Italy, October 1991 (with C. Ghezzi).

"Covert Flow Trees: A Visual Approach to Analyzing Covert Storage Channels," *IEEE Transactions on Software Engineering,* Vol. 17, No. 11, November 1991 (with P. Porras).

"SoundWorks: An Object Oriented Distributed System for Manipulating Digital Sound," *Computer,* March, 1992 (with J. Reichbach).

"A Formal Support Environment for the Software Development of Realtime Systems," - position paper, Trusted Computer Systems Technology Workshop, sponsored by the Air Force Satellite Control Network, Newport Beach, California, September 1992.

"Guest Editors' Introduction: Specification and Analysis of Real-Time Systems," *IEEE Transactions on Software Engineering*, Vol. 18, No. 9, September 1992 (with C. Ghezzi).

"Penetration State Transition Analysis A Rule-Based Intrusion Detection Approach," *Proceedings of the Eighth Annual Computer Security Applications Conference*, San Antonio, Texas, December 1992 (with P. Porras).

"The Composability of ASTRAL Realtime Specifications," *Proceedings of the International Symposium on Software Testing and Analysis*, Cambridge, Massachusetts, June 1993 (with Alberto Coen-Porisini).

"A Formal Framework for ASTRAL Intra-Level Proof Obligations," *Proceedings of the Fourth European Software Engineering Conference*, Garmisch, Germany, September 1993 (with Alberto Coen-Porisini and Dino Mandrioli).

"Guest Editors' Preface: Special Issue from 1992 Security and Privacy Symposium," *Journal of Computer Security, Vol. 2, No. 2, 1993 (with John McLean).*

"Using Formal Methods to Analyze Encryption Protocols," extended abstract, Workshop on Selected Areas in Cryptography, Kingston, Ontario, Canada, May 1994.

"Three Systems for Cryptographic Protocol Analysis," *Journal of Cryptography*, Vol. 7, No. 2, 1994 (with Cathy Meadows and Jon Millen).

"Aslantest: A Symbolic Execution Tool for Testing Aslan Formal Specifications," *Proceedings of the International Symposium on Software Testing and Analysis*, Seattle, Washington, August 1994 (with Jeffery Douglas).

"A Formal Framework for ASTRAL Intra-Level Proof Obligations," *IEEE Transactions on Software Engineering*, Vol. 20, No. 8, August 1994, (with Alberto Coen-Porisini and Dino Mandrioli).

"State Transition Analysis: A Rule-Based Intrusion Detection Approach," *IEEE Transactions on Software Engineering*, Vol. 21, No. 3, March 1995, (with Koral Ilgun and Phillip Porras).

"A Formal Framework for ASTRAL Inter-Level Proof Obligations," *Proceedings of the Fifth European Software Engineering Conference*, Barcelona, Spain, September 1995 (with Alberto Coen-Porisini and Dino Mandrioli).

"A Modular Covert Channel Analysis Methodology for Trusted DG/UX," *Proceedings of the Twelfth Annual Computer Security Applications Conference*, pp. 224-235, San Diego, California, December 1996 (with Tad Taylor).

"Using the ASTRAL Model Checker for Cryptographic Protocol Analysis," *Proceedings of the DIMACS Workshop on the Design and Formal Verification of Security Protocols*, Plainfield, New Jersey, August 1997 (with Zhe Dang).

"Specification of Realtime Systems Using ASTRAL," *IEEE Transactions on Software Engineering*, Vol. 23, No. 9, pp. 572-598, September, 1997 (with Alberto Coen-Porisini and Carlo Ghezzi).

"Security Issues in Distributed Software," *Proceedings of the Sixth European Software Engineering Conference*, pp. 52-59, Zurich, Switzerland, September 1997.

"Vulnerability of 'Secure' Web Browsers," *Proceedings of the Twentieth National Information Systems Security Conference*, pp. 476-487, Baltimore, Maryland, October 1997 (with Flavio De Paoli and Andre Dos Santos).

"Formally Specifying and Verifying Real-Time Systems," *Proceedings of the First IEEE International Conference on Formal Engineering Methods*, pp. 112-120, Hiroshima, Japan, November 1997 (with Paul Kolano).

"Hoare's Axiomatic Semantics," *Proceedings of the International Symposium on Software Testing and Analysis*, Clearwater Beach, Florida, March 1998.

"Web Browsers and Security," in Mobile Agents and Security, G. Vigna, Ed., *Lecture Notes in Computer Science*, Vol. 1419, pp. 235-256, Springer-Verlag, June 1998 (with Flavio De Paoli and Andre Dos Santos).

"Specification and Analysis of Mobile IP Using ASTRAL," *Proceedings of the Workshop on Formal Methods and Security Protocols*, Indianapolis, Indiana, June 1998 (with Zhe Dang).

"Secure Computing on the Internet," *Proceedings of Softwaretechnik 98*, pp. 1-2, Paderborn, Germany, September 1998.

"NetSTAT: A Network-based Intrusion Detection Approach," *Proceedings of the Fourteenth Annual Computer Security Applications Conference*, Scottsdale, Arizona, December 1998 (with G. Vigna). This paper won the Outstanding Paper Award of the Conference.

"NetSTAT: A Network-based Intrusion Detection System", *Journal of Computer Security*, Vol. 7, No. 1, pp. 37-71, IOS Press, 1999 (with G. Vigna).

"The Design and Analysis of Real-Time Systems Using the ASTRAL Software Development Environment, *Annals of Software Engineering* Vol. 7, pp. 177-210, Baltzer Science Publishers, 1999 (with Z. Dang and P. Kolano).

"Using the ASTRAL Model Checker to Analyze Mobile IP," *Proceedings of the 21st International Conference on Software Engineering (ICSE 99)*, Los Angeles, California, May 1999 (with Z. Dang).

"Safe Areas of Computation for Secure Computing with Insecure Applications," *Proceedings of the Fifteenth Annual Computer Security Applications Conference (ACSAC'99)*, Phoenix, Arizona, December 1999 (with A. dos Santos).

"A Symbolic Model Checker for Testing ASTRAL Real-Time Specifications," *Proceedings of the 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99)*, Hong Kong, December 1999 (with Z. Dang).

"The STAT Tool Suite," *Proceedings of DISCEX 2000*, Hilton Head Island, South Carolina, January 2000 (with G. Vigna and S. Eckmann).

"Parallel Refinement Mechanisms for Real-Time Systems," *Proceedings of Fundamental Approaches to Software Engineering - 2000 (FASE 2000),*, LNCS 1783, pp. 35-50, Berlin, Germany, March 2000 (with P. Kolano and D. Mandrioli).

"Three Approximation Techniques for ASTRAL Symbolic Model Checking of Infinite State Real-time Systems," *Proceedings of the 22nd International Conference on Software Engineering (ICSE 2000)*, Limerick, Ireland, June 2000 (with Z. Dang).

"Binary Reachability Analysis of Discrete Pushdown Timed Automata," *Proceedings of the International Conference on Computer Aided Verification (CAV 2000), Chicago, Illinois, July 2000 (with T. Bultan, Z. Dang, O. Ibarra, and J. Su).*

"Classification Schemes to Aid in the Analysis of Real-Time System Specifications," *Proceedings of the International Symposium on Software Testing and Analysis 2000 (ISSTA 2000)*, Portland, Oregon, August 2000 (with P. Kolano).

"Counter Machines: Decidable Properties and Applications to Verification Problems," *Proceedings of the 25th International Symposium on Mathematical Foundations of Computer Science (MFCS 2000)*, Bratislava, Slovak Republic, August 2000 (with T. Bultan, Z. Dang, O. Ibarra, and J. Su).

"Attack Languages," *Proceedings of the Third Information Survivability Workshop (ISW-2000)*, Boston, Massachusetts, October 2000 (with S. Eckmann and G. Vigna).

"Security Testing of the Online Banking Service of a Large International Bank," *Proceedings of the First Workshop on Security and Privacy in E-Commerce (WSPEC),* Athens, Greece, November 2000 (with A. dos Santos and G. Vigna).

"STATL: An Attack Language for State-based Intrusion Detection," *Proceedings of the Intrusion Detection and Prevention Workshop (WIDS)*, Athens, Greece, November 2000 (with S. Eckmann and G. Vigna).

"Implementing Security Policies Using the Safe Areas of Computation Approach," *Proceedings of the Sixteenth Annual Computer Security Applications Conference (ACSAC'00),* pp. 90-99, New Orleans, Louisiana, December 2000 (with A. dos Santos).

"On Presburger Liveness of Discrete Timed Automata," *Proceedings of the 18th International Symposium on Theoretical Aspects of Computer Science (STACS 2001),* pp. 132-143, Dresden, Germany, February 2001 (with Z. Dang and P. San Pietro).

"Past Pushdown Timed Automata," *Proceedings of the Sixth International Conference on Implementation and Application of Automata, (CIAA 2001),* Pretoria, South Africa, July 2001 (with Z. Dang, T. Bultan, and O. Ibarra).

"Decidable Approximations on Generalized and Parameterized Discrete Timed Automata," *Proceedings of the 7th Annual International Computing and Combinatorics Conference (COCOON 2001),* pp. 529-539, Guilin, China, August 2001 (with Z. Dang and O. Ibarra).

"Designing a Web of Highly-Configurable Intrusion Detection Sensors," *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001),* Vol. 2212 of LNCS, pp. 69-84, Davis, California, October 2001 (with P. Blix and G. Vigna).

"Evaluating the Security Of Three Java-Based Mobile Agent Systems," *Proceedings of the 5th International Conference on Mobile Agents,* Lecture Notes in Computer Science, Vol. 2240, pp. 31-41, Springer-Verlag, Atlanta, GA, December 2001 (with S. Fischmeister and G. Vigna).

"STATL: An Attack Language for State-based Intrusion Detection," *Journal of Computer Security,* Vol. 10, Nos. 1,2, pp. 71-103, 2002 (with S. Eckmann and G. Vigna).

"Intrusion Detection a Brief History and Overview," *Security and Privacy,* supplement to *IEEE Computer,* April 2002 (with G. Vigna). Also translated to Russian and printed in the Russian computer science journal *Open Systems,* November 2002.

"Stateful Intrusion Detection for High-Speed Networks," *Proceedings of IEEE Symposium on Security and Privacy,* Oakland, CA, May 2002 (with C. Kruegel, F. Valeur, and G. Vigna).

"Counter Machines and Verification Problems," *Theoretical Computer Science,* Vol. 289, pp. 165-189, October 2002 (with O. Ibarra, J. Su, Z. Dang, and T. Bultan).

"A Practical Approach to Storage and Timing Channels: Twenty Years Later," *Proceedings of the Eighteenth Annual Computer Security Applications Conference (ACSAC'02),* Las Vegas, Nevada, pp. 109-118, December 2002 (Invited).

"Composable Tools For Network Discovery and Security Analysis," *Proceedings of the Eighteenth Annual Computer Security Applications Conference (ACSAC'02),* Las Vegas, Nevada, pp. 14-24, December 2002 (with G. Vigna, F. Valeur, and J. Zhou).

"Generalized Discrete Timed Automata: Decidable Approximations for Safety Verification," *Theoretical Computer Science,* Vol. 296 (1), pp. 59-74, March 2003 (with Z. Dang and O. Ibarra).

"Presburger Liveness Verification for Discrete Timed Automata," *Theoretical Computer Science,* Vol. 299, pp. 413-438, April 2003 (with Z. Dang and P. San Pietro).

"Cybersecurity," *Proceedings of the 25th International Conference on Software Engineering,* pp. 705-717, Portland, Oregon, May 2003.

"Designing and Implementing A Family of Intrusion Detection Systems," *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2003)*, Helsinki, Finland, September 2003 (with F. Valeur and G. Vigna).

"A Stateful Intrusion Detection System for World-Wide Web Servers," *Proceedings of the Annual Computer Security Applications Conference (ACSAC 2003)*, pp. 34-43, Las Vegas, Nevada, December 2003 (with V. Kher, W. Robertson and G. Vigna).

"An Experience Developing an IDS Stimulator for the Black-Box Testing of Network Intrusion Detection Systems," *Proceedings of the Annual Computer Security Applications Conference (ACSAC 2003)*, pp. 374-383, Las Vegas, Nevada, December 2003 (with D. Mutz and G. Vigna).

"Past Pushdown Timed Automata and Safety Verification," *Theoretical Computer Science*, Vol. 313, pp. 57-71, February 2004 (with T. Bultan, Z. Dang, O. Ibarra).

"A Comprehensive Approach to Intrusion Detection Alert Correlation," *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 3, pp. 146-169, July-September 2004 (with F. Valeur, G. Vigna, and C. Kruegel).

"An Intrusion Detection Tool for AODV-based Ad Hoc Wireless Networks," *Proceedings of the Annual Computer Security Applications Conference (ACSAC 2004)*, pp. 16-27 Tucson, AZ, December 2004 (with G. Vigna, S. Gwalani, K. Srinivasan, and E. Belding-Royer)

"Reverse Engineering of Network Signatures," *Proceedings of the AusCERT Asia Pacific Information Technology Security Conference*, pp. 1-12, Gold Coast, Australia, May 2005 (with D. Mutz, C. Kruegel, W. Robertson, and G. Vigna). This paper won the Best Paper Award of the Conference.

"Hi-DRA: Intrusion Detection for Internet Security," *Proceedings of the IEEE*, special issue on Blue-Sky Electronic Technologies, Vol. 93, No. 10, pp. 1848-1857, October 2005 (with G. Vigna).

"Information Assurance Technology Forecast 2005," *IEEE Security and Privacy Magazine, Vol. 4, No. 1, pp. 62-69, January 2006 (with V. Gligor, T. Haigh, C. Landwehr, S. Lipner, and J. McLean).*

"Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks," *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS06)*, San Diego, CA, February 2006 (with W. Robertson, G. Vigna, and C. Kruegel).

"Digital Forensic Reconstruction and the Virtual Security Testbed ViSe," *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA06)*, pp. 144-163, Berlin, Germany, July 2006 (with A. Arnes, P. Haas, and G. Vigna).

"Behavior-based Spyware Detection," *Proceedings of the 15th USENIX Security Symposium (Security '06)*, Vancouver, B.C., Canada, August 2006 (with G. Banks, E. Kirda, C. Kruegel, and G. Vigna).

"Toward a Stateful NetwOrk prOtocol fuzZEr," *Proceedings of the 9th International Information Security Conference (ISC 2006)*, pp. 343-358, Samos Island, Greece, August 2006 (with G. Banks, M. Cove, V. Felmetsger, K. Almeroth, and G. Vigna).

"Using Hidden Markov Models to Evaluate the Risks of Intrusions: System Architecture and Model Validation," *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 145-164, Hamburg, Germany, September 2006 (with A. Arnes, F. Valeur, and G. Vigna).

"Using a Virtual Security Testbed for Digital Forensic Reconstruction," to appear *Journal in Computer Virology*, Springer, Paris, France (with A. Arnes, P. Haas, and G. Vigna).

BOOKS AND BOOK CHAPTERS

"Towards Modular Verifiable Exception Handling," *Tutorial: Programming Language Design*, A. Wasserman, Editor, IEEE Computer Society Press, 1980 (with D.M. Berry, A. von Staa and S. Yemini).

Formal Verification of an Operating System Security Kernel, UMI Research Press, Ann Arbor, Michigan, 1982.

"RT-ASLAN: A Specification Language for Real-Time Systems," *Hard Real-Time Systems* J.A. Stankovic and K. Ramamritham, Editors, IEEE Computer Society Press, 1988 (with B. Auernheimer).

Computers at Risk: Safe Computing in the Information Age, National Academy Press, Washington, D.C., 1991 (System Security Study Committee of the National Research Council).

"SoundWorks: An Object-Oriented Distributed System for Digital Sound," *Readings in Computer Generated Music*, Denis Baggi, Editor, IEEE Computer Society Press, 1992 (with J. Reichbach).

"Quality Assurance Working Group," *Formal Methods in Systems Engineering*, Peter Ryan and Chris Sennett, Editors, Springer-Verlag, 1993.

"Computer Security," *Encyclopedia of Software Engineering*, John J. Marciniak, Editor-in-Chief, John Wiley & Sons, INC., New York, N.Y., 1994.

For the Record: Protecting Electronic Health Information, National Academy Press, Washington, D.C., 1997, (Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure of the National Research Council).

Realizing the Potential of C4I: Fundamental Challenges, National Academy Press, Washington, D.C., 1999, (Committee on the Review of Programs for Command, Control, Communication, Computers, and Intelligence (C4I) in the Department of Defense of the National Research Council).

"Introduction to On ICSE'S 'Most Influential' Papers," *Software Fundamentals: Collected Papers by David L. Parnas*, D. Hoffman and D. Weiss, editors, Addison Wesley, pp. 569-570, 2001.

"Security Testing of an Online Banking Service," *E-Commerce Security and Privacy*, A. Ghosh, editor, pp. 3-16, Kluwer, 2001 (with A. dos Santos, and G. Vigna).

"Computer Security," *Encyclopedia of Software Engineering*, Second Edition, pp. 206-217, John J. Marciniak, Editor-in-Chief, John Wiley and Sons, INC., New York, N.Y., 2002.

"Sensor Families for Intrusion Detection Infrastructures," *Managing Cyber Threats: Issues, Approaches and Challenges*, pp.181-220, V. Kumar, J. Srivastava, and A. Lazarevic, Editors, Kluwer Academic Publishers, January 2005 (with G. Vigna).