Joshua D. Guttman

The MITRE Corporation and
Worcester Polytechnic Institute
617 610 2765
joshua.guttman@gmail.com
guttman@{mitre.org, wpi.edu} [1]

Employment

The MITRE Corporation Bedford, MA, 1984–2009, full-time employee.
Aug. 2009–Oct. 2010, Sept. 2012–Mar. 2013, part-time employee.
Mar. 2013–present, full-time employee.

2000–present Senior Principal Scientist.

1996–2000 Principal Scientist and Section Leader

1995–96 Principal Scientist.

1994–95 Lead Scientist.

1986–94 Group Leader, Formal Methods.

1984–86 Member of Technical Staff.

Worcester Polytechnic Institute Worcester, MA.

July 2013–present Research Professor of Computer Science.

Aug. 2009–July 2013 Professor of Computer Science.

University of Chicago Spring, 1984. Lecturer. Computer Science.
Summer, 1978. Lecturer. Philosophy.

University of Wisconsin/Milwaukee 1982–83. Lecturer. Philosophy.

Illinois Institute of Technology Winter 1981. Lecturer, Philosophy.

Specialization. Information security theory and applications; logic and formal methods; programming languages.

Education

University of Chicago 1984. Ph.D., philosophy.
Specialized in foundations of mathematics and philosophy of logic. Thesis: "Logical Concepts and Logical Objects." Adviser: William W. Tait.

1976. M.A., philosophy.

Princeton University 1975. A.B. with high honors.

[1] Version of January 4, 2017.

Refereed Journal Publications

1. Joshua D. Guttman and Moses D. Liskov and Paul D. Rowe. Measuring Protocol Strength with Security Goals. Forthcoming, *International Journal of Information Security*. DOI 10.1007/s10207-016-0319-z, February 2016. Springer Link to view-anywhere version: `http://rdcu.be/mF3G`. Author's preliminary version: pubs/ijis_measuring-security.pdf

2. Joshua D. Guttman. Establishing and Preserving Protocol Security Goals. *Journal of Computer Security*, 22(2), pp. 203–267, 2014. pubs/goals_xtended.pdf

3. Ming Li, Sucheng Yu, Joshua D. Guttman, Wenjing Lou, and Kui Ren. Secure ad-hoc trust initialization and key management in wireless body area networks. *ACM Transactions on Sensor Networks (TOSN)*. 9(2), 2013. `http://doi.acm.org/10.1145/2422966.2422975`. pubs/Li_TOSN_2012.pdf

4. Joshua D. Guttman. State and Progress in Strand Spaces: Proving Fair Exchange. *Journal of Automated Reasoning*, 48(2): 159–195, 2012. `http://dx.doi.org/10.1007/s10817-010-9202-1`. pubs/fair_exchange.pdf

5. George S. Coker, Joshua D. Guttman, Peter A. Loscocco, Amy Herzog, Jonathan Millen, Brian O'Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen. Principles of Remote Attestation. *International Journal for Information Security*. 10(2): 63-81, 2011. pubs/remote_attest.pdf

6. Joshua D. Guttman, Amy L. Herzog, John D. Ramsdell, and Clement W. Skorupka. Verifying Information-Flow Goals in Security-Enhanced Linux. *Journal of Computer Security*, 13(1), 2005. Winner, MITRE Best Paper Competition. pubs/selinux_jcs_published_version.pdf

7. Joshua D. Guttman and Amy L. Herzog. Rigorous automated network security management. *International Journal for Information Security*, 3(3), 2005. pubs/ransm_galley_IJIS0052.pdf

8. Joshua D. Guttman, F. Javier Thayer, and Lenore D. Zuck. The faithfulness of abstract protocol analysis: Message authentication. *Journal of Computer Security*, 12(6):865–891, 2004. pubs/faithfulness_abstract_encr.pdf

9. Joshua D. Guttman. Authentication tests and disjoint encryption: a design method for security protocols. *Journal of Computer Security*, 12(3–4):409–433, 2004. pubs/at-design-jcs.pdf

10. J. D. Guttman and F. J. Thayer. Authentication Tests and the Structure of Bundles. *Theoretical Computer Science*, June, 2002. Winner, MITRE Best Paper Competition. pubs/auth_tests_long.pdf

11. W. M. Farmer and J. D. Guttman. A set theory with support for partial functions. *Studia Logica*, 66:59–78, 2000. pubs/set_theory_partial_fns.pdf

12. F. J. Thayer, J. C. Herzog, and J. D. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7(2/3):191–230, 1999. Winner, MITRE Best Paper Competition. pubs/jcs_strand_spaces.pdf

13. Joshua D. Guttman, John D. Ramsdell, and Mitchell Wand. VLISP: A verified implementation of Scheme. *Lisp and Symbolic Computation*, 8(1/2):5–32, 1995. pubs/vlisp_overview.ps

14. Joshua D. Guttman, John D. Ramsdell, and Vipin Swarup. The VLISP verified Scheme system. *Lisp and Symbolic Computation*, 8(1/2):33–110, 1995. pubs/vlisp_scheme.ps

15. W. M. Farmer, J. D. Guttman, and F. J. Thayer. Contexts in mathematical reasoning and computation. *Journal of Symbolic Computation*, 19:201–216, 1995. pubs/jsc_contexts.ps

16. W. M. Farmer and J. D. Guttman. A simple theory of types with partial functions and subtypes. Journal of Symbolic Logic, 58:754, 1993. Abstract.

17. W. M. Farmer, J. D. Guttman, and F. J. Thayer. IMPS: An Interactive Mathematical Proof System. *Journal of Automated Reasoning*, 11:213–248, 1993. Winner, MITRE Best Paper Competition. pubs/imps-overview.pdf

Books and Special Journal Issues Edited

18. Pierpaolo Degano and Joshua D. Guttman. Principles of Security and Trust: Special issue. *Journal of Computer Security*. 21(6), 2013.

19. Pierpaolo Degano and Joshua D. Guttman, eds. *Principles of Security and Trust*. First International Conference, POST 2012, held as part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012. Tallinn, Estonia. Proceedings, Springer LNCS, 2012.

20. Pierpaolo Degano, Sandro Etalle, and Joshua D. Guttman, eds. *Formal Aspects of Security and Trust: Revised Selected Papers*. 7th International Workshop, FAST 2010. Pisa, Italy. Springer LNCS, 2011.

21. Pierpaolo Degano and Joshua D. Guttman, eds. *Formal Aspects of Security and Trust: Revised Selected Papers*. 6th International Workshop, FAST 2009. Eindhoven, Netherlands. Springer LNCS, 2010.

22. Pierpaolo Degano, Joshua D. Guttman, and Fabio Martinelli, eds. *Formal Aspects of Security and Trust: Revised Selected Papers.* 5th International Workshop, FAST 2008. Malaga, Spain. Springer LNCS, 2009.

23. Joshua D. Guttman, ed. *Journal of Computer Security.* Special issue, selected revised papers. Computer Security Foundations Workshop. 17(5). 2009.

24. Joshua D. Guttman, ed. *Journal of Computer Security.* Special issue, selected revised papers. Workshop on Issues in the Theory of Security. 12(1). 2004

25. Li Gong, Joshua D. Guttman, Peter Y. A. Ryan, Steve A. Schneider, eds. *IEEE Journal on Selected Areas in Communications.* Special Issue on Information Security. 21(1). 2003.

26. Joshua D. Guttman and Mitchell Wand, eds. *VLISP: A Verified Implementation of Scheme.* (Special double issue of *Lisp and Symbolic Computation*, 8(1–2).) Kluwer Academic Publishers. 1995.

Refereed Conferences and Invited Publications

27. Joshua D. Guttman, John D. Ramsdell, Paul D. Rowe. Cross-Tool Semantics for Protocol Security Goals. *Security Standardisation Research.* Gaithersburg, MD. Forthcoming, Springer Lecture Notes in Computer Science. Dec. 2016. pubs/cross_tool_ssr16.pdf

28. Stephen Chong, Joshua Guttman, Anupam Datta, Andrew Myers, Benjamin Pierce, Patrick Schaumont, Tim Sherwood, Nickolai Zeldovich. Report on the NSF Workshop on Formal Methods for Security. arXiv:1608.00678

29. Pedro Adão, Riccardo Focardi, Joshua D. Guttman, and Flaminia L. Luccio. Localizing Firewall Security Policies. pubs/localizer_csf16.pdf *IEEE Symposium on Computer Security Foundations.* June 2016.

30. Megumi Ando, Joshua D. Guttman, Alberto R. Papaleo, and John Scire. Hash-based TPM Signatures for the Quantum World. *Intl. Conf. Applied Cryptography and Network Security.* Springer LNCS. June 2016. pubs/qTPM_acns2016.pdf

31. Joshua D. Guttman, Moses D. Liskov, John D. Ramsdell and Paul D. Rowe. Formal Support for Standardizing Protocols with State. *Security Standardisation Research.* Springer LNCS 9497. December 2015. arxiv.org/abs/1509.07552

32. Joshua D Guttman and Paul D Rowe. A Cut Principle for Information Flow. *IEEE Symposium on Computer Security Foundations.* July 2015. pubs/csf-ccut.pdf

33. Joshua D. Guttman. Limited Disclosure and Locality in Graphs. *Programming Languages with Applications to Biology and Security - Essays Dedicated to Pierpaolo Degano on the Occasion of His 65th Birthday.* Springer LNCS 9465, pp. 44–46. November, 2015.

34. Megumi Ando and Joshua D Guttman. Composable Bounds on Information Flow from Distribution Differences. *Data Privacy Management, and Security Assurance, DPM 2015 and QASA 2015*. Springer LNCS 9481, pp. 13–29. September, 2015.

35. Joshua D Guttman and Moses D Liskov and Paul D Rowe. Security Goals and Evolving Standards. *Security Standardisation Research*. Springer LNCS 8893. December, 2014. pubs/ssr_evolving-standards.pdf

36. John D. Ramsdell and Daniel J. Dougherty and Joshua D. Guttman and Paul D. Rowe. A Hybrid Analysis for Security Protocols with State. *Integrated Formal Methods*. LNCS 8739. September 2014. pubs/iFM_stateful_protocols.pdf

37. Daniel J. Dougherty and Joshua D. Guttman. Decidability for Lightweight Diffie-Hellman Protocols. *IEEE Symposium on Computer Security Foundations*. July 2014. pubs/decidable_dh.pdf

38. Yantian Hou, Ming Li and Joshua Guttman. Chorus: Scalable In-band Trust Initialization for Multiple Constrained Devices over the Insecure Wireless Channel. *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*. April 2013. pubs/WiSec13-HouMingGuttman.pdf

39. Marco Carbone and Joshua D. Guttman. Sessions and Separability in Security Protocols. *Principles of Security and Trust*, an ETAPS main conference. To appear, *LNCS ARCoSS* series. March 2013. pubs/CG13_short.pdf, extended version at pubs/CG13_long.pdf.

40. Chuan Lei, Elke A. Rundensteiner and Joshua D. Guttman. Robust Distributed Stream Processing. *IEEE International Conference on Data Engineering*. April, 2013. pubs/ICDE13_conf_full_684.pdf

41. Daniel J. Dougherty and Joshua D. Guttman. An Algebra for Symbolic Diffie-Hellman Protocol Analysis. *Trustworthy Global Computing*, Newcastle, September 2012. Post-proceedings to appear in LNCS. pubs/dh_algebra.pdf

42. Joshua D. Guttman. Security Goals and Protocol Transformations. In *Theory of Security and Applications (TOSCA)*, an ETAPS associated event, March 2011, LNCS. pubs/goals_transformations.pdf

43. Joshua D. Guttman. Shapes: Surveying Crypto Protocol Runs. Invited chapter in *Formal Models and Techniques for Analyzing Security Protocols*, ed. Véronique Cortier and Steve Kremer. IOS Press, 2011, Cryptology and Information Security Series. pubs/shapes_surveying.pdf

44. F. Javier Thayer, Vipin Swarup, and Joshua D. Guttman. Metric Strand Spaces for Locale Authentication Protocols. IFIP Trust Management. pp. 79–94. 2010. pubs/metric_strands.pdf

45. Marco Carbone and Joshua Guttman. Choreographies with Secure Boxes and Compromised Principals. *Interaction and Concurrency Experience (ICE 09)*. Workshop affiliated with Concur. September 2009. Electronic Proceedings in Theoretical Computer Science, `http://eptcs.org/content.cgi?ICE2009`.

46. Joshua D. Guttman. Security Theorems via Model Theory. In *Express 2009: Expressiveness in Concurrency*. Bologna, Sept. 2009. Electronic Proceedings in Theoretical Computer Science. `http://eptcs.org/content.cgi?EXPRESS2009`.

47. Joshua D. Guttman. Fair Exchange in Strand Spaces. *SecCo: 7th International Workshop on Security Issues in Concurrency*. Bologna, Sept. 2009. Electronic Proceedings in Theoretical Computer Science. `http://eptcs.org/content.cgi?SECCO2009`.

48. Joshua D. Guttman. Transformations between Cryptographic Protocols. In *Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security*, ETAPS, March 2009. LNCS. pubs/arpsa-wits-transformations.pdf

49. Joshua D. Guttman. Cryptographic Protocol Composition via the Authentication Tests. In *Foundations of Software Science and Computation Structures (FOSSACS, 2009)*, LNCS, March 2009. pubs/fossacs_disjoint.pdf

50. George S. Coker, Joshua D. Guttman, Peter A. Loscocco, Justin Sheehy, and Brian T. Sniffen. Attestation: Evidence and Trust. In *International Conference on Information and Communications Security*, LNCS 5308, October 2008. Invited lecture. pubs/icics_attestation.pdf

51. Joshua D. Guttman. How to Do Things with Cryptographic Protocols. In *Asian Computer Science Conference*, LNCS 4846. December 2007. Invited lecture.

52. Jay A. McCarthy, Shriram Krishnamurthi, Joshua D. Guttman, and John D. Ramsdell. Compiling cryptographic protocols for deployment on the web. In *16th International Conference on World Wide Web, WWW*. ACM. 2007. pubs/www-compiling-web.pdf

53. Shaddin F. Doghmi, Joshua D. Guttman, and F. Javier Thayer. Completeness of the Authentication Tests. In *European Symposium on Research in Computer Security (ESORICS)*, Springer Lecture Notes in Computer Science, September 2007. pubs/esorics-at-completeness.pdf

54. Shaddin F. Doghmi, Joshua D. Guttman, and F. Javier Thayer. Skeletons, Homomorphisms, and Shapes: Characterizing Protocol Executions. In *Mathematical Foundations of Program Semantics*, Electronic Notes in Theoretical Computer Science, North Holland, April 2007. pubs/mfps_characterizing.pdf

55. Shaddin F. Doghmi, Joshua D. Guttman, and F. Javier Thayer. Skeletons and the Shapes of Bundles. In *Workshop on Issues in the Theory of Security (WITS)*, ETAPS, Braga, Portugal, March 2007. pubs/wits_skeletons.pdf

56. Shaddin F. Doghmi, Joshua D. Guttman, and F. Javier Thayer. Searching for shapes in cryptographic protocols. In *Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, number 4424 in LNCS, pages 523–538. Springer, March 2007. Extended version at URL: `http://eprint.iacr.org/2006/435`. Published version at pubs/tacas_shapes.pdf

57. Joshua D. Guttman, Jonathan C. Herzog, John D. Ramsdell, and Brian T. Sniffen. Programming cryptographic protocols. In Rocco De Nicola and Davide Sangiorgi, editors, *Trust in Global Computing*, LNCS 3705, pages 116–145. Springer, 2005. pubs/pcp_final.pdf

58. Joshua D. Guttman, F. Javier Thayer, Jay C. Carlson, Jonathan C. Herzog, John D. Ramsdell, and Brian T. Sniffen. Trust Management in Strand Spaces. European Symposium on Programming. Springer Verlag LNCS, March 2004. pubs/trust_mgt_in_strand_spaces.pdf

59. Joshua D. Guttman. Security protocol design via authentication tests. In *Proceedings, 15th Computer Security Foundations Workshop*. IEEE Computer Society Press, June 2002. pubs/at_design.pdf

60. Joshua D. Guttman, F. Javier Thayer, and Lenore D. Zuck. The Faithfulness of Abstract Protocol Analysis: Message Authentication. *Proceedings, Eighth ACM Conference on Computer and Communications Security*. November 2001. pubs/ccs_faithful.pdf

61. Joshua D. Guttman. Key compromise and the authentication tests. *Electronic Notes in Theoretical Computer Science*, 47, 2001. Editor, M. Mislove. Invited lecture, *Mathematical Foundations of Programming Semantics*. pubs/compromise.pdf

62. Joshua D. Guttman. *Security goals: Packet trajectories and strand spaces*, in: R. Gorrieri and R. Focardi, editors, *Foundations of Security Analysis and Design*, LNCS 2171, Springer Verlag, 2001. pubs/fosad.pdf

63. Joshua D. Guttman, Amy L. Herzog and F. Javier Thayer. Authentication and Confidentiality via IPsec. In *ESORICS 2000: European Symposium on Research in Computer Security*. Springer Verlag, LNCS 1895, October 2000. pubs/esorics-ipsec.pdf

64. Joshua D. Guttman and F. Javier Thayer. Authentication tests. In *Proceedings, 2000 IEEE Symposium on Security and Privacy*. May 2000. pubs/auth_tests.pdf

65. Joshua D. Guttman and F. Javier Thayer. Protocol Independence via Disjoint Encryption. In *Proceedings of the 13th IEEE Computer Security Foundations Workshop*. July 2000. pubs/disjoint.pdf

66. F. Javier Thayer, Jonathan C. Herzog, and Joshua D. Guttman. Mixed strand spaces. In *Proceedings of the 12th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, June 1999. pubs/mixed_protocols.pdf

67. F. Javier Thayer, Jonathan C. Herzog, and Joshua D. Guttman. Strand Spaces: Why is a Security Protocol Correct? In *Proceedings, 1998 IEEE Symposium on Security and Privacy*. May 1998. pubs/strands_oakland.pdf

68. F. Javier Thayer, Jonathan C. Herzog, and Joshua D. Guttman. Honest ideals on strand spaces. In *Proceedings of the 11th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, June 1998. pubs/honest.pdf

69. Joshua D. Guttman. Filtering Postures: Local enforcement for global security policies. In *Proceedings, 1997 IEEE Symposium on Security and Privacy*. May 1997. pubs/npt-oakland.pdf

70. Shimshon Berkovits, Joshua D. Guttman, and Vipin Swarup. Authentication for Mobile Agents. In *Mobile Agents and Security*, G. Vigna (Ed.). Springer, LNCS 1419. 1998. pubs/sema-lncs98.pdf

71. William M. Farmer, Joshua D. Guttman, and Vipin Swarup. Security for mobile agents: authentication and state appraisal. In *ESORICS '96*. Springer Verlag Lecture Notes in Computer Science, September 1996. pubs/sema-esorics96.pdf

72. William M. Farmer, Joshua D. Guttman, and Vipin Swarup. Security for mobile agents: Issues and Requirements. In *19th National Information Systems Security Conference*. National Institute of Standards and Technology. 1996. pubs/sema-nissc96.pdf

73. William M. Farmer, Joshua D. Guttman, Mark E. Nadel, and F. Javier Thayer. Proof Script Pragmatics in IMPS. In *Automated Deduction: CADE-12*. LNCS 814. 1994. pubs/cade_pragmatics.pdf

74. Joshua D. Guttman and Dale M. Johnson. Three Applications of Formal Methods at MITRE. In *Symposium of Formal Methods Europe, FME*. LNCS 873. 1994.

75. William M. Farmer, Joshua D. Guttman, and F. Javier Thayer. Reasoning with Contexts. In *Design and Implementation of Symbolic Computation Systems, International Symposium, DISCO '93*. LNCS 722. 1993.

76. William M. Farmer, Joshua D. Guttman, and F. Javier Thayer. Little theories. In *Automated Deduction: CADE-11*, LNCS 607. 1992. pubs/cade_little-theories.pdf

77. William M. Farmer, Joshua D. Guttman, and F. Javier Thayer. IMPS: An Interactive Mathematical Proof System. System Description. In *Conference on Automated Deduction (CADE)*. LNCS 449. 1990. (Updated in CADE 1992 and 1996.)

78. Joshua D. Guttman and H.-P. Ko. Verifying a Hardware Security Architecture. In *Proceedings, 1990 IEEE Symposium on Security and Privacy*. May 1990.

79. Joshua D. Guttman and Mark E. Nadel. What Needs Securing. in *Computer Security Foundations Workshop, I*. 1988.

80. Joshua D. Guttman. Information Flow and Invariance. In *Proceedings, 1987 IEEE Symposium on Security and Privacy*. May 1987.

Grants received

MARS *Measuring resilient security*. NSF Eager grant, Sept 2009–Aug 2012. Principal investigator. $290,000.

GLASS *Geometric Logic and Strand Spaces.* Supplement to *Analysis for a Cloud of Policies.* NSF CyberTrust grant, Aug 2012–July 2014. Co-PI. $192,000 supplement.

Courses Taught

Algorithms Sophomore-level undergraduate. D term 2010, B term 2010, B term 2011, B term 2012.

Foundations of Security in Distributed Systems Graduate special topics in theoretical computer science. Spring 2011, Fall 2012.

Logic in Coputer Science Graduate course, Spring 2010, Fall 2011.

Programming Languages Graduate and undergraduate versions concurrently, C term 2012 and Spring 2012.

Software Security Engineering Undergraduate, A term, 2011.

Software Security Graduate, Spring semester 2013, Fall semester 2014.

Tutorials and Short Courses

BISS Bertinoro International Spring School, Italian national graduate program in informatics. Lecturer, 12 hours. March 2013.

FOSAD Summer school in *Foundations of Security: Analysis and Design*, University of Bologna (Bertinoro), invited lecturer (8 hours), September 2000.

MFPS Mathematical Foundations of Programming Semantics, tutorial lecturer (2 hours), Birmingham, May 2005.

NSA National Security Agency. One week course on protocol analysis, jointly with Jonathan C. Herzog and Shaddin F. Doghmi, December 2004.

Pisa Dipartimento dell'Informatica, Università di Pisa, Italy, Doctoral program short course (20 hours), October 2003.

VMCAI Verification, Model Checking and Abstract Interpretation, invited tutorial on security, 2004.

WSSA Winter School on Semantics and its Applications, sponsored by Centre Internationale de Mathématiques Pures et Appliquées and Facultad di Inginiería, Universidad de la República, Montevideo, Uruguay, invited lecturer, six hour sequence of lectures, July 2003.

Program Committees and Editing

ACM CCS ACM Computer and Communications Security conference, Program committee member, 2001, 2002, 2005.

CSF IEEE Computer Security Foundations Workshop. Since 2007, IEEE Symposium on Computer Security Foundations. Steering committee member. Program committee member, 1999, 2001–07, 2009, 2011, 2014–2015.

Program chair, 2005–06.

ESOP European Symposium on Programming, Program Committee member, 2003, 2004, 2007.

ESORICS European Symposium on Research in Computer Security, Program committee member, 2000, 2004, 2015.

FAST Formal Aspects of Security and Trust. Steering committee member. Program Committee member, 2006.

Program co-chair, October 2008, November 2009, September 2010.

FCC Formal and Computational Cryptography, program committee member, 2006, 2007.

FCS LICS Workshop on Foundations of Computer Security. Program Committee Member, 2003–2006, steering committee member.

IEEE JSAC *Journal on Selected Areas in Communication*, Guest editor with Schneider, Ryan, and Gong; January 2003.

IFIP WG 1.7 Working group, Theory of Security. Founding member.

INRIA Institut National de Recherche en Informatique et Automatique, international reviewer, Symbolic Computation A, November 2006.

Evaluation Seminar, March 2011.

JCS *Journal of Computer Security*, Editorial Board member, 2000–2012.

MFPS Mathematical Foundations of Program Semantics, Program Committee member, 2006, 2009.

NASA NASA/Langley formal methods program, program review committee member, 1991.

POST Principles of Security and Trust. Founding program co-chair, with Degano, March 2013. New main conference within the Joint European Conferences on Theory and Practice of Software (ETAPS). First addition to ETAPS since it began in 1998. ETAPS steering committee member.

PLAS ACM Workshop on Programming Languages and Security. Program co-chair, June 2011, with Askarov.

VMCAI Verification, Model Checking and Abstract Interpretation, Program Committee member, 2003.

WITS Workshop on Issues in the Theory of Security, Program Committee member, 2000–2007, 2009–2011.

Program chair, Portland, January 2002.

Invited lectures and colloquium talks

Asian Asian Computing Science Conference, invited lecture, December 2007.

Brown Brown University Computer Science Dept., colloquium talk, Feb. 2006.

CalTech California Institute of Technology, Workshop on Classical and Quantum Information Security, Invited Lecture, December 2005.

Cambridge Cambridge University Computer Science Department, seminar talk, February 2001.

Cornell Cornell University Computer Science Dept., security research technical exchange day and seminar talk, March 2003.

CUNY City University of New York Graduate Center, Department of Computer Science, Colloquium talk, October 2002.

Clifford Lectures Invited lecturer, Tulane University Mathematics Department, March 2002.

DTU Danish Technical University, seminar talk, May 2005.

Darmstadt Technische Universität Darmstadt, Distinguished lecture, June 2010.

DIMACS Invited Lecturer, Discrete Mathematics and Computer Science institute at Rutgers University. Lattice Theory Workshop, July 2003, organizers J. Lawson, M. Mislove.

Invited Lecturer, Security Protocol Workshop, June 2004, organizers R. Canetti, J. Mitchell.

ENS École Normale Supérieure, Abstract Interpretation group, invited lecture, November 2006.

FAST Formal Aspects of Security and Trust, invited lecture, August 2006.

FCS-WITS-Arspa Foundations of Computer Security, Workshop on Issues in the Theory of Security, Automated Reasoning for Security Protocol Analysis (joint meeting). June 2008. Invited lecture.

FMSE ACM Workshop on Formal Methods in Security Engineering. Invited lecture, November 2006.

KSU Distinguished Lecturer Two invited lectures, Kansas State University Computer and Information Science Department, February 2003.

Luxembourg Distinguished Lecture, University of Luxembourg, Nov. 2009.

MFPS Mathematical Foundations of Programming Semantics, Invited lecturer, Aarhus, May 2001. Invited talk, Philadelphia, May 2008.

NPS Naval Postgraduate School, protocol exchange talks, 2004, 2007, 2008.

NCL University of Newcastle, Newcastle, UK, colloquium, Feb. 2008.

Penn University of Pennsylvania, Computer Science Dept., colloquium talk, April 1999.

Security seminar, December 2003.

QMC Queen Mary College, University of London, colloquium, May 2005.

TGC Trustworthy Global Computing, ETAPS, invited lecturer, Edinburgh, April 2005.

UCL Université Catholique de Louvain, Louvain-la-neuve, Belgium, talk, workshop on theory of security, Feb. 2008.

WEBS Workshop on Event-Based Semantics. Cyber-Physical Systems Week, St. Louis, April 2008. Invited talk.

WPI Worcester Polytechnic Institute, colloquium talk, Jan. 2008.

Theses Examined

1. James Heather, PhD, Royal Holloway College, University of London (UK). 2000. External examiner.
2. Emilio Tuosto, PhD, Università di Pisa (Italy). 2002. International reviewer.
3. Alessandro Aldini, PhD, Università di Bologna (Italy). 2002. International reviewer.
4. Olivier Pereira, PhD, Université Catholique de Louvain (Belgium). 2003. Member of jury.
5. Federico Crazzolara, PhD, University of Aarhus (Denmark). 2003. External examiner.
6. Mikael Buchholtz, PhD, Danish Technical University (Denmark), 2005. External examiner.
7. Roberto Delicata, PhD, University of Surrey (UK). 2006. External examiner.

8. Matteo Maffei, PhD, Università di Venezia (Italy). 2006. International reviewer.

9. Aslan Askarov, Licentiate degree, Chalmers University of Technology (Sweden). 2007. Licentiate discussant.

10. Mohammad Torabi Dashti, PhD, Vrije Universiteit (Netherlands). 2008. External examiner.

11. Jay McCarthy, PhD, Brown University (US). 2008. Committee member.

12. Allaa Kamil, DPhil, Oxford University (UK). 2009. External examiner.

13. Veronique Cortier, Habilitation à Diriger la Recherche, LORIA, France. 2009. Examinateur.

14. Pierre-Malo Deniélou, PhD, Université Paris VII, France. 2010. Rapporteur.

15. Danny Yoo, PhD, Worcester Polytechnic Institute. 2012. Committee Member.

16. Simone Frau, PhD, ETH Zurich. 2012. External examiner.

17. Timothy Nelson, PhD, Worcester Polytechnic Institute. 2013. Committee Member.

18. Thomas Gibson-Robinson, DPhil, Oxford University (UK). 2013. External examiner.

19. Robert Künnemann, Doctorate, ENS de Cachan, France. 2014. Jury member.

20. Salman Saghafi, PhD, Worcester Polytechnic Institute. 2015. Committee Member.

21. Juan Diego Campo, PhD, Universidad de la Republica, Montevideo, Uruguay. 2015. External Examiner.