

# Michael K. Reiter

Curriculum Vitae

Last Updated: November 11, 2009

Department of Computer Science  
University of North Carolina at Chapel Hill  
Campus Box 3175, Sitterson Hall  
Chapel Hill, NC 27599-3175 USA

phone: +1-919-962-1836  
<http://www.cs.unc.edu/~reiter/>

## Education

[Cornell University](#), Ithaca, New York, USA.

- Ph.D., Computer Science, August 23, 1993. Thesis: [160]
- M.S., Computer Science, August 26, 1991.

[The University of North Carolina](#), Chapel Hill, North Carolina, USA.

- B.S., Mathematical Sciences with Highest Honors, May 14, 1989.  
Highest Distinction (class rank: 1 of 3476).

## Professional Experience

*Lawrence M. Slifkin Distinguished Professor* (July 2007 – present)

Department of Computer Science, University of North Carolina at Chapel Hill, USA

*Professor of Electrical & Computer Engineering and Computer Science* (October 2001 – June 2007)

*Founding Technical Director, CyLab*

Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

*Director, Secure Systems Research* (September 1998 – September 2001)

Bell Laboratories, Lucent Technologies, Murray Hill, New Jersey, USA

*Principal Technical Staff Member* (June 1996 – September 1998)

*Technical Staff Member* (August 1993 – May 1996)

AT&T Labs – Research, Florham Park, New Jersey, USA (formerly AT&T Bell Laboratories)

*Adjunct Assistant Professor* (spring semester, 1998)

Department of Computer Science, New York University, New York, New York, USA

# Awards and Honors

**ACM Fellow**, named in 2008.

Awards for scientific papers

- Outstanding Paper Award. 1994 IEEE Symposium on Research in Security and Privacy (for [36]).
- Best Paper Award. 3<sup>rd</sup> USENIX Workshop on Electronic Commerce (for [52]).
- Best Paper Award. 8<sup>th</sup> USENIX Security Symposium (for [58]).
- Best Student Paper Award. 8<sup>th</sup> USENIX Security Symposium (for [58]).
- Best Paper Award. 12<sup>th</sup> ISOC Network and Distributed System Security Symposium (for [95]).

Papers invited from the following conferences to appear in journals

- 1994 IEEE Symposium on Research in Security and Privacy ([36] invited, appears as [5])
- 1995 IEEE Symposium on Security and Privacy ([38] invited, appears as [6])
- 3<sup>rd</sup> ACM Conference on Computer and Communications Security ([41] invited, appears as [7])
- 9<sup>th</sup> IEEE Computer Security Foundations Workshop ([43] invited, appears as [8])
- 17<sup>th</sup> IEEE Symposium on Reliable Distributed Systems ([54] invited, appears as [15])
- 13<sup>th</sup> ACM Conference on Computer and Communications Security ([117] invited, appears as [30])
- 13<sup>th</sup> ACM Symposium on Access Control Models and Technologies ([140] invited)

Scholarships, fellowships, and research awards

- John Motley Morehead Scholar. The University of North Carolina, 1985–89.
- United States National Science Foundation (NSF) Graduate Fellow. Cornell University, 1989–92.
- IBM Faculty Partnership Award, 2002–2003.

Excellence in Teaching Award of the Computer Science Student Association, Department of Computer Science, University of North Carolina at Chapel Hill, 2009.

## Scientific Lectures

Since 1993, Dr. Reiter has delivered numerous scientific lectures at scientific symposia, leading universities, and industrial research institutions. Below is a sample of noteworthy invited lectures.

- 6<sup>th</sup> Annual International Workshop on Selected Areas in Cryptography (Kingston, Ontario, Canada). August 10, 1999.
- 2<sup>nd</sup> Conference on Security in Communications Networks (Amalfi, Italy). September 17, 1999.
- 1999 Frontiers in Engineering Symposium, National Academy of Engineering (Irvine, CA, USA). October 14, 1999.
- Keynote address, 2002 Internet Society Symposium on Network and Distributed System Security (San Diego, CA, USA). February 8, 2002.
- Department colloquium, Department of Computer Science, Yale University (New Haven, CT, USA). April 3, 2003.
- Information Security Institute Seminar, Johns Hopkins University (Baltimore, MD, USA). April 8, 2003.
- 2<sup>nd</sup> NJITES Symposium on Cybersecurity and Trustworthy Software, Stevens Institute of Technology (Hoboken, NJ, USA). April 28, 2003.
- Triangle Computer Science Distinguished Lecture, hosted by Duke University, North Carolina State University, and the University of North Carolina (North Carolina, USA). March 1, 2004.
- Conference on Future Directions in Informatics, School of Informatics, Indiana University (Bloomington, IN, USA), September 11, 2004.
- Keynote address, 7<sup>th</sup> International Conference on Information Security and Cryptology (Seoul, Korea). December 2, 2004.
- Distinguished Lecture, Computer Science Department, Stony Brook University (Stony Brook, NY, USA), March 11, 2005.
- Department colloquium, Department of Computer Science, Columbia University (New York, NY, USA). April 6, 2005.
- Institute for Security Technology Studies, Dartmouth College (Hanover, NH, USA). May 19, 2005.
- Advanced Networks Colloquium, hosted by the Center for Satellite and Hybrid Communication Networks, the Department of Electrical and Computer Engineering, and the Institute for Systems Research at the University of Maryland (College Park, MD, USA). September 16, 2005.
- Cornell Computer Science 40<sup>th</sup> Anniversary Symposium, Cornell University (Ithaca, NY, USA). October 1, 2005.
- Distinguished Lecture, Information Trust Institute, University of Illinois at Urbana-Champaign (Urbana, IL, USA). January 18, 2006.
- Information Science & Technology Colloquium, NASA Goddard Space Flight Center (Greenbelt, MD, USA). February 8, 2006.
- ZISC Information Security Colloquium, ETH Zurich (Zurich, Switzerland). May 30, 2006.
- Information Security Institute Seminar, Johns Hopkins University (Baltimore, MD, USA). November 29, 2006.
- Department colloquium, Department of Computer Science, University of North Carolina (Chapel Hill, NC, USA). December 13, 2006.
- Second Workshop of the EU-US Summit Series on Cyber Trust: System Dependability and Security, hosted by the Information Trust Institute, University of Illinois at Urbana-Champaign (Monticello, IL, USA). April 26, 2007.
- Keynote address, 12<sup>th</sup> European Symposium on Research in Computer Security (Dresden, Germany). September 24, 2007.

- Distinguished Lecture, Department of Computer and Information Science, University of Pennsylvania (Philadelphia, PA, USA). October 9, 2007.
- A 30-Year Perspective on Replication (Monte Verita, Ascona, Switzerland). November 7, 2007.
- 3<sup>rd</sup> Bertinoro Ph.D. School on Security of Wireless Networking (Bertinoro, Italy). July 27 – August 1, 2008.
- Distinguished Lecturer Seminar Series, Computer Science Department, University of California at Irvine (Irvine, CA, USA). November 21, 2008.
- Keynote address, 10<sup>th</sup> International Symposium on Stabilization, Safety, and Security of Distributed Systems (Detroit, MI, USA). November 23, 2008.
- School of Electrical and Computer Engineering, Purdue University (West Lafayette, IN, USA). May 7, 2009.
- 7th International Conference on Applied Cryptography and Network Security (Paris-Rocquencourt, France). June 4, 2009.
- Keynote address, 29<sup>th</sup> International Conference on Distributed Computing Systems (Montreal, Canada). June 25, 2009.
- IFIP WG11.3 Conference on Data and Application Security (Montreal, Canada). July 12, 2009.
- Distinguished Speaker, Cray Colloquium Lecture Series, Department of Computer Science and Engineering, University of Minnesota (Minneapolis, MN, USA). October 19, 2009.
- Center for Applied Cybersecurity Research, Indiana University (Bloomington, IN, USA). December 3, 2009.
- Distinguished Colloquium, School of Informatics and Computing, Indiana University (Bloomington, IN, USA). December 4, 2009.
- Distinguished Lecture, Departments of Electrical & Computer Engineering and Computer Science, Iowa State University (Ames, IA, USA). March 12, 2010.

# Professional Service

## Journal editorships

- *ACM Transactions on Information and System Security*  
**Associate Editor** (January 2000–July 2004)  
**Editor-in-Chief** (August 2004–December 2008)
- *Communications of the ACM*  
**Editorial Board member** (November 2007–present)
- *IEEE Transactions on Software Engineering*  
**Associate Editor** (2000–2004)
- *International Journal on Information Security*  
**Associate Editor** (2001–2006)
- *IEEE Transactions on Dependable and Secure Computing*  
**Associate Editor** (2004)  
 Note: Position resigned in 2005 due to other obligations.
- *IEEE Internet Computing*  
 Guest Editor, special issue on Survivable Distributed Systems (November/December 1999 issue)  
 Guest Editor, special issue on Homeland Security (November/December 2004 issue)

## Conference program committees

\* = *Program Chair or Co-Chair*; + = *Program Subcommittee Chair*

ACM Conference on Computer and Communications Security (CCS)	1996, 1997, 1998*, 1999, 2001, 2002, 2003, 2008
ACM Conference on Electronic Commerce	1999, 2003, 2005*
ACM Conference on Information, Computer and Communications Security	2006
ACM Conference on Principles of Distributed Computing (PODC)	1999, 2002, 2005
ACM SIGCOMM Conference	2008
Asia Conference on Computer and Communication Security	2008
CQRE—Secure Networking Conference	1999
Cryptographer's Track, RSA Conference	2001
DARPA Information Survivability Conference and Exposition	2003
European Symposium on Research in Computer Security (ESORICS)	2010
IEEE Computer Security Foundations (CSF)	1995, 1996, 2000, 2004
IEEE Symposium on Reliable Distributed Systems (SRDS)	2005
IEEE Symposium on Security and Privacy	1994, 1995, 1996, 1997, 1998, 1999*, 2000*, 2004, 2005, 2010
IEEE Workshop on Resource Sharing in Massively Distributed Systems	2002
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)	2006, 2007, 2008, 2009

IFIP International Working Conference on Dependable Computing for Critical Applications (DCCA)	1999
IFIP Working Conference on Communications and Multimedia Security	1999
Information Hiding Workshop	2001, 2002, 2004*
Information Security Conference (ISC)	2003, 2004
Information/System Survivability Workshop	2001
International Conference on Distributed Computing Systems (ICDCS)	1999, 2001, 2002, 2005 <sup>†</sup> , 2008, 2010
International Conference on Information and Communications Security	2002
International Conference on Principles of Distributed Systems	2005
International Symposium on Distributed Computing (DISC)	1999, 2004, 2007
International Workshop on Electronic Commerce	2001
International Workshop on Security	1999
Network and Distributed System Security Symposium (NDSS)	2003*, 2004*, 2007, 2009, 2010
Privacy Enhancing Technologies Workshop (PET)	2006, 2007
USENIX Security Symposium	1998, 2002, 2006, 2008, 2009
USENIX Workshop on Hot Topics in Security (HotSec)	2009
Workshop on Intrusion Tolerant Systems	2002
Workshop on Secure Network Protocols	2008
World Wide Web Conference (WWW)	2006

#### Other conference service

- Publicity Chair, 4th ACM Conference on Computer and Communications Security (1997)
- Vice Chair, 1997 IEEE Symposium on Security and Privacy
- General Chair, 1998 IEEE Symposium on Security and Privacy
- General Chair, 8<sup>th</sup> ACM Conference on Computer and Communications Security (2001)
- Steering Committee, ACM Conference on Computer and Communications Security (1999–2002)

#### IEEE Technical Committee on Security and Privacy

- Chair, Subcommittee on Conferences (1998)
- **Vice Chair** (2000–2001)
- **Chair** (2002–2003)

Board of Visitors, [Software Engineering Institute](#), Carnegie Mellon University (July 2003–Aug 2009).

Central Selection Committee, [The Morehead-Cain Scholars Program](#), 2009.

#### U.S. Government service

- INFOSEC Science and Technology Study Group of the INFOSEC Research Council (1997–98)
- DARPA Study Panel on Self-Healing Systems (2001–02)
- Chair, DARPA Workshop on Self-Regenerative Systems (October 2002)
- Chair, National Science Foundation Principal Investigator Meeting (August 2004)
- Organizing Committee, National Science Foundation Study on Grand Challenges in Distributed Computing (July–September 2005)

- NSF Global Environment for Network Innovations (GENI)
  - Distributed Services Working Group (December 2005 – May 2007)
  - Planning Group (March 2006 – May 2007)
- IARPA NICIAR Study on Safely Taking on New Executable Stuff of Uncertain Provenance (May 2008 – August 2008)
- Department of Commerce Emerging Technology and Research Advisory Committee (September 2008 onward)

# Scientific Publications

## Publications in refereed journals

- [1] M. K. Reiter and K. P. Birman. [How to securely replicate services](#). *ACM Transactions on Programming Languages and Systems* 16(3):986–1009, May 1994.
- [2] M. Blaze, J. Lacy, T. London, and M. Reiter. **Issues and mechanisms for trustworthy systems: Creating transparent mistrust**. *AT&T Technical Journal* 73(5):30–39, September 1994.
- [3] M. K. Reiter, K. P. Birman, and R. van Renesse. [A security architecture for fault-tolerant systems](#). *ACM Transactions on Computer Systems* 12(4):340–371, November 1994.
- [4] M. K. Reiter and L. Gong. [Securing causal relationships in distributed systems](#). *The Computer Journal* 38(8):633–642, Oxford University Press, 1995. Preliminary version appears as [35].
- [5] M. K. Reiter. [A secure group membership protocol](#). *IEEE Transactions on Software Engineering* 22(1):31–42, January 1996. Preliminary version appears as [36].
- [6] M. K. Franklin and M. K. Reiter. [The design and implementation of a secure auction service](#). *IEEE Transactions on Software Engineering* 22(5):302–312, May 1996. Preliminary version appears as [38].
- [7] M. K. Reiter, M. K. Franklin, J. B. Lacy, and R. N. Wright. **The  $\Omega$  key management service**. *Journal of Computer Security* 4(4):267–287, IOS Press, 1996. Preliminary version appears as [41].
- [8] D. Malkhi and M. Reiter. **A high-throughput secure reliable multicast protocol**. *Journal of Computer Security* 5:113–127, IOS Press, 1997. Preliminary version appears as [43].
- [9] D. Malkhi and M. Reiter. [Byzantine quorum systems](#). *Distributed Computing* 11(4):203–213, 1998. Preliminary version appears as [46].
- [10] M. K. Reiter and A. D. Rubin. [Crowds: Anonymity for web transactions](#). *ACM Transactions on Information and System Security* 1(1):66–92, November 1998.
- [11] M. K. Reiter and S. G. Stubblebine. [Resilient authentication using path independence](#). *IEEE Transactions on Computers* 47(12):1351–1362, December 1998. Preliminary version appears as [45].
- [12] V. Anupam, A. Mayer, K. Nissim, B. Pinkas, and M. K. Reiter. [On the security of pay-per-click and other web advertising schemes](#). *Computer Networks* 31:1091–1100, 1999. Also appears as [57].
- [13] M. K. Reiter and S. G. Stubblebine. [Authentication metric analysis and design](#). *ACM Transactions on Information and System Security* 2(2):138–158, May 1999. Preliminary version appears as [47].
- [14] D. Malkhi, M. K. Reiter, and A. Wool. [The load and availability of Byzantine quorum systems](#). *SIAM Journal of Computing* 29(6):1889–1906, 2000. Preliminary version appears as [49].
- [15] D. Malkhi and M. K. Reiter. [An architecture for survivable coordination in large distributed systems](#). *IEEE Transactions on Knowledge and Data Engineering* 12(2):187–202, March/April 2000. Combines and extends [53][54].
- [16] D. Malkhi and M. K. Reiter. [Secure execution of Java applets using a remote playground](#). *IEEE Transactions on Software Engineering* 26(12):1197–1209, December 2000. Preliminary version appears as [51].
- [17] R. De Prisco, D. Malkhi, and M. K. Reiter. [On  \$k\$ -set consensus problems in asynchronous systems](#). *IEEE Transactions on Parallel and Distributed Systems* 12(1):7–21, January 2001. Preliminary version appears as [56].
- [18] L. Alvisi, D. Malkhi, E. Pierce, and M. K. Reiter. [Fault detection for Byzantine quorum systems](#). *IEEE Transactions on Parallel and Distributed Systems* 12(9):996–1007, September 2001. Preliminary version appears as [55].
- [19] D. Malkhi, M. K. Reiter, A. Wool, and R. N. Wright. [Probabilistic quorum systems](#). *Information and Computation* 170(2): 184–206, November 1, 2001. Preliminary version appears as [50].

- [20] P. Samarati, M. K. Reiter and S. Jajodia. [An authorization model for a public key management service](#). *ACM Transactions on Information and System Security* 4(4):453–482, November 2001.
- [21] F. Monrose, M. K. Reiter, and S. G. Wetzel. [Password hardening based on keystroke dynamics](#). *International Journal of Information Security* 1(2):69–83, February 2002. Preliminary version appears as [60].
- [22] P. Felber and M. K. Reiter. [Advanced concurrency control in Java](#). *Concurrency and Computation: Practice and Experience* 14(4):261–285, Wiley, 2002.
- [23] D. Malkhi, Y. Mansour and M. K. Reiter. [Diffusion without false rumors: On propagating updates in a Byzantine environment](#). *Theoretical Computer Science* 299:289–306, 2003. Preliminary version appears as [59].
- [24] D. Malkhi, M. Merritt, M. K. Reiter, and G. Taubenfeld. [Objects shared by Byzantine processes](#). *Distributed Computing* 16(1):37–48, 2003. Preliminary version appears as [62].
- [25] P. MacKenzie and M. K. Reiter. [Networked cryptographic devices resilient to capture](#). *International Journal of Information Security* 2(1):1–20, November 2003. Preliminary version appears as [65].
- [26] P. MacKenzie and M. K. Reiter. [Delegation of cryptographic servers for capture-resilient devices](#). *Distributed Computing* 16(4):307–327, December 2003. Preliminary version appears as [72].
- [27] P. MacKenzie and M. K. Reiter. [Two-party generation of DSA signatures](#). *International Journal of Information Security* 2(3–4):218–239, August 2004. Preliminary version appears as [70].
- [28] X. Wang and M. K. Reiter. [A multi-layer framework for puzzle-based denial-of-service defense](#). *International Journal of Information Security*, August 2007. Combines and extends [76][92].
- [29] M. K. Reiter and A. Samar. [Quiver: Consistent object sharing for edge services](#). *IEEE Transactions on Parallel and Distributed Systems* 19(7):878–889, July 2008.
- [30] X. Wang, Z. Li, J. Y. Choi, J. Xu, M. K. Reiter, and C. Kil. [Fast and black-box exploit detection and signature generation for commodity software](#). *ACM Transactions on Information and System Security* 12(2), 2008. Preliminary version appears as [117].
- [31] J. M. McCune, A. Perrig and M. K. Reiter. [Seeing-is-believing: Using camera-phones for human-verifiable authentication](#). *International Journal on Security and Networks* 4(1–2):43–56, 2009. Preliminary version appears as [98].
- [32] D. Gao, M. K. Reiter and D. Song. [Beyond output voting: Detecting compromised replicas using HMM-based behavioral distance](#). *IEEE Transactions on Dependable and Secure Computing* 6(2):96–110, April–June 2009. Preliminary version appears as [115].
- [33] X. Wang and M. K. Reiter. [Using web-referral architectures to mitigate denial-of-service threats](#). *IEEE Transactions on Dependable and Secure Computing*. To appear. Preliminary version appears as [116].

#### Symposium, conference, and workshop publications

- [34] M. K. Reiter, K. P. Birman, and L. Gong. [Integrating security in a group oriented distributed systems](#). In *Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy*, pages 18–32, May 1992. Also appears as [160].
- [35] M. K. Reiter and L. Gong. [Preventing denial and forgery of causal relationships in distributed systems](#). In *Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy*, pages 30–40, May 1993.
- [36] M. K. Reiter. [A secure group membership protocol](#). In *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*, pages 176–189, May 1994. Received **Outstanding Paper Award**.
- [37] M. K. Reiter. [Secure agreement protocols: Reliable and atomic group multicast in Rampart](#). In *Proceedings of the 2<sup>nd</sup> ACM Conference on Computer and Communication Security*, pages 68–80,

- November 1994.
- [38] M. K. Franklin and M. K. Reiter. [The design and implementation of a secure auction service](#). In *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, pages 2–14, May 1995.
  - [39] M. K. Franklin and M. K. Reiter. **Verifiable signature sharing**. In *Advances in Cryptology—EUROCRYPT '95* (Lecture Notes in Computer Science 921), pages 50–63, Springer-Verlag, 1995.
  - [40] M. K. Reiter. **The Rampart toolkit for building high-integrity services**. In *Theory and Practice in Distributed Systems* (Lecture Notes in Computer Science 938), pages 99–110, Springer-Verlag, 1995.
  - [41] M. K. Reiter, M. K. Franklin, J. B. Lacy, and R. N. Wright. [The  \$\Omega\$  key management service](#). In *Proceedings of the 3<sup>rd</sup> ACM Conference on Computer and Communications Security*, pages 38–47, March 1996.
  - [42] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. **Low-exponent RSA with related messages**. In *Advances in Cryptology – EUROCRYPT '96* (Lecture Notes in Computer Science 1070), pages 1–9, Springer-Verlag, 1996.
  - [43] D. Malkhi and M. Reiter. [A high-throughput secure reliable multicast protocol](#). In *Proceedings of the 9<sup>th</sup> IEEE Computer Security Foundations Workshop*, pages 9–17, June 1996.
  - [44] M. K. Franklin and M. K. Reiter. [Fair exchange with a semi-trusted third party](#). In *Proceedings of the 4<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 1–6, April 1997.
  - [45] M. K. Reiter and S. G. Stubblebine. [Path independence for authentication in large-scale systems](#). In *Proceedings of the 4<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 57–66, April 1997.
  - [46] D. Malkhi and M. Reiter. [Byzantine quorum systems](#). In *Proceedings of the 29<sup>th</sup> ACM Symposium on Theory of Computing*, pages 569–578, May 1997.
  - [47] M. K. Reiter and S. G. Stubblebine. [Toward acceptable metrics of authentication](#). In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pages 10–20, May 1997.
  - [48] D. Malkhi and M. Reiter. [Unreliable intrusion detection in distributed computations](#). In *Proceedings of the 10<sup>th</sup> IEEE Computer Security Foundations Workshop*, pages 116–124, June 1997.
  - [49] D. Malkhi, M. Reiter, and A. Wool. [The load and availability of Byzantine quorum systems](#). In *Proceedings of the 16<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, pages 249–257, August 1997.
  - [50] D. Malkhi, M. Reiter, and R. Wright. [Probabilistic quorum systems](#). In *Proceedings of the 16<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, pages 267–273, August 1997.
  - [51] D. Malkhi, M. Reiter, and A. Rubin. [Secure execution of Java applets using a remote playground](#). In *Proceedings of the 1998 IEEE Symposium on Security and Privacy*, pages 40–51, May 1998.
  - [52] M. K. Reiter, V. Anupam, and A. Mayer. **Detecting hit shaving in click-through payment schemes**. In *Proceedings of the 3<sup>rd</sup> USENIX Workshop on Electronic Commerce*, pages 155–166, August 1998. Received **Best Paper Award**.
  - [53] D. Malkhi and M. Reiter. [Survivable consensus objects](#). In *Proceedings of the 17<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 271–279, October 1998.
  - [54] D. Malkhi and M. Reiter. [Secure and scalable replication in Phalanx](#). In *Proceedings of the 17<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 51–58, October 1998.
  - [55] L. Alvisi, D. Malkhi, L. Pierce, and M. K. Reiter. [Fault detection for Byzantine quorum systems](#). In *Proceedings of the 7<sup>th</sup> IFIP Working Conference on Dependable Computing for Critical Applications*, pages 357–371, January 1999.
  - [56] R. De Prisco, D. Malkhi, and M. K. Reiter. [On  \$k\$ -set consensus problems in asynchronous systems](#). In *Proceedings of the 18<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, pages 257–265, May 1999.
  - [57] V. Anupam, A. Mayer, K. Nissim, B. Pinkas, and M. K. Reiter. **On the security of pay-per-click and other web advertising schemes**. In *Proceedings of the 8<sup>th</sup> International World Wide Web*

- Conference, May 1999.
- [58] I. Jermyn, A. Mayer, F. Monrose, A. Rubin, and M. K. Reiter. **The design and analysis of graphical passwords.** In *Proceedings of the 8<sup>th</sup> USENIX Security Symposium*, pages 1–14, August 1999. Received **Best Paper Award**.
  - [59] D. Malkhi, Y. Mansour, and M. K. Reiter. [On diffusing updates in a Byzantine environment.](#) In *Proceedings of the 18<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 134–143, October 1999.
  - [60] F. Monrose, M. K. Reiter, and S. Wetzel. [Password hardening based on keystroke dynamics.](#) In *Proceedings of the 6<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 73–82, November 1999.
  - [61] L. Alvisi, D. Malkhi, E. Pierce, M. K. Reiter, and R. N. Wright. [Dynamic Byzantine quorum systems.](#) In *Proceedings of the 30<sup>th</sup> IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 283–292, June 2000.
  - [62] D. Malkhi, M. Merritt, M. K. Reiter, and G. Taubenfeld. **Objects shared by Byzantine processes.** In *Proceedings of the 14<sup>th</sup> International Symposium on Distributed Computing* (Lecture Notes in Computer Science 1914), pages 345–359, Springer, October 2000.
  - [63] R. M. Arlein, B. Jai, M. Jakobsson, F. Monrose, and M. K. Reiter. [Privacy-preserving global customization.](#) In *Proceedings of the 2000 ACM Conference on Electronic Commerce*, pages 176–184, October 2000.
  - [64] G. Chockler, D. Malkhi, and M. K. Reiter. [Backoff protocols for distributed mutual exclusion and ordering.](#) In *Proceedings of the 21<sup>st</sup> International Conference on Distributed Computing Systems*, pages 11–20, April 2001.
  - [65] P. MacKenzie and M. K. Reiter. [Networked cryptographic devices resilient to capture.](#) In *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, pages 12–25, May 2001.
  - [66] F. Monrose, M. K. Reiter, Q. Li and S. Wetzel. [Cryptographic key generation from voice.](#) In *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, pages 202–213, May 2001.
  - [67] D. Malkhi, M. K. Reiter, D. Tulone, and E. Ziskind. [Persistent objects in the Fleet system.](#) In *Proceedings of the 2<sup>nd</sup> DARPA Information Survivability Conference and Exposition (DISCEX II)*, Vol. II, pages 126–136, June 2001.
  - [68] F. Monrose, M. K. Reiter, Q. Li and S. Wetzel. **Using voice to generate cryptographic keys.** In *Proceedings of 2001: A Speaker Odyssey, The Speaker Recognition Workshop*, pages 237–242, June 2001.
  - [69] R. Canetti, Y. Ishai, R. Kumar, M. K. Reiter, R. Rubinfeld, and R. N. Wright. [Selective private function evaluation with applications to private statistics.](#) In *Proceedings of the 20<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, August 2001.
  - [70] P. MacKenzie and M. K. Reiter. **Two party generation of DSA signatures.** In *Advances in Cryptology—CRYPTO 2001* (Lecture Notes in Computer Science 2139), pages 137–154, August 2001.
  - [71] D. Malkhi, M. K. Reiter, O. Rodeh and Y. Sella. [Efficient update diffusion in Byzantine environments.](#) In *Proceedings of 20<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 90–98, October 2001.
  - [72] P. MacKenzie and M. K. Reiter. [Delegation of cryptographic servers for capture-resilient devices.](#) In *Proceedings of the 8<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 10–19, November 2001.
  - [73] M. Jakobsson and M. K. Reiter. **Discouraging software piracy using software aging.** In *Proceedings of the 2001 Workshop on Security and Privacy in Digital Rights Management*, November 2001.
  - [74] Y. Xie, D. O'Hallaron and M. K. Reiter. [A secure distributed search system.](#) In *Proceedings of the 11<sup>th</sup> IEEE International Symposium on High Performance Distributed Computing*, pages 321–330, July 2002.

- [75] F. Monrose, M. K. Reiter, Q. Li, D. P. Lopresti, and C. Shih. **Toward speech-generated cryptographic keys on resource constrained devices.** In *Proceedings of the 11<sup>th</sup> USENIX Security Symposium*, pages 283–296, August 2002.
- [76] X. Wang and M. K. Reiter. [Defending against denial-of-service attacks with puzzle auctions.](#) In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 78–92, May 2003.
- [77] A. Akella, A. Bharambe, M. Reiter and S. Seshan. **Detecting DDoS attacks on ISP networks.** In *Proceedings of the ACM SIGMOD/PODS Workshop on Management and Processing of Data Streams*, June 2003.
- [78] M. K. Reiter, A. Samar and C. Wang. [The design and implementation of a JCA-compliant capture protection infrastructure.](#) In *Proceedings of the 22<sup>nd</sup> IEEE Symposium on Reliable Distributed Systems*, October 2003.
- [79] P. MacKenzie, A. Oprea, and M. K. Reiter. [Automatic generation of two-party cryptographic protocols.](#) In *Proceedings of the 10<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 210–219, November 2003.
- [80] P. MacKenzie, M. K. Reiter and K. Yang. **Alternatives to non-malleability: Definitions, constructions and applications.** In *Theory of Cryptography: Proceedings of the 1<sup>st</sup> Theory of Cryptography Conference*, (Lecture Notes in Computer Science 2951), pages 171–190, February 2004.
- [81] B. Levine, M. K. Reiter, C. Wang, and M. Wright. **Timing attacks in low-latency mix-based systems.** In *Financial Cryptography: 8<sup>th</sup> International Conference, FC 2004* (Lecture Notes in Computer Science 3110), pages 251–265, February 2004.
- [82] M. Collins and M. K. Reiter. [An empirical analysis of target-resident DoS filters.](#) In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, pages 103–114, May 2004.
- [83] G. Perng, C. Wang and M. K. Reiter. **Providing content-based services in a peer-to-peer environment.** In *Proceedings of the 3<sup>rd</sup> International Workshop on Distributed Event-Based Systems*, May 2004.
- [84] L. Kissner, A. Oprea, M. K. Reiter, D. Song, and K. Yang. **Private keyword-based push and pull with applications to anonymous communication.** In *Proceedings of the 2nd International Conference on Applied Cryptography and Network Security* (Lecture Notes in Computer Science 3089), pages 16–30, June 2004.
- [85] G. Goodson, J. Wylie, G. Ganger and M. K. Reiter. [Efficient Byzantine-tolerant erasure-coded storage.](#) In *Proceedings of the 34<sup>th</sup> IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2004.
- [86] D. Gao, M. K. Reiter, and D. Song. **On gray-box program tracking for anomaly detection.** In *Proceedings of the 13<sup>th</sup> USENIX Security Symposium*, pages 103–118, August 2004.
- [87] D. Davis, F. Monrose and M. K. Reiter. **On user choice in graphical password schemes.** In *Proceedings of the 13<sup>th</sup> USENIX Security Symposium*, pages 151–164, August 2004.
- [88] Y. Xie, H. Kim, D. R. O’Hallaron, M. K. Reiter and H. Zhang. **Seurat: A pointillist approach to anomaly detection.** In *Recent Advances in Intrusion Detection: 7th International Symposium, RAID 2004* (Lecture Notes in Computer Science 3224), pages 238–257, September 2004.
- [89] C. Fry and M. K. Reiter. [Nested objects in a Byzantine quorum-replicated system.](#) In *Proceedings of the 23<sup>rd</sup> IEEE Symposium on Reliable Distributed Systems*, pages 79–89, October 2004.
- [90] D. Davis, F. Monrose, and M. K. Reiter. **Efficient time-scoped searching of encrypted audit logs.** In *Information and Communications Security: 6<sup>th</sup> International Conference, ICICS 2004* (Lecture Notes in Computer Science 3269), pages 532–545, October 2004.
- [91] M. K. Reiter and X. Wang. [Fragile mixing.](#) In *Proceedings of the 11<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 227–235, October 2004.
- [92] X. Wang and M. K. Reiter. [Mitigating bandwidth-exhaustion attacks using congestion puzzles.](#) In *Proceedings of the 11<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 257–

267, October 2004.

- [93] D. Gao, M. K. Reiter and D. Song. [Gray-box extraction of execution graphs for anomaly detection](#). In *Proceedings of the 11<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 318–329, October 2004.
- [94] V. Sekar, Y. Xie, D. Maltz, M. K. Reiter and H. Zhang. **Toward a framework for Internet forensic analysis**. In *Proceedings of the 3<sup>rd</sup> Workshop on Hot Topics in Networks (HOTNETS-III)*, November 2004.
- [95] A. Oprea, M. K. Reiter and K. Yang. **Space-efficient block storage integrity**. In *Proceedings of the 12<sup>th</sup> Network and Distributed System Security Symposium*, February 2005. Received **Best Paper Award**.
- [96] J. M. McCune, E. Shi, A. Perrig and M. K. Reiter. [Detection of denial-of-message attacks on sensor network broadcasts](#). In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 64–78, May 2005.
- [97] L. Bauer, S. Garriss and M. K. Reiter. [Distributed proving in access-control systems](#). In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 81–95, May 2005.
- [98] J. M. McCune, A. Perrig and M. K. Reiter. [Seeing-is-believing: Using camera phones for human-verifiable authentication](#). In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 110–124, May 2005.
- [99] Y. Xie, V. Sekar, D. A. Maltz, M. K. Reiter and H. Zhang. [Worm origin identification using random moonwalks](#). In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 242–256, May 2005.
- [100] M. K. Reiter, X. Wang and M. Wright. [Building reliable mix networks with fair exchange](#). In *Applied Cryptography and Network Security: Third International Conference, ACNS 2005 (Lecture Notes in Computer Science 3531)*, pages 378–392, June 2005.
- [101] G. Perng, M. K. Reiter and C. Wang. [Censorship resistance revisited](#). In *Information Hiding: 7th International Workshop, IH 2005 (Lecture Notes in Computer Science 3727)*, pages 62–76, June 2005.
- [102] A. Gupta, B. M. Maggs, F. Oprea and M. K. Reiter. [Quorum placement in networks to minimize access delays](#). In *Proceedings of the 24<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, pages 87–96, July 2005.
- [103] L. Bauer, S. Garriss, J. McCune, M. K. Reiter, J. Rouse and P. Rutenbar. [Device-enabled authorization in the Grey system](#). In *Information Security: 8<sup>th</sup> International Conference, ISC 2005 (Lecture Notes in Computer Science 3650)*, pages 431–446, Springer-Verlag, September 2005.
- [104] D. Gao, M. K. Reiter and D. Song. [Behavioral distance for intrusion detection](#). In *Recent Advances in Intrusion Detection: 8<sup>th</sup> International Symposium, RAID 2005 (Lecture Notes in Computer Science 3858)*, pages 63–81, September 2005.
- [105] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter and J. J. Wylie. [Fault-scalable Byzantine fault-tolerant services](#). In *Proceedings of the 20<sup>th</sup> ACM Symposium on Operating Systems Principles*, pages 59–74, October 2005.
- [106] M. K. Reiter, A. Samar and C. Wang. [Distributed construction of a fault-tolerant network from a tree](#). In *Proceedings of the 24<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 155–165, October 2005.
- [107] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie. [Lazy verification in fault-tolerant distributed storage systems](#). In *Proceedings of the 24<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 179–190, October 2005.
- [108] J. M. McCune, A. Perrig and M. K. Reiter. **Bump in the ether: A framework for securing sensitive user input**. In *Proceedings of the 2006 USENIX Annual Technical Conference*, pages 185–198, June 2006.

- [109] V. Sekar, Y. Xie, M. K. Reiter and H. Zhang. [A multi-resolution approach to worm detection and containment](#). In *Proceedings of the 36<sup>th</sup> IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 189–198, June 2006.
- [110] G. Perng, M. K. Reiter and C. Wang. [M2: Multicasting mixes for efficient and anonymous communication](#). In *Proceedings of the 26<sup>th</sup> International Conference on Distributed Computing Systems*, July 2006.
- [111] D. Golovin, A. Gupta, B. M. Maggs, F. Oprea and M. K. Reiter. [Quorum placement in networks: Minimizing network congestion](#). In *Proceedings of the 25<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, pages 16–25, July 2006.
- [112] A. Oprea and M. K. Reiter. [On consistency of encrypted files](#). In *Distributed Computing: 20<sup>th</sup> International Symposium, DISC 2006* (Lecture Notes in Computer Science 4167), pages 254–268, September 2006.
- [113] M. P. Collins and M. K. Reiter. [Finding peer-to-peer file-sharing using coarse network behaviors](#). In *Computer Security – ESORICS 2006: 11<sup>th</sup> European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 4189), pages 1–17, September 2006.
- [114] D. Garg, L. Bauer, K. Bowers, F. Pfenning and M. K. Reiter. [A linear logic of authorization and knowledge](#). In *Computer Security – ESORICS 2006: 11<sup>th</sup> European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 4189), pages 297–312, September 2006.
- [115] D. Gao, M. K. Reiter and D. Song. [Behavioral distance measurement using hidden Markov models](#). In *Recent Advances in Intrusion Detection: 9<sup>th</sup> International Symposium, RAID 2006* (Lecture Notes in Computer Science 4219), pages 19–40, September 2006.
- [116] X. Wang and M. K. Reiter. [WRAPS: Denial-of-service defense through web referrals](#). In *Proceedings of the 25<sup>th</sup> IEEE Symposium on Reliable Distributed Systems*, pages 51–60, October 2006.
- [117] X. Wang, Z. Li, J. Xu, M. K. Reiter, C. Kil and J. Y. Choi. [Packet vaccine: Black-box exploit detection and signature generation](#). In *Proceedings of the 13<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 37–46, October 2006.
- [118] Y. Xie, V. Sekar, M. K. Reiter and H. Zhang. [Forensic analysis for epidemic attacks in federated networks](#). In *Proceedings of the 14<sup>th</sup> IEEE International Conference on Network Protocols*, pages 43–53, November 2006.
- [119] Y. Xie, M. K. Reiter and D. R. O’Hallaron. [Protecting privacy in key-value search systems](#). In *Proceedings of the 22<sup>nd</sup> Annual Computer Security Applications Conference*, pages 493–504, December 2006.
- [120] S. Coull, C. Wright, F. Monrose, M. P. Collins and M. K. Reiter. **Playing devil’s advocate: Inferring sensitive information from anonymized network traces**. In *Proceedings of the 14<sup>th</sup> Network and Distributed System Security Symposium*, pages 35–47, February 2007.
- [121] K. Bowers, L. Bauer, D. Garg, F. Pfenning and M. K. Reiter. **Consumable credentials in linear-logic-based access-control systems**. In *Proceedings of the 14<sup>th</sup> Network and Distributed System Security Symposium*, pages 143–157, February 2007.
- [122] J. Cornwell, I. Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor, J. Hong, B. McLaren, M. Reiter and N. Sadeh. **User-controllable security and privacy for pervasive computing**. In *Proceedings of the 8<sup>th</sup> IEEE Workshop on Mobile Computing Systems and Applications*, February 2007.
- [123] J. M. McCune, B. Parno, A. Perrig, M. K. Reiter, and A. Seshadri. [Minimal TCB code execution \(extended abstract\)](#). In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 267–272, May 2007.
- [124] F. Oprea and M. K. Reiter. [Minimizing response time for quorum-system protocols over wide-area networks](#). In *Proceedings of the 37<sup>th</sup> IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 409–418, June 2007.

- [125] L. Bauer, L. Cranor, M. K. Reiter and K. Vaniea. [Lessons learned from the deployment of a smartphone-based access-control system](#). In *Proceedings of the 3<sup>rd</sup> Symposium on Usable Privacy and Security*, pages 64–75, July 2007.
- [126] A. Oprea and M. K. Reiter. **Integrity checking in cryptographic file systems with constant trusted storage**. In *Proceedings of the 16<sup>th</sup> USENIX Security Symposium*, pages 183–198, August 2007.
- [127] S. Coull, M. P. Collins, C. Wright, F. Monrose and M. K. Reiter. **On web browsing privacy in anonymized NetFlows**. In *Proceedings of the 16<sup>th</sup> USENIX Security Symposium*, pages 339–352, August 2007.
- [128] J. Hendricks, G. R. Ganger and M. K. Reiter. [Verifying distributed erasure-coded data](#). In *Proceedings of the 26<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, pages 139–146, August 2007.
- [129] M. P. Collins and M. K. Reiter. [Hit-list worm detection and bot identification in large networks using protocol graphs](#). In *Recent Advances in Intrusion Detection: 10<sup>th</sup> International Symposium, RAID 2007* (Lecture Notes in Computer Science 4637), pages 276–295, August 2007.
- [130] M. G. Merideth and M. K. Reiter. [Probabilistic opaque quorum systems](#). In *Distributed Computing: 21<sup>st</sup> International Symposium, DISC 2007* (Lecture Notes in Computer Science 4731), pages 403–419, September 2007.
- [131] L. Bauer, S. Garriss and M. K. Reiter. [Efficient proving for practical distributed access-control systems](#). *Computer Security – ESORICS 2007: 12<sup>th</sup> European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 4734), pages 19–37, September 2007.
- [132] J. Hendricks, G. R. Ganger and M. K. Reiter. [Low-overhead Byzantine fault-tolerant storage](#). In *Proceedings of the 21<sup>st</sup> ACM Symposium on Operating Systems Principles*, pages 73–86, October 2007.
- [133] S. E. Coull, C. V. Wright, A. D. Keromytis, F. Monrose and M. K. Reiter. **Taming the devil: Techniques for evaluating anonymized network data**. In *Proceedings of the 15<sup>th</sup> Network and Distributed System Security Symposium*, February 2008.
- [134] J. M. McCune, B. Parno, A. Perrig, M. K. Reiter and A. Seshadri. [How low can you go? Recommendations for hardware-supported minimal TCB code execution](#). In *Proceedings of the 13<sup>th</sup> International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 14–25, March 2008.
- [135] J. M. McCune, B. Parno, A. Perrig, M. K. Reiter, and H. Isozaki. [Flicker: An execution infrastructure for TCB minimization](#). In *Proceedings of the 3<sup>rd</sup> ACM SIGOPS/EuroSys European Conference on Computer Systems*, pages 315–328, April 2008.
- [136] L. Bauer, L. F. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. [A user study of policy creation in a flexible access-control system](#). In *Proceedings of the 26<sup>th</sup> ACM Conference on Human Factors in Computing Systems*, pages 543–552, April 2008.
- [137] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. [Expandable grids for visualizing and authoring computer security policies](#). In *Proceedings of the 26<sup>th</sup> ACM Conference on Human Factors in Computing Systems*, page 1473–1482, April 2008.
- [138] M. K. Reiter, A. Samar, and C. Wang. [Self-optimizing distributed trees](#). In *Proceedings of the 22<sup>nd</sup> IEEE International Parallel and Distributed Processing Symposium*, April 2008.
- [139] V. Sekar, M. K. Reiter, W. Willinger, H. Zhang, R. R. Kompella and D. G. Anderson. **cSAMP: A system for network-wide flow monitoring**. In *Proceedings of the 5<sup>th</sup> USENIX Symposium on Network Systems Design and Implementation*, pages 233–246, April 2008.
- [140] L. Bauer, S. Garriss and M. K. Reiter. [Detecting and resolving policy misconfigurations in access-control systems](#). In *Proceedings of the 13<sup>th</sup> ACM Symposium on Access Control Models and Technologies*, pages 185–194, June 2008.

- [141] Z. Li, X. Wang, Z. Liang, and M. K. Reiter. [AGIS: Towards automatic generation of infection signatures](#). In *Proceedings of the 38<sup>th</sup> IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 237–246, June 2008.
- [142] T.-F. Yen and M. K. Reiter. [Traffic aggregation for malware detection](#). In *Detection of Intrusions and Malware, and Vulnerability Assessment, 5<sup>th</sup> International Conference, DIMVA 2008* (Lecture Notes in Computer Science 5137), pages 207–227, July 2008.
- [143] L. Ballard, S. Kamara and M. K. Reiter. **The practical subtleties of biometric key generation**. In *Proceedings of the 17<sup>th</sup> USENIX Security Symposium*, pages 61–74, August 2008.
- [144] M. P. Collins and M. K. Reiter. [On the limits of payload-oblivious network attack detection](#). In *Recent Advances in Intrusion Detection: 11<sup>th</sup> International Symposium, RAID 2008* (Lecture Notes in Computer Science 5230), pages 251–270, September 2008.
- [145] D. Gao, M. K. Reiter and D. Song. [BinHunt: Automatically finding semantic differences in binary programs](#). In *Information and Communications Security, 10th International Conference, ICICS 2008* (Lecture Notes in Computer Science 5308), pages 238–255, October 2008.
- [146] L. Ballard, S. Kamara, F. Monrose and M. K. Reiter. [Towards practical biometric key generation with randomized biometric templates](#). In *Proceedings of the 15<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 235–244, October 2008.
- [147] M. G. Merideth and M. K. Reiter. [Write markers for probabilistic quorum systems](#). In *Principles of Distributed Systems, 12<sup>th</sup> International Conference, OPODIS 2008* (Lecture Notes in Computer Science 5401), pages 5–21, December 2008.
- [148] J. M. McCune, A. Perrig and M. K. Reiter. **Safe passage for passwords and other sensitive data**. In *Proceedings of the 16<sup>th</sup> ISOC Network and Distributed Systems Security Symposium*, pages 301–320, February 2009.
- [149] L. Bauer, L. F. Cranor, R. W. Reeder, M. K. Reiter and K. Vaniea. [Real life challenges in access-control management](#). In *Proceedings of the 27<sup>th</sup> ACM Conference on Human Factors in Computing Systems*, pages 899–908, April 2009.
- [150] L. Bauer, L. Jia, M. K. Reiter and D. Swasey. [xDomain: Cross-border proofs of access](#). In *Proceedings of the 14<sup>th</sup> ACM Symposium on Access Control Models and Technologies*, pages 43–52, June 2009.
- [151] Y.-H. Oh, P. Ning, Y. Liu and M. K. Reiter. **Authenticated data compression in delay tolerant wireless sensor networks**. In *Proceedings of the 6<sup>th</sup> International Conference on Networked Sensing Systems*, pages 137–144, June 2009.
- [152] T.-F. Yen, X. Huang, F. Monrose and M. K. Reiter. [Browser fingerprinting from coarse traffic summaries: Techniques and implications](#). In *Detection of Intrusions and Malware, and Vulnerability Assessment, 6<sup>th</sup> International Conference, DIMVA 2009* (Lecture Notes in Computer Science 5587), pages 157–175, July 2009.
- [153] D. Bethia and M. K. Reiter. [Data structures with unpredictable timing](#). In *Computer Security – ESORICS 2009: 14<sup>th</sup> European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 5789), pages 456–471, September 2009.
- [154] P. Li, D. Gao and M. K. Reiter. [Automatically adapting a trained anomaly detector to software patches](#). In *Recent Advances in Intrusion Detection: 12<sup>th</sup> International Symposium, RAID 2009* (Lecture Notes in Computer Science 5758), pages 142–160, September 2009.
- [155] M. G. Merideth, F. Oprea and M. K. Reiter. [When and how to change quorums on wide-area networks](#). In *Proceedings of the 28<sup>th</sup> International Symposium on Reliable Distributed Systems*, pages 12–21, September 2009.
- [156] Y. Liu, P. Ning, and M. K. Reiter. [False data injection attacks against state estimation in electric power grids](#). In *Proceedings of the 16<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 21–32, November 2009.

- [157] R. Wang, X. Wang, Z. Li, H. Tang, M. K. Reiter and Z. Dong. [Privacy-preserving genomic computation through program specialization](#). In *Proceedings of the 16<sup>th</sup> ACM Conference on Computer and Communications Security*, pages 338–347, November 2009.
- [158] M. K. Reiter, V. Sekar, C. Spensky and Z. Zhang. **Making peer-assisted content distribution robust to collusion using bandwidth puzzles**. In *Information Systems Security, 5<sup>th</sup> International Conference, ICISS 2009* (Lecture Notes in Computer Science 5905), pages 132–147, December 2009. To appear.
- [159] V. Sekar, A. Gupta, M. K. Reiter and H. Zhang. **Coordinated sampling sans origin-destination identifiers: Algorithms and analysis**. In *Proceedings of the 2<sup>nd</sup> International Conference on Communication Systems and Networks*, January 2010. To appear.

#### Other reviewed publications

- [160] M. K. Reiter. **A security architecture for fault-tolerant systems**. Ph.D. Thesis, Department of Computer Science, Cornell University, August 1993.
- [161] M. K. Reiter, K. P. Birman, and L. Gong. **Integrating security in a group oriented distributed system**. In K. P. Birman and R. van Renesse, editors, *Reliable Distributed Computing with the Isis Toolkit*, chapter 9, pages 148–166. IEEE Press, 1994. Reprint of [34].
- [162] M. K. Reiter. [Distributing trust with the Rampart toolkit](#). *Communications of the ACM* 39(4):71–74, April 1996. Invited paper.
- [163] M. K. Reiter. **Distributing trust with the Rampart toolkit**. In M. N. Huhns and M. P. Singh, editors, *Readings in Agents*, pages 306–309. Morgan Kaufmann, 1998. Reprint of [162].
- [164] M. K. Reiter and A. D. Rubin. **Privacy on the Web: How to be just a face in the Crowd**. *The Journal of Electronic Commerce* 11(4):70–73, Thomson EC Resources, 1998. Invited paper.
- [165] M. K. Reiter and A. D. Rubin. [Anonymous web transactions with Crowds](#). *Communications of the ACM* 42(2):32–38, February 1999. Invited paper.
- [166] M. K. Reiter. **Network survivability and information warfare**. In *Frontiers of Engineering 1999*, pages 20–23. National Academy Press, 2000.
- [167] F. Monrose and M. K. Reiter. **Graphical passwords**. In L. F. Cranor and S. Garfinkel, eds., *Security and Usability*, pages 169–186, O’Reilly Media Inc., 2005. Invited paper.
- [168] S. E. Coull, F. Monrose, M. K. Reiter, and M. Bailey. **The challenges of effectively anonymizing network data**. In *Proceedings of the Cybersecurity Applications and Technology Conference for Homeland Security*, pages 230–236, March 2009.