Michael K. Reiter

Curriculum Vitae
Last Updated: April 27, 2007

Carnegie Mellon University
2123 Collaborative Innovation Center
Pittsburgh, PA 15213 USA

phone: +412−268−1318
reiter@cmu.edu
http://www.ece.cmu.edu/~reiter/

Education

Cornell University, Ithaca, New York, USA.
- Ph.D., Computer Science, August 23, 1993. Thesis: [121]
- 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

Professor of Electrical & Computer Engineering and Computer Science (October 2001 – present)
Carnegie Mellon University, Pittsburgh, Pennsylvania, USA
My primary responsibilities in this position include training both undergraduate and graduate students through formal classes and supervised research; raising funds to support this research; and contributing to the management of the university through service on committees and other university bodies. In this role, I helped create and presently serve as Technical Director (formerly as Associate Director) for CyLab, a CMU center focused on advancing research, technology and education in the areas of computer security and trustworthy computing. I also presently serve as the Principal Investigator for one of two National Science Foundation "Cyber Trust" centers awarded nationwide in 2004. I created the curriculum for CMU's Master of Science in Information Security Technology and Management (MSISTM) degree, and I created and teach two of the courses in this curriculum: "Introduction to Computer Security" (first taught Spring 2003) and "Applied Cryptography" (first taught Spring 2004).

Director, Secure Systems Research (September 1998 – September 2001)
Bell Laboratories, Lucent Technologies, Murray Hill, New Jersey, USA
In this position, I was responsible for setting research priorities and strategies in computer and network security for Bell Labs; for representing the research of my department to Lucent business units and outsiders; for identifying and pursuing technology transfer opportunities for this research; and for excelling in my own research program. Example activities in this capacity include fostering the creation of a new venture in October 2000 from technology developed in my department; co-authoring a strategic assessment of Lucent's security offerings relative to its competitors and recommendations for action; evaluating possible acquisition targets in the security industry;

representing Lucent in an industry alliance with Sun, Cisco, Network Associates, Entrust Technologies and others that support research in computer security; and numerous technical consulting projects for Lucent.

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)
My primary responsibility in this position was to initiate and execute innovative research projects in computer security with potential to provide differentiating products and services for AT&T. My responsibilities also included assisting in the transfer of these projects to AT&T business units when possible. The Omega service [7] and the Rampart system on which it was built [5][31][34] are examples: AT&T registered Omega as a certification authority in Netscape 2.x and 3.x browsers and used it to certify AT&T web servers until the breakup of the company in 1996. For those projects that I was unable to transfer to business units, I typically released them to the research community in prototype form. For example, PathServer [11] was available for over two years and was used extensively by the outside community as a means of authenticating public keys in PGP-based applications, and similarly AT&T distributed the Crowds [10] prototype until I left the company.

Adjunct Assistant Professor (spring semester, 1998)

Department of Computer Science, New York University, New York, New York, USA
In this position I co-created and co-taught a course on privacy in computer networks.

Awards and Honors

Awards for scientific papers

- Outstanding Paper Award. 1994 IEEE Symposium on Research in Security and Privacy (for [30]).
- Best Paper Award. 3rd USENIX Workshop on Electronic Commerce (for [46]).
- Best Paper Award. 8th USENIX Security Symposium (for [52]).
- Best Student Paper Award. 8th USENIX Security Symposium (for [52]).
- Best Paper Award. 12th ISOC Network and Distributed System Security Symposium (for [88]).

Papers invited from the following conferences to appear in journals

- 1994 IEEE Symposium on Research in Security and Privacy ([30] invited, appears as [5])
- 1995 IEEE Symposium on Security and Privacy ([32] invited, appears as [6])
- 3rd ACM Conference on Computer and Communications Security ([35] invited, appears as [7])
- 9th IEEE Computer Security Foundations Workshop ([37] invited, appears as [8])
- 17th IEEE Symposium on Reliable Distributed Systems ([48] invited, appears as [15])
- 13th ACM Conference on Computer and Communications Security ([110] 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.

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.

- 6th Annual International Workshop on Selected Areas in Cryptography (Kingston, Ontario, Canada). August 10, 1999.
- 2nd 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.
- 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.
- 2nd NJITES Symposium on Cybersecurity and Trustworthy Software, Stevens Institute of Technology (Hoboken, NJ, USA). April 28, 2003.
- Triangle Computer Science Distinguished Lecturer Series, 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, 7th International Conference on Information Security and Cryptology (Seoul, Korea). December 2, 2004.
- Distinguished Lecturer Series, 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 40th Anniversary Symposium, Cornell University (Ithaca, NY, USA). October 1, 2005.
- Distinguished Lecture Series, 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.

Professional Service

Journal editorships

- *ACM Transactions on Information and System Security*
  Associate Editor (2000–2004)
  Editor-in-Chief (2004–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)

IEEE Technical Committee on Security and Privacy

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

Board of Visitors member, Software Engineering Institute, Carnegie Mellon University (July 2003–present)
The Board of Visitors of the Software Engineering Institute (SEI) advises the Carnegie Mellon University provost and the SEI director on SEI plans and operations. It monitors SEI activities and reports to the provost on the state of the SEI and recommendations for improvement. For more information, see http://www.sei.cmu.edu/about/bov/.

Conference program committees

- 1994 IEEE Symposium on Research in Security and Privacy (Oakland, CA, USA; May 1994)
- 1995 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1995)
- 8th IEEE Computer Security Foundations Workshop (Kenmare, County Kerry, Ireland; June 1995)
- 3rd ACM Conference on Computer and Communications Security (New Delhi, India; March 1996)
- 1996 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1996)
- 9th IEEE Computer Security Foundations Workshop (Kenmare, County Kerry, Ireland; June 1996)
- 4th ACM Conference on Computer and Communications Security (Zurich, Switzerland; April 1997)
- 1997 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1997)
- 7th USENIX Security Symposium (San Antonio, TX, USA; January 1998)
- 1998 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1998)
- **Program Chair**, 5th ACM Conference on Computer and Communications Security (San Francisco, CA, USA; November 1998)
- 7th IFIP International Working Conference on Dependable Computing for Critical Applications (San Jose, CA, USA; January 1999)
- **Program Co-Chair**, 1999 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1999)
- 18th ACM Symposium on Principles of Distributed Computing (Atlanta, GA, USA; May 1999)
- 19th IEEE International Conference on Distributed Computing Systems (Austin, TX, USA; June 1999)
- 1999 International Symposium on Distributed Computing (Bratislava, Slovakia; September 1999)
- 1999 International Workshop on Security (Aizu, Japan; September 1999)

- 1999 IFIP Working Conference on Communications and Multimedia Security (Leuven, Belgium; September 1999)
- 1999 CQRE—Secure Networking Conference (Dusseldorf, Germany, November 1999)
- 6th ACM Conference on Computer and Communications Security (Singapore, November 1999)
- 1st ACM Conference on Electronic Commerce (Denver, CO, USA; November 1999)
- **Program Co-Chair**, 2000 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 2000)
- 13th IEEE Computer Security Foundations Workshop (Cambridge, England; July 2000)
- 4th International Information Hiding Workshop (Pittsburgh, PA, USA; April 2001)
- Cryptographer's Track, RSA Conference 2001 (San Francisco, CA, USA; April 2001)
- 21st International Conference on Distributed Computing Systems (Phoenix, AZ, USA; April 2001)
- Information/System Survivability Workshop (Göteborg, Sweden; July 2001)
- 8th ACM Conference on Computer and Communications Security (Philadelphia, PA, USA; November 2001)
- 2nd International Workshop on Electronic Commerce (Heidelberg, Germany; November 2001)
- Workshop on Intrusion Tolerant Systems (Washington, DC, USA; June 2002)
- 22nd International Conference on Distributed Computing Systems (Vienna, Austria; July 2002)
- IEEE Workshop on Resource Sharing in Massively Distributed Systems (Vienna, Austria; July 2002)
- 21st ACM Symposium on Principles of Distributed Computing (Monterey, CA, USA; July 2002)
- 11th USENIX Security Symposium (San Jose, CA, USA; August 2002)
- 5th International Information Hiding Workshop (Eindhoven, Netherlands; September 2002)
- 4th International Conference on Information and Communications Security (Singapore; December 2002)
- 9th ACM Conference on Computer and Communications Security (Washington, DC, USA; November 2002)
- **Program Co-Chair**, 2003 ISOC Network and Distributed System Security Symposium (San Diego, CA, USA; February 2003)
- 3rd DARPA Information Survivability Conference and Exposition (Washington, DC, USA; April 2003)
- 2003 ACM Conference on Electronic Commerce (San Diego, CA, USA; June 2003)
- 6th Information Security Conference (Bristol, United Kingdom; October 2003)
- 10th ACM Conference on Computer and Communications Security (Washington, DC, USA; November 2003)
- **Program Co-Chair**, 2004 ISOC Network and Distributed System Security Symposium (San Diego, CA; February 2004)
- 2004 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 2004)
- **Program Co-Chair**, 2004 Information Hiding Workshop (Toronto, Canada; May 2004)
- 17th IEEE Computer Security Foundations Workshop (Pacific Grove, CA, USA; June 2004)
- 7th Information Security Conference (Palo Alto, CA, USA; September 2004)
- 18th International Symposium on Distributed Computing (Amsterdam, Netherlands; October 2004)
- **Area Vice Chair for Security**, 25th IEEE International Conference on Distributed Computing Systems (Columbus, Ohio; June 2005)
- **Program Co-Chair**, 2005 ACM Conference on Electronic Commerce (2005)
- 2005 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 2005)
- 24th ACM Symposium on Principles of Distributed Computing (Las Vegas, Nevada, USA; July 2005)
- 24th IEEE Symposium on Reliable Distributed Systems (Orlando, Florida, USA; October 2005)
- 9th International Conference on Principles of Distributed Systems (Pisa, Italy; December 2005)
- 1st ACM Conference on Information, Computer and Communications Security (Taipei, Taiwan; March 2006)
- Security, Privacy, and Ethics track of the 15th World Wide Web Conference (Edinburgh, Scotland; May 2006)

- 2006 International Conference on Dependable Systems and Networks (Philadelphia, PA, USA; June 2006)
- 6th Privacy Enhancing Technologies Workshop (Cambridge, UK; June 2006)
- 15th USENIX Security Symposium (Vancouver, BC, Canada; August 2006)
- 2007 ISOC Network and Distributed System Security Symposium (San Diego, CA, USA; February 2007)
- 7th Privacy Enhancing Technologies Workshop (Ottawa, CA; June 2007)
- 2007 International Conference on Dependable Systems and Networks (Edinburgh, UK; June 2007)
- 21st International Symposium on Distributed Computing (Lemesos, Cyprus; September 2007)
- 2008 International Conference on Dependable Systems and Networks (Anchorage, AK, USA; June 2008)

Other conference service

- Publicity Chair, 4th ACM Conference on Computer and Communications Security (Zurich, Switzerland; April 1997)
- Vice Chair, 1997 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1997)
- General Chair, 1998 IEEE Symposium on Security and Privacy (Oakland, CA, USA; May 1998)
- General Chair, 8th ACM Conference on Computer and Communications Security (Philadelphia, PA, USA; November 2001)
- Steering Committee, ACM Conference on Computer and Communications Security (1999–2002)

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–present)
    - Planning Group (March 2006–present)

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 [29].

[5] M. K. Reiter. **A secure group membership protocol**. *IEEE Transactions on Software Engineering* 22(1):31–42, January 1996. Preliminary version appears as [30].

[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 [32].

[7] M. K. Reiter, M. K. Franklin, J. B. Lacy, and R. N. Wright. **The Ω key management service**. *Journal of Computer Security* 4(4):267–287, IOS Press, 1996. Preliminary version appears as [35].

[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 [37].

[9] D. Malkhi and M. Reiter. **Byzantine quorum systems**. *Distributed Computing* 11(4):203–213, 1998. Preliminary version appears as [40].

[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 [39].

[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 [51].

[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 [41].

[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 [43].

[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 [47][48].

[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 [45].

[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 [50].

[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 [49].

[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 [44].

[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 on Information Security* 1(2):69–83, February 2002. Preliminary version appears as [54].

[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 [53].

[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 [56].

[25] P. MacKenzie and M. K. Reiter. **Networked cryptographic devices resilient to capture**. *International Journal on Information Security* 2(1):1–20, November 2003. Preliminary version appears as [59].

[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 [66].

[27] P. MacKenzie and M. K. Reiter. **Two-party generation of DSA signatures**. *International Journal on Information Security* 2(3–4):218–239, August 2004. Preliminary version appears as [64].

Symposium, conference, and workshop publications

[28] 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 [121].

[29] 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.

[30] 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**.

[31] M. K. Reiter. **Secure agreement protocols: Reliable and atomic group multicast in Rampart**. In *Proceedings of the 2nd ACM Conference on Computer and Communication Security*, pages 68–80, November 1994.

[32] 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.

[33] 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.

[34] 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.

[35] M. K. Reiter, M. K. Franklin, J. B. Lacy, and R. N. Wright. **The Ω key management service**. In *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pages 38–47, March 1996.

[36] 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.

[37] D. Malkhi and M. Reiter. **A high-throughput secure reliable multicast protocol**. In *Proceedings of the 9th IEEE Computer Security Foundations Workshop*, pages 9–17, June 1996.

[38] M. K. Franklin and M. K. Reiter. **Fair exchange with a semi-trusted third party**. In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 1–6, April 1997.

[39] M. K. Reiter and S. G. Stubblebine. **Path independence for authentication in large-scale systems**. *In Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 57–66, April 1997.

[40] D. Malkhi and M. Reiter. **Byzantine quorum systems**. In *Proceedings of the 29th ACM Symposium on Theory of Computing*, pages 569–578, May 1997.

[41] 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.

[42] D. Malkhi and M. Reiter. **Unreliable intrusion detection in distributed computations**. In *Proceedings of the 10th IEEE Computer Security Foundations Workshop*, pages 116–124, June 1997.

[43] D. Malkhi, M. Reiter, and A. Wool. **The load and availability of Byzantine quorum systems**. In *Proceedings of the 16th ACM Symposium on Principles of Distributed Computing*, pages 249–257, August 1997.

[44] D. Malkhi, M. Reiter, and R. Wright. **Probabilistic quorum systems**. In *Proceedings of the 16th ACM Symposium on Principles of Distributed Computing*, pages 267–273, August 1997.

[45] 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.

[46] M. K. Reiter, V. Anupam, and A. Mayer. **Detecting hit shaving in click-through payment schemes**. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, pages 155–166, August 1998. Received **Best Paper Award**.

[47] D. Malkhi and M. Reiter. **Survivable consensus objects**. In *Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems*, pages 271–279, October 1998.

[48] D. Malkhi and M. Reiter. **Secure and scalable replication in Phalanx**. In *Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems*, pages 51–58, October 1998.

[49] L. Alvisi, D. Malkhi, L. Pierce, and M. K. Reiter. **Fault detection for Byzantine quorum systems**. In *Proceedings of the 7th IFIP Working Conference on Dependable Computing for Critical Applications*, pages 357–371, January 1999.

[50] R. De Prisco, D. Malkhi, and M. K. Reiter. **On *k*-set consensus problems in asynchronous systems**. In *Proceedings of the 18th ACM Symposium on Principles of Distributed Computing*, pages 257–265, May 1999.

[51] 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 8th International World Wide Web Conference*, May 1999.

[52] I. Jermyn, A. Mayer, F. Monrose, A. Rubin, and M. K. Reiter. **The design and analysis of graphical passwords**. In *Proceedings of the 8th USENIX Security Symposium*, pages 1–14, August 1999. Received **Best Paper Award**.

[53] D. Malkhi, Y. Mansour, and M. K. Reiter. **On diffusing updates in a Byzantine environment**. In *Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems*, pages 134–143, October 1999.

[54] F. Monrose, M. K. Reiter, and S. Wetzel. **Password hardening based on keystroke dynamics**. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 73–82, November 1999.

[55] L. Alvisi, D. Malkhi, E. Pierce, M. K. Reiter, and R. N. Wright. **Dynamic Byzantine quorum systems**. In *Proceedings of the International Conference on Dependable Systems and Networks*, pages 283–292, June 2000.

[56] D. Malkhi, M. Merritt, M. K. Reiter, and G. Taubenfeld. **Objects shared by Byzantine processes**. In *Proceedings of the 14th International Symposium on Distributed Computing* (Lecture Notes in Computer Science 1914), pages 345–359, Springer, October 2000.

[57] 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.

[58] G. Chockler, D. Malkhi, and M. K. Reiter. **Backoff protocols for distributed mutual exclusion and ordering**. In *Proceedings of the 21st International Conference on Distributed Computing Systems*, pages 11–20, April 2001.

[59] 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.

[60] 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.

[61] D. Malkhi, M. K. Reiter, D. Tulone, and E. Ziskind. **Persistent objects in the Fleet system**. In *Proceedings of the 2nd DARPA Information Survivability Conference and Exposition* (DISCEX II), Vol. II, pages 126–136, June 2001.

[62] 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.

[63] 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 20th ACM Symposium on Principles of Distributed Computing*, August 2001.

[64] P. MacKenzie and M. K. Reiter. **Two party generation of DSA signatures**. In *Advances in Cryptology—CRYPTO 2001* (Lecture Notes in Computer Science 2139), August 2001.

[65] D. Malkhi, M. K. Reiter, O. Rodeh and Y. Sella. **Efficient update diffusion in Byzantine environments**. In *Proceedings of 20th IEEE Symposium on Reliable Distributed Systems*, pages 90–98, October 2001.

[66] P. MacKenzie and M. K. Reiter. **Delegation of cryptographic servers for capture-resilient devices**. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 10–19, November 2001.

[67] 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.

[68] Y. Xie, D. O'Hallaron and M. K. Reiter. **A secure distributed search system**. In *Proceedings of the 11th IEEE International Symposium on High Performance Distributed Computing*, pages 321–330, July 2002.

[69] 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 11th USENIX Security Symposium*, pages 283–296, August 2002.

[70] 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.

[71] M. K. Reiter, A. Samar and C. Wang. **The design and implementation of a JCA-compliant capture protection infrastructure**. In *Proceedings of the 22nd IEEE Symposium on Reliable Distributed Systems*, October 2003.

[72] P. MacKenzie, A. Oprea, and M. K. Reiter. **Automatic generation of two-party cryptographic protocols**. In *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pages 210–219, November 2003.

[73] P. MacKenzie, M. K. Reiter and K. Yang. **Alternatives to non-malleability: Definitions, constructions and applications**. In *Theory of Cryptography: Proceedings of the 1st Theory of Cryptography Conference*, (Lecture Notes in Computer Science 2951), pages 171–190, February 2004.

[74] B. Levine, M. K. Reiter, C. Wang, and M. Wright. **Timing attacks in low-latency mix-based systems**. In *Financial Cryptography: 8th International Conference, FC 2004* (Lecture Notes in

Computer Science 3110), pages 251–265, February 2004.

[75] 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.

[76] G. Perng, C. Wang and M. K. Reiter. **Providing content-based services in a peer-to-peer environment**. In *Proceedings of the 3rd International Workshop on Distributed Event-Based Systems*, May 2004.

[77] 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.

[78] G. Goodson, J. Wylie, G. Ganger and M. K. Reiter. **Efficient Byzantine-tolerant erasure-coded storage**. In *Proceedings of the 2004 International Conference on Dependable Systems and Networks*, June 2004.

[79] D. Gao, M. K. Reiter, and D. Song. **On gray-box program tracking for anomaly detection**. In *Proceedings of the 13th USENIX Security Symposium*, pages 103–118, August 2004.

[80] D. Davis, F. Monrose and M. K. Reiter. **On user choice in graphical password schemes**. In *Proceedings of the 13th USENIX Security Symposium*, pages 151–164, August 2004.

[81] 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.

[82] C. Fry and M. K. Reiter. **Nested objects in a Byzantine quorum-replicated system**. In *Proceedings of the 23rd IEEE Symposium on Reliable Distributed Systems*, pages 79–89, October 2004.

[83] D. Davis, F. Monrose, and M. K. Reiter. **Efficient time-scoped searching of encrypted audit logs**. In *Information and Communications Security: 6th International Conference, ICICS 2004* (Lecture Notes in Computer Science 3269), pages 532–545, October 2004.

[84] M. K. Reiter and X. Wang. **Fragile mixing**. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 227–235, October 2004.

[85] X. Wang and M. K. Reiter. **Mitigating bandwidth-exhaustion attacks using congestion puzzles**. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 257–267, October 2004.

[86] D. Gao, M. K. Reiter and D. Song. **Gray-box extraction of execution graphs for anomaly detection**. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 318–329, October 2004.

[87] V. Sekar, Y. Xie, D. Maltz, M. K. Reiter and H. Zhang. **Toward a framework for Internet forensic analysis**. In *Proceedings of the 3rd Workshop on Hot Topics in Networks* (HOTNETS-III), November 2004.

[88] A. Oprea, M. K. Reiter and K. Yang. **Space-efficient block storage integrity**. In *Proceedings of the 12th Network and Distributed System Security Symposium*, February 2005. Received **Best Paper Award**.

[89] 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.

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] A. Gupta, B. M. Maggs, F. Oprea and M. K. Reiter. **Quorum placement in networks to minimize access delays**. In *Proceedings of the 24th ACM Symposium on Principles of Distributed Computing*, pages 87–96, July 2005.

[96] L. Bauer, S. Garriss, J. McCune, M. K. Reiter, J. Rouse and P. Rutenbar. **Device-enabled authorization in the Grey system**. In *Information Security: 8th International Conference, ISC 2005* (Lecture Notes in Computer Science 3650), pages 431–446, Springer-Verlag, September 2005.

[97] D. Gao, M. K. Reiter and D. Song. **Behavioral distance for intrusion detection**. In *Recent Advances in Intrusion Detection: 8th International Symposium, RAID 2005* (Lecture Notes in Computer Science 3858), pages 63–81, September 2005.

[98] 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 20th ACM Symposium on Operating Systems Principles*, pages 59–74, October 2005.

[99] M. K. Reiter, A. Samar and C. Wang. **Distributed construction of a fault-tolerant network from a tree**. In *Proceedings of the 24th IEEE Symposium on Reliable Distributed Systems*, pages 155–165, October 2005.

[100] 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 24th IEEE Symposium on Reliable Distributed Systems*, pages 179–190, October 2005.

[101] 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.

[102] V. Sekar, Y. Xie, M. K. Reiter and H. Zhang. **A multi-resolution approach to worm detection and containment**. In *Proceedings of the 2006 International Conference on Dependable Systems and Networks*, pages 189–198, June 2006.

[103] G. Perng, M. K. Reiter and C. Wang. **M2: Multicasting mixes for efficient and anonymous communication**. In *Proceedings of the 26th International Conference on Distributed Computing Systems*, July 2006.

[104] D. Golovin, A. Gupta, B. M. Maggs, F. Oprea and M. K. Reiter. **Quorum placement in networks: Minimizing network congestion**. In *Proceedings of the 25th ACM Symposium on Principles of Distributed Computing*, pages 16–25, July 2006.

[105] A. Oprea and M. K. Reiter. **On consistency of encrypted files**. In *Distributed Computing: 20th International Symposium, DISC 2006* (Lecture Notes in Computer Science 4167), pages 254–268, September 2006.

[106] M. P. Collins and M. K. Reiter. **Finding peer-to-peer file-sharing using coarse network behaviors**. In *Computer Security – ESORICS 2006: 11th European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 4189), pages 1–17, September 2006.

[107] D. Garg, L. Bauer, K. Bowers, F. Pfenning and M. K. Reiter. **A linear logic of authorization and knowledge**. In *Computer Security – ESORICS 2006: 11th European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 4189), pages 297–312, September 2006.

[108] D. Gao, M. K. Reiter and D. Song. **Behavioral distance measurement using hidden Markov models**. In *Recent Advances in Intrusion Detection: 9th International Symposium, RAID 2006* (Lecture Notes in Computer Science 4219), pages 19–40, September 2006.

[109] X. Wang and M. K. Reiter. **WRAPS: Denial-of-service defense through web referrals**. In *Proceedings of the 25th IEEE Symposium on Reliable Distributed Systems*, pages 51–60, October 2006.

[110] 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 13th ACM Conference on Computer and Communications Security*, pages 37–46, October 2006.

[111] Y. Xie, V. Sekar, M. K. Reiter and H. Zhang. **Forensic analysis for epidemic attacks in federated networks**. In *Proceedings of the 14th IEEE International Conference on Network Protocols*, pages 43–53, November 2006.

[112] Y. Xie, M. K. Reiter and D. R. O'Hallaron. **Protecting privacy in key-value search systems**. In *Proceedings of the 22nd Annual Computer Security Applications Conference*, pages 493–504, December 2006.

[113] 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 14th Network and Distributed System Security Symposium*, pages 35–47, February 2007.

[114] 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 14th Network and Distributed System Security Symposium*, pages 143–157, February 2007.

[115] 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 8th IEEE Workshop on Mobile Computing Systems and Applications*, February 2007.

[116] 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*, May 2007. To appear.

[117] F. Oprea and M. K. Reiter. **Minimizing response time for quorum-system protocols over wide-area networks**. In *Proceedings of the 2007 International Conference on Dependable Systems and Networks*, June 2007. To appear.

[118] 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 3rd Symposium on Usable Privacy and Security*, July 2007. To appear.

[119] A. Oprea and M. K. Reiter. **Integrity checking in cryptographic file systems with constant trusted storage**. In *Proceedings of the 16th USENIX Security Symposium*, August 2007. To appear.

[120] S. Coull, M. P. Collins, C. Wright, F. Monrose and M. K. Reiter. **Assessing the threat to client privacy in anonymized NetFlows**. In *Proceedings of the 16th USENIX Security Symposium*, August 2007. To appear.

Other reviewed publications

[121] M. K. Reiter. **A security architecture for fault-tolerant systems**. Ph.D. Thesis, Department of Computer Science, Cornell University, August 1993.

[122] 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 [28].

[123] M. K. Reiter. **Distributing trust with the Rampart toolkit**. *Communications of the ACM* 39(4):71–74, April 1996. Invited paper.

[124] 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 [123].

[125] 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.

[126] M. K. Reiter and A. D. Rubin. **Anonymous web transactions with Crowds**. *Communications of the ACM* 42(2):32–38, February 1999. Invited paper.
[127] M. K. Reiter. **Network survivability and information warfare**. In *Frontiers of Engineering 1999*, pages 20–23. National Academy Press, 2000.
[128] 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.