Michael K. Reiter

Curriculum Vitae
Last Updated: August 15, 2024

Duke Computer Science
LSRC Building D310
308 Research Drive
Duke Box 90129
Durham, NC 27708-0129 USA

Web: https://reitermk.github.io/

Education 2

Professional Experience 2

Awards and Honors 3

Scientific Lectures 4

Professional Service 8

Scientific Publications 11

Education

Cornell University, Ithaca, New York, USA.
- Ph.D., Computer Science, August 23, 1993.
- 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 (rank 1 of 3476).

Professional Experience

Duke University, Computer Science and Electrical & Computer Engineering Departments
- James B. Duke Distinguished Professor (July 2021 − present)
- Professor (Jan 2021 − June 2021)

Chainlink Labs
- Researcher (Jan 2022 − present)

VMware Research Group
- Affiliated Researcher (May 2017 − July 2022)

The University of North Carolina at Chapel Hill, Computer Science Department
- Lawrence M. Slifkin Distinguished Professor (Jul 2007 − Dec 2020)
- Associate Chair for Diversity and Inclusion (Aug 2016 − Dec 2020)

Carnegie Mellon University, Electrical & Computer Engineering and Computer Science Departments
- Professor (Oct 2001 − Jun 2007)
- Founding Technical Director, CyLab

Bell Laboratories, Lucent Technologies
- Director, Secure Systems Research (Sep 1998 – Sep 2001)

AT&T Labs – Research (formerly AT&T Bell Laboratories)
- Principal Technical Staff Member (Jun 1996 – Sep 1998)
- Technical Staff Member (Aug 1993 – May 1996)

New York University, Computer Science Department
- Adjunct Assistant Professor (spring semester, 1998)

Awards and Honors

Named an **ACM Fellow** (2008) and **IEEE Fellow** (2014) for “contributions to computer security and fault-tolerant distributed computing.”

ACM SIGSAC Outstanding Contributions Award for “pioneering research contributions and leadership in computer and information security,” 2016.

ACM CODASPY Lasting Research Award for “vulnerability detection in systems, applications, and machine learning models as well as developing innovative solutions to combat cyber attacks for over three decades,” 2024.

Awards for scientific papers

- Outstanding Paper Award, 15th IEEE Symposium on Research in Security and Privacy, for *A secure group membership protocol*.
- Best Paper Award, 3rd USENIX Workshop on Electronic Commerce, for *Detecting hit shaving in click-through payment schemes*.
- Best Paper Award, 8th USENIX Security Symposium, for *The design and analysis of graphical passwords*.
- Best Paper Award, 12th ISOC Network and Distributed System Security Symposium, for *Server-side verification of client behavior in online games*.
- Best Paper Award, 17th ISOC Network and Distributed System Security Symposium, for *Space-efficient block storage integrity*.
- Best Paper Award, 6th International Conference on Internet Monitoring and Protection, for *Towards optimized probe scheduling for active measurement studies*.
- Winner, 4th Annual Best Scientific Cybersecurity Paper Competition, for *Nomad: Mitigating arbitrary cloud side channels via provider-assisted migration*.
- Best Student Paper Award, 14th European Conference on Computer Systems, for *Efficient and safe network updates with suffix causal consistency*.
- **Test of Time Award**, ACM Conference on Computer and Communications Security, for *False data injection attacks against state estimation in electric power grids*.
- **Test of Time Award**, ACM Conference on Computer and Communications Security, for *Cross-VM side channels and their use to extract private keys*.
- **Test of Time Award**, Intel Hardware Security Academic Awards, for *Flicker: An execution infrastructure for TCB minimization*.

Papers invited from the following conferences to appear in journals

- 15th IEEE Symposium on Research in Security and Privacy
- 16th IEEE Symposium on Security and Privacy
- 3rd ACM Conference on Computer and Communications Security
- 9th IEEE Computer Security Foundations Workshop
- 17th IEEE Symposium on Reliable Distributed Systems
- 13th ACM Conference on Computer and Communications Security
- 13th ACM Symposium on Access Control Models and Technologies

Scholarships and fellowships

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

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

Scientific Lectures

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.
- 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.
- 2nd 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, 7th 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 40th 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, 12th 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.
- 3rd 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, 10th 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, 29th 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.
- IBM T.J. Watson Research Center (Hawthorne, NY, USA). March 16, 2010.
- Plenary lecture, MITACS International Focus Period: Advances in Network Analysis & its Applications − Network Security & Cryptography (Toronto, Ontario, Canada). June 24, 2010.
- MITACS Speaker Series on Privacy, University of Waterloo (Waterloo, Ontario, Canada). June 25, 2010.
- Distinguished Speaker Seminar, NEC Labs (Princeton, NJ, USA). August 13, 2010.
- Department of Electrical Engineering and Computer Science, University of Michigan (Ann Arbor, MI, USA). September 17, 2010.
- Distinguished Lecture, Department of Computer Science, University of Pittsburgh (Pittsburgh, PA, USA). January 21, 2011.
- Distinguished Lecture, Center for Advanced Security Research Darmstadt (Darmstadt, Germany). June 30, 2011.
- Distinguished Lecture, Department of Computer Science, University of Illinois at Urbana-Champaign (Urbana, IL, USA). October 24, 2011.
- Cyber Forum Speaker, Sandia National Labs (Albuquerque, NM, USA). June 5, 2012.
- CSE Colloquium and Distinguished Lecture, Department of Computer Science and Engineering, University of California at San Diego (San Diego, CA, USA). June 6, 2012.
- Keynote address, 3rd ACM Conference on Data and Application Security and Privacy (San Antonio, TX, USA). February 18, 2013.
- Distinguished Lecture, Department of Computing and Information Sciences, Kansas State University (Manhattan, KS, USA). March 6−7, 2013.
- Distinguished Lecture, Department of Computer Science, University of Texas at Dallas (Dallas, Texas, USA). March 8, 2013.
- Eminent Scholars Lecture Series, College of Engineering, University of South Florida (Tampa, FL, USA). March 22, 2013.
- CrySP Speaker Series on Privacy, School of Computer Science, University of Waterloo (Waterloo, Ontario, Canada). April 16, 2013.

- Distinguished Lecture, Department of Computer and Information Science, University of Pennsylvania (Philadelphia, PA, USA). September 24, 2013.
- Keynote address, 6th Symposium on Security Analytics and Automation (Washington, DC, USA). October 16, 2013.
- Keynote address, 16th Information Security Conference (Dallas, TX, USA). November 13, 2013.
- CyLab Seminar, Carnegie Mellon University (Pittsburgh, PA, USA). October 10, 2014.
- Keynote address, 22nd IEEE International Conference on Network Protocols (The Research Triangle, NC, USA). October 22, 2014.
- Distinguished Lecture, Department of Computer Science, University of Calgary (Calgary, Alberta, Canada). November 20, 2014.
- Computer Science Colloquium, Viterbi School of Engineering, University of Southern California (Los Angeles, California, USA). January 20, 2015.
- Department Colloquium, Computer Science Department, Duke University (Durham, NC, USA). February 2, 2015.
- Keynote address, Symposium and Bootcamp on the Science of Security, University of Illinois at Urbana-Champaign (Urbana, IL, USA). April 21, 2015.
- Keynote address, 7th ACM Cloud Computing Security Workshop (Denver, CO, USA). October 16, 2015.
- Keynote address, 9th International Conference on Network and System Security (New York, NY, USA). November 4, 2015.
- Distinguished Lecture, Department of Computer and Information Science and Engineering, University of Florida (Gainesville, FL, USA). November 20, 2015.
- Distinguished Lecture, College of Information and Computer Sciences, University of Massachusetts Amherst (Amherst, MA, USA). December 2, 2015.
- Distinguished Lecture, Computer Science and Engineering Department, University of California – Riverside (Riverside, CA, USA). January 11, 2016.
- Keynote address, GENI Regional Workshop (Clemson, SC, USA). December 2, 2016.
- Distinguished Lecture, Texas A&M Cybersecurity Distinguished Lecture Series (College Station, TX, USA). December 6, 2016.
- VMware Research Group (Palo Alto, CA, USA). January 12, 2017.
- Distinguished Lecture, Department of Computer Science, University of Illinois at Chicago (Chicago, IL, USA). September 14, 2017.
- CyLab Distinguished Seminar, Carnegie Mellon University (Pittsburgh, PA, USA). November 27, 2017.
- Distinguished Speaker Series, Department of Computer Science, Colorado School of Mines (Denver, CO, USA). January 11, 2018.
- Washington Area Trustworthy Computing Hour (WATCH) seminar, National Science Foundation (Alexandria, VA, USA). January 18, 2018.
- Distinguished Lecture, Northeastern Cybersecurity and Privacy Institute, Northeastern University (Boston, MA, USA). September 18, 2018.
- Distinguished Lecture, Computer Science and Engineering Department, The Ohio State University (Columbus, OH, USA). April 18, 2019.
- Computer Science Laboratory, SRI International (Menlo Park, CA, USA). August 8, 2019.
- Distinguished Lecture, Great Lakes Security Day, Department of Computer Science and Engineering, University of Buffalo (Buffalo, NY, USA). September 6, 2019.
- Qatar Computing Research Institute (Doha, Qatar). March 1, 2020.
- Computer Science Colloquium, Worcester Polytechnic Institute (Worcester, MA, USA). September 11, 2020.
- CyLab Seminar, Carnegie Mellon University (Pittsburgh, PA, USA). November 2, 2020.
- IBM Back to School Seminar (Research Triangle Park, NC, USA). November 19, 2020.

- Department colloquium, Department of Electrical Engineering and Computer Science, University of California, Irvine (Irvine, CA, USA). October 1, 2021.
- Cybersecurity Distinguished Lecture, University of Colorado, Colorado Springs (Colorado Springs, CO, USA). November 12, 2021.
- Distinguished Lecture, Department of Electrical and Computer Engineering, University of California at Los Angeles (Los Angeles, CA, USA). March 6, 2023.
- Distinguished Lecture, Resilient Computing and Cybersecurity Center, King Abdullah University of Science and Technology (Thuwal, Saudi Arabia). March 20, 2023.
- Keynote address, 13th ACM Conference on Data and Application Security and Privacy (Charlotte, NC, USA). April 24, 2023.
- Keynote address, 30th ACM Conference on Computer and Communications Security (Copenhagen, Denmark). November 27, 2023.
- Joint Computer Engineering and Computer Science Seminar, Purdue University (West Lafayette, IN, USA). April 18, 2024.

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−November 2011)
- *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 (Nov/Dec 1999 issue)
  Guest Editor, special issue on Homeland Security (Nov/Dec 2004 issue)

Conference program committees

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

ACM Cloud Computing Security Workshop	2014, 2016*
ACM Conference on Computer and Communications Security (CCS)	1996, 1997, 1998*, 1999, 2001, 2002, 2003, 2008, 2011, 2012, 2013, 2014, 2019, 2020
ACM Conference on Data and Application Security and Privacy (CODASPY)	2013
ACM Conference on Electronic Commerce	1999, 2003, 2005*
ACM Conference on Principles of Distributed Computing (PODC)	1999, 2002, 2005
ACM SIGCOMM Conference	2008
ACM Symposium on Operating Systems Principles (SOSP)	2017
ACM Symposium on Information, Computer and Communications Security (ASIACCS)	2006, 2008, 2012*
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, 2021
IEEE Computer Security Foundations (CSF)	1995, 1996, 2000, 2004
IEEE INFOCOM	2011
IEEE Symposium on Reliable Distributed Systems (SRDS)	2005
IEEE Symposium on Security and Privacy	1994, 1995, 1996, 1997, 1998, 1999*, 2000*, 2004, 2005, 2010, 2011, 2015, 2016, 2019, 2024

IEEE Workshop on Resource Sharing in Massively Distributed Systems	2002
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)	2006, 2007, 2008, 2009, 2013, 2014*
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 Cryptology and Network Security (CANS)	2015*
International Conference on Distributed Computing Systems (ICDCS)	1999, 2001, 2002, 2005+, 2008, 2010
International Conference on Information and Communications Security	2002
International Conference on Principles of Distributed Systems	2005
International Conference on Trust and Trustworthy Computing	2012*
International Symposium on Distributed Computing (DISC)	1999, 2004, 2007
International Workshop on Electronic Commerce	2001
International Workshop on Security	1999
International Workshop on Security and Privacy in Cloud Computing (SPCC)	2010
Network and Distributed System Security Symposium (NDSS)	2003*, 2004*, 2007, 2009, 2010, 2012, 2013, 2016, 2017, 2018, 2019
Privacy Enhancing Technologies Symposium (PETS)	2006, 2007, 2015, 2018, 2020
Symposium on Usable Privacy and Security (SOUPS)	2012, 2013, 2014, 2015, 2018
USENIX Annual Technical Conference	2019, 2021
USENIX Security Symposium	1998, 2002, 2006, 2008, 2009, 2022
USENIX Workshop on Hot Topics in Dependability (HotDep)	2012, 2013
USENIX Workshop on Hot Topics in Security (HotSec)	2009
Workshop on Intrusion Tolerant Systems	2002
Workshop on Privacy Enhancing Tools (PETools)	2013
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, 8th ACM Conference on Computer and Communications Security (2001)
- Steering Committee, ACM Conference on Computer and Communications Security (1999−2002)
- Steering Committee, ACM Symposium on Information, Computer and Communications Security (2010−2013)
- Steering Committee, IEEE/IFIP International Conference on Dependable Systems and Networks (2011−2014)
- Steering Committee, Symposium on Usable Security and Privacy (2018−present)
- Steering Committee, IEEE Symposium on Security and Privacy (2021−present)
- Chair, Test-of-Time Award Committee, 31st ISOC Network and Distributed System Security Symposium (2024)
- Steering Committee, ISOC Network and Distributed System Security Symposium (2024−present)
- ACM SIGSAC Doctoral Dissertation Award Committee (2024)

IEEE Technical Committee on Security and Privacy
- Chair, Subcommittee on Conferences (1998)
- Vice Chair (2000−2001)
- Chair (2002−2003)

External Advisory Committees
- Board of Visitors, Software Engineering Institute, Carnegie Mellon University (July 2003−August 2009)
- Board of Visitors, Army Research Laboratory − Army Research Office Computing Sciences Division Review (May 5−6, 2010)
- Information Security M.S. program of the College of Computing, Georgia Institute of Technology (April 2014)
- Cyber Security Group, Qatar Computing Research Institute (March 2020)
- Department of Computer Science, Swiss Federal Institute of Technology in Zürich (October 2022)

The Morehead-Cain Scholars Program
- Central Selection Committee (2009, 2011−14)
- Alumni Reader (2010)

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)
- Board of Visitors, Army Research Laboratory − Army Research Office Computing Sciences Division Review (May 5−6, 2010)
- Department of Commerce Emerging Technology and Research Advisory Committee (September 2008 − September 2012)

- Steering Committee, NSF Cyberspace 2025 Workshop (November 2013 − April 2014)
- Co-organizer, NSF Secure and Trustworthy Computing (SaTC) Principal Investigator meeting (June 1−2, 2022)

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.

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

[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.

[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.

[8] D. Malkhi and M. Reiter. **A high-throughput secure reliable multicast protocol**. *Journal of Computer Security* 5:113–127, IOS Press, 1997.

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

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.
[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.
[24] D. Malkhi, M. Merritt, M. K. Reiter, and G. Taubenfeld. **Objects shared by Byzantine processes**. *Distributed Computing* 16(1):37−48, 2003.
[25] P. MacKenzie and M. K. Reiter. **Networked cryptographic devices resilient to capture**. *International Journal of Information Security* 2(1):1−20, November 2003.
[26] P. MacKenzie and M. K. Reiter. **Delegation of cryptographic servers for capture-resilient devices**. *Distributed Computing* 16(4):307–327, December 2003.
[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.
[28] 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.
[29] X. Wang and M. K. Reiter. **A multi-layer framework for puzzle-based denial-of-service defense**. *International Journal of Information Security* 7(4):243−263, August 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), December 2008.
[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.
[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.
[33] X. Wang and M. K. Reiter. **Using web-referral architectures to mitigate denial-of-service threats**. *IEEE Transactions on Dependable and Secure Computing* 7(2):203−216, April−June 2010.
[34] L. Bauer, S. Garriss and M. K. Reiter. **Detecting and resolving policy misconfigurations in access-control systems**. *ACM Transactions on Information and System Security* 14(1), May 2011.
[35] Y. Liu, P. Ning and M. K. Reiter. **False data injection attacks against state estimation in electric power grids**. *ACM Transactions on Information and System Security* 14(1), May 2011.
[36] D. Bethea, R. A. Cochran and M. K. Reiter. **Server-side verification of client behavior in online games**. *ACM Transactions on Information and System Security* 14(4), December 2011.
[37] A. A. Yavuz, P. Ning and M. K. Reiter. **BAF and FI-BAF: Efficient and publicly verifiable cryptographic schemes for secure logging in resource-constrained systems**. *ACM Transactions on Information and System Security* 15(2), July 2012.
[38] M. Abd-El-Malek, M. Wachs, J. Cipar, K. Sanghi, G. R. Ganger, G. A. Gibson, and M. K. Reiter. **File system virtual appliances: Portable file system implementations**. *ACM Transactions on Storage* 8(3), September 2012.
[39] S. E. Coull, A. M. White, T.-F. Yen, F. Monrose and M. K. Reiter. **Understanding domain registration abuses**. *Computers & Security* 31(7):806−815, October 2012.

[40] H.-C. Kum, A. Krishnamurthy, A. Machanavajjhala, M. K. Reiter, and S. Ahalt. **Privacy preserving interactive record linkage (PPIRL)**. *Journal of the American Medical Informatics Association*, November 2013.

[41] P. Li, D. Gao, and M. K. Reiter. **StopWatch: A cloud architecture for timng channel mitigation**. *ACM Transactions on Information and System Security* 17(2), November 2014.

[42] L. Wei and M. K. Reiter. **Toward practical encrypted email that supports private, regular-expression searches**. *International Journal on Information Security* 14(5):397−416, October 2015.

[43] Q. Xiao, M. K. Reiter, and Y. Zhang. **Persistent pseudonyms for servers in the cloud**. *Proceedings on Privacy Enhancing Technologies* 4:271−289, 2017.

[44] Q. Ismail, T. Ahmed, K. Caine, A. Kapadia, and M. Reiter. **To permit or not to permit, that is the usability question: Crowdsourcing mobile apps' privacy permission settings**. *Proceedings on Privacy Enhancing Technologies* 4:119−137, 2017.

[45] Z. Mi, H. Chen, Y. Zhang, S. Peng, X. Wang, and M. Reiter. **CPU elasticity to mitigate cross-VM runtime monitoring**. *IEEE Transactions on Dependable and Secure Computing*, June 2018.

[46] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter. **A general framework for adversarial examples with objectives**. *ACM Transactions on Privacy and Security* 22(3), June 2019.

[47] Z. Zhou and M. K. Reiter. **Interpretable noninterference measurement and its application to processor designs**. *Proceedings of the ACM on Programming Languages* 5(OOPSLA), October 2021.

[48] X. Zhang, J. Hamm, M. K. Reiter, and Y. Zhang. **Defeating traffic analysis via differential privacy: A case study on streaming traffic**. *International Journal of Information Security*, January 2022.

Symposium, conference, and workshop publications

[49] M. K. Reiter, K. P. Birman, and L. Gong. **Integrating security in a group oriented distributed systems**. In *Proceedings of the 13th IEEE Symposium on Research in Security and Privacy*, pages 18–32, May 1992.

[50] M. K. Reiter and L. Gong. **Preventing denial and forgery of causal relationships in distributed systems**. In *Proceedings of the 14th IEEE Symposium on Research in Security and Privacy*, pages 30–40, May 1993.

[51] M. K. Reiter. **A secure group membership protocol**. In *Proceedings of the 15th IEEE Symposium on Research in Security and Privacy*, pages 176–189, May 1994. Received *Outstanding Paper Award*.

[52] 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.

[53] M. K. Franklin and M. K. Reiter. **The design and implementation of a secure auction service**. In *Proceedings of the 16th IEEE Symposium on Security and Privacy*, pages 2–14, May 1995.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

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

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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*.

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

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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*.

[74] 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.

[75] 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.
[76] L. Alvisi, D. Malkhi, E. Pierce, M. K. Reiter, and R. N. Wright. **Dynamic Byzantine quorum systems**. In *Proceedings of the 30th IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 283−292, June 2000.
[77] 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.
[78] 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.
[79] 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.
[80] 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.
[81] 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.
[82] 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.
[83] 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.
[84] 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.
[85] 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.
[86] 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.
[87] 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.
[88] M. Jakobsson and M. K. Reiter. **Discouraging software piracy using software aging**. In *Security and Privacy in Digital Rights Management* (Lecture Notes in Computer Science 2320), pages 1−12, November 2001.
[89] 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.
[90] 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.
[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] L. Kissner, A. Oprea, M. K. Reiter, D. Song, and K. Yang. **Private keyword-based push and pull with applications to anonymous communication**. In *Applied Cryptography and Network Security, Second International Conference, ACNS 2004* (Lecture Notes in Computer Science 3089), pages 16–30, June 2004.

[100] G. Goodson, J. Wylie, G. Ganger and M. K. Reiter. **Efficient Byzantine-tolerant erasure-coded storage**. In *Proceedings of the 34th IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2004.

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] D. Davis, F. Monrose, and M. K. Reiter. **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.

[106] 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.

[107] 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.

[108] 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.

[109] 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.

[110] 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*.

[111] 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.

[112] 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.

[113] 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.

[114] 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.

[115] 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.

[116] 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.

[117] 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.

[118] 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.

[119] 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.

[120] 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.

[121] 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.

[122] 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.

[123] 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.

[124] V. Sekar, Y. Xie, M. K. Reiter and H. Zhang. **A multi-resolution approach to worm detection and containment**. In *Proceedings of the 36th IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 189−198, June 2006.

[125] 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.

[126] 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.

[127] 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.

[128] 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.

[129] 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.

[130] 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.

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] 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.

[136] 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.

[137] 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.

[138] 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.

[139] F. Oprea and M. K. Reiter. **Minimizing response time for quorum-system protocols over wide-area networks**. In *Proceedings of the 37th IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 409−418, June 2007.

[140] 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*, pages 64−75, July 2007.

[141] A. Oprea and M. K. Reiter. **Integrity checking in cryptographic file systems with constant trusted storage**. In *Proceedings of the 16th USENIX Security Symposium*, pages 183−198, August 2007.

[142] S. Coull, M. P. Collins, C. Wright, F. Monrose and M. K. Reiter. **On web browsing privacy in anonymized NetFlows**. In *Proceedings of the 16th USENIX Security Symposium*, pages 339−352, August 2007.

[143] J. Hendricks, G. R. Ganger and M. K. Reiter. **Verifying distributed erasure-coded data**. In *Proceedings of the 26th ACM Symposium on Principles of Distributed Computing*, pages 139−146, August 2007.

[144] 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: 10th International Symposium, RAID 2007* (Lecture Notes in Computer Science 4637), pages 276−295, August 2007.

[145] M. G. Merideth and M. K. Reiter. **Probabilistic opaque quorum systems**. In *Distributed Computing: 21st International Symposium, DISC 2007* (Lecture Notes in Computer Science 4731), pages 403−419, September 2007.

[146] L. Bauer, S. Garriss and M. K. Reiter. **Efficient proving for practical distributed access-control systems**. *Computer Security − ESORICS 2007: 12th European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 4734), pages 19−37, September 2007.

[147] J. Hendricks, G. R. Ganger and M. K. Reiter. **Low-overhead Byzantine fault-tolerant storage**. In *Proceedings of the 21st ACM Symposium on Operating Systems Principles*, pages 73−86, October 2007.

[148] 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 15th Network and Distributed System Security Symposium*, February 2008.

[149] 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 13th International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 14−25, March 2008.

[150] J. M. McCune, B. Parno, A. Perrig, M. K. Reiter, and H. Isozaki. **Flicker: An execution infrastructure for TCB minimization**. In *Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems*, pages 315−328, April 2008. Received *Test of Time Award*, Intel Hardware Security Academic Awards, 2024.

[151] 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 26th ACM Conference on Human Factors in Computing Systems*, pages 543−552, April 2008.

[152] 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 26th ACM Conference on Human Factors in Computing Systems*, page 1473−1482, April 2008.

[153] M. K. Reiter, A. Samar, and C. Wang. **Self-optimizing distributed trees**. In *Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium*, April 2008.

[154] 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 5th USENIX Symposium on Network Systems Design and Implementation*, pages 233−246, April 2008.

[155] L. Bauer, S. Garriss and M. K. Reiter. **Detecting and resolving policy misconfigurations in access-control systems**. In *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, pages 185−194, June 2008.

[156] Z. Li, X. Wang, Z. Liang, and M. K. Reiter. **AGIS: Towards automatic generation of infection signatures**. In *Proceedings of the 38th IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 237−246, June 2008.
[157] T.-F. Yen and M. K. Reiter. **Traffic aggregation for malware detection**. In *Detection of Intrusions and Malware, and Vulnerability Assessment, 5th International Conference, DIMVA 2008* (Lecture Notes in Computer Science 5137), pages 207−227, July 2008.
[158] L. Ballard, S. Kamara and M. K. Reiter. **The practical subtleties of biometric key generation**. In *Proceedings of the 17th USENIX Security Symposium*, pages 61−74, August 2008.
[159] M. P. Collins and M. K. Reiter. **On the limits of payload-oblivious network attack detection**. In *Recent Advances in Intrusion Detection: 11th International Symposium, RAID 2008* (Lecture Notes in Computer Science 5230), pages 251–270, September 2008.
[160] 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.
[161] L. Ballard, S. Kamara, F. Monrose and M. K. Reiter. **Towards practical biometric key generation with randomized biometric templates**. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pages 235–244, October 2008.
[162] M. G. Merideth and M. K. Reiter. **Write markers for probabilistic quorum systems**. In *Principles of Distributed Systems, 12th International Conference, OPODIS 2008* (Lecture Notes in Computer Science 5401), pages 5–21, December 2008.
[163] J. M. McCune, A. Perrig and M. K. Reiter. **Safe passage for passwords and other sensitive data**. In *Proceedings of the 16th ISOC Network and Distributed Systems Security Symposium*, pages 301–320, February 2009.
[164] 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.
[165] 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 27th ACM Conference on Human Factors in Computing Systems*, pages 899–908, April 2009.
[166] L. Bauer, L. Jia, M. K. Reiter and D. Swasey. **xDomain: Cross-border proofs of access**. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, pages 43–52, June 2009.
[167] Y.-H. Oh, P. Ning, Y. Liu and M. K. Reiter. **Authenticated data compression in delay tolerant wireless sensor networks**. In *Proceedings of the 6th International Conference on Networked Sensing Systems*, pages 137–144, June 2009.
[168] 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, 6th International Conference, DIMVA 2009* (Lecture Notes in Computer Science 5587), pages 157–175, July 2009.
[169] D. Bethea and M. K. Reiter. **Data structures with unpredictable timing**. In *Computer Security − ESORICS 2009: 14th European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 5789), pages 456–471, September 2009.
[170] P. Li, D. Gao and M. K. Reiter. **Automatically adapting a trained anomaly detector to software patches**. In *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009* (Lecture Notes in Computer Science 5758), pages 142–160, September 2009.
[171] M. G. Merideth, F. Oprea and M. K. Reiter. **When and how to change quorums on wide-area networks**. In *Proceedings of the 28th International Symposium on Reliable Distributed Systems*, pages 12–21, September 2009.

[172] Y. Liu, P. Ning, and M. K. Reiter. **False data injection attacks against state estimation in electric power grids**. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pages 21–32, November 2009. Received *Test of Time Award*.

[173] 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 16th ACM Conference on Computer and Communications Security*, pages 338–347, November 2009.

[174] 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, 5th International Conference, ICISS 2009* (Lecture Notes in Computer Science 5905), pages 132–147, December 2009.

[175] V. Sekar, A. Gupta, M. K. Reiter and H. Zhang. **Coordinated sampling sans origin-destination identifiers: Algorithms and analysis**. In *Proceedings of the 2nd International Conference on Communication Systems and Networks*, January 2010.

[176] D. Bethea, R. A. Cochran and M. K. Reiter. **Server-side verification of client behavior in online games**. In *Proceedings of the 17th ISOC Network and Distributed System Security Symposium*, pages 21–36, February 2010. Received *Best Paper Award*.

[177] M. L. Mazurek, J. P. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. F. Cranor, G. R. Ganger, and M. K. Reiter. **Access control for home data sharing: Attitudes, needs and practices**. In *Proceedings of the 28th ACM Conference on Human Factors in Computing Systems*, pages 645–654, April 2010.

[178] T.-F. Yen and M. K. Reiter. **Are your hosts trading or plotting? Telling P2P file-sharing and bots apart**. In *Proceedings of the 30th International Conference on Distributed Computing Systems*, pages 241–252, June 2010.

[179] J. Hendricks, S. Sinnamohideen, G. R. Ganger and M. K. Reiter. **Zzyzx: Scalable fault tolerance through Byzantine locking**. In *Proceedings of the 40th IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 363–372, June 2010.

[180] S. E. Coull, A. M. White, T.-F. Yen, F. Monrose and M. K. Reiter. **Understanding domain registration abuses**. In *Security and Privacy – Silver Linings in the Cloud, 25th IFIP TC-11 International Information Security Conference, SEC 2010*, pages 68–79, September 2010.

[181] P. Li, L. Liu, D. Gao and M. K. Reiter. **On challenges in evaluating malware clustering**. In *Recent Advances in Intrusion Detection: 13th International Symposium, RAID 2010* (Lecture Notes in Computer Science 6307), pages 238–255, September 2010.

[182] Y. Zhang, F. Monrose and M. K. Reiter. **The security of modern password expiration: An algorithmic framework and empirical analysis**. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, pages 176–186, October 2010.

[183] V. Sekar, M. K. Reiter and H. Zhang. **Revisiting the case for a minimalist approach for network flow monitoring**. In *Proceedings of the 10th Internet Measurement Conference*, pages 328–341, November 2010.

[184] V. Sekar, R. Krishnaswamy, A. Gupta and M. K. Reiter. **Network-wide deployment of intrusion detection and prevention systems**. In *Proceedings of the 6th International Conference on Emerging Network Experiments and Technologies*, November 2010.

[185] L. Wei, M. K. Reiter and K. Mayer-Patel. **Summary-invisible networking: Techniques and defenses**. In *Information Security, 13th International Conference, ISC 2010* (Lecture Notes in Computer Science 6531), pages 210–225, 2011.

[186] A. Libonati, J. M. McCune and M. K. Reiter. **Usability testing a malware-resistant input mechanism**. In *Proceedings of the 18th ISOC Network and Distributed System Security Symposium*, pages 435–451, February 2011.

[187] L. Wei, S. Coull and M. K. Reiter. **Bounded vector signatures and their applications**. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pages 277–285, March 2011.

[188] N. D. Kumar, F. Monrose and M. K. Reiter. **Towards optimized probe scheduling for active measurement studies**. In *Proceedings of the 6th International Conference on Internet Monitoring and Protection*, pages 26–31, March 2011. Received *Best Paper Award*.

[189] R. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter and K. Vaniea. **More than skin deep: Measuring effects of the underlying model on access-control system usability**. In *Proceedings of the 29th ACM Conference on Human Factors in Computing Systems*, pages 2065–2074, May 2011.

[190] Y. Zhang, A. Juels, A. Oprea and M. K. Reiter. **HomeAlone: Co-residency detection in the cloud via side-channel analysis**. In *Proceedings of the 32nd IEEE Symposium on Security and Privacy*, pages 313–328, May 2011.

[191] X. Huang, F. Monrose and M. K. Reiter. **Amplifying limited expert input to sanitize large network traces**. In *Proceedings of the 41st IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 495–505, June 2011.

[192] V. Sekar, S. Ratnasamy, M. K. Reiter, N. Egi and G. Shi. **The middlebox manifesto: Enabling innovation in middlebox deployment**. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, November 2011.

[193] L. Bauer, Y. Liang, M. K. Reiter and C. Spensky. **Discovering access-control misconfigurations: New approaches and evaluation methodologies**. In *Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy*, pages 95–104, February 2012.

[194] A. A. Yavuz, P. Ning and M. K. Reiter. **Efficient, compromise resilient and append-only cryptographic schemes for secure audit logging**. In *Financial Cryptography and Data Security, 16th International Conference* (Lecture Notes in Computer Science 7397), pages 148–163, February 2012.

[195] T.-F. Yen and M. K. Reiter. **Revisiting botnet models and their implications for takedown strategies**. In *Principles of Security and Trust, First International Conference, POST 2012* (Lecture Notes in Computer Science 7215), pages 249–268, March 2012.

[196] V. Sekar, N. Egi, S. Ratnasamy, M. K. Reiter and G. Shi. **Design and implementation of a consolidated middlebox architecture**. In *Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation*, April 2012.

[197] P. F. Klemperer, Y. Liang, M. L. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta and M. K. Reiter. **Tag, you can see it! Using tags for access control in photo sharing**. In *Proceedings of the 30th ACM Conference on Human Factors in Computing Systems*, pages 377–386, May 2012.

[198] K. Vaniea, L. Bauer, L. F. Cranor and M. K. Reiter. **Out of sight, out of mind: Effects of displaying access-control information near the item it controls**. In *Proceedings of the 10th Conference on Privacy, Security and Trust*, pages 128–136, July 2012.

[199] K. Vaniea, L. Bauer, L. F. Cranor and M. K. Reiter. **Studying access-control usability in the lab: Lessons learned from four studies**. In *Proceedings of LASER 2012 _ Learning from Authoritative Security Experiment Results*, pages 31–40, July 2012.

[200] L. Wei and M. K. Reiter. **Third-party private DFA evaluation on encrypted files in the cloud**. In *Computer Security − ESORICS 2012: 17th European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 7459), pages 523–540, September 2012.

[201] Y. Zhang, A. Juels, M. K. Reiter and T. Ristenpart. **Cross-VM side channels and their use to extract private keys**. In *Proceedings of the 19th ACM Conference on Computer and Communications Security*, pages 305–316, October 2012. Received *Test of Time Award*.

[202] V. Heorhiadi, M. K. Reiter and V. Sekar. **New opportunities for load balancing in network-wide intrusion detection systems**. In *Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies*, pages 361–372, December 2012.

[203] R. A. Cochran and M. K. Reiter. **Toward online verification of client behavior in distributed applications**. In *Proceedings of the 20th ISOC Network and Distributed System Security Symposium*, February 2013.

[204] P. Li, D. Gao and M. K. Reiter. **Mitigating access-driven timing channels in clouds using StopWatch**. In *Proceedings of the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2013.

[205] L. Wei and M. K. Reiter. **Ensuring file authenticity in private DFA evaluation on encrypted files in the cloud**. In *Computer Security − ESORICS 2013: 18th European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 8134), pages 147–163, September 2013.

[206] H.-C. Kum, A. Krishnamurthy, D. Pathak, M. K. Reiter, and S. Ahalt. **Secure Decoupled Linkage (SDLink) system for building a social genome**. In *Proceedings of the 2013 IEEE International Conference on Big Data*, pages 7–11, October 2013.

[207] L. Bauer, L. F. Cranor, S. Komanduri, M. L. Mazurek, M. K. Reiter, M. Sleeper, and B. Ur. **The post anachronism: The temporal dimension of Facebook privacy**. In *Proceedings of the 12th Workshop on Privacy in the Electronic Society*, pages 1–12, November 2013.

[208] Y. Zhang and M. K. Reiter. **Düppel: Retrofitting commodity operating systems to mitigate cache side channels in the cloud**. In *Proceedings of the 20th ACM Conference on Computer and Communications Security*, pages 827–837, November 2013.

[209] S. K. Fayazbakhsh, M. K. Reiter, and V. Sekar. **Verifiable network function outsourcing: Requirements, challenges, and roadmap**. In *Proceedings of the Workshop on Hot Topics in Middleboxes and Network Function Virtualization*, pages 25–30, December 2013.

[210] M. L. Mazurek, Y. Liang, W. Melicher, M. Sleeper, L. Bauer, G. R. Ganger, N. Gupta, and M. K. Reiter. **Toward strong, usable access control for shared distributed data**. In *Proceedings of the 12th USENIX Conference on File and Storage Technologies*, pages 89–103, February 2014.

[211] A. Libonati, K. Caine, A. Kapadia, and M. K. Reiter. **Defending against device theft with human notarization**. In *Proceedings of the 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, October 2014. Invited paper.

[212] Y. Zhang, A. Juels. M. K. Reiter, and T. Ristenpart. **Cross-tenant side-channel attacks in PaaS clouds.** In *Proceedings of the 21st ACM Conference on Computer and Communications Security*, pages 990–1003, November 2014.

[213] T.-F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels. **An epidemiological study of malware encounters in a large enterprise**. In *Proceedings of the 21st ACM Conference on Computer and Communications Security*, pages 1117–1130, November 2014.

[214] V. Heorhiadi, S. K. Fayaz, M. K. Reiter, and V. Sekar. **SNIPS: A software-defined approach for scaling intrusion prevention systems via offloading**. In *Information Systems Security 10th International Conference, ICISS 2014* (Lecture Notes in Computer Science 8880), pages 9–29, December 2014. Invited paper.

[215] Q. Ismail, T. Ahmed, A. Kapadia, and M. K. Reiter. **Crowdsourced exploration of security configurations**. In *Proceedings of the 33rd ACM Conference on Human Factors in Computing Systems*, April 2015.

[216] M. Moradi, F. Qian, Q. Xu, Z. M. Mao, D. Bethea, and M. K. Reiter. **Caesar: High-speed and memory-efficient forwarding engine for future Internet architecture**. In *Proceedings of the 11th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, pages 171–182, May 2015.

[217] P. Li, D. Gao, and M. K. Reiter. **Replica placement for availability in the worst case**. In *Proceedings of the 35th IEEE International Conference on Distributed Computing Systems*, pages 599–608, June 2015.

[218] S. J. Andrabi, M. K. Reiter, and C. Sturton. **Usability of augmented reality for revealing secret messages to users but not their devices**. In *Proceedings of the 11th Symposium on Usable Privacy and Security*, pages 89–102, July 2015.

[219] Q. Xiao, M. K. Reiter, and Y. Zhang. **Mitigating storage side channels using statistical privacy mechanisms**. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security*, pages 1582–1594, October 2015.

[220] S.-J. Moon, V. Sekar, and M. K. Reiter. **Nomad: Mitigating arbitrary cloud side channels via provider-assisted migration**. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security*, pages 1595–1606, October 2015. Winner of the 4th Annual Best Scientific Cybersecurity Paper Competition.

[221] D. Bethea, M. K. Reiter, F. Qian, Q. Xu, and Z. M. Mao. **WACCO and LOKO: Strong consistency at global scale**. In *Proceedings of the 1st IEEE International Conference on Collaboration and Internet Computing*, pages 130–141, October 2015. Invited paper.

[222] J. Aljuraidan, L. Bauer, M. K. Reiter, and M. Beckerle. **Introducing reputation systems to the economics of outsourcing computations to rational workers**. In *Financial Cryptography and Data Security, 20th International Conference* (Lecture Notes in Computer Science 9603), pages 60–77, February 2016.

[223] V. Heorhiadi, M. K. Reiter, and V. Sekar. **Simplifying software-defined network optimization using SOL**. In *Proceedings of the 13th USENIX Symposium on Networked System Design and Implementation*, March 2016.

[224] P. Snyder, C. Kanich, and M. K. Reiter. **The effect of repeated login prompts on phishing susceptibility**. In *Proceedings of the LASER Workshop: Learning from Authoritative Security Experiment Results*, pages 13–19, May 2016.

[225] V. Heorhiadi, S. Rajagopalan, H. Jamjoom, M. K. Reiter, and V. Sekar. **Gremlin: Systematic resilience testing of microservices**. In *Proceedings of the 36th IEEE International Conference on Distributed Computing Systems*, pages 57–66, June 2016.

[226] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart. **Stealing machine learning models via prediction APIs**. In *Proceedings of the 25th USENIX Security Symposium*, pages 601–618, August 2016.

[227] Z. Zhou, M. K. Reiter, and Y. Zhang. **A software approach to defeating side channels in last-level caches**. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security*, pages 871–882, October 2016.

[228] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter. **Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition**. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security*, pages 1528–1540, October 2016.

[229] A. Chi, R. Cochran, M. Nesfield, M. K. Reiter, and C. Sturton. **A system to verify network behavior of known cryptographic clients**. In *Proceedings of the 14th USENIX Symposium on Networked System Design and Implementation*, pages 177–195, March 2017.

[230] S. Chen, X. Zhang, M. K. Reiter, and Y. Zhang. **Detecting privileged side-channel attacks in shielded execution with Déjà Vu**. In *Proceedings of the 12th ACM Asia Conference on Computer and Communications Security*, pages 7–18, April 2017.

[231] S. Liu, M. K. Reiter, and V. Sekar. **Flow reconnaissance via timing attacks on SDN switches**. In *Proceedings of the 37th IEEE International Conference on Distributed Computing Systems*, June 2017.

[232] S. Duan, M. K. Reiter, and H. Zhang. **Secure causal atomic broadcast, revisited**. In *Proceedings of the 47th IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2017.

[233] W. Liu, D. Gao, and M. K. Reiter. **On-demand time blurring to support side-channel defense**. In *Computer Security − ESORICS 2017: 22nd European Symposium on Research in Computer Security* (Lecture Notes in Computer Science 10493), pages 210–228, September 2017.

[234] G. Chen, T.-H. Lai, M. K. Reiter, and Y. Zhang. **Differentially private access patterns for searchable symmetric encryption**. In *Proceedings of the IEEE International Conference on Computer Communications*, April 2018.

[235] Z. Zhou, Z. Qian, M. K. Reiter, and Y. Zhang. **Static evaluation of noninterference using approximate model counting**. In *Proceedings of the 39th IEEE Symposium on Security and Privacy*, pages 514–528, May 2018.

[236] M. Sharif, L. Bauer, and M. K. Reiter. **On the suitability of L_p-norms for creating and preventing adversarial examples**. In *Proceedings of the 2018 Workshop on The Bright and Dark Sides of Computer Vision: Challenges and Opportunities for Privacy and Security*, pages 1718–1726, June 2018.

[237] S. Duan, M. K. Reiter, and H. Zhang. **BEAT: Asynchronous BFT made practical**. In *Proceedings of the 25th ACM Conference on Computer and Communications Security*, pages 2028–2041, October 2018.

[238] V. Heorhiadi, S. Chandrasekaran, M. K. Reiter, and V. Sekar. **Intent-driven composition of resource-management SDN applications**. In *Proceedings of the 14th International Conference on Emerging Networking Experiments and Technologies*, December 2018.

[239] K. C. Wang and M. K. Reiter. **How to end password reuse on the web**. In *Proceedings of the 26th ISOC Network and Distributed System Security Symposium*, February 2019.

[240] X. Zhang, J. Hamm, M. K. Reiter, and Y. Zhang. **Statistical privacy for streaming traffic**. In *Proceedings of the 26th ISOC Network and Distributed System Security Symposium*, February 2019.

[241] S. Liu, T. Benson, and M. K. Reiter. **Efficient and safe network updates with suffix causal consistency**. In *Proceedings of the 14th ACM SIGOPS/EuroSys European Conference on Computer Systems*, March 2019. Received *Best Student Paper Award*.

[242] G. G. Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. K. Reiter, D.-A. Seredinschi, O. Tamir, and A. Tomescu. **SBFT: A scalable and decentralized trust infrastructure**. In *Proceedings of the 49th IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 568–580, June 2019.

[243] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham. **HotStuff: BFT consensus with linearity and responsiveness**. In *Proceedings of the 38th ACM Symposium on Principles of Distributed Computing*, July 2019.

[244] S. Basu, A. Tomescu, I. Abraham, D. Malkhi, M. K. Reiter, and E. G. Sirer. **Efficient verifiable secret sharing with share recovery in BFT protocols**. In *Proceedings of the 26th ACM Conference on Computer and Communications Security*, November 2019.

[245] I. Polinsky, K. Martin, W. Enck, and M. K. Reiter. ***n-m*-variant systems: Adversarial-resistant software rejuvenation for cloud-based web applications**. In *Proceedings of the 10th ACM Conference on Data and Application Security and Privacy*, March 2020.

[246] Q. Xiao, B. Subialdea, L. Bauer, and M. K. Reiter. **Metering graphical data leakage with Snowman**. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, June 2020.

[247] C. M. Bender, Y. Li, Y. Shi, M. K. Reiter, and J. Oliva. **Defense through diverse directions**. In *Proceedings of the 37th International Conference on Machine Learning*, July 2020.

[248] K. C. Wang and M. K. Reiter. **Detecting stuffing of a user's credentials at her own accounts**. In *Proceedings of the 29th USENIX Security Symposium*, August 2020.

[249] A. Humphries, K. Cating-Subramanian, and M. K. Reiter. **TASE: Reducing latency of symbolic execution with transactional memory**. In *Proceedings of the 28th ISOC Network and Distributed System Security Symposium*, February 2021.

[250] I. Anjum, M. Zhu, I. Polinsky, W. Enck, M. K. Reiter, and M. Singh. **Role-based deception in enterprise networks**. In *Proceedings of the 11th ACM Conference on Data and Application Security and Privacy*, April 2021.

[251] K. Lucas, M. Sharif, L. Bauer, M. K. Reiter, and S. Shintre. **Malware makeover: Breaking ML-based static analysis by modifying executable bytes**. In *Proceedings of the 16th ACM Asia Conference on Computer and Communications Security*, June 2021.

[252] C. Guo, B. Campbell, A. Kapadia, M. K. Reiter, and K. Caine. **Effect of mood, location, trust, and presence of others on video-based social authentication**. In *Proceedings of the 30th USENIX Security Symposium*, August 2021.

[253] K. C. Wang and M. K. Reiter. **Using Amnesia to detect credential database breaches**. In *Proceedings of the 30th USENIX Security Symposium*, August 2021.

[254] K. Wang, L. Xu, A. Perrault, M. K. Reiter, and M. Tambe. **Coordinating followers to reach better equilibria: End-to-end gradient descent for Stackelberg games**. In *Proceedings of the 36th AAAI Conference on Artificial Intelligence*, February 2022.

[255] C. M. Bender, P. Emmanuel, M. K. Reiter, and J. Oliva. **Practical integration via separable bijective networks**. In *Proceedings of the 10th International Conference on Learning Representations*, April 2022.

[256] W. Lin, K. Lucas, L. Bauer, M. K. Reiter, and M. Sharif. **Constrained gradient descent: A powerful and principled evasion attack against neural networks**. In *Proceedings of the 39th International Conference on Machine Learning*, July 2022.

[257] W. Wang, S. Deng, J. Niu, M. K. Reiter, and Y. Zhang. **ENGRAFT: Enclave-guarded Raft on Byzantine faulty nodes**. In *Proceedings of the 29th ACM Conference on Computer and Communications Security*, November 2022.

[258] S. Yandamuri, I. Abraham, K. Nayak, and M. K. Reiter. **Communication-efficient BFT using small trusted hardware to tolerate minority corruption**. In *Proceedings of the 26th International Conference on Principles of Distributed Systems*, December 2022. Brief announcement appears in *Proceedings of the 35th International Symposium on Distributed Computing*, October 2021.

[259] A. Bhat, A. Bandarupalli, S. Bagchi, A. Kate, and M. K. Reiter. **The unique chain rule and its applications**. In *Proceedings of the 27th International Conference on Financial Cryptography and Data Security*, May 2023.

[260] S. Liu, M. K. Reiter, and T. A. Benson. **Nimble: Fast and safe migration of network functions**. In *Proceedings of the 42nd IEEE International Conference on Computer Communications*, May 2023.

[261] A. Chakraborti and M. K. Reiter. **Privately evaluating region overlaps with applications to collaborative sensor output validation**. In *Proceedings of the 8th IEEE European Symposium on Security and Privacy*, July 2023.

[262] A. C. Reed and M. K. Reiter. **Optimally hiding object sizes with constrained padding**. In *Proceedings of the 36th IEEE Computer Security Foundations Symposium*, July 2023.

[263] A. Chakraborti, G. Fanti, and M. K. Reiter. **Distance-aware private set intersection**. In *Proceedings of the 32nd USENIX Security Symposium*, August 2023.

[264] K. Lucas, S. Pai, W. Lin, L. Bauer, M. K. Reiter, and M. Sharif. **Adversarial training for raw-binary malware classifiers**. In *Proceedings of the 32nd USENIX Security Symposium*, August 2023.

[265] A. Chi, B. Anderson, and M. K. Reiter. **Prioritizing remediation of enterprise hosts by malware execution risk**. In *Proceedings of the 39th Annual Computer Security Applications Conference*, December 2023.

[266] A. Bhat, A. Bandarupalli, M. Nagaraj, S. Bagchi, A. Kate, and M. K. Reiter. **EESMR: Energy efficient BFT-SMR for the masses**. In *Proceedings of the 24th ACM/IFIP International Middleware Conference*, December 2023.

[267] K. C. Wang and M. K. Reiter. **Bernoulli honeywords**. In *Proceedings of the 31st ISOC Network and Distributed System Security Symposium*, February 2024.

[268] W. Lin, K. Lucas, N. Eyal, L. Bauer, M. K. Reiter, and M. Sharif. **Group-based robustness: A general framework for customized robustness in the real world**. In *Proceedings of the 31st ISOC Network and Distributed System Security Symposium*, February 2024.

[269] A. Bandarupalli, A. Bhat, S. Bagchi, A. Kate, C.-D. Liu-Zhang, and M. K. Reiter. **Delphi: Efficient asynchronous approximate agreement for distributed oracles**. In *Proceedings of the 54th IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2024.

[270] W. Wang, J. Niu, M. K. Reiter, and Y. Zhang. **Formally verifying a rollback-prevention protocol for TEEs**. In *Proceedings of the 44th International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (Lecture Notes in Computer Science 14678), pages 155–173, June 2024.

[271] A. Bandarupalli, A. Bhat, S. Chaterji, M. K. Reiter, A. Kate and S. Bagchi. **SensorBFT: Fault-tolerant target localization using Voronoi diagrams and approximate agreement**. In *Proceedings of the 44th IEEE International Conference on Distributed Computing Systems*, July 2024.

[272] H. Liu, M. K. Reiter, and N. Gong. **Mudjacking: Patching backdoor vulnerabilities in foundation models**. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.

[273] Z. Huang, L. Bauer, and M. K. Reiter. **The impact of exposed passwords on honeyword efficacy**. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.

[274] J. Xing, S. Yoo, X. Foukas, D. Kim, and M. K. Reiter. **On the criticality of integrity protection in 5G fronthaul networks**. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.

[275] P. Jain, A. C. Reed, and M. K. Reiter. **Near-optimal constrained padding for object retrievals with dependencies**. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.

[276] L. Zhou, Z. Liu, F. Zhang, and M. K. Reiter. **CrudiTEE: A stick-and-carrot approach to building trustworthy cryptocurrency wallets with TEEs**. In *Proceedings of the 6th International Conference on Advances in Financial Technologies*, September 2024. To appear.

[277] A. Bandarupalli, A. Bhat, S. Bagchi, A. Kate, and M. K. Reiter. **Random beacons in Monte Carlo: Efficient asynchronous random beacon without threshold cryptography**. In *Proceedings of the 31st ACM Conference on Computer and Communications Security*, October 2024. To appear.

[278] C. Jin, C. Yin, M. van Dijk, S. Duan, F. Massacci, M. K. Reiter, and H. Zhang. **PG: Byzantine fault-tolerant and privacy-preserving sensor fusion with guaranteed output delivery**. In *Proceedings of the 31st ACM Conference on Computer and Communications Security*, October 2024. To appear.

[279] Z. Huang, N. Gong, and M. K. Reiter. **A general framework for data-use auditing of ML models**. In *Proceedings of the 31st ACM Conference on Computer and Communications Security*, October 2024. To appear.

[280] K. Lucas, W. Lin, L. Bauer, M. K. Reiter, and M. Sharif. **Training robust ML-based raw-binary malware detectors in hours, not months**. In *Proceedings of the 31st ACM Conference on Computer and Communications Security*, October 2024. To appear.

Other publications

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

[282] 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.

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

[284] 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.

[285] 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.

[286] M. K. Reiter and A. D. Rubin. **Anonymous web transactions with Crowds**. *Communications of the ACM* 42(2):32−38, February 1999. Invited paper.

[287] M. K. Reiter. **Network survivability and information warfare**. In *Frontiers of Engineering 1999*, pages 20−23. National Academy Press, 2000.

[288] 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.

[289] M. G. Merideth and M. K. Reiter. **Selected results from the latest decade of quorum systems research**. In *Replication, Theory and Practice* (Lecture Notes in Computer Science 5959), pages 185–206, 2010.

[290] J. Aikat, A. Akella, J. Chase, A, Juels, M. K. Reiter, R. Ristenpart, V. Sekar, and M. Swift. **Rethinking security in the era of cloud computing**. *IEEE Security and Privacy* 15(3):60–69, May/June 2017.

[291] J. Severini, R. N. Mysore, V. Sekar, S. Banerjee, and M. K. Reiter. **The Netivus manifesto: Making collaborative network management easier for the rest of us**. *ACM SIGCOMM Computer Communication Review*, May 2021.

[292] K. Lucas, M. Sharif, L. Bauer, M. K. Reiter, and S. Shintre. **Deceiving ML-based friend-or-foe identification for executables**. In *Cyber Deception: Techniques,Strategies, and Human Aspects*, Springer 2023. Invited paper.

[293] K. C. Wang and M. K. Reiter. **Using Amnesia to detect credential database breaches**. In *Cyber Deception: Techniques,Strategies, and Human Aspects*, Springer 2023. Invited paper.

[294] C. Landwehr, M. K. Reiter, L. Williams, G. Tsudik, T. Jaeger, T. Kohno, and A. Kapadia. **Looking backwards (and forwards): NSF Secure and Trustworthy Computing 20-year retrospective panel transcription**. *IEEE Security & Privacy*, January 2023.