A Complete Bibliography of *ACM Transactions on Information and System Security*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

14 October 2017
Version 1.58

Title word cross-reference

References

Antonatos:2008:PMW

[AALA08] Spiros Antonatos, Periklis Akritidis, Vinh The Lam, and Kostas G. Anagnostakis. Puppetnets: Misusing Web browsers as a distributed attack infrastructure. *ACM Transactions on Information and System Security*, 12(2):12:1–12:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ali:2015:RBI

[AAS15] Muhammad Qasim Ali and Ehab Al-Shaer. Randomization-based intrusion detection system for advanced metering infrastructure*. *ACM Transactions on Information and System Security*, 18(2):7:1–7:??, December 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ali:2013:AAD

[AASKK13] Muhammad Qasim Ali, Ehab Al-Shaer, Hassan Khan, and Syed Ali Khayam. Automated anomaly detector adaptation using adaptive threshold tuning. *ACM Transactions on Information and System Security*, 15(4):

17:1–17:??, April 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Aiello:2004:JFK

[ABB+04] William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile Internet. *ACM Transactions on Information and System Security*, 7(2):242–273, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ateniese:2011:RDC

[ABC+11] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Osama Khan, Lea Kissner, Zachary Peterson, and Dawn Song. Remote data checking using provable data possession. *ACM Transactions on Information and System Security*, 14(1):12:1–12:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Abadi:2009:CFI

[ABEL09] Martín Abadi, Mihai Budiu, Úlfar Erlingsson, and Jay Ligatti. Control-flow integrity principles, implementations, and applications. *ACM Transactions on Information and System Security*, 13(1):4:1–4:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Abadi:2007:JFK

[ABF07] Martín Abadi, Bruno Blanchet, and Cédric Fournet. Just fast keying in the pi calculus. *ACM Transactions on Information and System Security*, 10 (3):9:1–9:??, July 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Atallah:2009:DEK

[ABFF09] Mikhail J. Atallah, Marina Blanton, Nelly Fazio, and Keith B. Frikken. Dynamic and efficient key management for access hierarchies. *ACM Transactions on Information and System Security*, 12(3):18:1–18:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Arkoudas:2014:SAC

[ACC14] Konstantine Arkoudas, Ritu Chadha, and Jason Chiang. Sophisticated access control via SMT and logical frameworks. *ACM Transactions on Information and System Security*, 16(4): 17:1–17:??, April 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Awerbuch:2008:ODS

[ACH+08] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens. ODSBR: an on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. *ACM Transactions on Information and System Security*, 10(4):6:1–6:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ateniese:2006:IPR

[AFGH06] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security*, 9(1):1–30, February 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Atluri:2002:AMT

[AG02] Vijayalakshmi Atluri and Avigdor Gal. An authorization model for temporal and derived data: securing information portals. *ACM Transactions on Information and System Security*, 5(1):62–94, February 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ahn:2007:GES

[Ahn07] Gail-Joon Ahn. Guest editorial: Special issue on access control models and technologies. *ACM Transactions on Information and System Security*, 10(1): 1:1–1:??, February 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Avoine:2008:CIT

[AJO08] Gildas Avoine, Pascal Junod, and Philippe Oechslin. Characterization and improvement of time-memory trade-off based on perfect tables. *ACM Transactions on Information and System Security*, 11(4):17:1–17:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Amir:2004:PGK

[AKNRT04] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, and Gene Tsudik. On the performance of group key agreement protocols. *ACM Transactions on Information and System Security*, 7(3):457–488, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Allodi:2014:CVS

[AM14] Luca Allodi and Fabio Massacci. Comparing vulnerability severity and exploits using case-control studies. *ACM Transactions on Information and System Security*, 17(1):1:1–1:??, August 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Abadi:2012:PLR

[AP12] Martín Abadi and Gordon D. Plotkin. On protection by layout randomization. *ACM Transactions on Information and System Security*, 15(2):8:1–8:??, July 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Alexander:2015:MCD

[APLC15] Perry Alexander, Lee Pike, Peter Loscocco, and George

Coker. Model checking distributed mandatory access control policies. *ACM Transactions on Information and System Security*, 18(2):6:1–6:??, December 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Appel:2011:SSV

[App11] Andrew W. Appel. Security seals on voting machines: a case study. *ACM Transactions on Information and System Security*, 14(2):18:1–18:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ahn:2000:RBA

[AS00] Gail-Joon Ahn and Ravi Sandhu. Role-based authorization constraints specification. *ACM Transactions on Information and System Security*, 3(4):207–226, November 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ahmed:2007:SVS

[AT07] Tanvir Ahmed and Anand R. Tripathi. Specification and verification of security requirements in a programming model for decentralized CSCW systems. *ACM Transactions on Information and System Security*, 10 (2):7:1–7:??, May 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ateniese:2004:VED

[Ate04] Giuseppe Ateniese. Verifiable encryption of digital signatures and applications. *ACM Transactions on Information and System Security*, 7(1):1–20, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Au:2011:PPT

[ATK11] M. Ho Au, P. P. Tsang, and A. Kapadia. PEREA: Practical TTP-free revocation of repeatedly misbehaving anonymous users. *ACM Transactions on Information and System Security*, 14(4):29:1–29:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Atluri:2005:P

[Atl05] Vijay Atluri. Preface. *ACM Transactions on Information and System Security*, 8(1): 2, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Axelsson:2000:BRF

[Axe00] Stefan Axelsson. The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security*, 3(3):186–205, August 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Barrantes:2005:RIS

[BAFS05] Elena Gabriela Barrantes, David H. Ackley, Stephanie Forrest, and

Darko Stefanović. Randomized instruction set emulation. *ACM Transactions on Information and System Security*, 8 (1):3–40, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Brennan:2012:ASC

[BAG12] Michael Brennan, Sadia Afroz, and Rachel Greenstadt. Adversarial stylometry: Circumventing authorship recognition to preserve privacy and anonymity. *ACM Transactions on Information and System Security*, 15(3): 12:1–12:??, November 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bertino:2001:TTR

[BBF01] Elisa Bertino, Piero Andrea Bonatti, and Elena Ferrari. TRBAC: a temporal role-based access control model. *ACM Transactions on Information and System Security*, 4(3):191–223, August 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Basin:2012:DEA

[BBK12] David Basin, Samuel J. Burri, and Günter Karjoth. Dynamic enforcement of abstract separation of duty constraints. *ACM Transactions on Information and System Security*, 15(3): 13:1–13:??, November 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Basin:2014:KYE

[BC14] David Basin and Cas Cremers. Know your enemy: Compromising adversaries in protocol analysis. *ACM Transactions on Information and System Security*, 17(2):7:1–7:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bertino:2001:NTM

[BCF01] Elisa Bertino, Barbara Catania, and Elena Ferrari. A nested transaction model for multilevel secure database management systems. *ACM Transactions on Information and System Security*, 4(4):321–370, November 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bhargavan:2007:SSW

[BCFG07] Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, and Andrew D. Gordon. Secure sessions for Web services. *ACM Transactions on Information and System Security*, 10 (2):8:1–8:??, May 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bertino:2003:LFR

[BCFP03] Elisa Bertino, Barbara Catania, Elena Ferrari, and Paolo Perlasca. A logical framework for reasoning about access control models. *ACM Transactions on Information and System Security*, 6(1):71–127, February 2003.

CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bresson:2007:PSA

[BCP07] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably secure authenticated group Diffie–Hellman key exchange. *ACM Transactions on Information and System Security*, 10(3):10:1–10:??, July 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bergadano:1998:HDC

[BCR98] Francesco Bergadano, Bruno Crispo, and Giancarlo Ruffo. High dictionary compression for proactive password checking. *ACM Transactions on Information and System Security*, 1(1): 3–25, November 1998. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1998-1-1/p3-bergadano/`.

Bethea:2011:SSV

[BCR11] Darrell Bethea, Robert A. Cochran, and Michael K. Reiter. Server-side verification of client behavior in online games. *ACM Transactions on Information and System Security*, 14(4): 32:1–32:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Basin:2011:FRA

[BCSS11] David Basin, Srdjan Capkun, Patrick Schaller, and Benedikt Schmidt. Formal reasoning about physical properties of security protocols. *ACM Transactions on Information and System Security*, 14(2):16:1–16:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Burkhart:2011:PPD

[BD11] Martin Burkhart and Xenofontas Dimitropoulos. Privacy-preserving distributed network troubleshooting—bridging the gap between theory and practice. *ACM Transactions on Information and System Security*, 14(4): 31:1–31:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bertino:1998:EBI

[BDFS98] Elisa Bertino, Sabrina De Capitani Di Vimercati, Elena Ferrari, and Pierangela Samarati. Exception-based information flow control in object-oriented systems. *ACM Transactions on Information and System Security*, 1(1):26–65, November 1998. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1998-1-1/p26-bertino/`.

Bonatti:2002:ACA

[BDS02] Piero Bonatti, Sabrina De Capitani di Vimercati, and

Pierangela Samarati. An algebra for composing access control policies. *ACM Transactions on Information and System Security*, 5(1):1–35, February 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bertino:2002:SSD

[BF02] Elisa Bertino and Elena Ferrari. Secure and selective dissemination of XML documents. *ACM Transactions on Information and System Security*, 5(3): 290–331, August 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bertino:1999:SEA

[BFA99] Elisa Bertino, Elena Ferrari, and Vijay Atluri. The specification and enforcement of authorization constraints in workflow management systems. *ACM Transactions on Information and System Security*, 2(1):65–104, February 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1999-2-1/p65-bertino/`.

Bhargavan:2012:VCI

[BFCZ12] Karthikeyan Bhargavan, Cédric Fournet, Ricardo Corin, and Eugen Zalinescu. Verified cryptographic implementations for TLS. *ACM Transactions on Information and System Security*, 15(1):3:1–3:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bobba:2010:ABM

[BFK+10] Rakesh Bobba, Omid Fatemieh, Fariba Khan, Arindam Khan, Carl A. Gunter, Himanshu Khurana, and Manoj Prabhakaran. Attribute-based messaging: Access control and confidentiality. *ACM Transactions on Information and System Security*, 13(4): 31:1–31:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bhatti:2005:XGX

[BGBJ05] Rafae Bhatti, Arif Ghafoor, Elisa Bertino, and James B. D. Joshi. X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control. *ACM Transactions on Information and System Security*, 8 (2):187–227, May 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bernaschi:2002:RSE

[BGM02] Massimo Bernaschi, Emanuele Gabrielli, and Luigi V. Mancini. REMUS: a security-enhanced operating system. *ACM Transactions on Information and System Security*, 5(1):36–61, February 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Boldyreva:2008:NMS

[BGOY08] Alexandra Boldyreva, Craig Gentry, Adam O'Neill, and

Dae Hyun Yum. New multiparty signature schemes for network routing applications. *ACM Transactions on Information and System Security*, 12(1): 3:1–3:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bergadano:2002:UAT

[BGP02] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*, 5(4):367–397, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bauer:2011:DRP

[BGR11] Lujo Bauer, Scott Garriss, and Michael K. Reiter. Detecting and resolving policy misconfigurations in access-control systems. *ACM Transactions on Information and System Security*, 14(1):2:1–2:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bruns:2011:ACB

[BH11] Glenn Bruns and Michael Huth. Access control via Belnap logic: Intuitive, expressive, and analyzable policy composition. *ACM Transactions on Information and System Security*, 14 (1):9:1–9:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Blaze:2002:TMI

[BIK02] Matt Blaze, John Ioannidis, and Angelos D. Keromytis. Trust management for IPsec. *ACM Transactions on Information and System Security*, 5 (2):95–118, May 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Basin:2013:ESP

[BJKZ13] David Basin, Vincent Jugé, Felix Klaedtke, and Eugen Zalinescu. Enforceable security policies revisited. *ACM Transactions on Information and System Security*, 16(1):3:1–3:??, June 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Benhamouda:2016:NFP

[BJL16] Fabrice Benhamouda, Marc Joye, and BenoîT Libert. A new framework for privacy-preserving aggregation of time-series data. *ACM Transactions on Information and System Security*, 18(3):10:1–10:??, April 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bellare:2004:BPR

[BKN04] Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: a case study of the encode-then-encrypt-and-MAC paradigm. *ACM Transactions on Information and System Security*, 7(2):206–241, May 2004.

CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Biskup:2010:EE

[BL10] Joachim Biskup and Javier Lopez. Editorial: ESORICS 2007. *ACM Transactions on Information and System Security*, 13(3):19:1–19:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Burmester:2009:UCR

[BLDT09] Mike Burmester, Tri Van Le, Breno De Medeiros, and Gene Tsudik. Universally composable RFID identification and authentication protocols. *ACM Transactions on Information and System Security*, 12(4):21:1–21:??, April 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Burmester:2011:LRA

[BM11] Mike Burmester and Jorge Munilla. Lightweight RFID authentication with forward and backward security. *ACM Transactions on Information and System Security*, 14(1):11:1–11:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bisht:2010:CDC

[BMV10] Prithvi Bisht, P. Madhusudan, and V. N. Venkatakrishnan. CANDID: Dynamic candidate evaluations for automatic prevention of SQL injection attacks. *ACM Transactions on Information and System Security*, 13(2):14:1–14:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bacon:2002:MOR

[BMY02] Jean Bacon, Ken Moody, and Walt Yao. A model of OASIS role-based access control and its support for active security. *ACM Transactions on Information and System Security*, 5(4):492–540, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Becker:2010:LSM

[BN10] Moritz Y. Becker and Sebastian Nanz. A logic for state-modifying authorization policies. *ACM Transactions on Information and System Security*, 13 (3):20:1–20:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bouganim:2008:DAC

[BNP08] Luc Bouganim, François Dang Ngoc, and Philippe Pucheral. Dynamic access-control policies on XML encrypted data. *ACM Transactions on Information and System Security*, 10(4):4:1–4:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bella:2006:APF

[BP06] Giampaolo Bella and Lawrence C. Paulson. Accountability protocols: Formalized and verified. *ACM Transactions on In-*

formation and System Security, 9(2):138–161, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bohli:2011:RAP

[BP11] Jens-Matthias Bohli and Andreas Pashalidis. Relations among privacy notions. *ACM Transactions on Information and System Security*, 14(1): 4:1–4:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Barthe:2010:SMP

[BRRS10] Gilles Barthe, Tamara Rezk, Alejandro Russo, and Andrei Sabelfeld. Security of multithreaded programs by compilation. *ACM Transactions on Information and System Security*, 13(3):21:1–21:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Barker:2003:FAC

[BS03] Steve Barker and Peter J. Stuckey. Flexible access control policy specification with constraint logic programming. *ACM Transactions on Information and System Security*, 6(4): 501–546, November 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Brandt:2008:EUP

[BS08] Felix Brandt and Tuomas Sandholm. On the existence of unconditionally privacy-preserving auction protocols. *ACM Transactions on Information and System Security*, 11(2):6:1–6:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bhatti:2005:XGA

[BSB+05] Rafae Bhatti, Basit Shafiq, Elisa Bertino, Arif Ghafoor, and James B. D. Joshi. X-gtrbac admin: a decentralized administration model for enterprise-wide access control. *ACM Transactions on Information and System Security*, 8(4):388–423, November 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bilge:2014:EPD

[BSB+14] Leyla Bilge, Sevil Sen, Davide Balzarotti, Engin Kirda, and Christopher Kruegel. EXPOSURE: a passive DNS analysis service to detect and report malicious domains. *ACM Transactions on Information and System Security*, 16(4):14:1–14:??, April 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Barker:2008:SBA

[BSW08] Steve Barker, Marek J. Sergot, and Duminda Wijesekera. Status-based access control. *ACM Transactions on Information and System Security*, 12(1): 1:1–1:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bethencourt:2009:NTP

[BSW09] John Bethencourt, Dawn Song, and Brent Waters. New techniques for private stream searching. *ACM Transactions on Information and System Security*, 12(3):16:1–16:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Blanton:2013:SVO

[BZF13] Marina Blanton, Yihua Zhang, and Keith B. Frikken. Secure and verifiable outsourcing of large-scale biometric computations. *ACM Transactions on Information and System Security*, 16(3):11:1–11:??, November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cobb:2013:LMS

[CBL13] William E. Cobb, Rusty O. Baldwin, and Eric D. Laspe. Leakage mapping: a systematic methodology for assessing the side-channel information leakage of cryptographic implementations. *ACM Transactions on Information and System Security*, 16 (1):2:1–2:??, June 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cabuk:2009:ICC

[CBS09] Serdar Cabuk, Carla E. Brodley, and Clay Shields. IP covert channel detection. *ACM Transactions on Information and System Security*, 12(4):22:1–22:29, April 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chandramouli:2006:BPA

[CBSU06] R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, and R. N. Uma. Battery power-aware encryption. *ACM Transactions on Information and System Security*, 9(2):162–180, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chari:2003:BPD

[CC03] Suresh N. Chari and Pau-Chen Cheng. BlueBoX: a policy-driven, host-based intrusion detection system. *ACM Transactions on Information and System Security*, 6(2):173–200, May 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ceselli:2005:MAI

[CDD+05] Alberto Ceselli, Ernesto Damiani, Sabrina De Capitani Di Vimercati, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Modeling and assessing inference exposure in encrypted databases. *ACM Transactions on Information and System Security*, 8(1):119–152, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cheng:2013:DVB

[CDD13] Yueqiang Cheng, Xuhua Ding, and Robert H. Deng. Driver-

Guard: Virtualization-based fine-grained protection on I/O flows. *ACM Transactions on Information and System Security*, 16(2):6:1–6:??, September 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ciriani:2010:CFE

[CDF+10] Valentina Ciriani, Sabrina De Capitani Di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Combining fragmentation and encryption to protect privacy in data storage. *ACM Transactions on Information and System Security*, 13 (3):22:1–22:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Carminati:2010:FEA

[CFCT10] Barbara Carminati, Elena Ferrari, Jianneng Cao, and Kian Lee Tan. A framework to enforce access control over data streams. *ACM Transactions on Information and System Security*, 13 (3):28:1–28:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Carminati:2009:EAC

[CFP09] Barbara Carminati, Elena Ferrari, and Andrea Perego. Enforcing access control in Web-based social networks. *ACM Transactions on Information and System Security*, 13(1):6:1–6:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Camenisch:2012:EAA

[CG12] Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. *ACM Transactions on Information and System Security*, 15(1): 4:1–4:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Coull:2011:ACO

[CGH11] Scott E. Coull, Matthew Green, and Susan Hohenberger. Access controls for oblivious and anonymous systems. *ACM Transactions on Information and System Security*, 14(1):10:1–10:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cadar:2008:EAG

[CGP+08] Cristian Cadar, Vijay Ganesh, Peter M. Pawlowski, David L. Dill, and Dawson R. Engler. EXE: Automatically generating inputs of death. *ACM Transactions on Information and System Security*, 12(2):10:1–10:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Crampton:2013:PCK

[CGY13] Jason Crampton, Gregory Gutin, and Anders Yeo. On the parameterized complexity and kernelization of the workflow satisfiability problem. *ACM Transactions on*

Information and System Security, 16(1):4:1–4:??, June 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cheon:2008:PST

[CHKO08] Jung Hee Cheon, Nicholas Hopper, Yongdae Kim, and Ivan Osipkov. Provably Secure Timed-Release Public Key Encryption. *ACM Transactions on Information and System Security*, 11 (2):4:1–4:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Crampton:2003:ASF

[CL03] Jason Crampton and George Loizou. Administrative scope: a foundation for role-based administrative models. *ACM Transactions on Information and System Security*, 6(2):201–231, May 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chen:2014:CDP

[CLY14] Liqun Chen, Hoon Wei Lim, and Guomin Yang. Cross-domain password-based authenticated key exchange revisited. *ACM Transactions on Information and System Security*, 16(4): 15:1–15:??, April 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Crampton:2011:PEC

[Cra11] Jason Crampton. Practical and efficient cryptographic enforcement of interval-based access control policies. *ACM Transactions on Information and System Security*, 14(1):14:1–14:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Culnane:2015:VVV

[CRST15] Chris Culnane, Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague. vVote: a verifiable voting system. *ACM Transactions on Information and System Security*, 18(1):3:1–3:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cramer:2000:SSB

[CS00] Ronald Cramer and Victor Shoup. Signature schemes based on the strong RSA assumption. *ACM Transactions on Information and System Security*, 3(3): 161–185, August 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Carrier:2004:STP

[CS04] Brian Carrier and Clay Shields. The session token protocol for forensics and traceback. *ACM Transactions on Information and System Security*, 7(3):333–362, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chang:2008:DAP

[CS08] Katharine Chang and Kang G. Shin. Distributed authentication of program integrity verification in wireless sensor networks.

ACM Transactions on Information and System Security, 11(3): 14:1–14:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chapin:2014:SRP

[CS14] Peter Chapin and Christian Skalka. SpartanRPC: Remote procedure call authorization in wireless sensor networks. *ACM Transactions on Information and System Security*, 17(2):5:1–5:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chen:2014:APS

[CSDM14] Teh-Chung Chen, Torin Stepan, Scott Dick, and James Miller. An anti-phishing system employing diffused information. *ACM Transactions on Information and System Security*, 16(4): 16:1–16:??, April 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chan:2011:PCR

[CSS11] T.-H. Hubert Chan, Elaine Shi, and Dawn Song. Private and continual release of statistics. *ACM Transactions on Information and System Security*, 14(3): 26:1–26:??, November 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chan-Tin:2011:FBA

[CTHHK11] Eric Chan-Tin, Victor Heorhiadi, Nicholas Hopper, and Yongdae Kim. The Frog-Boiling attack: Limitations of secure network coordinate systems. *ACM Transactions on Information and System Security*, 14(3):27:1–27:??, November 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chong:2015:UAR

[CV15] Stephen Chong and Ron Van Der Meyden. Using architecture to reason about information security. *ACM Transactions on Information and System Security*, 18(2):8:1–8:??, December 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Crosby:2011:ADR

[CW11] Scott A. Crosby and Dan S. Wallach. Authenticated dictionaries: Real-world costs and trade-offs. *ACM Transactions on Information and System Security*, 14 (2):17:1–17:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chang:2001:RTP

[CWJ01] Ho-Yen Chang, S. Felix Wu, and Y. Frank Jou. Real-time protocol analysis for detecting link-state routing protocol attacks. *ACM Transactions on Information and System Security*, 4(1):1–36, February 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Crosby:2009:OLR

[CWR09] Scott A. Crosby, Dan S. Wallach, and Rudolf H. Riedi. Opportunities and limits of remote timing attacks. *ACM Transactions on Information and System Security*, 12(3):17:1–17:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chakrabarti:2008:ETR

[CWW+08] Deepayan Chakrabarti, Yang Wang, Chenxi Wang, Jurij Leskovec, and Christos Faloutsos. Epidemic thresholds in real networks. *ACM Transactions on Information and System Security*, 10(4):1:1–1:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Damiani:2007:GRS

[DBCP07] Maria Luisa Damiani, Elisa Bertino, Barbara Catania, and Paolo Perlasca. GEO-RBAC: a spatially aware RBAC. *ACM Transactions on Information and System Security*, 10(1):2:1–2:??, February 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dojen:2005:CLP

[DC05] Reiner Dojen and Tom Coffey. The concept of layered proving trees and its application to the automation of security protocol verification. *ACM Transactions on Information and System Security*, 8(3):287–311, August 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

diVimercati:2010:GES

[dCdVS10] Sabrina de Capitani di Vimercati and Paul Syverson. Guest editorial: Special issue on computer and communications security. *ACM Transactions on Information and System Security*, 13(2):11:1–11:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Danev:2012:TPI

[DCMB12] Boris Danev, Srdjan Capkun, Ramya Jayaram Masti, and Thomas S. Benjamin. Towards practical identification of HF RFID devices. *ACM Transactions on Information and System Security*, 15(2):7:1–7:??, July 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dong:2011:PDA

[DCNR11] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru. Practical defenses against pollution attacks in wireless network coding. *ACM Transactions on Information and System Security*, 14(1):7:1–7:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Du:2005:PKP

[DDH+05] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram

Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security*, 8(2):228–258, May 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Danner:2012:EDD

[DDKKL12] Norman Danner, Sam Defabbia-Kane, Danny Krizanc, and Marc Liberatore. Effectiveness and detection of denial-of-service attacks in Tor. *ACM Transactions on Information and System Security*, 15(3):11:1–11:??, November 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Damiani:2002:FGA

[DDPS02] Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati. A fine-grained access control system for XML documents. *ACM Transactions on Information and System Security*, 5(2):169–202, May 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Demsky:2011:CAD

[Dem11] Brian Demsky. Cross-application data provenance and policy enforcement. *ACM Transactions on Information and System Security*, 14(1):6:1–6:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ding:2015:VED

[DFD15] Steven H. H. Ding, Benjamin C. M. Fung, and Mourad Debbabi. A visualizable evidence-driven approach for authorship attribution. *ACM Transactions on Information and System Security*, 17(3):12:1–12:??, March 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dean:2002:AAI

[DFS02] Drew Dean, Matt Franklin, and Adam Stubblefield. An algebraic approach to IP traceback. *ACM Transactions on Information and System Security*, 5(2):119–137, May 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dorrendorf:2009:CRN

[DGP09] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. *ACM Transactions on Information and System Security*, 13(1):10:1–10:32, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Driessen:2013:ESA

[DHW+13] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. An experimental security analysis of two satphone standards. *ACM Transactions on Information and System Security*, 16(3):10:1–

10:??, November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Doychev:2015:CTS

[DKMR15] Goran Doychev, Boris Köpf, Laurent Mauborgne, and Jan Reineke. CacheAudit: a tool for the static analysis of cache side channels. *ACM Transactions on Information and System Security*, 18(1):4:1–4:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

DeCarneDeCarnavalet:2015:LSE

[DM15] Xavier De Carné De Carnavalet and Mohammad Mannan. A large-scale evaluation of high-impact password strength meters. *ACM Transactions on Information and System Security*, 18(1):1:1–1:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

DiPietro:2008:RSN

[DMM+08] Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, Alessandro Panconesi, and Jaikumar Radhakrishnan. Redoubtable sensor networks. *ACM Transactions on Information and System Security*, 11(3):13:1–13:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dolev:2000:XTE

[DO00] Shlomi Dolev and Rafail Ostrovsky. Xor-trees for efficient anonymous multicast and reception. *ACM Transactions on Information and System Security*, 3(2):63–84, May 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Pietro:2015:SGE

[DO15] Roberto Di Pietro and Gabriele Oligeri. Silence is golden: Exploiting jamming and radio silence to communicate. *ACM Transactions on Information and System Security*, 17(3): 9:1–9:??, March 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ellison:2003:PKS

[ED03] Carl Ellison and Steve Dohrmann. Public-key support for group collaboration. *ACM Transactions on Information and System Security*, 6(4):547–565, November 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Erway:2015:DPD

[EKPT15] C. Chris Erway, Alptekin Küpçü, Charalampos Papamanthou, and Roberto Tamassia. Dynamic provable data possession. *ACM Transactions on Information and System Security*, 17(4): 15:1–15:??, April 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Etalle:2009:MCW

[EW09] Sandro Etalle and William H. Winsborough. Maintaining control while delegating trust: Integrity constraints in trust management. *ACM Transactions on Information and System Security*, 13(1):5:1–5:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Frank:2013:RMP

[FBB13] Mario Frank, Joachim M. Buhman, and David Basin. Role mining with probabilistic models. *ACM Transactions on Information and System Security*, 15 (4):15:1–15:??, April 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ferraiolo:1999:RBA

[FBK99] David F. Ferraiolo, John F. Barkley, and D. Richard Kuhn. A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and System Security*, 2(1):34–64, February 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1999-2-1/p34-ferraiolo/`.

Ferrari:2005:GES

[Fer05] Elena Ferrari. Guest editorial: Special issue on access control models and technologies. *ACM Transactions on Information and System Security*, 8(4): 349–350, November 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Feigenbaum:2012:PAO

[FJS12] Joan Feigenbaum, Aaron Johnson, and Paul Syverson. Probabilistic analysis of onion routing in a black-box model. *ACM Transactions on Information and System Security*, 15(3):14:1–14:??, November 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Futoransky:2006:FAS

[FKSW06] Ariel Futoransky, Emiliano Kargieman, Carlos Sarraute, and Ariel Waissbein. Foundations and applications for secure triggers. *ACM Transactions on Information and System Security*, 9(1):94–112, February 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Fu:2013:BSG

[FL13] Yangchun Fu and Zhiqiang Lin. Bridging the semantic gap in virtual machine introspection via online kernel data redirection. *ACM Transactions on Information and System Security*, 16(2): 7:1–7:??, September 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Frincke:2000:BCR

[Fri00] Deborah Frincke. Balancing cooperation and risk in intrusion detection. *ACM Transactions on Information and System Security*, 3(1):1–29, February 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ferraiolo:2001:PNS

[FSG+01] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, August 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gorantla:2011:MKC

[GBNM11] M. C. Gorantla, Colin Boyd, Juan Manuel González Nieto, and Mark Manulis. Modeling key compromise impersonation attacks on group key exchange protocols. *ACM Transactions on Information and System Security*, 14(4):28:1–28:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gabber:1999:SPC

[GGK+99] Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, and Alain Mayer. On secure and pseudonymous client-relationships with multiple servers. *ACM Transactions on Information and System Security*, 2(4):390–415, November 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-4/p390-gabber/`.

Gilad:2012:LDA

[GH12] Yossi Gilad and Amir Herzberg. LOT: a defense against IP spoofing and flooding attacks. *ACM Transactions on Information and System Security*, 15(2):6:1–6:??, July 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gilad:2013:FCV

[GH13] Yossi Gilad and Amir Herzberg. Fragmentation considered vulnerable. *ACM Transactions on Information and System Security*, 15(4):16:1–16:??, April 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gilad:2014:PTI

[GH14] Yossi Gilad and Amir Herzberg. Off-path TCP injection attacks. *ACM Transactions on Information and System Security*, 16(4):13:1–13:??, April 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gordon:2002:EIS

[GL02] Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gennaro:2006:FPB

[GL06] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. *ACM Transactions on Information and System Security*, 9(2):181–234, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gotzfried:2014:MAT

[GM14] Johannes Götzfried and Tilo Müller. Mutual authentication and trust bootstrapping towards secure disk encryption. *ACM Transactions on Information and System Security*, 17(2): 6:1–6:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Golle:2008:DCS

[GMM08] Philippe Golle, Frank McSherry, and Ilya Mironov. Data collection with self-enforcing privacy. *ACM Transactions on Information and System Security*, 12(2): 9:1–9:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gunetti:2005:KAF

[GP05] Daniele Gunetti and Claudia Picardi. Keystroke analysis of free text. *ACM Transactions on Information and System Security*, 8(3):312–347, August 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ganeriwal:2008:STS

[GPČS08] Saurabh Ganeriwal, Christina Pöpper, Srdjan Čapkun, and Mani B. Srivastava. Secure time synchronization in sensor networks. *ACM Transactions on Information and System Security*, 11(4):23:1–23:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gassend:2008:CPR

[GVC+08] Blaise Gassend, Marten Van Dijk, Dwaine Clarke, Emina Torlak, Srinivas Devadas, and Pim Tuyls. Controlled physical random functions and applications. *ACM Transactions on Information and System Security*, 10(4): 3:1–3:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Hess:2004:CTT

[HHJS04] Adam Hess, Jason Holt, Jared Jacobson, and Kent E. Seamons. Content-triggered trust negotiation. *ACM Transactions on Information and System Security*, 7(3):428–456, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Halevi:1999:PKC

[HK99a] Shai Halevi and Hugo Krawczyk. Public-key cryptography and password protocols. *ACM Transactions on Information and System Security*, 2(3):230–268, August 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-3/p230-halevi/`.

Hevia:1999:STD

[HK99b] Alejandro Hevia and Marcos Kiwi. Strength of two Data Encryption Standard implementations under timing attack. *ACM Transactions on Information and System Security*, 2(4):416–437, November 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-4/p416-hevia/`.

Harbitter:2002:MAP

[HM02] Alan Harbitter and Daniel A. Menascé. A methodology for analyzing the performance of authentication protocols. *ACM Transactions on Information and System Security*, 5(4):458–491, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Huang:2004:KCB

[HM04] Dijiang Huang and Deep Medhi. A key-chain-based keying scheme for many-to-many secure group communication. *ACM Transactions on Information and System Security*, 7(4):523–552, November 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Halpern:2008:SMS

[HO08] Joseph Y. Halpern and Kevin R. O'Neill. Secrecy in multiagent systems. *ACM Transactions on Information and System Security*, 12(1):5:1–5:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Halpern:2003:RBS

[HP03] Joseph Y. Halpern and Riccardo Pucella. On the relationship between strand spaces and multi-agent systems. *ACM Transactions on Information and System Security*, 6(1):43–70, February 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Hicks:2010:LSA

[HRS+10] Boniface Hicks, Sandra Rueda, Luke St. Clair, Trent Jaeger, and Patrick McDaniel. A logical specification and analysis for SELinux MLS policy. *ACM Transactions on Information and System Security*, 13 (3):26:1–26:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Hengartner:2005:ACP

[HS05] Urs Hengartner and Peter Steenkiste. Access control to people location information. *ACM Transactions on Information and System Security*, 8(4): 424–456, November 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Hopper:2010:HMA

[HVCT10] Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-TIN. How much anonymity does network latency leak? *ACM*

Transactions on Information and System Security, 13(2):13:1–13:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Halpern:2008:UFO

[HW08] Joseph Y. Halpern and Vicky Weissman. Using first-order logic to reason about policies. *ACM Transactions on Information and System Security*, 11 (4):21:1–21:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Iwaihara:2007:RBA

[IHC+07] Mizuho Iwaihara, Ryotaro Hayashi, Somchai Chatvichienchai, Chutiporn Anutariya, and Vilas Wuwongse. Relevancy-based access control and its evaluation on versioned XML documents. *ACM Transactions on Information and System Security*, 10(1): 3:1–3:??, February 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Joshi:2008:FFH

[JBGZ08] James B. D. Joshi, Elisa Bertino, Arif Ghafoor, and Yue Zhang. Formal foundations for hybrid hierarchies in GTRBAC. *ACM Transactions on Information and System Security*, 10(4): 2:1–2:??, January 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Joshi:2011:GES

[JC11] James Joshi and Barbara Carminati. Guest editorial: SACMAT 2009 and 2010. *ACM Transactions on Information and System Security*, 14(3):22:1–22:??, November 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Jaeger:2004:CAA

[JEZ04] Trent Jaeger, Antony Edwards, and Xiaolan Zhang. Consistency analysis of authorization hook placement in the Linux security modules framework. *ACM Transactions on Information and System Security*, 7(2):175–205, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ji:2016:GGD

[JLS+16] Shouling Ji, Weiqing Li, Mudhakar Srivatsa, Jing Selena He, and Raheem Beyah. General graph data de-anonymization: From mobility traces to social networks. *ACM Transactions on Information and System Security*, 18(4):12:1–12:??, May 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Jaeger:1999:FCD

[JPLI99] Trent Jaeger, Atul Prakash, Jochen Liedtke, and Nayeem Islam. Flexible control of downloaded executable content. *ACM Transactions on Information and System Security*, 2(2):177–228, May 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://`

www.acm.org/pubs/citations/journals/tissec/1999-2-2/p177-jaeger/.

Jafari:2014:FEE

[JSNFB14] Mohammad Jafari, Reihaneh Safavi-Naini, Philip W. L. Fong, and Ken Barker. A framework for expressing and enforcing purpose-based privacy policies. *ACM Transactions on Information and System Security*, 17 (1):3:1–3:??, August 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Jaeger:2001:PSF

[JT01] Trent Jaeger and Jonathon E. Tidswell. Practical safety in flexible access control models. *ACM Transactions on Information and System Security*, 4 (2):158–190, May 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Jayaraman:2013:MAR

[JTG+13] Karthick Jayaraman, Mahesh Tripunitara, Vijay Ganesh, Martin Rinard, and Steve Chapin. Mohawk: Abstraction-refinement and bound-estimation for verifying access control policies. *ACM Transactions on Information and System Security*, 15(4):18:1–18:??, April 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Julisch:2003:CID

[Jul03] Klaus Julisch. Clustering intrusion detection alarms to support root cause analysis. *ACM Transactions on Information and System Security*, 6(4):443–471, November 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Juels:2009:DSP

[JW09] Ari Juels and Stephen A. Weis. Defining strong privacy for RFID. *ACM Transactions on Information and System Security*, 13(1):7:1–7:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Jiang:2010:SMD

[JWX10] Xuxian Jiang, Xinyuan Wang, and Dongyan Xu. Stealthy malware detection and monitoring through VMM-based “out-of-the-box” semantic view reconstruction. *ACM Transactions on Information and System Security*, 13(2):12:1–12:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Jaeger:2003:PMU

[JZC03] Trent Jaeger, Xiaolan Zhang, and Fidel Cacheda. Policy management using access control spaces. *ACM Transactions on Information and System Security*, 6(3):327–364, August 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kaliski:2001:UKS

[Kal01] Burton S. Kaliski. An unknown key-share attack on the MQV key agreement protocol. *ACM Transactions on Information and System Security*, 4(3): 275–288, August 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Karjoth:2003:ACI

[Kar03] Günter Karjoth. Access control with IBM Tivoli access manager. *ACM Transactions on Information and System Security*, 6(2):232–257, May 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Karame:2015:MBS

[KAR+15] Ghassan O. Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Capkun. Misbehavior in bitcoin: a study of double-spending and accountability. *ACM Transactions on Information and System Security*, 18(1):2:1–2:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kihlstrom:2001:SGC

[KMMS01] Kim Potter Kihlstrom, L. E. Moser, and P. M. Melliar-Smith. The securering group communication system. *ACM Transactions on Information and System Security*, 4(4):371–406, November 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Koch:2002:GBF

[KMPP02] Manuel Koch, Luigi V. Mancini, and Francesco Parisi-Presicce. A graph-based formalism for RBAC. *ACM Transactions on Information and System Security*, 5(3):332–365, August 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Krishnan:2011:GCS

[KNSW11] Ram Krishnan, Jianwei Niu, Ravi Sandhu, and William H. Winsborough. Group-centric secure information-sharing models for isolated groups. *ACM Transactions on Information and System Security*, 14(3):23:1–23:??, November 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kim:2004:TBG

[KPT04] Yongdae Kim, Adrian Perrig, and Gene Tsudik. Tree-based group key agreement. *ACM Transactions on Information and System Security*, 7(1): 60–96, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kogan:2006:PRS

[KSW06] Noam Kogan, Yuval Shavitt, and Avishai Wool. A practical revocation scheme for broadcast encryption using smartcards. *ACM Transactions on Information and System Security*, 9(3):325–351, August 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kogan:2006:IER

[KT06] Noam Kogan and Tamir Tassa. Improved efficiency for revocation schemes via Newton interpolation. *ACM Transactions on Information and System Security*, 9(4):461–486, November 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Khoury:2012:CEN

[KT12] Raphaël Khoury and Nadia Tawbi. Corrective enforcement: a new paradigm of security policy enforcement by monitors. *ACM Transactions on Information and System Security*, 15 (2):10:1–10:??, July 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kate:2010:PBO

[KZG10] Aniket Kate, Greg M. Zaverucha, and Ian Goldberg. Pairing-based onion routing with improved forward secrecy. *ACM Transactions on Information and System Security*, 13(4):29:1–29:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lane:1999:TSL

[LB99] Terran Lane and Carla E. Brodley. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions on Information and System Security*, 2(3):295–331, August 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-3/p295-lane/`.

Leighton:2011:ACP

[LB11] Gregory Leighton and Denilson Barbosa. Access control policy translation, verification, and minimization within heterogeneous data federations. *ACM Transactions on Information and System Security*, 14(3): 25:1–25:??, November 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ligatti:2009:RTE

[LBW09] Jay Ligatti, Lujo Bauer, and David Walker. Run-time enforcement of nonsafety policies. *ACM Transactions on Information and System Security*, 12(3): 19:1–19:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Levi:2004:UNC

[LCK04] Albert Levi, M. Ufuk Caglayan, and Cetin K. Koc. Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. *ACM Transactions on Information and System Security*, 7(1):21–59, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2011:TRP

[LDLM11] Yingjiu Li, Robert H. Deng, Junzuo Lai, and Changshe Ma. On two RFID privacy notions and their relations. *ACM Transactions on Information and System Security*, 14(4):30:1–30:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2003:DLL

[LGF03] Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum. Delegation logic: a logic-based approach to distributed authorization. *ACM Transactions on Information and System Security*, 6(1):128–171, February 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2014:SCA

[LGR14] Peng Li, Debin Gao, and Michael K. Reiter. StopWatch: a cloud architecture for timing channel mitigation. *ACM Transactions on Information and System Security*, 17(2):8:1–8:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2010:AIS

[LHKR10] Feifei Li, Marios Hadjieleftheriou, George Kollios, and Leonid Reyzin. Authenticated index structures for aggregation queries. *ACM Transactions on Information and System Security*, 13(4):32:1–32:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Leonard:2013:MAP

[LHMS13] Thomas Leonard, Martin Hall-May, and Mike Surridge. Modelling access propagation in dynamic systems. *ACM Transactions on Information and System Security*, 16(2):5:1–5:??, September 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2011:ISS

[Li11] Ninghui Li. Introduction to special section SACMAT'08. *ACM Transactions on Information and System Security*, 14 (1):1:1–1:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2009:ATN

[LLW09] Jiangtao Li, Ninghui Li, and William H. Winsborough. Automated trust negotiation using cryptographic credentials. *ACM Transactions on Information and System Security*, 13(1): 2:1–2:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2010:CDP

[LMW10] Adam J. Lee, Kazuhiro Minami, and Marianne Winslett. On the consistency of distributed proofs with hidden subtrees. *ACM Transactions on Information and System Security*, 13 (3):25:1–25:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Liu:2005:EPK

[LNL05] Donggang Liu, Peng Ning, and Rongfang Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security*, 8(1):41–77, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Liu:2008:ARL

[LNL+08] Donggang Liu, Peng Ning, An Liu, Cliff Wang, and Wenliang Kevin Du. Attack-resistant location estimation in wireless sensor networks. *ACM Transactions on Information and System Security*, 11(4):22:1–22:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Liu:2011:FDI

[LNR11] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 14 (1):13:1–13:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Libert:2010:KES

[LQY10] Benoît Libert, Jean-Jacques Quisquater, and Moti Yung. Key evolution systems in untrusted update environments. *ACM Transactions on Information and System Security*, 13(4): 37:1–37:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2000:FCF

[LS00] Wenke Lee and Salvatore J. Stolfo. A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security*, 3(4): 227–261, November 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2008:CPK

[LS08] Jooyoung Lee and Douglas R. Stinson. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. *ACM Transactions on Information and System Security*, 11(2):1:1–1:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2015:GAP

[LSF+15] Hyojeong Lee, Jeff Seibert, Dylan Fistrovic, Charles Killian, and Cristina Nita-Rotaru. Gatling: Automatic performance attack discovery in large-scale distributed systems. *ACM Transactions on Information and System Security*, 17(4): 13:1–13:??, April 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Liang:2009:AIE

[LSVS09] Zhenkai Liang, Weiqing Sun, V. N. Venkatakrishnan, and

R. Sekar. Alcatraz: An isolated environment for experimenting with untrusted software. *ACM Transactions on Information and System Security*, 12(3):14:1–14:37, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2006:SAR

[LT06] Ninghui Li and Mahesh V. Tripunitara. Security analysis in role-based access control. *ACM Transactions on Information and System Security*, 9(4): 391–420, November 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2007:MER

[LTB07] Ninghui Li, Mahesh V. Tripunitara, and Ziad Bizri. On mutually exclusive roles and separation-of-duty. *ACM Transactions on Information and System Security*, 10(2):5:1–5:??, May 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lysyanskaya:2010:AEC

[LTT10] Anna Lysyanskaya, Roberto Tamassia, and Nikos Triandopoulos. Authenticated error-correcting codes with applications to multicast authentication. *ACM Transactions on Information and System Security*, 13(2):17:1–17:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Loughry:2002:ILO

[LU02] Joe Loughry and David A. Umphress. Information leakage from optical emanations. *ACM Transactions on Information and System Security*, 5(3): 262–289, August 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2008:ESC

[LW08] Adam J. Lee and Marianne Winslett. Enforcing safety and consistency constraints in policy-based authorization systems. *ACM Transactions on Information and System Security*, 12(2): 8:1–8:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lee:2008:TAS

[LWBW08] Adam J. Lee, Marianne Winslett, Jim Basney, and Von Welch. The Traust Authorization Service. *ACM Transactions on Information and System Security*, 11(1):2:1–2:??, February 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2009:RPA

[LWT09] Ninghui Li, Qihua Wang, and Mahesh Tripunitara. Resiliency policies in access control. *ACM Transactions on Information and System Security*, 12(4): 20:1–20:??, April 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Liu:2005:IBM

[LZY05] Peng Liu, Wanyu Zang, and Meng Yu. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security*, 8(1): 78–118, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mittal:2012:ILS

[MB12] Prateek Mittal and Nikita Borisov. Information leaks in structured peer-to-peer anonymous communication systems. *ACM Transactions on Information and System Security*, 15 (1):5:1–5:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mano:2008:RRI

[MBL+08] Chad D. Mano, Andrew Blaich, Qi Liao, Yingxin Jiang, David A. Cieslak, David C. Salyers, and Aaron Striegel. RIPPS: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning. *ACM Transactions on Information and System Security*, 11(2): 2:1–2:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Montenegro:2004:CBI

[MC04] Gabriel Montenegro and Claude Castelluccia. Crypto-based identifiers (CBIDs): Concepts and applications. *ACM Transactions on Information and System Security*, 7(1):97–127, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

McHugh:2000:TID

[McH00] John McHugh. Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory. *ACM Transactions on Information and System Security*, 3(4):262–294, November 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Molloy:2010:MRM

[MCL+10] Ian Molloy, Hong Chen, Tiancheng Li, Qihua Wang, Ninghui Li, Elisa Bertino, Seraphin Calo, and Jorge Lobo. Mining roles with multiple objectives. *ACM Transactions on Information and System Security*, 13(4):36:1–36:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mazzoleni:2008:XPI

[MCSB08] Pietro Mazzoleni, Bruno Crispo, Swaminathan Sivasubramanian, and Elisa Bertino. XACML Policy Integration Algorithms. *ACM Transactions on Information and System Security*, 11(1): 4:1–4:??, February 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Marinovic:2014:RIB

[MDS14] Srdjan Marinovic, Naranker Dulay, and Morris Sloman. Rumpole: an introspective break-glass access control language. *ACM Transactions on Information and System Security*, 17(1):2:1–2:??, August 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Meadows:2009:IAT

[Mea09] Catherine Meadows. Introduction to ACM TISSEC special issue on CCS 2005. *ACM Transactions on Information and System Security*, 13(1):1:1–1:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mella:2006:CCU

[MFBK06] Giovanni Mella, Elena Ferrari, Elisa Bertino, and Yunhua Koglin. Controlled and cooperative updates of XML documents in Byzantine and failure-prone distributed systems. *ACM Transactions on Information and System Security*, 9(4):421–460, November 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Michael:2002:SSB

[MG02] C. C. Michael and Anup Ghosh. Simple, state-based approaches to program-based anomaly detection. *ACM Transactions on Information and System Security*, 5(3):203–237, August 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mao:2011:CDP

[MLCJ11] Ziqing Mao, Ninghui Li, Hong Chen, and Xuxian Jiang. Combining discretionary policy with mandatory information flow in operating systems. *ACM Transactions on Information and System Security*, 14(3):24:1–24:??, November 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Malvestuto:2006:ASQ

[MMM06] Francesco M. Malvestuto, Mauro Mezzini, and Marina Moscarini. Auditing sum-queries to make a statistical database secure. *ACM Transactions on Information and System Security*, 9(1): 31–60, February 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Moran:2010:SBV

[MN10] Tal Moran and Moni Naor. Split-ballot voting: Everlasting privacy with distributed trust. *ACM Transactions on Information and System Security*, 13(2): 16:1–16:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Molva:2000:SMS

[MP00] Refik Molva and Alain Pannetrat. Scalable multicast security with dynamic recipient groups. *ACM Transactions on*

Information and System Security, 3(3):136–160, August 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

McDaniel:2006:MLS

[MP06] Patrick McDaniel and Atul Prakash. Methods and limitations of security policy reconciliation. *ACM Transactions on Information and System Security*, 9(3):259–291, August 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mukhamedov:2010:IEP

[MR10] Aybek Mukhamedov and Mark D. Ryan. Identity escrow protocol and anonymity analysis in the applied pi-calculus. *ACM Transactions on Information and System Security*, 13(4):41:1–41:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Murata:2006:XAC

[MTKH06] Makoto Murata, Akihiko Tozawa, Michiharu Kudo, and Satoshi Hada. XML access control using static analysis. *ACM Transactions on Information and System Security*, 9(3):292–324, August 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Mutz:2006:ASC

[MVVK06] Darren Mutz, Fredrik Valeur, Giovanni Vigna, and Christopher Kruegel. Anomalous system call detection. *ACM Transactions on Information and System Security*, 9(1):61–93, February 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ni:2010:PAR

[NBL+10] Qun Ni, Elisa Bertino, Jorge Lobo, Carolyn Brodie, Clare-Marie Karat, John Karat, and Alberto Trombeta. Privacy-aware role-based access control. *ACM Transactions on Information and System Security*, 13 (3):24:1–24:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ning:2004:TTA

[NCRX04] Peng Ning, Yun Cui, Douglas S. Reeves, and Dingbang Xu. Techniques and tools for analyzing intrusion alerts. *ACM Transactions on Information and System Security*, 7 (2):274–318, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ning:2001:ABI

[NJW01] Peng Ning, Sushil Jajodia, and Xiaoyang Sean Wang. Abstraction-based intrusion detection in distributed environments. *ACM Transactions on Information and System Security*, 4(4):407–452, November 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Nyanchama:1999:RGM

[NO99] Matunda Nyanchama and Sylvia Osborn. The role graph model and conflict of interest. *ACM Transactions on Information and System Security*, 2 (1):3–33, February 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1999-2-1/p3-nyanchama/`.

Ning:2004:HRA

[NX04] Peng Ning and Dingbang Xu. Hypothesizing and reasoning about attacks missed by intrusion detection systems. *ACM Transactions on Information and System Security*, 7(4):591–627, November 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Oligeri:2011:REA

[OCDG11] Gabriele Oligeri, Stefano Chessa, Roberto Di Pietro, and Gaetano Giunta. Robust and efficient authentication of video stream broadcasting. *ACM Transactions on Information and System Security*, 14(1):5:1–5:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Oren:2015:AIU

[OK15] Yossef Oren and Angelos D. Keromytis. Attacking the Internet using broadcast digital television. *ACM Transactions on Information and System Security*, 17(4):16:1–16:??, April 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Osborn:2000:CRB

[OSM00] Sylvia Osborn, Ravi Sandhu, and Qamar Munawer. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security*, 3(2):85–106, May 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Oh:2006:ERA

[OSZ06] Sejong Oh, Ravi Sandhu, and Xinwen Zhang. An effective role administration model using organization structure. *ACM Transactions on Information and System Security*, 9 (2):113–137, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Paulson:1999:IAI

[Pau99] Lawrence C. Paulson. Inductive analysis of the Internet protocol TLS. *ACM Transactions on Information and System Security*, 2(3):332–351, August 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-3/p332-paulson/`.

Peng:2007:BZK

[PBD07] Kun Peng, Colin Boyd, and Ed Dawson. Batch zero-knowledge proof and verification and its applications. *ACM Transactions on Information and System Security*, 10(2): 6:1–6:??, May 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Park:2003:EMS

[PCS03] Jung Min Park, Edwin K. P. Chong, and Howard Jay Siegel. Efficient multicast stream authentication using erasure codes. *ACM Transactions on Information and System Security*, 6 (2):258–285, May 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Pennington:2010:SBI

[PGB+10] Adam G. Pennington, John Linwood Griffin, John S. Bucy, John D. Strunk, and Gregory R. Ganger. Storage-based intrusion detection. *ACM Transactions on Information and System Security*, 13(4):30:1–30:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ponec:2010:NPA

[PGWB10] Miroslav Ponec, Paul Giura, Joel Wein, and Hervé Brönnimann. New payload attribution methods for network forensic investigations. *ACM Transactions on Information and System Security*, 13(2):15:1–15:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Park:2004:UUC

[PS04] Jaehong Park and Ravi Sandhu. The UCON_{ABC} usage control model. *ACM Transactions on Information and System Security*, 7(1):128–174, February 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Park:2001:RBA

[PSA01] Joon S. Park, Ravi Sandhu, and Gail-Joon Ahn. Role-based access control on the Web. *ACM Transactions on Information and System Security*, 4(1): 37–71, February 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Pang:2008:VCR

[PT08] Hweehwa Pang and Kian-Lee Tan. Verifying completeness of relational query answers from online servers. *ACM Transactions on Information and System Security*, 11(2):5:1–5:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Persiano:2003:SPS

[PV03] Pino Persiano and Ivan Visconti. A secure and private system for subscription-based remote services. *ACM Transactions on Information and System Security*, 6(4):472–500, November 2003. CODEN ATISBQ.

ISSN 1094-9224 (print), 1557-7406 (electronic).

Philippaerts:2013:CMC

[PYM+13] Pieter Philippaerts, Yves Younan, Stijn Muylle, Frank Piessens, Sven Lachmund, and Thomas Walter. CPM: Masking code pointers to prevent code injection attacks. *ACM Transactions on Information and System Security*, 16(1):1:1–1:??, June 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ray:2008:E

[Ray08] Indrakshi Ray. Editorial. *ACM Transactions on Information and System Security*, 11(1):1:1–1:??, February 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Rogaway:2003:OBC

[RBB03] Phillip Rogaway, Mihir Bellare, and John Black. OCB: a block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security*, 6(3):365–403, August 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Rodeh:2001:APS

[RBD01] Ohad Rodeh, Kenneth P. Birman, and Danny Dolev. The architecture and performance of security protocols in the Ensemble Group Communication System: Using diamonds to guard the castle. *ACM Transactions on Information and System Security*, 4(3):289–319, August 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Rupp:2015:CTM

[RBHP15] Andy Rupp, Foteini Baldimtsi, Gesine Hinterwälder, and Christof Paar. Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport. *ACM Transactions on Information and System Security*, 17(3):10:1–10:??, March 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Roemer:2012:ROP

[RBSS12] Ryan Roemer, Erik Buchanan, Hovav Shacham, and Stefan Savage. Return-oriented programming: Systems, languages, and applications. *ACM Transactions on Information and System Security*, 15(1):2:1–2:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Radosavac:2008:AFM

[RMBK08] Svetlana Radosavac, George Moustakides, John S. Baras, and Iordanis Koutsopoulos. An analytic framework for modeling and detecting access layer misbehavior in wireless networks. *ACM Transactions on Information and System Security*, 11(4):19:1–19:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Reiter:1998:CAW

[RR98] Michael K. Reiter and Aviel D. Rubin. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, November 1998. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1998-1-1/p66-reiter/`.

Ryu:2008:EID

[RR08] Young U. Ryu and Hyeun-Suk Rhee. Evaluation of intrusion detection systems under a resource constraint. *ACM Transactions on Information and System Security*, 11(4):20:1–20:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Reiter:1999:AMA

[RS99] Michael K. Reiter and Stuart G. Stubblebine. Authentication metric analysis and design. *ACM Transactions on Information and System Security*, 2(2):138–158, May 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-2/p138-reiter/`.

Rudys:2002:TLB

[RW02] Algis Rudys and Dan S. Wallach. Termination in language-based systems. *ACM Transactions on Information and System Security*, 5(2):138–168, May 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sandhu:1998:E

[San98] Ravi Sandhu. Editorial. *ACM Transactions on Information and System Security*, 1(1):1–2, November 1998. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1998-1-1/p1-sandhu/`.

Sandhu:1999:E

[San99] Ravi Sandhu. Editorial. *ACM Transactions on Information and System Security*, 2(1):1–2, February 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-1/p1-sandhu/`.

Sandhu:2005:E

[San05] Ravi Sandhu. Editorial. *ACM Transactions on Information and System Security*, 8(1):1, February 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sarkar:2010:SGC

[Sar10] Palash Sarkar. A simple and generic construction of authenticated encryption with associated data. *ACM Transactions on Information and System Security*, 13(4):33:1–33:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Steiner:2001:SPB

[SBEW01] Michael Steiner, Peter Buhler, Thomas Eirich, and Michael Waidner. Secure password-based cipher suite for TLS. *ACM Transactions on Information and System Security*, 4 (2):134–157, May 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Squicciarini:2007:PTX

[SBF+07] A. Squicciarini, E. Bertino, Elena Ferrari, F. Paci, and B. Thuraisingham. PP-trust-X: a system for privacy preserving trust negotiations. *ACM Transactions on Information and System Security*, 10(3):12:1–12:??, July 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sandhu:1999:AMR

[SBM99] Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer. The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security*, 2(1): 105–135, February 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1999-2-1/p105-sandhu/`.

Shacham:2004:CSC

[SBR04] Hovav Shacham, Dan Boneh, and Eric Rescorla. Client-side caching for TLS. *ACM Transactions on Information and System Security*, 7(4):553–575, November 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Shabtai:2016:BSU

[SBR+16] Asaf Shabtai, Maya Bercovitch, Lior Rokach, Ya'akov (Kobi) Gal, Yuval Elovici, and Erez Shmueli. Behavioral study of users when interacting with active honeytokens. *ACM Transactions on Information and System Security*, 18(3):9:1–9:??, April 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sandhu:1998:MRM

[SC98] Ravi Sandhu and Fang Chen. The multilevel relational (MLR) data model. *ACM Transactions on Information and System Security*, 1(1):93–132, November 1998. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org:80/pubs/citations/journals/tissec/1998-1-1/p93-sandhu/`.

Syta:2014:SAA

[SCGW+14] Ewa Syta, Henry Corrigan-Gibbs, Shu-Chun Weng, David Wolinsky, Bryan Ford, and

Aaron Johnson. Security analysis of accountable anonymity in Dissent. *ACM Transactions on Information and System Security*, 17(1):4:1–4:??, August 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schneider:2000:ESP

[Sch00] Fred B. Schneider. Enforceable security policies. *ACM Transactions on Information and System Security*, 3(1):30–50, February 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Swift:2002:IGA

[SHB+02] Michael M. Swift, Anne Hopkins, Peter Brundrett, Cliff Van Dyke, Praerit Garg, Shannon Chan, Mario Goertzel, and Gregory Jensenworth. Improving the granularity of access control for Windows 2000. *ACM Transactions on Information and System Security*, 5(4):398–437, November 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Stubblefield:2004:KRA

[SIR04] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Transactions on Information and System Security*, 7(2):319–332, May 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Syverson:2012:GES

[SJ12] Paul Syverson and Somesh Jha. Guest editorial: Special issue on computer and communications security. *ACM Transactions on Information and System Security*, 15(1):1:1–1:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Serra:2015:POA

[SJP+15] Edoardo Serra, Sushil Jajodia, Andrea Pugliese, Antonino Rullo, and V. S. Subrahmanian. Pareto-optimal adversarial defense of enterprise systems. *ACM Transactions on Information and System Security*, 17(3):11:1–11:??, March 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Shands:2001:SVE

[SJYS01] Deborah Shands, Jay Jacobs, Richard Yee, and E. John Sebes. Secure virtual enclaves: Supporting coalition use of distributed application technologies. *ACM Transactions on Information and System Security*, 4(2):103–133, May 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schneier:1999:SAL

[SK99] Bruce Schneier and John Kelsey. Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security*, 2(2):159–176, May 1999. CODEN ATISBQ. ISSN

1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-2/p159-schneier/.

Shay:2016:DPP

[SKD+16] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security*, 18 (4):13:1–13:??, May 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schultz:2010:MMP

[SLL10] David Schultz, Barbara Liskov, and Moses Liskov. MPSS: Mobile Proactive Secret Sharing. *ACM Transactions on Information and System Security*, 13(4): 34:1–34:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Smith:2001:CPH

[Smi01] Richard E. Smith. Cost profile of a highly assured, secure operating system. *ACM Transactions on Information and System Security*, 4(1):72–101, February 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schreuders:2011:EEU

[SMP11] Z. Cliffe Schreuders, Tanya McGill, and Christian Payne. Empowering end users to confine their own applications: The results of a usability study comparing SELinux, AppArmor, and FBAC-LSM. *ACM Transactions on Information and System Security*, 14(2):19:1–19:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Strembeck:2004:IAE

[SN04] Mark Strembeck and Gustaf Neumann. An integrated approach to engineer and enforce context constraints in RBAC environments. *ACM Transactions on Information and System Security*, 7(3):392–427, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Serwadda:2013:ELK

[SP13] Abdul Serwadda and Vir V. Phoha. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Transactions on Information and System Security*, 16(2): 8:1–8:??, September 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Spinellis:2000:RMS

[Spi00] Diomidis Spinellis. Reflection as a mechanism for software integrity verification. *ACM Transactions on Information and Sys-*

tem Security, 3(1):51–62, February 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Serwadda:2016:TRR

[SPW+16] Abdul Serwadda, Vir V. Phoha, Zibo Wang, Rajesh Kumar, and Diksha Shukla. Toward robotic robbery on the touch screen. *ACM Transactions on Information and System Security*, 18 (4):14:1–14:??, May 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Samarati:2001:AMP

[SRJ01] Pierangela Samarati, Michael K. Reiter, and Sushil Jajodia. An authorization model for a public key management service. *ACM Transactions on Information and System Security*, 4(4): 453–482, November 2001. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sang:2009:ESP

[SS09] Yingpeng Sang and Hong Shen. Efficient and secure protocols for privacy-preserving set operations. *ACM Transactions on Information and System Security*, 13(1):9:1–9:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Stubblebine:1999:UST

[SSG99] Stuart G. Stubblebine, Paul F. Syverson, and David M. Goldschlag. Unlinkable serial transactions: protocols and applications. *ACM Transactions on Information and System Security*, 2(4):354–389, November 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/articles/journals/tissec/1999-2-4/p354-stubblebine/p354-stubblebine.pdf`; `http://www.acm.org/pubs/citations/journals/tissec/1999-2-4/p354-stubblebine/`.

Sun:2013:BJW

[STS+13] Mengtao Sun, Gang Tan, Joseph Siefers, Bin Zeng, and Greg Morrisett. Bringing Java's wild native world under control. *ACM Transactions on Information and System Security*, 16(3):9:1–9:??, November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schneider:2011:NAL

[SWS11] Fred B. Schneider, Kevin Walsh, and Emin Gün Sirer. Nexus Authorization Logic (NAL): Design rationale and applications. *ACM Transactions on Information and System Security*, 14 (1):8:1–8:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Tsang:2010:BRR

[TAKS10] Patrick P. Tsang, Man Ho Au, Apu Kapadia, and Sean W. Smith. BLAC: Revoking repeatedly misbehaving anonymous users without relying on TTPs. *ACM Transactions on Information and System Security*, 13(4):

39:1–39:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Traynor:2008:NMH

[TCW+08] Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Noninvasive methods for host certification. *ACM Transactions on Information and System Security*, 11(3):16:1–16:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Thompson:2003:CBA

[TEM03] Mary R. Thompson, Abdelilah Essiari, and Srilekha Mudumbai. Certificate-based authorization policy in a PKI environment. *ACM Transactions on Information and System Security*, 6(4):566–588, November 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Thuraisingham:2010:ES

[Thu10] Bhavani Thuraisingham. Editorial: SACMAT 2007. *ACM Transactions on Information and System Security*, 13(3):23:1–23:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Tan:2015:IAR

[TKYK15] Rui Tan, Varun Badrinath Krishna, David K. Y. Yau, and Zbigniew Kalbarczyk. Integrity attacks on real-time pricing in electric power grids. *ACM Transactions on Information and System Security*, 18(2):5:1–5:??, December 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Tsudik:2008:E

[Tsu08] Gene Tsudik. Editorial. *ACM Transactions on Information and System Security*, 11(3):11:1–11:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Vaidya:2010:RMP

[VAG10] Jaideep Vaidya, Vijayalakshmi Atluri, and Qi Guo. The role mining problem: a formal perspective. *ACM Transactions on Information and System Security*, 13(3):27:1–27:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Viega:2002:TBS

[VBKM02] John Viega, J. T. Bloch, Tadayoshi Kohno, and Gary McGraw. Token-based scanning of source code for security problems. *ACM Transactions on Information and System Security*, 5(3):238–261, August 2002. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

vanOorschot:2008:PMU

[vOT08] P. C. van Oorschot and Julie Thorpe. On predictive models and user-drawn graphical passwords. *ACM Transactions on Information and System Security*, 10(4):5:1–5:??, January 2008.

CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

vanOorschot:2007:IRS

[vOWK07] P. C. van Oorschot, Tao Wan, and Evangelos Kranakis. On interdomain routing security and pretty secure BGP (psBGP). *ACM Transactions on Information and System Security*, 10 (3):11:1–11:??, July 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

VanOorschot:2006:COD

[VS06] Paul C. Van Oorschot and Stuart Stubblebine. On countering online dictionary attacks with login histories and humans-in-the-loop. *ACM Transactions on Information and System Security*, 9(3):235–258, August 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wright:2004:PAA

[WALS04] Matthew K. Wright, Micah Adler, Brian Neil Levine, and Clay Shields. The predecessor attack: an analysis of a threat to anonymous communications systems. *ACM Transactions on Information and System Security*, 7(4):489–522, November 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wright:2008:PLA

[WALS08] Matthew K. Wright, Micah Adler, Brian Neil Levine, and Clay Shields. Passive-logging Attacks Against Anonymous Communications Systems. *ACM Transactions on Information and System Security*, 11(2): 3:1–3:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Walcott:2004:TMR

[WB04] Tom Walcott and Matt Bishop. Traducement: a model for record security. *ACM Transactions on Information and System Security*, 7(4):576–590, November 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wright:2010:USP

[WBC+10] Charles V. Wright, Lucas Ballard, Scott E. Coull, Fabian Monrose, and Gerald M. Masson. Uncovering spoken phrases in encrypted voice over IP conversations. *ACM Transactions on Information and System Security*, 13(4):35:1–35:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wei:2011:ARH

[WCBR11] Qiang Wei, Jason Crampton, Konstantin Beznosov, and Matei Ripeanu. Authorization recycling in hierarchical RBAC systems. *ACM Transactions on Information and System Security*, 14(1):3:1–3:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wang:2008:GBA

[WD08] Wei Wang and Thomas E. Daniels. A graph based approach toward network forensics analysis. *ACM Transactions on Information and System Security*, 12 (1):4:1–4:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wang:2010:DVT

[WGJT10] Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deterring voluntary trace disclosure in re-encryption mix-networks. *ACM Transactions on Information and System Security*, 13(2):18:1–18:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wijesekera:2003:PPA

[WJ03] Duminda Wijesekera and Sushil Jajodia. A propositional policy algebra for access control. *ACM Transactions on Information and System Security*, 6 (2):286–325, May 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wedde:2004:MAA

[WL04] Horst F. Wedde and Mario Lischka. Modular authorization and administration. *ACM Transactions on Information and System Security*, 7(3):363–391, August 2004. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Winsborough:2006:SAT

[WL06] William H. Winsborough and Ninghui Li. Safety in automated trust negotiation. *ACM Transactions on Information and System Security*, 9(3):352–390, August 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wang:2010:SRW

[WL10] Qihua Wang and Ninghui Li. Satisfiability and resiliency in workflow authorization systems. *ACM Transactions on Information and System Security*, 13(4): 40:1–40:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wang:2008:FBB

[WLC+08] Xiaofeng Wang, Zhuowei Li, Jong Youl Choi, Jun Xu, Michael K. Reiter, and Chongkyung Kil. Fast and black-box exploit detection and signature generation for commodity software. *ACM Transactions on Information and System Security*, 12(2): 11:1–11:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wool:2000:KME

[Woo00] Avishai Wool. Key management for encrypted broadcast. *ACM Transactions on Information and System Security*, 3 (2):107–134, May 2000. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wright:2008:GES

[WS08] Rebecca N. Wright and Sabrina De Capitanidi Vimercati. Guest editorial: Special issue on computer and communications security. *ACM Transactions on Information and System Security*, 12(2):7:1–7:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Williams:2013:APC

[WS13] Peter Williams and Radu Sion. Access privacy and correctness on untrusted storage. *ACM Transactions on Information and System Security*, 16(3):12:1–12:??, November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Williams:2011:POO

[WSS11] Peter Williams, Radu Sion, and Miroslava Sotakova. Practical oblivious outsourced storage. *ACM Transactions on Information and System Security*, 14 (2):20:1–20:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wang:2011:CAF

[WWGZ11] Tielei Wang, Tao Wei, Guofei Gu, and Wei Zou. Checksum-aware fuzzing combined with dynamic taint analysis and symbolic execution. *ACM Transactions on Information and System Security*, 14(2):15:1–15:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Xu:2008:DSB

[XČ08] Shouhuai Xu and Srdjan Čapkun. Distributed and secure bootstrapping of mobile ad hoc networks: Framework and constructions. *ACM Transactions on Information and System Security*, 12(1):2:1–2:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Xiang:2011:CFR

[XHRC11] Guang Xiang, Jason Hong, Carolyn P. Rose, and Lorrie Cranor. CANTINA+: a feature-rich machine learning framework for detecting phishing Web sites. *ACM Transactions on Information and System Security*, 14 (2):21:1–21:??, September 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Xu:1999:DHP

[XS99] Jun Xu and Mukesh Singhal. Design of a high-performance ATM firewall. *ACM Transactions on Information and System Security*, 2(3):269–294, August 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL `http://www.acm.org/pubs/citations/journals/tissec/1999-2-3/p269-xu/`.

Xie:2008:TMS

[XYW08] Mengjun Xie, Heng Yin, and Haining Wang. Thwarting E-mail spam laundering. *ACM Transactions on Information and System Security*, 12(2):13:1–13:??, December 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Xie:2008:MDA

[XZ08] Liang Xie and Sencun Zhu. Message dropping attacks in overlay networks: Attack detection and attacker identification. *ACM Transactions on Information and System Security*, 11(3):15:1–15:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yao:2008:PIR

[YFAT08] Danfeng Yao, Keith B. Frikken, Mikhail J. Atallah, and Roberto Tamassia. Private information: To reveal or not to reveal. *ACM Transactions on Information and System Security*, 12(1):6:1–6:??, October 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yavuz:2012:BFB

[YNR12] Attila A. Yavuz, Peng Ning, and Michael 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):9:1–9:??, July 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ye:2005:TPB

[YSA05] Zishuang (Eileen) Ye, Sean Smith, and Denise Anthony. Trusted paths for browsers. *ACM Transactions on Information and System Security*, 8(2):153–186, May 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yao:2009:CAR

[YT09] Danfeng Yao and Roberto Tamassia. Compact and anonymous role-based authorization chain. *ACM Transactions on Information and System Security*, 12(3):15:1–15:??, January 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yu:2003:SSC

[YWS03] Ting Yu, Marianne Winslett, and Kent E. Seamons. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. *ACM Transactions on Information and System Security*, 6(1):1–42, February 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yang:2008:SSH

[YWZC08] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao. SDAP: a secure hop-by-hop data aggregation protocol for sensor networks. *ACM Transactions on In-*

formation and System Security, 11(4):18:1–18:??, July 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhang:2003:RBF

[ZAC03] Longhua Zhang, Gail-Joon Ahn, and Bei-Tseng Chu. A rule-based framework for role-based delegation and revocation. *ACM Transactions on Information and System Security*, 6(3):404–441, August 2003. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhao:2015:PGA

[ZAH15] Ziming Zhao, Gail-Joon Ahn, and Hongxin Hu. Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. *ACM Transactions on Information and System Security*, 17(4):14:1–14:??, April 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhu:2009:CAC

[ZB09] Ye Zhu and Riccardo Bettati. Compromising anonymous communication systems using blind source separation. *ACM Transactions on Information and System Security*, 13(1):8:1–8:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhou:2007:MNI

[ZHR+07] Jingmin Zhou, Mark Heckman, Brennen Reynolds, Adam Carlson, and Matt Bishop. Modeling network intrusion detection alerts for correlation. *ACM Transactions on Information and System Security*, 10(1):4:1–4:??, February 2007. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhang:2008:TUB

[ZNCS08] Xinwen Zhang, Masayuki Nakae, Michael J. Covington, and Ravi Sandhu. Toward a Usage-Based Security Framework for Collaborative Computing Systems. *ACM Transactions on Information and System Security*, 11(1): 3:1–3:??, February 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zage:2010:RDV

[ZNR10] David Zage and Cristina Nita-Rotaru. Robust decentralized virtual coordinate systems in adversarial environments. *ACM Transactions on Information and System Security*, 13(4):38:1–38:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhang:2005:FMP

[ZPPSP05] Xinwen Zhang, Francesco Parisi-Presicce, Ravi Sandhu, and Jaehong Park. Formal model and policy specification of usage control. *ACM Transactions on Information and System Security*, 8(4):351–387, November 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zheng:2016:EUV

[ZPW16] Nan Zheng, Aaron Paloski, and Haining Wang. An efficient user verification system using angle-based mouse movement biometrics. *ACM Transactions on Information and System Security*, 18(3):11:1–11:??, April 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhou:2005:APS

[ZSV05] Lidong Zhou, Fred B. Schneider, and Robbert Van Renesse. APSS: proactive secret sharing in asynchronous systems. *ACM Transactions on Information and System Security*, 8(3): 259–286, August 2005. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhang:2008:FIC

[ZYN08] Qing Zhang, Ting Yu, and Peng Ning. A framework for identifying compromised nodes in wireless sensor networks. *ACM Transactions on Information and System Security*, 11(3): 12:1–12:??, March 2008. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhuang:2009:KAE

[ZZT09] Li Zhuang, Feng Zhou, and J. D. Tygar. Keyboard acoustic emanations revisited. *ACM Transactions on Information and System Security*, 13(1):3:1–3:??, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).