A Complete Bibliography of *ACM Transactions on Privacy and Security (TOPS)*

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

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

16 April 2025
Version 1.25

Title word cross-reference

#PrettyFlyForAWiFi [BBEM21].

B^3 [GCY+23]. K [SCL+17, CHMM22].

-Means [SCL+17]. **-Nearest** [CHMM22].

2.0 [HKW25, NVM+17].

5G [SM24].

Abstract [AM21, GM18]. **Accelerate** [BMN+22]. **Access** [BCLR22, BFT25, CHK24, IM22]. **Accompanying** [HKW25]. **Account** [CGG+24]. **Accountable** [FMJS22]. **Accurate** [RPA16, SBP21]. **Acoustic** [dGBSS22]. **Across** [MJA+18, Wag23]. **Action** [RSR23]. **Active** [SWAS+23]. **Adapted** [BKSR24]. **Adaptive** [ACA+24, AHF23, CHK24, HZL21, NKS+19]. **Adblocking** [LEMS25]. **Administrative** [BFT25]. **Adversarial** [BBG+23, CSL+24, DCB+21, DWL+25, HWB25, HGP+25, KSG+25, ODZ+24, PK24, QGS+22, SBBR19, URK23, WYW+23, YTF+20, YZC+25, ZZYY23, CGG+24]. **AdverSPAM** [CGG+24]. **Advertising** [BKÖ20]. **Advice** [MM23]. **Against** [DWL+25, HKHWH23, HWB25, HZL21, LIKB23, MT24, PPK+18, VWMV23, WDA+24, GCY+23, HHGC24, PK24, QGS+22, ZZYY23]. **agent** [AHF23, HWZ+23, WWG25]. **Ages** [Wag23]. **Aggregation** [ACA+24, LSWR22]. **Agitated** [PK24]. **Agnostic** [OB22].

References

Acar:2021:LPA

[AAK+21] Abbas Acar, Shoukat Ali, Koray Karabina, Cengiz Kaygusuz, Hidayet Aksu, Kemal Akkaya, and Selcuk Uluagac. A lightweight Privacy-Aware Continuous Authentication Protocol — PACA. *ACM Transactions on Privacy and Security (TOPS)*, 24(4): 24:1–24:28, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3464690`.

Abuhamad:2021:LSR

[AAMN21] Mohammed Abuhamad, Tamer Abuhmed, David Mohaisen, and Daehun Nyang. Large-scale and robust code authorship identification with deep feature learning. *ACM Transactions on Privacy and Security (TOPS)*, 24 (4):23:1–23:35, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3461666`.

Ahmed:2024:DDE

[ACA+24] Mukhtar Ahmed, Jinfu Chen, Ernest Akpaku, Rexford Nii Ayitey Sosu, and Ajmal Latif. DELM: Deep ensemble learning model for anomaly detection in malicious network traffic-based adaptive feature aggregation and network optimization. *ACM Transactions on Privacy and Security (TOPS)*, 27(4): 32:1–32:??, November 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3690637`.

Arias-Cabarcos:2023:PUE

[ACFH+23] Patricia Arias-Cabarcos, Matin Fallahi, Thilo Habrich, Karen Schulze, Christian Becker, and Thorsten Strufe. Performance and usability evaluation of brainwave authentication techniques with consumer devices. *ACM Transactions on Privacy and Security (TOPS)*, 26(3): 26:1–26:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3579356`.

Alvim:2022:ILG

[ACKP22] Mário S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi. Information leakage games: Exploring information as a utility function. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):20:1–20:36, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3517330`.

Abrath:2020:CRN

[ACV+20] Bert Abrath, Bart Coppens, Jens Van Den Broeck, Brecht

Wyseur, Alessandro Cabutto, Paolo Falcarin, and Bjorn De Sutter. Code renewability for native software protection. *ACM Transactions on Privacy and Security (TOPS)*, 23(4): 20:1–20:31, August 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3404891`.

Amro:2023:ACR

[AGK23] Ahmed Amro, Vasileios Gkioulos, and Sokratis Katsikas. Assessing cyber risk in cyber-physical systems using the ATT&CK framework. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):22:1–22:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3571733`.

Aloufi:2023:PPP

[AHB23] Ranya Aloufi, Hamed Haddadi, and David Boyle. Paralinguistic privacy protection at the edge. *ACM Transactions on Privacy and Security (TOPS)*, 26(2): 19:1–19:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3570161`.

AlMallah:2023:RDA

[AHF23] Ranwa Al Mallah, Talal Halabi, and Bilal Farooq. Resilience-by-design in adaptive multi-agent traffic control systems. *ACM Transactions on Privacy and Security (TOPS)*, 26(3): 40:1–40:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3592799`.

Alexopoulos:2021:TIM

[AHSM21] Nikolaos Alexopoulos, Sheikh Mahbub Habib, Steffen Schulz, and Max Mühlhäuser. The tip of the iceberg: On the merits of finding security bugs. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):3:1–3:33, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3406112`.

Alex:2023:EES

[AJP23] Sona Alex, Dhanaraj K. J., and Deepthi P. P. Energy efficient and secure neural network-based disease detection framework for mobile healthcare network. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):29:1–29:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3585536`.

Alper:2022:OEM

[AK22] Handan Kilinç Alper and Alptekin Küpçü. Optimally efficient multi-party fair exchange and fair secure multi-party computation. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):3:1–3:34, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3477530`.

Ami:2021:SMB

[AKM+21] Amit Seal Ami, Kaushal Kafle, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk. Systematic mutation-based evaluation of the soundness of security-focused Android static analysis techniques. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):15:1–15:37, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3439802`.

Aonghusa:2016:DLG

[AL16] Pól Mac Aonghusa and Douglas J. Leith. Don't let Google know I'm lonely. *ACM Transactions on Privacy and Security (TOPS)*, 19(1):3:1–3:??, August 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Akavia:2022:PPD

[ALR+22] Adi Akavia, Max Leibovich, Yehezkel S. Resheff, Roey Ron, Moni Shahar, and Margarita Vald. Privacy-preserving decision trees training and prediction. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):24:1–24:30, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3517197`.

Arceri:2021:ADC

[AM21] Vincenzo Arceri and Isabella Mastroeni. Analyzing dynamic code: a sound abstract interpreter for evil eval. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):10:1–10:38, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3426470`.

Ahmed:2021:NPD

[AMO21] Chuadhry Mujeeb Ahmed, Aditya P. Mathur, and Martín Ochoa. NoiSense print: Detecting data integrity attacks on sensor measurements using hardware-based fingerprints. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):2:1–2:35, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3410447`.

Argyros:2017:EPG

[APS+17] George Argyros, Theofilos Petsios, Suphannee Sivakorn, Angelos D. Keromytis, and Jason Polakis. Evaluating the privacy guarantees of location proximity services. *ACM Transactions on Privacy and Security (TOPS)*, 19(4):12:1–12:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Ameer:2024:ZIN

[APS+24] Safwa Ameer, Lopamudra Praharaj, Ravi Sandhu, Smriti Bhatt, and Maanak Gupta. ZTA-IoT: a novel architecture for zero-trust in IoT systems and an ensuing usage control model. *ACM Transactions on Privacy and Security (TOPS)*, 27(3):22:1–22:??, August 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3671147`.

Ahmed:2024:SAC

[APSA24] Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, and Tuomas Aura. Security analysis of the consumer remote SIM provisioning protocol. *ACM Transactions on Privacy and Security (TOPS)*, 27(3):23:1–23:??, August 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3663761`.

Anwar:2020:CFC

[AS20] Fatima M. Anwar and Mani Srivastava. A case for feedforward control with feedback trim to mitigate time transfer attacks. *ACM Transactions on Privacy and Security (TOPS)*, 23(2):11:1–11:25, May 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3382503`.

Alrabaee:2018:FRE

[ASWD18] Saed Alrabaee, Paria Shirani, Lingyu Wang, and Mourad Debbabi. FOSSIL: A resilient and efficient system for identifying FOSS functions in malware binaries. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):8:1–8:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3175492`.

Antonioli:2020:KND

[ATR20] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Key negotiation downgrade attacks on Bluetooth and Bluetooth low energy. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):14:1–14:28, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3394497`.

Abdou:2018:SLV

[AV18] Abdelrahman Abdou and P. C. Van Oorschot. Server location verification (SLV) and server location pinning: Augmenting TLS authentication. *ACM Transactions on Privacy and Security (TOPS)*, 21(1):1:1–1:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3139294`.

Alotaibi:2023:TIE

[AWK23] Norah Alotaibi, John Williamson, and Mohamed Khamis. ThermoSecure: Investigating the effectiveness of AI-driven thermal attacks on commonly used computer keyboards. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):12:1–12:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3563693.

Botacin:2021:OSD

[BAO+21] Marcus Botacin, Hojjat Aghakhani, Stefano Ortolani, Christopher Kruegel, Giovanni Vigna, Daniela Oliveira, Paulo Lício De Geus, and André Grégio. One size does not fit all: a longitudinal analysis of Brazilian financial malware. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):11:1–11:31, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3429741.

Birnbach:2021:PRW

[BBEM21] Simon Birnbach, Richard Baker, Simon Eberz, and Ivan Martinovic. #PrettyFlyForAWiFi: Real-world detection of privacy invasion attacks by drones. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):31:1–31:34, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3473672.

Barbosa:2023:MPA

[BBG+23] Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, and Pierre-Yves Strub. Mechanized proofs of adversarial complexity and application to universal composability. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):41:1–41:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3589962.

Barrera:2023:SBP

[BBV23] David Barrera, Christopher Bellman, and Paul Van Oorschot. Security best practices: a critical analysis using IoT as a case study. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):13:1–13:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3563392.

Baccarini:2025:UID

[BBZ25] Alessandro Baccarini, Marina Blanton, and Shaofeng Zou. Understanding information disclosure from secure computation output: a comprehensive study of average salary computation. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):12:1–12:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (elec-

tronic). URL https://dl.acm.org/doi/10.1145/3705004.

Brandenburger:2017:DTC

[BCK17] Marcus Brandenburger, Christian Cachin, and Nikola Knezević. Don't trust the cloud, verify: Integrity and consistency for cloud object stores. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):8:1–8:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Berlato:2022:FMA

[BCLR22] Stefano Berlato, Roberto Carbone, Adam J. Lee, and Silvio Ranise. Formal modelling and automated tradeoff analysis of enforcement architectures for cryptographic access control in the cloud. *ACM Transactions on Privacy and Security (TOPS)*, 25(1): 2:1–2:37, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3474056.

Bolton:2023:PTR

[BDBM23] Tom Bolton, Tooska Dargahi, Sana Belguith, and Carsten Maple. PrivExtractor: Toward redressing the imbalance of understanding between virtual assistant users and vendors. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):31:1–31:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3588770.

Botacin:2018:EBM

[BDG18] Marcus Botacin, Paulo Lício De Geus, and André Grégio. Enhancing branch monitoring for security purposes: From control flow integrity to malware analysis and debugging. *ACM Transactions on Privacy and Security (TOPS)*, 21(1): 4:1–4:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3152162.

Braun:2022:MFM

[BDST22] Lennart Braun, Daniel Demmler, Thomas Schneider, and Oleksandr Tkachenko. MOTION — a framework for mixed-protocol multi-party computation. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):8:1–8:35, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3490390.

Bertolissi:2025:CBA

[BFT25] Clara Bertolissi, Maribel Fernandez, and Bhavani Thuraisingham. Category-based administrative access control policies. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):3:1–3:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3698199.

Bazai:2022:NHA

[BJJA22] Sibghat Ullah Bazai, Julian Jang-Jaccard, and Hooman Alavizadeh. A novel hybrid approach for multi-dimensional data anonymization for Apache Spark. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):5:1–5:25, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3484945`.

Bansal:2023:SAR

[BKH+23] Ayoosh Bansal, Anant Kandikuppa, Monowar Hasan, Chien-Ying Chen, Adam Bates, and Sibin Mohan. System auditing for real-time systems. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):50:1–50:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3625229`.

Boshrooyeh:2020:PPP

[BKÖ20] Sanaz Taheri Boshrooyeh, Alptekin Küpçü, and Öznur Özkasap. Privado: Privacy-preserving group-based advertising using multiple independent social network providers. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):12:1–12:36, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3386154`.

Bayer:2024:CDA

[BKSR24] Markus Bayer, Philipp Kuehn, Ramin Shanehsaz, and Christian Reuter. CySecBERT: a domain-adapted language model for the cybersecurity domain. *ACM Transactions on Privacy and Security (TOPS)*, 27(2):18:1–18:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3652594`.

Bhattacharya:2018:UPC

[BM18] Sarani Bhattacharya and Debdeep Mukhopadhyay. Utilizing performance counters for compromising public key ciphers. *ACM Transactions on Privacy and Security (TOPS)*, 21(1):5:1–5:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3156015`.

Blair:2022:HDT

[BMA+22] William Blair, Andrea Mambretti, Sajjad Arshad, Michael Weissbacher, William Robertson, Engin Kirda, and Manuel Egele. HotFuzz: Discovering temporal and spatial denial-of-service vulnerabilities through guided micro-fuzzing. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):33:1–33:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3532184`.

Botacin:2022:TSC

[BMN+22] Marcus Botacin, Francis B. Moreira, Philippe O. A. Navaux, André Grégio, and Marco A. Z. Alves. Terminator: a secure coprocessor to accelerate real-time AntiViruses using inspection breakpoints. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):9:1–9:34, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3494535`.

Balliu:2021:FFC

[BMPS21] Musard Balliu, Massimo Merro, Michele Pasqua, and Mikhail Shcherbakov. Friendly fire: Cross-app interactions in IoT platforms. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):16:1–16:40, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3444963`.

Bhattacharjee:2021:ACE

[BMSD21] Shameek Bhattacharjee, Venkata Praveen Kumar Madhavarapu, Simone Silvestri, and Sajal K. Das. Attack context embedded data driven trust diagnostics in smart metering infrastructure. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):9:1–9:36, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3426739`.

Blass:2024:FSC

[BN24] Erik-Oliver Blass and Guevara Noubir. Forward security with crash recovery for secure logs. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):3:1–3:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3631524`.

Bollegala:2025:MDP

[BOMiK25] Danushka Bollegala, Shuichi Otake, Tomoya Machide, and Ken ichi Kawarabayashi. A metric differential privacy mechanism for sentence embeddings. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):20:1–20:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Belman:2020:DPT

[BP20] Amith K. Belman and Vir V. Phoha. Discriminative power of typing features on desktops, tablets, and phones for user identification. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):4:1–4:36, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3377404`.

Bhuiyan:2023:LRC

[BR23] Farzana Ahamed Bhuiyan and Akond Rahman. Log-related coding patterns to conduct postmortems of attacks in supervised learning-based projects. *ACM Transactions on Privacy and Security (TOPS)*, 26(2): 17:1–17:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3568020.

Bjurling:2025:CTI

[BR25] Björn Bjurling and Shahid Raza. Cyber threat intelligence meets the analytic tradecraft. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):6:1–6:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3701299.

Bernabe-Rodriguez:2024:DPD

[BRGL24] Julen Bernabé-Rodríguez, Albert Garreta, and Oscar Lage. A decentralized private data marketplace using blockchain and secure multi-party computation. *ACM Transactions on Privacy and Security (TOPS)*, 27(2): 19:1–19:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3652162.

Bostani:2025:LMV

[BZLM25] Hamid Bostani, Zhengyu Zhao, Zhuoran Liu, and Veelasha Moonsamy. Level up with ML vulnerability identification: Leveraging domain constraints in feature space for robust Android malware detection. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):17:1–17:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Bao:2025:EDT

[BZY+25] Yubing Bao, Jianping Zeng, Jirui Yang, Ruining Yang, and Zhihui Lu. The effect of domain terms on password security. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):9:1–9:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3703350.

Cheng:2021:ETD

[CAL+21] Long Cheng, Salman Ahmed, Hans Liljestrand, Thomas Nyman, Haipeng Cai, Trent Jaeger, N. Asokan, and Danfeng (Daphne) Yao. Exploitation techniques for data-oriented attacks with existing and potential defense approaches. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):26:1–26:36, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3462699.

Cecconello:2019:STK

[CCC+19] Stefano Cecconello, Alberto Compagno, Mauro Conti, Daniele Lain, and Gene Tsudik. Skype & Type: Keyboard eavesdropping in Voice-over-IP. *ACM Transactions on Privacy and Security (TOPS)*, 22(4):24:1–24:??, December 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3365366`.

Chen:2024:SHG

[CDNW24] Liqun Chen, Changyu Dong, Christopher J. P. Newton, and Yalan Wang. Sphinx-in-the-head: Group signatures from symmetric primitives. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):11:1–11:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3638763`.

Cantali:2019:AMS

[CEÇE19] Gokcan Cantali, Orhan Ermis, Mehmet Ufuk Çaglayan, and Cem Ersoy. Analytical models for the scalability of dynamic group-key agreement protocols and secure file sharing systems. *ACM Transactions on Privacy and Security (TOPS)*, 22(4):20:1–20:??, December 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3342998`.

Crampton:2022:VAP

[CEG+22] Jason Crampton, Eduard Eiben, Gregory Gutin, Daniel Karapetyan, and Diptapriyo Majumdar. Valued authorization policy existence problem: Theory and experiments. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):28:1–28:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3528101`.

Crampton:2025:BOO

[CEG+25] Jason Crampton, Eduard Eiben, Gregory Gutin, Daniel Karapetyan, and Diptapriyo Majumdar. Bi-objective optimization in role mining. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):5:1–5:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3697833`.

Ceragioli:2024:SVI

[CGDB24] Lorenzo Ceragioli, Letterio Galletta, Pierpaolo Degano, and David Basin. Specifying and verifying information flow control in SELinux configurations. *ACM Transactions on Privacy and Security (TOPS)*, 27(4):31:1–31:??, November 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3690636`.

Crampton:2016:WSP

[CGG+16] Jason Crampton, Andrei Gagarin, Gregory Gutin, Mark Jones, and Magnus Wahlström. On the workflow satisfiability problem with class-independent constraints for hierarchical organizations. *ACM Transactions on Privacy and Security (TOPS)*, 19(3):8:1–8:??, December 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Concone:2024:AAS

[CGG+24] Federico Concone, Salvatore Gaglio, Andrea Giammanco, Giuseppe Lo Re, and Marco Morana. AdverSPAM: Adversarial SPam account manipulation in online social networks. *ACM Transactions on Privacy and Security (TOPS)*, 27(2): 15:1–15:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3643563.

Cho:2020:SUI

[CHK+20] Geumhwan Cho, Jun Ho Huh, Soolin Kim, Junsung Cho, Heesung Park, Yenah Lee, Konstantin Beznosov, and Hyoungshick Kim. On the security and usability implications of providing multiple authentication choices on smartphones: The more, the better? *ACM Transactions on Privacy and Security (TOPS)*, 23(4):22:1–22:32, August 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3410155.

Chen:2024:MMS

[CHK24] Jiayi Chen, Urs Hengartner, and Hassan Khan. MRAAC: a multi-stage risk-aware adaptive authentication and access control framework for Android. *ACM Transactions on Privacy and Security (TOPS)*, 27(2): 17:1–17:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3648372.

Clifton:2022:DPN

[CHMM22] Chris Clifton, Eric J. Hanson, Keith Merrill, and Shawn Merrill. Differentially private k-nearest neighbor missing data imputation. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):16:1–16:23, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3507952.

Chen:2025:ESE

[CLTY25] Long Chen, Ya-Nan Li, Qiang Tang, and Moti Yung. End-to-same-end encryption: Modularly augmenting an app with an efficient, portable, and blind cloud storage. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):14:1–14:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Choo:2023:DDD

[CNA+23] Euijin Choo, Mohamed Nabeel, Mashael Alsabah, Issa Khalil, Ting Yu, and Wei Wang. DeviceWatch: a data-driven network analysis approach to identifying compromised mobile devices with graph-inference. *ACM Transactions on Privacy and Security (TOPS)*, 26(1): 9:1–9:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3558767`.

Chernikova:2022:FFE

[CO22] Alesia Chernikova and Alina Oprea. FENCE: Feasible evasion attacks on neural networks in constrained environments. *ACM Transactions on Privacy and Security (TOPS)*, 25(4): 34:1–34:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3544746`.

Carminati:2018:SEB

[CPC+18] Michele Carminati, Mario Polino, Andrea Continella, Andrea Lanzi, Federico Maggi, and Stefano Zanero. Security evaluation of a banking fraud analysis system. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):11:1–11:??, June 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3178370`.

Cui:2021:PPD

[CSA+21] Shujie Cui, Xiangfu Song, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello. Privacy-preserving dynamic symmetric searchable encryption with controllable leakage. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):18:1–18:35, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3446920`.

Chen:2023:TME

[CSC+23] Jinfu Chen, Luo Song, Saihua Cai, Haodi Xie, Shang Yin, and Bilal Ahmad. TLS-MHSA: an efficient detection model for encrypted malicious traffic based on multi-head self-attention mechanism. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):44:1–44:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3613960`.

Cao:2024:EHD

[CSL+24] Han Cao, Qindong Sun, Yaqi Li, Rong Geng, and Xiaoxiong Wang. Efficient history-driven adversarial perturbation distribution learning in low frequency domain. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):4:1–4:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3632293`.

Cui:2022:DBT

[CSS+22] Jinhua Cui, Shweta Shinde,

Satyaki Sen, Prateek Saxena, and Pinghai Yuan. Dynamic binary translation for SGX enclaves. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):32:1–32:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3532862.

Cordero:2021:GNT

[CVW+21] Carlos Garcia Cordero, Emmanouil Vasilomanolakis, Aidmar Wainakh, Max Mühlhäuser, and Simin Nadjm-Tehrani. On generating network traffic datasets with synthetic attacks for intrusion detection. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):8:1–8:39, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3424155.

Chen:2022:SMA

[CZY+22] Yuxuan Chen, Jiangshan Zhang, Xuejing Yuan, Shengzhi Zhang, Kai Chen, Xiaofeng Wang, and Shanqing Guo. SoK: a modularized approach to study the security of automatic speech recognition systems. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):17:1–17:31, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3510582.

Daoudi:2022:DDI

[DABK22] Nadia Daoudi, Kevin Allix, Tegawendé François Bissyandé, and Jacques Klein. A deep dive inside DREBIN: an explorative analysis beyond Android malware detection scores. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):13:1–13:28, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3503463.

Dambra:2023:CSS

[DBB23] Savino Dambra, Leyla Bilge, and Davide Balzarotti. A comparison of systemic and systematic risks of malware encounters in consumer and enterprise environments. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):16:1–16:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3565362.

Daniel:2023:BRS

[DBR23] Lesly-Ann Daniel, Sébastien Bardin, and Tamara Rezk. Binsec/Rel: Symbolic binary analyzer for security with applications to constant-time and secret-erasure. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):11:1–11:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3563037.

Demetrio:2021:AES

[DCB+21] Luca Demetrio, Scott E. Coull, Battista Biggio, Giovanni Lagorio, Alessandro Armando, and Fabio Roli. Adversarial EXEmples: a survey and experimental evaluation of practical attacks on machine learning for Windows malware detection. *ACM Transactions on Privacy and Security (TOPS)*, 24 (4):27:1–27:31, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3473039.

Dai:2025:AEP

[DCD+25] Huan Dai, Yuefeng Chen, Yicong Du, Luping Wang, Ziyu Shao, Hongbo Liu, Yanzhi Ren, Jiadi Yu, and Bo Liu. ArmSpy++: Enhanced PIN inference through video-based fine-grained arm posture analysis. *ACM Transactions on Privacy and Security (TOPS)*, 28(1): 2:1–2:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3696418.

Debant:2022:NYF

[DDW22] Alexandre Debant, Stéphanie Delaune, and Cyrille Wiedling. So near and yet so far — symbolic verification of distance-bounding protocols. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):11:1–11:39, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3501402.

Briseno:2022:IUI

[dGBSS22] Julian de Gortari Briseno, Akash Deep Singh, and Mani Srivastava. InkFiltration: Using inkjet printers for acoustic data exfiltration from air-gapped networks. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):15:1–15:26, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3510583.

Dong:2016:DRC

[DKC16] Zheng Dong, Kevin Kane, and L. Jean Camp. Detection of rogue certificates from trusted certificate authorities using deep neural networks. *ACM Transactions on Privacy and Security (TOPS)*, 19(2): 5:1–5:??, September 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Diamantaris:2020:SDS

[DMIP20] Michalis Diamantaris, Francesco Marcantoni, Sotiris Ioannidis, and Jason Polakis. The seven deadly sins of the HTML5 WebAPI: a large-scale study on the risks of mobile sensor-based attacks. *ACM Transactions on Privacy and Security (TOPS)*, 23(4):19:1–19:31, August 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (elec-

tronic). URL https://dl.acm.org/doi/10.1145/3403947.

DiTizio:2023:POD

[DSS+23] Giorgio Di Tizio, Patrick Speicher, Milivoj Simeonovski, Michael Backes, Ben Stock, and Robert Künnemann. Pareto-optimal defenses for the Web infrastructure: Theory and practice. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):18:1–18:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3567595.

Dong:2025:SDA

[DWL+25] Yingkai Dong, Li Wang, Zheng Li, Hao Li, Peng Tang, Chengyu Hu, and Shanqing Guo. Safe driving adversarial trajectory can mislead: Toward more stealthy adversarial attack against autonomous driving prediction module. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):19:1–19:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Eren:2023:SSC

[EBJ+23] Maksim E. Eren, Manish Bhattarai, Robert J. Joyce, Edward Raff, Charles Nicholas, and Boian S. Alexandrov. Semi-supervised classification of malware families under extreme class imbalance via hierarchical non-negative matrix factorization with automatic model selection. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):48:1–48:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3624567.

Ebrahimpour:2024:BFS

[EH24] Ghader Ebrahimpour and Mohammad Sayad Haghighi. Is bitcoin future as secure as we think? Analysis of bitcoin vulnerability to bribery attacks launched through large transactions. *ACM Transactions on Privacy and Security (TOPS)*, 27(2):14:1–14:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3641546.

Engstrom:2023:ASA

[EJL+23] Viktor Engström, Pontus Johnson, Robert Lagerström, Erik Ringdahl, and Max Wällstedt. Automated security assessments of Amazon Web services environments. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):20:1–20:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3570903.

Eberz:2016:LLE

[ERLM16] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. Looks like Eve: Exposing insider threats using eye movement biometrics. *ACM Transactions on Privacy and Security (TOPS)*, 19(1): 1:1–1:??, August 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Fischer:2022:CED

[FFK+22] Andreas Fischer, Benny Fuhry, Jörn Kußmaul, Jonas Janneck, Florian Kerschbaum, and Eric Bodden. Computation on encrypted data using dataflow authentication. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):21:1–21:36, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3513005`.

Fenske:2022:APS

[FMJS22] Ellis Fenske, Akshaya Mani, Aaron Johnson, and Micah Sherr. Accountable private set cardinality for distributed measurement. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):25:1–25:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3477531`.

Farris:2018:VSV

[FSC+18] Katheryn A. Farris, Ankit Shah, George Cybenko, Rajesh Ganesan, and Sushil Jajodia. VULCON: A system for vulnerability prioritization, mitigation, and management. *ACM Transactions on Privacy and Security (TOPS)*, 21(4):16:1–16:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3196884`.

Fang:2025:DDM

[FZS25] Shuaijv Fang, Zhiyong Zhang, and Bin Song. Deepfake detection model combining texture differences and frequency domain information. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):21:1–21:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Gunasinghe:2024:PPP

[GAB24] Hasini Gunasinghe, Mikhail Atallah, and Elisa Bertino. PEBASI: a privacy preserving, efficient biometric authentication scheme based on irises. *ACM Transactions on Privacy and Security (TOPS)*, 27(3):25:1–25:??, August 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3677017`.

Gil:2023:AFI

[GAHD23] Gonzalo Gil, Aitor Arnaiz, Mariví Higuero, and Francisco Javier Diez. Assessment framework for the identification and evaluation of main features for distributed usage control solutions. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):10:1–10:??, February 2023. CODEN ????

ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3561511.

Gutierrez:2016:IDO

[GAS+16] Christopher N. Gutierrez, Mohammed H. Almeshekah, Eugene H. Spafford, Mikhail J. Atallah, and Jeff Avery. Inhibiting and detecting offline password cracking using ErsatzPasswords. *ACM Transactions on Privacy and Security (TOPS)*, 19(3):9:1–9:??, December 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Gong:2023:BBA

[GCY+23] Xueluan Gong, Yanjiao Chen, Wenbin Yang, Huayang Huang, and Qian Wang. B^3: Backdoor attacks against black-box machine learning models. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):43:1–43:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3605212.

Garay:2016:MPA

[GKM16] Juan A. Garay, Vladimir Kolesnikov, and Rae Mclellan. MAC precomputation with applications to secure memory. *ACM Transactions on Privacy and Security (TOPS)*, 19(2):6:1–6:??, September 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Gong:2018:AIA

[GL18] Neil Zhenqiang Gong and Bin Liu. Attribute inference attacks in online social networks. *ACM Transactions on Privacy and Security (TOPS)*, 21(1):3:1–3:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3154793.

Giacobazzi:2018:ANI

[GM18] Roberto Giacobazzi and Isabella Mastroeni. Abstract non-interference: A unifying framework for weakening information-flow. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):9:1–9:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3175660.

Guo:2023:MUC

[GWXY23] Chun Guo, Xiao Wang, Xiang Xie, and Yu Yu. The multi-user constrained pseudorandom function security of generalized GGM trees for MPC and hierarchical wallets. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):37:1–37:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3592608.

Humbert:2017:QIR

[HAHT17] Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and

Amalio Telenti. Quantifying interdependent risks in genomic privacy. *ACM Transactions on Privacy and Security (TOPS)*, 20(1):3:1–3:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Hoang:2023:TAA

[HCF23] Anh-Tu Hoang, Barbara Carminati, and Elena Ferrari. Time-aware anonymization of knowledge graphs. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):14:1–14:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3565026`.

Hore:2025:DPD

[HGP+25] Soumyadeep Hore, Jalal Ghadermazi, Diwas Paudel, Ankit Shah, Tapas Das, and Nathaniel Bastian. Deep PackGen: a deep reinforcement learning framework for adversarial network packet generation. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):15:1–15:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

He:2024:CCL

[HHGC24] Xinyu He, Fengrui Hao, Tianlong Gu, and Liang Chang. CBAs: Character-level backdoor attacks against Chinese pre-trained language models. *ACM Transactions on Privacy and Security (TOPS)*, 27(3):24:1–24:??, August 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3678007`.

Habib:2023:RSB

[HKHWH23] Sohail Habib, Hassan Khan, Andrew Hamilton-Wright, and Urs Hengartner. Revisiting the security of biometric authentication systems against statistical attacks. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):21:1–21:??, May 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3571743`.

Helble:2021:FMR

[HKL+21] Sarah C. Helble, Ian D. Kretz, Peter A. Loscocco, John D. Ramsdell, Paul D. Rowe, and Perry Alexander. Flexible mechanisms for remote attestation. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):29:1–29:23, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3470535`.

Hosseyni:2025:FSA

[HKW25] Pedram Hosseyni, Ralf Küsters, and Tim Würtele. Formal security analysis of the OpenID FAPI 2.0 family of protocols: Accompanying a standardization process. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):4:1–4:??, February 2025. CODEN ????

ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3699716.

Hess:2023:SPC

[HMB23] Andreas V. Hess, Sebastian A. MÖdersheim, and Achim D. Brucker. Stateful protocol composition in Isabelle/HOL. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):25:1–25:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3577020.

Hwang:2023:BSP

[HOT23] Seoyeon Hwang, Ercan Ozturk, and Gene Tsudik. Balancing security and privacy in genomic range queries. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):23:1–23:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3575796.

Hurley-Smith:2020:QLC

[HSHC20] Darren Hurley-Smith and Julio Hernandez-Castro. Quantum leap and crash: Searching and finding bias in quantum random number generators. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):16:1–16:25, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3398726.

Hayden:2025:DAD

[HWB25] Blake Hayden, Timothy Walsh, and Armon Barton. Defending against deep learning-based traffic fingerprinting attacks with adversarial examples. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):1:1–1:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3698591.

Hagen:2023:CDM

[HWS+23] Christoph Hagen, Christian Weinert, Christoph Sendner, Alexandra Dmitrienko, and Thomas Schneider. Contact discovery in mobile messengers: Low-cost attacks, quantitative analyses, and efficient mitigations. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):2:1–2:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3546191.

Hou:2023:PPR

[HWZ+23] Jian Hou, Jing Wang, Mingyue Zhang, Zhi Jin, Chunlin Wei, and Zuohua Ding. Privacy-preserving resilient consensus for multi-agent systems in a general topology structure. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):34:1–34:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (elec-

tronic). URL https://dl.acm.org/doi/10.1145/3587933.

Hoang:2020:MSO

[HYG20] Thang Hoang, Attila A. Yavuz, and Jorge Guajardo. A multi-server ORAM framework with constant client bandwidth blowup. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):1:1–1:35, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3369108.

Hu:2021:ACD

[HZL21] Zhisheng Hu, Minghui Zhu, and Peng Liu. Adaptive cyber defense against multi-stage attacks using learning-based POMDP. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):6:1–6:25, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3418897.

Idan:2022:PFP

[IF22] Lihi Idan and Joan Feigenbaum. PRShare: a framework for privacy-preserving, interorganizational data sharing. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):29:1–29:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3531225.

Iyer:2022:LRB

[IM22] Padmavathi Iyer and Amirreza Masoumzadeh. Learning relationship-based access control policies from black-box systems. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):22:1–22:36, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3517121.

Ikram:2020:MAC

[IMT+20] Muhammad Ikram, Rahat Masood, Gareth Tyson, Mohamed Ali Kaafar, Noha Loizon, and Roya Ensafi. Measuring and analysing the chain of implicit trust: a study of third-party resources loading. *ACM Transactions on Privacy and Security (TOPS)*, 23(2):8:1–8:27, May 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3380466.

Ikram:2017:MCD

[IOF+17] Muhammad Ikram, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohammed Ali Kaafar, and M. Zubair Shafiq. Measuring, characterizing, and detecting Facebook like farms. *ACM Transactions on Privacy and Security (TOPS)*, 20(4):13:1–13:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Jarecki:2021:TFP

[JJK+21] Stanislaw Jarecki, Mohammed Jubur, Hugo Krawczyk, Nitesh Saxena, and Maliheh Shirvanian. Two-factor password-authenticated key exchange with end-to-end security. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):17:1–17:37, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3446807`.

Jacomme:2021:EFA

[JK21] Charlie Jacomme and Steve Kremer. An extensive formal analysis of multi-factor authentication protocols. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):13:1–13:34, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3440712`.

Jin:2019:RPP

[JP19] Hongyu Jin and Panos Papadimitratos. Resilient privacy protection for location-based services through decentralization. *ACM Transactions on Privacy and Security (TOPS)*, 22 (4):21:1–21:??, December 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3319401`.

Jansen:2018:KKI

[JTG+18] Rob Jansen, Matthew Traudt, John Geddes, Chris Wacek, Micah Sherr, and Paul Syverson. KIST: Kernel-informed socket transport for Tor. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):3:1–3:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3278121`.

Katsis:2025:ZSM

[KB25] Charalampos Katsis and Elisa Bertino. ZT-SDN: an ML-powered zero-trust architecture for software-defined networks. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):23:1–23:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Kim:2023:LSA

[KCS+23] Dohyun Kim, Mangi Cho, Hocheol Shin, Jaehoon Kim, Juhwan Noh, and Yongdae Kim. Lightbox: Sensor attack detection for photoelectric sensors via spectrum fingerprinting. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):46:1–46:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3615867`.

King:2023:EDN

[KH23] Isaiah J. King and H. Howie Huang. Euler: Detecting network lateral movement via scalable temporal link prediction. *ACM Transactions on Privacy* and Security (TOPS), 26(3): 35:1–35:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3588771.

Khan:2020:MAS

[KHV20] Hassan Khan, Urs Hengartner, and Daniel Vogel. Mimicry attacks on smartphone keystroke authentication. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):2:1–2:34, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3372420.

Khan:2023:SAC

[KKHM23] Shaharyar Khan, Ilya Kabanov, Yunke Hua, and Stuart Madnick. A systematic analysis of the capital one data breach: Critical lessons learned. *ACM Transactions on Privacy and Security (TOPS)*, 26(1): 3:1–3:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3546068.

Kim:2018:EPP

[KKK+18] Jinsu Kim, Dongyoung Koo, Yuna Kim, Hyunsoo Yoon, Junbum Shin, and Sungwook Kim. Efficient privacy-preserving matrix factorization for recommendation via fully homomorphic encryption. *ACM Transactions on Privacy and Security (TOPS)*, 21(4):17:1–17:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3212509.

Kluban:2024:DME

[KMY24] Maryna Kluban, Mohammad Mannan, and Amr Youssef. On detecting and measuring exploitable JavaScript functions in real-world applications. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):8:1–8:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3630253.

Kim:2025:RGS

[KNGK25] Chunghyo Kim, Juhwan Noh, Esmaeil Ghahremani, and Yongdae Kim. Revisiting GPS spoofing in phasor measurement: Real-world exploitation and practical detection in power grids. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):26:1–26:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Kelbert:2018:DUC

[KP18] Florian Kelbert and Alexander Pretschner. Data usage control for distributed systems. *ACM Transactions on Privacy and Security (TOPS)*, 21(3): 12:1–12:??, June 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3183342.

Karegar:2020:DUE

[KPFH20] Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. The dilemma of user engagement in privacy notices: Effects of interaction modes and habituation on user attention. *ACM Transactions on Privacy and Security (TOPS)*, 23(1): 5:1–5:38, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3372296`.

Karunanayake:2025:QEA

[KSG+25] Naveen Karunanayake, Bhanuka Silva, Yasod Ginige, Suranga Seneviratne, and Sanjay Chawla. Quantifying and exploiting adversarial vulnerability: Gradient-based input pre-filtering for enhanced performance in black-box attacks. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):24:1–24:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Kwon:2019:SEI

[KYCP19] Donghyun Kwon, Hayoon Yi, Yeongpil Cho, and Yunheung Paek. Safe and efficient implementation of a security system on ARM using intra-level privilege separation. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):10:1–10:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3309698`.

Kreutz:2019:ALC

[KYREV19] Diego Kreutz, Jiangshan Yu, Fernando M. V. Ramos, and Paulo Esteves-Verissimo. ANCHOR: Logically centralized security for software-defined networks. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):8:1–8:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3301305`.

Lehman:2022:HPS

[LAK+22] Sarah M. Lehman, Abrar S. Alrumayh, Kunal Kolhe, Haibin Ling, and Chiu C. Tan. Hidden in plain sight: Exploring privacy risks of mobile augmented reality applications. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):26:1–26:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3524020`.

Levesque:2018:THF

[LCSF18] Fanny Lalonde Lévesque, Sonia Chiasson, Anil Somayaji, and José M. Fernandez. Technological and human factors of malware attacks: A computer security clinical trial approach. *ACM Transactions on Privacy and Security (TOPS)*, 21(4):18:1–18:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3210311`.

Li:2023:VEB

[LDT+23] Litao Li, Steven H. H. Ding, Yuan Tian, Benjamin C. M. Fung, Philippe Charland, Weihan Ou, Leo Song, and Congwei Chen. VulANalyzeR: Explainable binary vulnerability detection with multi-task learning and attentional graph convolution. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):28:1–28:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3585386.

Le:2025:AAF

[LEMS25] Hieu Le, Salma Elmalaki, Athina Markopoulou, and Zubair Shafiq. AutoFR: Automated filter rule generation for adblocking. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):11:1–11:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3703836.

Lachtar:2023:RVA

[LIKB23] Nada Lachtar, Duha Ibdah, Hamza Khan, and Anys Bacha. RansomShield: a visualization approach to defending mobile systems against ransomware. *ACM Transactions on Privacy and Security (TOPS)*, 26(3): 27:1–27:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3579822.

Lanotte:2023:ICS

[LMM23] Ruggero Lanotte, Massimo Merro, and Andrei Munteanu. Industrial control systems security via runtime enforcement. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):4:1–4:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3546579.

Lanotte:2020:FAP

[LMMV20] Ruggero Lanotte, Massimo Merro, Andrei Munteanu, and Luca Viganò. A formal approach to physics-based attacks in cyber-physical systems. *ACM Transactions on Privacy and Security (TOPS)*, 23(1): 3:1–3:41, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3373270.

Lembke:2023:SRN

[LRRE23] James Lembke, Srivatsan Ravi, Pierre-Louis Roman, and Patrick Eugster. Secure and reliable network updates. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):8:1–8:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3556542.

Landauer:2022:DSA

[LSWR22] Max Landauer, Florian Skopik, Markus Wurzenberger, and Andreas Rauber. Dealing with security alert flooding: Using machine learning for domain-independent alert aggregation. *ACM Transactions on Privacy and Security (TOPS)*, 25(3): 18:1–18:36, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3510581`.

Lu:2023:PPD

[LYS23] Yang Lu, Zhengxin Yu, and Neeraj Suri. Privacy-preserving decentralized federated learning over time-varying communication graph. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):33:1–33:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3591354`.

Markert:2021:SSU

[MBG+21] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. On the security of smartphone unlock PINs. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):30:1–30:36, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3473040`.

Maqsood:2021:DDE

[MC21] Sana Maqsood and Sonia Chiasson. Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):28:1–28:37, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3469821`.

Meylan:2021:SUC

[MCC+21] Alexandre Meylan, Mauro Cherubini, Bertil Chapuis, Mathias Humbert, Igor Bilogrevic, and Kévin Huguenin. A study on the use of checksums for integrity verification of Web downloads. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):4:1–4:36, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3410154`.

Morkonda:2025:SLP

[MCvO25] Srivathsan G. Morkonda, S. Chiasson, and P. C. van Oorschot. "Sign in with ... Privacy": Timely disclosure of privacy differences among Web SSO login options. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):16:1–16:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Meutzner:2017:TIA

[MGN+17] Hendrik Meutzner, Santosh Gupta, Viet-Hung Nguyen, Thorsten Holz, and Dorothea Kolossa. Toward improved audio CAPTCHAs based on auditory perception and language understanding. *ACM Transactions on Privacy and Security (TOPS)*, 19(4):10:1–10:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Munoz-Gonzalez:2017:EAG

[MGSPL17] Luis Muñoz-González, Daniele Sgandurra, Andrea Paudice, and Emil C. Lupu. Efficient attack graph analysis through approximate inference. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):10:1–10:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Madi:2018:IAV

[MJA+18] Taous Madi, Yosr Jarraya, Amir Alimohammadifar, Suryadipta Majumdar, Yushun Wang, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi. ISOTOP: Auditing virtual networks isolation across cloud layers in OpenStack. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):1:1–1:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3267339`.

Martins:2022:GQT

[MM22] Cláudio Martins and Ibéria Medeiros. Generating quality threat intelligence leveraging OSINT and a cyber threat unified taxonomy. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):19:1–19:39, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3530977`.

Murray:2023:CBA

[MM23] Hazel Murray and David Malone. Costs and benefits of authentication advice. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):30:1–30:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3588031`.

Mohammady:2021:MVA

[MOW+21] Meisam Mohammady, Momen Oqaily, Lingyu Wang, Yuan Hong, Habib Louafi, Makan Pourzandi, and Mourad Debbabi. A multi-view approach to preserve privacy and utility in network trace anonymization. *ACM Transactions on Privacy and Security (TOPS)*, 24 (3):14:1–14:36, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3439732`.

Matsumoto:2017:ACG

[MRS+17] Stephanos Matsumoto, Raphael M. Reischuk, Pawel Szalachowski, Tiffany Hyun-Jin Kim, and Adrian Perrig. Authentication challenges in a global environment. *ACM Transactions on Privacy and Security (TOPS)*, 20(1):1:1–1:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Mitropoulos:2016:HTY

[MSSK16] Dimitris Mitropoulos, Konstantinos Stroggylos, Diomidis Spinellis, and Angelos D. Keromytis. How to train your browser: Preventing XSS attacks using contextual script fingerprints. *ACM Transactions on Privacy and Security (TOPS)*, 19(1):2:1–2:??, August 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Mohanty:2024:FFP

[MT24] Susil Kumar Mohanty and Somanath Tripathy. Flexichain: Flexible payment channel network to defend against channel exhaustion attack. *ACM Transactions on Privacy and Security (TOPS)*, 27(4):30:1–30:??, November 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3687476`.

Modersheim:2018:ABP

[MV18] Sebastian Mödersheim and Luca Viganò. Alpha–beta privacy. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):7:1–7:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3289255`.

Mayrhofer:2021:APS

[MVBK21] René Mayrhofer, Jeffrey Vander Stoep, Chad Brubaker, and Nick Kralevich. The Android platform security model. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):19:1–19:35, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3448609`.

Neera:2025:TUC

[NCAI25] Jeyamohan Neera, Xiaomin Chen, Nauman Aslam, and Biju Issac. A trustworthy and untraceable centralised payment protocol for mobile payment. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):22:1–22:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Nabeel:2020:FPD

[NKGY20] Mohamed Nabeel, Issa M. Khalil, Bei Guan, and Ting Yu. Following passive DNS traces to detect stealthy malicious domains via graph inference. *ACM Transactions on Privacy and Security (TOPS)*, 23(4):17:1–17:36, August 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3401897.

Noh:2019:TBS

[NKS+19] Juhwan Noh, Yujin Kwon, Yunmok Son, Hocheol Shin, Dohyun Kim, Jaeyeong Choi, and Yongdae Kim. Tractor Beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Transactions on Privacy and Security (TOPS)*, 22(2): 12:1–12:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3309735.

Naor:2020:SLU

[NRS20] Moni Naor, Lior Rotem, and Gil Segev. The security of lazy users in out-of-band authentication. *ACM Transactions on Privacy and Security (TOPS)*, 23(2):9:1–9:32, May 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3377849.

Nussbaum:2022:PAQ

[NS22] Eyal Nussbaum and Michael Segal. Privacy analysis of query-set-size control. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):31:1–31:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3532774.

Noorman:2017:SLC

[NVM+17] Job Noorman, Jo Van Bulck, Jan Tobias Mühlberg, Frank Piessens, Pieter Maene, Bart Preneel, Ingrid Verbauwhede, Johannes Götzfried, Tilo Müller, and Felix Freiling. Sancus 2.0: a low-cost security architecture for IoT devices. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):7:1–7:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Oliveri:2022:LMM

[OB22] Andrea Oliveri and Davide Balzarotti. In the land of MMUs: Multiarchitecture OS-agnostic virtual memory forensics. *ACM Transactions on Privacy and Security (TOPS)*, 25 (4):27:1–27:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3528102.

Osterweil:2017:IAI

[OBC+17] Leon J. Osterweil, Matt Bishop, Heather M. Conboy, Huong Phan, Borislava I. Simidchieva, George S. Avrunin, Lori A. Clarke, and Sean Peisert. Iterative analysis to improve key properties of critical human-intensive processes: an election security example. *ACM Transactions on Privacy and Security (TOPS)*, 20(2):5:1–5:??, March 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Ottmann:2024:EAI

[OBF24] Jenny Ottmann, Frank Breitinger, and Felix Freiling. An experimental assessment of inconsistencies in memory forensics. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):2:1–2:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3628600`.

Ou:2024:VMA

[ODZ+24] Weihan Ou, Steven Ding, Mohammad Zulkernine, Li Tao Li, and Sarah Labrosse. VeriBin: a malware authorship verification approach for APT tracking through explainable and functionality-debiasing adversarial representation learning. *ACM Transactions on Privacy and Security (TOPS)*, 27(3): 26:1–26:??, August 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3669901`.

Outkin:2019:GQT

[OEG+19] Alexander V. Outkin, Brandon K. Eames, Meghan A. Galiardi, Sarah Walsh, Eric D. Vugrin, Byron Heersink, Jacob Hobbs, and Gregory D. Wyss. GPLADD: Quantifying trust in government and commercial systems: a game-theoretic approach. *ACM Transactions on Privacy and Security (TOPS)*, 22(3):18:1–18:??, July 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3326283`.

Ozalp:2016:PPP

[OGNS16] Ismet Ozalp, Mehmet Emre Gursoy, Mehmet Ercan Nergiz, and Yucel Saygin. Privacy-preserving publishing of hierarchical data. *ACM Transactions on Privacy and Security (TOPS)*, 19(3):7:1–7:??, December 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Onwuzurike:2019:MDA

[OMA+19] Lucky Onwuzurike, Enrico Mariconti, Panagiotis Andriotis, Emiliano De Cristofaro, Gordon Ross, and Gianluca Stringhini. MaMaDroid: Detecting Android malware by building Markov chains of behavioral models (extended version). *ACM Transactions on Privacy and Security (TOPS)*, 22(2):14:1–14:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3313391`.

Otoni:2023:SAS

[OMA+23] Rodrigo Otoni, Matteo Marescotti, Leonardo Alt, Patrick Eugster, Antti Hyvärinen, and Natasha Sharygina. A solicitous approach to smart contract verification. *ACM Transactions on Privacy and Security (TOPS)*, 26(2):15:1–15:??, May 2023.

CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3564699.

Oser:2022:RPI

[OvdHLK22] Pascal Oser, Rens W. van der Heijden, Stefan Lüders, and Frank Kargl. Risk prediction of IoT devices based on vulnerability analysis. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):14:1–14:36, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3510360.

Papaevripides:2021:EMB

[PA21] Michalis Papaevripides and Elias Athanasopoulos. Exploiting mixed binaries. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):7:1–7:29, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3418898.

Pagani:2022:ATA

[PB22] Fabio Pagani and Davide Balzarotti. AutoProfile: Towards automated profile generation for memory analysis. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):6:1–6:26, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3485471.

Pagani:2019:ITD

[PFB19] Fabio Pagani, Oleksii Fedorov, and Davide Balzarotti. Introducing the temporal dimension to memory forensics. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):9:1–9:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3310355.

Parker:2020:BIB

[PHR+20] James Parker, Michael Hicks, Andrew Ruef, Michelle L. Mazurek, Dave Levin, Daniel Votipka, Piotr Mardziel, and Kelsey R. Fulton. Build it, break it, fix it: Contesting secure development. *ACM Transactions on Privacy and Security (TOPS)*, 23(2):10:1–10:36, May 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3383773.

Park:2024:TRA

[PK24] Namgyu Park and Jong Kim. Toward robust ASR system against audio adversarial examples using agitated logit. *ACM Transactions on Privacy and Security (TOPS)*, 27(2):20:1–20:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3661822.

Paladini:2023:FDU

[PMP+23] Tommaso Paladini, Francesco Monti, Mario Polino, Michele Carminati, and Stefano Zanero. Fraud detection under siege: Practical poisoning attacks and defense strategies. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):45:1–45:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3613244.

Powell:2019:MOH

[Pow19] Brian A. Powell. Malicious overtones: Hunting data theft in the frequency domain with one-class learning. *ACM Transactions on Privacy and Security (TOPS)*, 22(4):22:1–22:??, December 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3360469.

Pomonis:2018:KPA

[PPK+18] Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, and Vasileios P. Kemerlis. Kernel protection against just-in-time code reuse. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):5:1–5:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3277592.

Perillo:2022:SSE

[PPT22] Angelo Massimo Perillo, Giuseppe Persiano, and Alberto Trombetta. Secure selections on encrypted multi-writer streams. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):7:1–7:33, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3485470.

Polyakov:2017:FPR

[PRSV17] Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntanathan. Fast proxy re-encryption for publish/subscribe systems. *ACM Transactions on Privacy and Security (TOPS)*, 20(4):14:1–14:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Pinkas:2018:SPS

[PSZ18] Benny Pinkas, Thomas Schneider, and Michael Zohner. Scalable private set intersection based on OT extension. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):7:1–7:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3154794.

Qian:2022:MMT

[QGS+22] Yaguan Qian, Yankai Guo, Qiqi Shao, Jiamin Wang, Bin Wang, Zhaoquan Gu, Xiang Ling, and Chunming Wu. EI-MTD: Moving target defense for edge intelligence against adversarial attacks. *ACM Transactions on*

Privacy and Security (TOPS), 25(3):23:1–23:24, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3517806`.

Qin:2022:VUF

[QPL+22] Le Qin, Fei Peng, Min Long, Raghavendra Ramachandra, and Christoph Busch. Vulnerabilities of unattended face verification systems to facial components-based presentation attacks: an empirical study. *ACM Transactions on Privacy and Security (TOPS)*, 25(1): 4:1–4:28, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3491199`.

Qiao:2024:NIB

[QWK24] Yan Qiao, Kui Wu, and Majid Khabbazian. Non-intrusive balance tomography using reinforcement learning in the lightning network. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):12:1–12:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3639366`.

Ruoti:2019:USF

[RAD+19] Scott Ruoti, Jeff Andersen, Luke Dickinson, Scott Heidbrink, Tyler Monson, Mark O'Neill, Ken Reese, Brad Spendlove, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. A usability study of four secure email tools using paired participants. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):13:1–13:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3313761`.

Reaves:2017:MBM

[RBS+17] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):11:1–11:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Rao:2019:HPR

[RCBK19] Fang-Yu Rao, Jianneng Cao, Elisa Bertino, and Murat Kantarcioglu. Hybrid private record linkage: Separating differentially private synopses from matching records. *ACM Transactions on Privacy and Security (TOPS)*, 22(3): 15:1–15:??, July 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3318462`.

Rizvi:2020:EAG

[RF20] Syed Zain Raza Rizvi and Philip W. L. Fong. Efficient authorization of graph-database queries in an attribute-supporting ReBAC model. *ACM Transactions on Privacy and Security (TOPS)*, 23(4):18:1–18:33, August 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3401027`.

Rullo:2017:POS

[RMSB17] Antonino Rullo, Daniele Midi, Edoardo Serra, and Elisa Bertino. Pareto optimal security resource allocation for Internet of Things. *ACM Transactions on Privacy and Security (TOPS)*, 20(4):15:1–15:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Rahbarinia:2016:EAB

[RPA16] Babak Rahbarinia, Roberto Perdisci, and Manos Antonakakis. Efficient and accurate behavior-based tracking of malware-control domains in large ISP networks. *ACM Transactions on Privacy and Security (TOPS)*, 19(2):4:1–4:??, September 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Ruggia:2025:DSN

[RPD+25] Antonio Ruggia, Andrea Possemato, Savino Dambra, Alessio Merlo, Simone Aonzo, and Davide Balzarotti. The dark side of native code on Android. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):13:1–13:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Ramokapane:2023:WUW

[RSR23] Kopo Marvin Ramokapane, Jose Such, and Awais Rashid. What users want from cloud deletion and the information they need: a participatory action study. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):5:1–5:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3546578`.

Reaves:2018:CSS

[RVS+18] Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R. B. Butler. Characterizing the security of the SMS ecosystem with public gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):2:1–2:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3268932`.

Sakib:2023:MIL

[SAG23] Shahnewaz Karim Sakib, George T. Amariucai, and Yong Guan. Measures of information leakage for incomplete statistical information: Application to a binary privacy mechanism. *ACM Transactions on Privacy and

Security (TOPS), 26(4):47:1–47:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3624982`.

Stobert:2018:PLC

[SB18] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):13:1–13:??, June 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3183341`.

Sharif:2019:GFA

[SBBR19] Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. A general framework for adversarial examples with objectives. *ACM Transactions on Privacy and Security (TOPS)*, 22(3):16:1–16:??, July 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3317611`.

Salem:2021:MAA

[SBP21] Aleieldin Salem, Sebastian Banescu, and Alexander Pretschner. Maat: Automatically analyzing VirusTotal for accurate labeling and effective malware detection. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):25:1–25:35, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3465361`.

Su:2017:DPM

[SCL+17] Dong Su, Jianneng Cao, Ninghui Li, Elisa Bertino, Min Lyu, and Hongxia Jin. Differentially private K-means clustering and a hybrid approach to private optimization. *ACM Transactions on Privacy and Security (TOPS)*, 20(4):16:1–16:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Sciarretta:2020:FAM

[SCRV20] Giada Sciarretta, Roberto Carbone, Silvio Ranise, and Luca Viganò. Formal analysis of mobile multi-factor authentication with single sign-on login. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):13:1–13:37, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3386685`.

Senarath:2019:WTU

[SGA19] Awanthika Senarath, Marthie Grobler, and Nalin Asanka Gamagedara Arachchilage. Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies. *ACM Transactions on Privacy and Security (TOPS)*, 22(4):23:1–23:??, December 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https:/`

/dl.acm.org/citation.cfm?id=3364224.

Sommer:2024:CCS

[SGK+24] Florian Sommer, Mona Gierl, Reiner Kriesten, Frank Kargl, and Eric Sax. Combining cyber security intelligence to refine automotive cyber threats. *ACM Transactions on Privacy and Security (TOPS)*, 27(2): 16:1–16:??, May 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3644075.

Shreeve:2021:IMB

[SHE+21] Benjamin Shreeve, Joseph Hallett, Matthew Edwards, Pauline Anthonysamy, Sylvain Frey, and Awais Rashid. "So if Mr Blue Head here clicks the link..." risk thinking in cyber security decision making. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):5:1–5:29, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3419101.

Savvides:2022:CCB

[SKSE22] Savvas Savvides, Seema Kumar, Julian James Stephen, and Patrick Eugster. C3PO: Cloud-based confidentiality-preserving continuous query processing. *ACM Transactions on Privacy and Security (TOPS)*, 25(1): 1:1–1:36, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3472717.

Shams:2025:ADU

[SL25] Sulthana Shams and Douglas Leith. Attack detection using item vector shift in matrix factorisation recommenders. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):25:1–25:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

sathi:2024:BYI

[SM24] Vipin N. Sathi and C. Siva Ram Murthy. Boost your immunity: VACCINE for preventing a novel stealthy slice selection attack in 5G and beyond. *ACM Transactions on Privacy and Security (TOPS)*, 27(4):27:1–27:??, November 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3686152.

Shi:2018:HAV

[SMA18] Hao Shi, Jelena Mirkovic, and Abdulla Alwabel. Handling anti-virtual machine techniques in malicious software. *ACM Transactions on Privacy and Security (TOPS)*, 21(1):2:1–2:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3139292.

Shi:2024:UCC

[SMGS24] Zhenpeng Shi, Nikolay Matyunin, Kalman Graffi, and David Starobinski. Uncovering CWE-CVE-CPE relations with threat knowledge graphs. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):13:1–13:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3641819.

Shrestha:2024:SBT

[SMS24] Prakash Shrestha, Ahmed Tanvir Mahdad, and Nitesh Saxena. Sound-based two-factor authentication: Vulnerabilities and redesign. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):5:1–5:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3632175.

Son:2018:GFD

[SNCK18] Yunmok Son, Juhwan Noh, Jaeyeong Choi, and Yongdae Kim. GyrosFinger: Fingerprinting drones for location tracking based on the outputs of MEMS gyroscopes. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):10:1–10:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3177751.

Shin:2020:SCW

[SNKK20] Hocheol Shin, Juhwan Noh, Dohyun Kim, and Yongdae Kim. The system that cried wolf: Sensor security analysis of wide-area smoke detectors for critical infrastructure. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):15:1–15:32, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3393926.

Scopelliti:2023:EES

[SPN+23] Gianluca Scopelliti, Sepideh Pouyanrad, Job Noorman, Fritz Alder, Christoph Baumann, Frank Piessens, and Jan Tobias Mühlberg. End-to-end security for distributed event-driven enclave applications on heterogeneous TEEs. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):39:1–39:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3592607.

Sluganovic:2018:ARE

[SRRM18] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. Analysis of reflexive eye movements for fast replay-resistant biometric authentication. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):4:1–4:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https:

//dl.acm.org/citation.cfm?id=3281745.

Swarnkar:2024:OOC

[SS24] Mayank Swarnkar and Neha Sharma. OptiClass: an optimized classifier for application layer protocols using bit level signatures. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):6:1–6:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3633777.

Stojmenovic:2022:WBS

[SSSB22] Milica Stojmenović, Eric Spero, Milos Stojmenović, and Robert Biddle. What is beautiful is secure. *ACM Transactions on Privacy and Security (TOPS)*, 25(4):30:1–30:??, November 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3533047.

Shokri:2017:PGA

[STT17] Reza Shokri, George Theodorakopoulos, and Carmela Troncoso. Privacy games along location traces: a game-theoretic framework for optimizing location privacy. *ACM Transactions on Privacy and Security (TOPS)*, 19(4):11:1–11:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Sateesan:2024:SHO

[SVS+24] Arish Sateesan, Jo Vliegen, Simon Scherrer, Hsu-Chun Hsiao, Adrian Perrig, and Nele Mentens. SPArch: a hardware-oriented sketch-based architecture for high-speed network flow measurements. *ACM Transactions on Privacy and Security (TOPS)*, 27(4):29:1–29:??, November 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3687477.

Sajid:2023:SCV

[SWAS+23] Md Sajidul Islam Sajid, Jinpeng Wei, Ehab Al-Shaer, Qi Duan, Basel Abdeen, and Latifur Khan. symbSODA: Configurable and verifiable orchestration automation for active malware deception. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):51:1–51:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3624568.

Syros:2025:BAP

[SYB+25] Georgios Syros, Gokberk Yar, Simona Boboila, Cristina Nita-Rotaru, and Alina Oprea. Backdoor attacks in peer-to-peer federated learning. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):8:1–8:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https:

//dl.acm.org/doi/10.1145/3691633.

Shu:2017:LSP

[SYRJ17] Xiaokui Shu, Danfeng (Daphne) Yao, Naren Ramakrishnan, and Trent Jaeger. Long-span program behavior modeling and attack detection. *ACM Transactions on Privacy and Security (TOPS)*, 20(4):12:1–12:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Schulmann:2024:ZMB

[SZ24] Haya Schulmann and Shujie Zhao. ZPredict: ML-based IPID side-channel measurements. *ACM Transactions on Privacy and Security (TOPS)*, 27(4):28:1–28:??, November 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3672560.

Samtani:2020:PIE

[SZC20] Sagar Samtani, Hongyi Zhu, and Hsinchun Chen. Proactively identifying emerging hacker threats from the Dark Web: a diachronic graph embedding framework (D-GEF). *ACM Transactions on Privacy and Security (TOPS)*, 23(4):21:1–21:33, August 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3409289.

Toreini:2017:TRP

[TSH17] Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. Texture to the rescue: Practical paper fingerprinting based on texture patterns. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):9:1–9:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Tang:2024:DSR

[TYH+24] Li Tang, Qingqing Ye, Haibo Hu, Qiao Xue, Yaxin Xiao, and Jin Li. DeepMark: a scalable and robust framework for DeepFake video detection. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):9:1–9:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3629976.

Ugarte-Pedrero:2018:CLD

[UPGB18] Xabier Ugarte-Pedrero, Mariano Graziano, and Davide Balzarotti. A close look at a daily dataset of malware samples. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):6:1–6:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3291061.

Usynin:2023:BGE

[URK23] Dmitrii Usynin, Daniel Rueckert, and Georgios Kaissis. Beyond gradients: Exploiting adversarial priors in model inversion attacks. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):38:1–38:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3592800`.

Vidanage:2023:VAF

[VCRS23] Anushka Vidanage, Peter Christen, Thilina Ranbaduge, and Rainer Schnell. A vulnerability assessment framework for privacy-preserving record linkage. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):36:1–36:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3589641`.

Veras:2021:LSA

[VCT21] Rafael Veras, Christopher Collins, and Julie Thorpe. A large-scale analysis of the semantic password model and linguistic patterns in passwords. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):20:1–20:21, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3448608`.

Valentim:2024:XSA

[VDMC24] Rodolfo Vieira Valentim, Idilio Drago, Marco Mellia, and Federico Cerutti. X-squatter: AI multilingual generation of cross-language sound-squatting. *ACM Transactions on Privacy and Security (TOPS)*, 27(3):21:1–21:??, August 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3663569`.

Venkatesaramani:2023:DAM

[VWMV23] Rajagopal Venkatesaramani, Zhiyu Wan, Bradley A. Malin, and Yevgeniy Vorobeychik. Defending against membership inference attacks on beacon services. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):42:1–42:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3603627`.

Wagner:2017:ESG

[Wag17] Isabel Wagner. Evaluating the strength of genomic privacy metrics. *ACM Transactions on Privacy and Security (TOPS)*, 20(1):2:1–2:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Wagner:2023:PPA

[Wag23] Isabel Wagner. Privacy policies across the ages: Content of privacy policies 1996–2021. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):32:1–32:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3590152`.

Woo:2019:UEM

[WAK+19] Simon S. Woo, Ron Artstein, Elsi Kaiser, Xiao Le, and Jelena Mirkovic. Using episodic memory for user authentication. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):11:1–11:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3308992.

Wang:2024:SAS

[WDA+24] Shen Wang, Mahshid Delavar, Muhammad Ajmal Azad, Farshad Nabizadeh, Steve Smith, and Feng Hao. Spoofing against spoofing: Toward caller ID verification in heterogeneous telecommunication systems. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):1:1–1:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3625546.

Wang:2022:CPA

[WHR+22] Xueou Wang, Xiaolu Hou, Ruben Rios, Nils Ole Tippenhauer, and Martín Ochoa. Constrained proximity attacks on mobile targets. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):10:1–10:29, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3498543.

Wiefling:2023:PPS

[WJTL23] Stephan Wiefling, Paul René Jørgensen, Sigurd Thunem, and Luigi Lo Iacono. Pump up password security! Evaluating and enhancing risk-based authentication on a real-world large-scale online service. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):6:1–6:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3546069.

Wu:2020:CPM

[WL20] Fang-Jing Wu and Tie Luo. CrowdPrivacy: Publish more useful data with less privacy exposure in crowdsourced location-based services. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):6:1–6:25, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3375752.

Wang:2024:DUE

[WML+24] Li Wang, Xiangtao Meng, Dan Li, Xuhong Zhang, Shouling Ji, and Shanqing Guo. DEEPFAKER: a unified evaluation platform for facial deepfake and detection models. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):10:1–10:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (elec-

tronic). URL https://dl.acm.org/doi/10.1145/3634914.

Wedaj:2019:DDA

[WPR19] Samuel Wedaj, Kolin Paul, and Vinay J. Ribeiro. DADS: Decentralized attestation for device swarms. *ACM Transactions on Privacy and Security (TOPS)*, 22(3):19:1–19:??, July 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3325822.

Wei:2018:APG

[WROR18] Fengguo Wei, Sankardas Roy, Xinming Ou, and Robby. Amandroid: A precise and general inter-component data flow analysis framework for security vetting of Android apps. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):14:1–14:??, June 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3183575.

Wang:2025:MAD

[WWG25] Liang Wang, Zhuangkun Wei, and Weisi Guo. Multi-agent deep reinforcement learning-based key generation for graph layer security. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):18:1–18:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Wagner:2021:DSP

[WY21] Isabel Wagner and Iryna Yevseyeva. Designing strong privacy metrics suites using evolutionary optimization. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):12:1–12:35, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3439405.

Wang:2023:NCN

[WYW+23] Huanran Wang, Wu Yang, Wei Wang, Dapeng Man, and Jiguang Lv. A novel cross-network embedding for anchor link prediction with social adversarial attacks. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):7:1–7:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3548685.

Yang:2025:SSI

[YLJW25] Yuxin Yang, Qiang Li, Yuede Ji, and Binghui Wang. A secret sharing-inspired robust distributed backdoor attack to federated learning. *ACM Transactions on Privacy and Security (TOPS)*, 28(2):27:1–27:??, May 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Yan:2019:DAW

[YLV+19] Chao Yan, Bo Li, Yevgeniy Vorobeychik, Aron Laszka, Daniel Fabbri, and Bradley Malin. Database audit workload prioritization via game theory. *ACM Transactions on Privacy and Security (TOPS)*, 22(3): 17:1–17:??, July 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3323924`.

Ye:2018:VBA

[YTF+18] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Willy Wolff, Adam J. Aviv, and Zheng Wang. A video-based attack for Android pattern lock. *ACM Transactions on Privacy and Security (TOPS)*, 21(4):19:1–19:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3230740`.

Ye:2020:UGA

[YTF+20] Guixin Ye, Zhanyong Tang, Dingyi Fang, Zhanxing Zhu, Yansong Feng, Pengfei Xu, Xiaojiang Chen, Jungong Han, and Zheng Wang. Using generative adversarial networks to break and protect text captchas. *ACM Transactions on Privacy and Security (TOPS)*, 23(2): 7:1–7:29, May 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3378446`.

Yuan:2025:AAD

[YZC+25] Xuejing Yuan, Jiangshan Zhang, Kai Chen, Cheng'an Wei, Ruiyuan Li, Zhenkun Ma, and Xinqi Ling. Adversarial attack and defense for commercial black-box Chinese–English speech recognition systems. *ACM Transactions on Privacy and Security (TOPS)*, 28 (1):10:1–10:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3701725`.

Zhao:2021:EBS

[ZAK+21] Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Mohamed Ali Kaafar, Francesca Trevisan, and Haiyue Yuan. Exploiting behavioral side channels in observation resilient cognitive authentication schemes. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):1:1–1:33, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3414844`.

Zhang:2018:ISP

[ZBA18] Yihua Zhang, Marina Blanton, and Ghada Almashaqbeh. Implementing support for pointers to private data in a general-purpose secure multi-party compiler. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):6:1–6:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3154600`.

Zhuo:2023:SHC

[ZBK+23] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. SoK: Human-centered phishing susceptibility. *ACM Transactions on Privacy and Security (TOPS)*, 26(3):24:1–24:??, August 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3575797.

Zheng:2025:DPP

[ZCL+25] Haibin Zheng, Jinyin Chen, Tao Liu, Yao Cheng, Zhao Wang, Yun Wang, Lan Gao, Shouling Ji, and Xuhong Zhang. DP-Poison: Poisoning federated learning under the cover of differential privacy. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):7:1–7:??, February 2025. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3702325.

Zhao:2018:FFI

[ZD18] Siqi Zhao and Xuhua Ding. FIMCE: A fully isolated micro-computing environment for multicore systems. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):15:1–15:??, June 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3195181.

Zolotavkin:2022:IUA

[ZJK+22] Yevhen Zolotavkin, Jongkil Jay Jeong, Veronika Kuchta, Maksym Slavnenko, and Robin Doss. Improving unlinkability of attribute-based authentication through game theory. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):12:1–12:36, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3501260.

Zhang:2023:DPR

[ZKL23] Xueru Zhang, Mohammad Mahdi Khalili, and Mingyan Liu. Differentially private real-time release of sequential data. *ACM Transactions on Privacy and Security (TOPS)*, 26(1):1:1–1:??, February 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3544837.

Zeng:2024:ESH

[ZLD+24] Yong Zeng, Jiale Liu, Tong Dong, Qingqi Pei, Jianfeng Ma, and Yao Liu. Eyes see hazy while algorithms recognize who you are. *ACM Transactions on Privacy and Security (TOPS)*, 27(1):7:1–7:??, February 2024. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3632292.

Zhang:2018:VGP

[ZPK18] Yupeng Zhang, Charalampos

Papamanthou, and Jonathan Katz. Verifiable graph processing. *ACM Transactions on Privacy and Security (TOPS)*, 21 (4):20:1–20:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3233181`.

Zhang:2023:SQE

[ZZYY23] Chenhan Zhang, Shiyao Zhang, James J. Q. Yu, and Shui Yu. SAM: Query-efficient adversarial attacks against graph neural networks. *ACM Transactions on Privacy and Security (TOPS)*, 26(4):49:1–49:??, November 2023. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3611307`.