Active learning-based mobile malware detection utilizing auto-labeling and data drift detection
Deng, Zhe; Hubert, Arthur; **Ben Yahia, Sadok**; **Bahsi, Hayretdin** Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience, CSR 2024 2024 / p. 146 - 151 https://doi.org/10.1109/CSR61664.2024.10679343 Article at Scopus Article at WOS

Alliance attribution of global cyber attacks : the European Union
Alatalu, Siim National cyber emergencies: the return to civil defence 2020 / p. 171-185 https://doi.org/10.4324/9780429343438

Android malware concept drift using system calls : detection, characterization and challenges
Guerra Manzanares, Alejandro; Luckner, Marcin; **Bahsi, Hayretdin** Expert systems with applications 2022 / art. 117200, 19 p. : ill https://doi.org/10.1016/j.eswa.2022.117200 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Art and automation of teaching malware reverse engineering
Lepik, Toomas; **Maennel, Kaie**; **Ernits, Margus**; **Maennel, Olaf Manuel** Learning and Collaboration Technologies : Learning and Teaching : 5th International Conference : LCT 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018 : Proceedings, Part II 2018 / p. 461-472 https://doi.org/10.1007/978-3-319-91152-6_35 Conference Proceedings at Scopus Article at Scopus Conference Proceedings at WOS Article at WOS

Arvuti riistvarasse peidetud troojalane pakub häkkeritele hõlbuelu [Võrguväljaanne]
Oidermaa, Jaan-Juhan novaator.err.ee 2022 "Arvuti riistvarasse peidetud troojalane pakub häkkeritele hõlbuelu"

Assessment of malicious tweets impact on stock market prices
Ishikawa, Tatsuki; **Ben Sassi, Imen**; **Ben Yahia, Sadok** Research Challenges in Information Science : 15th International Conference, RCIS 2021, Limassol, Cyprus, May 11–14, 2021 : proceedings 2021 / p. 330–346 https://doi.org/10.1007/978-3-030-75018-3_22 Conference Proceedings at Scopus Article at Scopus Article at WOS

Benchmarking advanced security closure of physical layouts
Eslami, Mohammad; Knechtel, Johann; Sinanoglu, Ozgur; Karri, Ramesh; **Pagliarini, Samuel Nascimento** ISPD '23 : proceedings of the 2023 International Symposium on Physical Design 2023 / p. 256-264 https://doi.org/10.1145/3569052.3578924 https://dl.acm.org/doi/pdf/10.1145/3569052.3578924

Concept drift and cross-device behavior : challenges and implications for effective android malware detection
Guerra Manzanares, Alejandro; Luckner, Marcin; Bahsi, Hayretdin Computers & Security 2022 / art. 102757, 20 p. : ill https://doi.org/10.1016/j.cose.2022.102757 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Corrigendum to Concept drift and cross-device behavior: Challenges and implications for effective android malware detection Computers & Security, Volume 120, 102757 (Computers & Security (2022) 120, (S0167404822001523), (10.1016/j.cose.2022.102757))
Guerra-Manzanares, Alejandro; **Luckner, Marcin**; **Bahsi, Hayretdin** Computers and Security 2023 / art. 102998 https://doi.org/10.1016/j.cose.2022.102998 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Cross-device behavioral consistency : benchmarking and implications for effective android malware detection
Guerra Manzanares, Alejandro; **Välbe, Martin** Machine Learning with Applications 2022 / art. 100357, 15 p. : ill https://doi.org/10.1016/j.mlwa.2022.100357

Differences in Android behavior between real device and emulator : a malware detection perspective
Guerra Manzanares, Alejandro; **Bahsi, Hayretdin**; **Nõmm, Sven** 6th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, October 22-25, 2019 2019 / art. 8939268, p. 399-404 https://doi.org/10.1109/IOTSMS48152.2019.8939268

Experts still needed : boosting long-term android malware detection with active learning
Guerra-Manzanares, Alejandro; **Bahsi, Hayretdin** Journal of Computer Virology and Hacking Techniques 2024 / p. 901 - 918 https://doi.org/10.1007/s11416-024-00536-y Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Explainable federated learning for Botnet Detection in IoT networks
Kalakoti, Rajesh; **Bahsi, Hayretdin**; **Nõmm, Sven** Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR), September 2-4, 2024, London, UK 2024 / p. 22-29 https://doi.org/10.1109/CSR61664.2024.10679348 Article at Scopus Article at WOS

Improving IoT security with explainable AI : quantitative evaluation of explainability for IoT botnet detection
Kalakoti, Rajesh; **Bahsi, Hayretdin**; **Nõmm, Sven** IEEE Internet of Things Journal 2024 / p. 18237 - 18254 https://doi.org/10.1109/JIOT.2024.3360626 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

In-depth feature selection and ranking for automated detection of mobile malware
Guerra Manzanares, Alejandro; **Nõmm, Sven**; **Bahsi, Hayretdin** Proceedings of the 5th International Conference on Information Systems Security and Privacy : ICISSP 2019 : February 23-25, 2019, Prague, Czech Republic. Vol. 1 2019 / p. 274-283 : ill

https://doi.org/10.5220/0007349602740283

Integrating Cyber Threat Intelligence into Threat Modeling for Autonomous Ships Using PASTA and MISP
Erbas, Muhammed; Vanharanta, Jani; Paavola, Jarkko; **Tsiopoulos, Leonidas**; **Vaarandi, Risto** 2025 IEEE International Conference on Cyber Security and Resilience (CSR) 2025 / p. 133-139 https://ieeexplore.ieee.org/document/11130108 http://doi.org/10.1109/CSR64739.2025.11130108

KronoDroid : time-based hybrid-featured dataset for effective android malware detection and characterization
Guerra Manzanares, Alejandro; **Bahsi, Hayretdin**; **Nõmm, Sven** Computers & Security 2021 / art. 102399, 32 p https://doi.org/10.1016/j.cose.2021.102399 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Küberohud meie nina all: 4 igapäevast turvariski, mida tõsiselt ei võeta [Võrguväljaanne]
digipro.geenius.ee 2022 Küberohud meie nina all: 4 igapäevast turvariski, mida tõsiselt ei võeta

Latest trends in hardware security and privacy
Di Natale, Giorgio; Regazzoni, Francesco; Albanese, Vincent; Lhermet, Frank; Loisel, Yann; Sensaoui, Abderrahmane; **Pagliarini, Samuel Nascimento** 33rd IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) : ESA-ESRIN, Italy (On-line Virtual Event),October 19–21, 2020 2020 / 4 p. : ill https://doi.org/10.1109/DFT50435.2020.9250816

Leveraging the first line of defense : a study on the evolution and usage of android security permissions for enhanced android malware detection
Guerra Manzanares, Alejandro; Luckner, Marcin; **Bahsi, Hayretdin** Journal of Computer Virology and Hacking Techniques 2022 / 32 p. : ill https://doi.org/10.1007/s11416-022-00432-3 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Machine learning for android malware detection : mission accomplished? a comprehensive review of open challenges and future perspectives
Guerra-Manzanares, Alejandro Computers and Security 2024 / art. 103654 https://doi.org/10.1016/j.cose.2023.103654 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Machine learning-based detection and characterization of evolving threats in mobile and IoT Systems = Masinõppepõhine arenevate ohtude tuvastamine ning kirjeldamine mobiilseadmete ja värkvõrkude jaoks
Guerra Manzanares, Alejandro 2022 https://doi.org/10.23658/taltech.54/2022 https://digikogu.taltech.ee/et/Item/f56ae778-e5a5-4147-a8e4-4833e08fa789 https://www.ester.ee/record=b5511898*est

Mobiilse pahavara plahvatusele võib pakkuda leevendust masinõpe [Võrguväljaanne]
Oidermaa, Jaan-Juhan novaator.err.ee 2022 Mobiilse pahavara plahvatusele võib pakkuda leevendust masinõpe

Network IDS alert classification with active learning techniques
Vaarandi, Risto; Guerra-Manzanares, Alejandro Journal of Information Security and Applications 2024 / art. 103687 https://doi.org/10.1016/j.jisa.2023.103687 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

On the application of active learning to handle data evolution in Android malware detection
Guerra Manzanares, Alejandro; **Bahsi, Hayretdin** Digital forensics and cyber crime : 13th EAI international conference, ICDF2C 2022, Boston, MA, November 16-18, 2022 : proceedings 2023 / p. 256-273 https://doi.org/10.1007/978-3-031-36574-4_15

On the relativity of time : implications and challenges of data drift on long-term effective android malware detection
Guerra Manzanares, Alejandro; **Bahsi, Hayretdin** Computers & Security 2022 / art. 102835, 15 p. : ill https://doi.org/10.1016/j.cose.2022.102835 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

On the use of defensive schemes for hardware security = Kaitseskeemid riistvara turvalisuse tagamiseks
Eslami, Mohammad 2024 https://www.ester.ee/record=b5701420*est https://doi.org/10.23658/taltech.53/2024 https://digikogu.taltech.ee/et/Item/068530be-4810-4489-9604-fb838d298b45

Ransomware attack as Hardware Trojan : a feasibility and demonstration study
Almeida, Felipe; **Imran, Malik**; **Raik, Jaan**; **Pagliarini, Samuel Nascimento** IEEE Access 2022 / p. 44827-44839 https://doi.org/10.1109/ACCESS.2022.3168991 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Reusing verification assertions as security checkers for Hardware Trojan detection
Eslami, Mohammad; **Ghasempouri, Tara**; **Pagliarini, Samuel Nascimento** 2022 23rd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA : 06-07 April 2022 2022 / p. 1-6 : ill https://doi.org/10.1109/ISQED54688.2022.9806292

SALSy : security-aware layout synthesis
Eslami, Mohammad; **Perez, Tiago Diadami**; **Pagliarini, Samuel Nascimento** arXiv.org 2024 / 13 p. : ill https://doi.org/10.48550/arXiv.2308.06201

SCARF : securing chips with a robust framework against fabrication-time hardware trojans
Eslami, Mohammad; **Ghasempouri, Tara**; **Pagliarini, Samuel Nascimento** IEEE Transactions on Computers 2024 / p. 2761-2775 https://doi.org/10.1109/TC.2024.3449082 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

SCARF : securing chips with a robust framework against fabrication-time hardware Trojans : preprint
Eslami, Mohammad; **Ghasempouri, Tara**; **Pagliarini, Samuel Nascimento** arXiv.org 2024 / 14 p. : ill https://doi.org/10.48550/arXiv.2402.12162

Signature-based approach to detecting malicious outgoing traffic
Petliak, Nataliia; Klots, Yurii; Titova, Vira; Cheshun, Viktor; **Boyarchuk, Artem** IntelITSIS 2023: Intelligent Information Technologies & Systems of Information Security 2023 : proceedings of the 4th International Workshop on Intelligent Information Technologies & Systems of Information Security : Khmelnytskyi, Ukraine, March 22-24, 2023 2023 / p. 486 - 506 https://ceur-ws.org/Vol-3373/paper33.pdf Conference Proceedings at Scopus Article at Scopus

Time-frame analysis of system calls behavior in machine learning-based mobile malware detection
Guerra Manzanares, Alejandro; **Nõmm, Sven**; **Bahsi, Hayretdin** 2019 International Conference on Cyber Security for Emerging Technologies : CSET 2019, Doha, Qatar, 27 October 2019 through 29 October 2019 2019 / art. 89049088 ; 8 p. : ill https://doi.org/10.1109/CSET.2019.8904908