CURRICULUM VITAE

VYRON KAMPOURAKIS

Ph.D. Candidate & Research Fellow

Dept. of Information Security and Communication Technology
Norwegian University of Science and Technology

Gjøvik, Norway, September 30, 2025

Contents

1 CURRICULUM VITAE

1.1 Personal Information

Full Name:	Vyron Kampourakis
Date of Birth:	18th of Jul. 1998
Postal Address:	Teknologivegen 22, 2815 Gjøvik, Norway (Google maps)
Office:	Topasbygget, 435
Tel.:	+30 6955396586
E-mail:	vyron.kampourakis@ntnu.no
URL:	https://www.ntnu.edu/employees/vyron.kampourakis
Google Scholar:	Click
DBLP:	Click
Scopus Author ID:	Click
ORCID iD:	Click
Research Gate:	Click
LinkedIn:	Click

1.2 Research Interests

Network Security; Critical Infrastructure Protection; Cyber-Physical Systems Security; Security Education.

1.3 Current Occupation

Ph.D. Candidate and Research Fellow, Dept. of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway.

1.4 Studies/Degrees Obtained

- University of Patras, School of Engineering, Dept. of Computer Engineering and Informatics, Master of Engineering (M.Eng.), 2022.

1.5 Experience

1.5.1 R&D Activities

International Projects

- EUROPEAN DEFENCE FUND (EDF) 2022, "FACT: Federated Advanced Cyber physical Test range", Project ID 101121335, Norwegian University of Science and Technology (15.11.2024-14.05.2025).

1.5.2 Employment History

- Research Fellow, Dept. of Information Security and Communication Technology, Norwegian University of Science and Technology (2022+).

1.6 Research Record & List of Publications

1.6.1 Journal Publications (peer review)

J1. Alexandros Perrakis, E. Chatzoglou, V. Kampourakis, G. Kambourakis, "Cloud in the Crosshairs: Exposing Vulnerabilities Across Open-Source Cloud Platforms", International Journal of Information Security, Springer. [Under review]

J2. V. Kampourakis, G. Kavallieratos, V. Gkioulos, S. Katsikas, "Cracks in the Chain: A Technical Analysis of Real-Life Supply Chain Security Incidents", Computers & Security, Vol. 159, p. 104673, Elsevier.**[Contributed the Supply Chain Incidents dataset].

J3. Koffi A. Koffi, V. Kampourakis, J. Song, C. Kolias, R. C. Ivans, "Speeding-up fuzzing through directional seeds", International Journal of Information Security Vol. 24 (2), p. 77, 2025, Springer. [**IF**: 3.2]

J4. E. Chatzoglou, V. Kampourakis, Z. Tsiatsikas, G. Karopoulos, G. Kambourakis, "Unmasking the Hidden Credential Leaks in Password Managers and VPN Clients", Computers & Security, Vol. 150, p. 104298, 2025, Elsevier. [**IF**: 5.4]

J5. V. Kampourakis, V. Gkioulos, S. Katsikas, "A step-by-step definition of a reference architecture for cyber ranges", Journal of Information Security and Applications, Vol. 88, p. 103917, 2025, Elsevier. [**IF**: 3.7]

J6. Koffi A. Koffi, V. Kampourakis, J. Song, C. Kolias, R. C. Ivans, "StructuredFuzzer: Fuzzing Structured Text-Based Control Logic Applications", Electronics Vol. 13 (13), p. 2475, 2024, MDPI. [**IF**: 2.6]

J7. V. Kampourakis, G. M. Makrakis, C. Kolias, "From Seek-and-Destroy to Split-and-Destroy: Connection Partitioning as an Effective Tool against Low-Rate DoS Attacks", Future Internet Vol. 16 (4), p. 137, 2024, MDPI. [**IF**: 3.6] **[Contributed the Partitioning Defense Strategy Simulator and the Split and Destroy dataset].

J8. V. Kampourakis, V. Gkioulos, S. Katsikas, "A systematic literature review on wireless security testbeds in the cyber-physical realm", Computers & Security, Vol. 133, p. 103383, 2023, Elsevier. [**IF**: 5.4]

J9. V. Kampourakis, E. Chatzoglou, G. Kambourakis, A. Dolmes, C. Zaroliagis, "WPAxFuzz: Sniffing Out Vulnerabilities in Wi-Fi Implementations", Cryptography, Vol. 6(4), No. 53, pp. 1-12, 2022, MDPI. [**IF**: 2.1] **[Contributed the WPAxFuzz Wi-Fi fuzzer].

J10. V. Kampourakis, G. Kambourakis, E. Chatzoglou, C. Zaroliagis, "Revisiting man in the middle attacks against HTTP", Network Security, Vol. 2022, No. 3, 2022, MAG.

1.6.2 Refereed Conference Proceedings with full paper

C1. V. Kampourakis, C. Smiliotopoulos, V. Gkioulos, S. Katsikas, "In Numeris Veritas: An Empirical Measurement of Wi-Fi Integration in Industry", The 11th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS 2025), 2025, Springer, LNCS. [Accepted]

C2. E. Chatzoglou, V. Kampourakis, Z. Tsiatsikas, G. Karopoulos, G. Kambourakis, "Keep your memory dump shut: Unveiling data leaks in password managers", The 39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2024), 2024, Springer, DOI: 10.1007/978-3-031-65175-5_5. [**CORE**: B] **[Nominated for best paper award].

C3. E. Chatzoglou, V. Kampourakis, G. Kambourakis, "Bl0ck: Paralyzing 802.11 connections through Block Ack frames", The 38th International Conference on ICT Systems Security and Privacy Protection (IFIPSEC 2023), 2023, Springer, DOI: 10.1007/978-3-031-56326-3_18. [**CORE**: B] **[Contributed the Bl0ck Wi-Fi DoS attack tool].

C4. V. Kampourakis, "Secure infrastructures for cyber-physical ranges", Research Challenges in Information Science: Information Science and the Connected World (RCIS 2023), 2023, Springer, DOI: 10.1007/978-3-031-33080-3_45. [**CORE**: B]

1.6.3 Refereed Conference without full paper Proceedings

XC1. E. Chatzoglou, V. Kampourakis, Z. Tsiatsikas, "Pandora: Exploit Password Management Software To Obtain Credential From Memory", Black Hat Arsenal Europe, 2024. Link

1.7 Editing & Conference Organization Activities

1.7.1 Journals: Reviewer

- *Computers & Security (COSE)*, Elsevier.
- *Computer Communications (COMCOM)*, Elsevier.
- *Journal of Information Security and Applications (JISA)*, Elsevier.
- *International Journal of Information Security (IJIS)*, Springer.
- *Future Internet*, MDPI.
- *The Computer Journal (COMPJ)*, Oxford University Press.
- *Computers, Materials & Continua (CMC)*, Tech Science Press.
- *Journal of Cyber Security*, Tech Science Press.
- *Journal of Internet Services and Applications (JISA)*, Brazilian Computer Society (Sociedade Brasileira de Computação, SBC).

1.7.2 Conferences & Workshops: Reviewer

- The 26th International Conference on Web Information Systems Engineering (WISE 2025), (Marrakesh : Morocco), Dec. 15-17, 2025, Springer LNCS.
- The 21st International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2025) (Marrakesh : Morocco), Oct. 20-21, 2025, IEEE Press.
- The 27th International Conference on Information and Communications Security (ICICS 2025) (Nanjing : China), October 29-31, 2025, Springer LNCS.
- The 22nd International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2025) (Ghent : Belgium), August 11-14, 2025, Springer LNCS.

- The 1st International Conference on the Design of Cyber-Secure Water Plants (DCS-Water'24) (Buford, GA : United States), April 23-24, 2024.

1.8 Other Achievements

1.8.1 CVE IDs

The Common Vulnerabilities and Exposures (CVE) system provides a standardized reference for publicly known information security vulnerabilities and exposures. A CVE rating is a score between 1-10 that measures the severity of a vulnerability, i.e., how catastrophic the damage would be if a threat actor exploited a given vulnerability.

- **Critical Severity**: -
- **High Severity**: CVE-2022-32666 (7.5), CVE-2024-20137 (7.5).
- **Medium Severity**: CVE-2022-46740 (6.5), CVE-2022-32659 (6.7), CVE-2022-32658 (6.7), CVE-2022-32657 (6.7), CVE-2022-32656 (6.7), CVE-2022-32655 (6.7), CVE-2022-32654 (6.7), CVE-2024-50570 (5.0).
- **Low Severity**: CVE-2023-23349 (2.2), CVE-2024-9203 (2.0).

1.8.2 Open-Source Contributions

- WPAxFuzz, A full-featured open-source Wi-Fi fuzzer capable of fuzzing either any management, control, or data frames of the 802.11 protocol or the SAE exchange. [Major Contr.]
- Bl0ck, A Wi-Fi DoS tool that interrupts the transmission of QoS Data frames in Wi-Fi 5 and 6 networks. [Major Contr.]
- Pandora, A red team tool that assists in extracting/dumping master credentials and/or entries from different password managers. [Minor Contr.]
- Partitioning Defense Strategy Simulator, A simulator for connection partitioning as a tool against Low-Rate DoS attacks. [Major Contr.]
- Split and Destroy Data, Times for the checkpoint and restore of connections and their data in a Docker environment, as well as the results from the simulation part for the connections partitioning. [Major Contr.]
- Industrial WiFi dataset, Dataset of high-confidence industrial Wi-Fi networks. [Major Contr.]
- Supply Chain Incidents dataset, An elementary dataset that organizes the findings in a structured, machine-readable format, facilitating further research and analysis, including threat intelligence, incident response planning, and predictive analytics based on the documented real-world incidents. [Major Contr.]