

CYBERSECURITY DEFENCE AND ATTACK RESILIENCE LAB

Contact details

Name	Cybersecurity Defence and Attack Resilience (CYDAR) Lab Ro: Laboratorul de securitate pentru apărare și reziliență la atacuri cibernetice	N/A
Acronym	CYDAR	
Logo	Not yet established	
Site	https://os.cs.utcluj.ro/cydar	
Address	Barițiu 26-28, Room M02	
Faculty Department	Automation and Computer Science Computer Science	
Telephone	+40 264 401 478	
Fax	-	
Director	Associate Professor Adrian Coleșa	
e-mail	adrian.colesa@cs.utcluj.ro	

Areas of expertise

Malware Analysis, Ai and Big-Data Applied in Cybersecurity, Adversarial Emulation, Malicious Behavior Detection, Operating System Security, Virtualization-Based Security, Random Number Generation and Evaluation, Digital Identity Privacy and Protection

Team

Professor Alin Suci, Associate Professor Adrian Coleșa, Associate Professor Ciprian Oprea, Assistant Professor Kinga Marton, Assistant Professor Marius Joldos, Teaching Assistant Istvan Csaszar, PhD Radu Portase, PhD students: Andrei Muntea, Andrei Sântoma, Andrei Mihalca

Representative projects

- 2024 – 2026: “Cybersecurity Seminars”; Owner: Technical University of Cluj-Napoca (TUCN); Role: Director – Adrian Coleșa; Funder: Google.org (through Silicon Valley Community Foundation); Budget: 500,000 US \$
- 2023 – 2025: *CONSOLE*, GA 101128070; Owner: Bitdefender; Role: Technical coordinator (Bitdefender) – Ciprian Oprea; Funder: European Union's Digital Europe Program
- 2020 – 2022: *GEIGER Cybersecurity Counter*, UE, H2020-SU-DS03, Grant 883588/2020; Owner: ClujIT; Role: research member – Adrian Coleșa, Ciprian Oprea
- 2017 – 2020: *SMESEC*, GA 740787; Owner: Atos; Role: Technical coordinator (Bitdefender) – Ciprian Oprea; Funder European Union's Horizon 2020 Program
- 2017 – 2018: Grant 230PED/2017, PN-III-P2-2.1-PED-2016-2073 from UEFISCDI, “*STARG-VM: Server Triggered Protection of Client Applications by Running Their Security-Sensitive Phases in a Trusted VM*”; Owner: Technical University of Cluj-Napoca; Role: Director – Adrian Coleșa; Funder: Romanian Ministry of Education and Scientific Research, Budget: about 100,000 Euro (521,739 Ron)
- 2013 – 2018: *Industry funded research*, TUCN contract no. 44/24.05.2013 (renewed yearly); “*Research of virtualization-based security solutions*”; Owner: Technical University of Cluj-Napoca; Role: Director – Adrian Coleșa; Funder: Bitdefender, Romania; Budget: about 150,000 Euro

Significant results

Articles in ISI rated journals, in the past 5 years

- Bolundut, R.M., Coleșa, A. and Portase R.M. "A Path Sensitive and Scalable Approach for Mapping the Capabilities Required for Linux Kernel Defined System Calls Using Static Analysis Techniques." *IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2024.

2. Șandor, M, Portase, R, and Colesa, A. "Enhancing ML Model Resilience to Time-Evolving Data in Malware Detection Systems with Adversarial Learning." *IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2024.
3. Portase, Radu Marian, et al. "LEDA—Layered Event-Based Malware Detection Architecture." *Sensors* 24.19 (2024): 6393.
4. Portase, Radu Marian, Adrian Colesa, and Gheorghe Sebestyen. "SpecRep: Adversary Emulation Based on Attack Objective Specification in Heterogeneous Infrastructures." *Sensors* 24.17 (2024): 5601.
5. Portase, Radu Marian, et al. "Detection Strategies for COM, WMI, and ALPC-Based Multi-Process Malware." *Sensors (Basel, Switzerland)* 24.16 (2024): 5118.
6. Petrean, D. E., Potolea, R and Oprisa, C. "Packed Code Detection using Shannon Entropy and Homomorphic Encrypted Executables." *IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2024.
7. Portase, R. M., Coleșa, A. and Sebestyen, G. "Efficient Multi-Stage Detection of Malicious Windows Executable During Execution." *IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
8. Șandor, Marian, Radu Marian Portase, and Adrian Coleșa. "Ember Feature Dataset Analysis For Malware Detection." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
9. Mihalca, Andrei Vasile, and Ciprian Pavel Oprea. "Impact of Library Code in Binary Similarity Systems." *International Conference on Ubiquitous Security*. Singapore: Springer Nature Singapore, 2023.
10. Păcurar, Aralda, and Ciprian Oprea. "Using Artificial Intelligence to Fight Clickbait in Romanian News Articles." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
11. Moșolea, V., and Oprea, C. "Detecting Domain Generation Algorithms in Malware Traffic Using Constrained Resources." *IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
12. Mărmureanu, Marius, and Ciprian Oprea. "MITRE Tactics Inference from Splunk Queries." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
13. Fălămaș, Diana-Elena, Kinga Marton, and Alin Suciu. "Assessment of two privacy preserving authentication methods using secure multiparty computation based on secret sharing." *Symmetry* 13.5 (2021): 894.
14. Suciu, Alin, et al. "Parallel implementation of a PIC simulation algorithm using OpenMP." *15th Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2020.
15. Marton, Kinga, et al. "COSTS AND BENEFITS OF ADAPTIVE TESTING IN ASSESSMENT OF RANDOM NUMBER SEQUENCES." *PROCEEDINGS OF THE ROMANIAN ACADEMY SERIES A-MATHEMATICS PHYSICS TECHNICAL SCIENCES INFORMATION SCIENCE* 21.1 (2020): 37-44.

Significant solutions

N/A

Products and technologies

N/A

Patents

1. Lukacs, Sandor, and **Adrian V. Colesa**. "Anti-malware systems and methods using hardware-assisted code injection." U.S. Patent No. 9,881,157. 30 Jan. 2018. <https://patents.google.com/patent/US9881157B1/en>
2. Lukacs, Sandor, Radu I Ciocas, Vlad I Topan, **Adrian V Colesa**, Raul V Tosa. "Enabling a secure environment through operating system switching." U.S. Patent No. 9,563,457. 7 Feb. 2017. <https://patents.google.com/patent/US9563457B2/en>
3. Lukacs, Sandor, and **Adrian V. Colesa**. "Systems and methods for batch processing of samples using a bare-metal computer security appliance." U.S. Patent No. 9,507,939. 29 Nov. 2016. <https://patents.google.com/patent/US9507939B1/en>
4. Lukacs, Sandor, and **Adrian V. Colesa**. "Bare-metal computer security appliance." U.S. Patent No. 9,383,934. 5 Jul. 2016. <https://patents.google.com/patent/US9383934B1/en>
5. Lukacs, Sandor, and **Adrian V. Colesa**. "Below-OS security solution for distributed network endpoints." U.S. Patent No. 9,319,380. 19 Apr. 2016. <https://patents.google.com/patent/US9319380B2/en>
6. Lukacs, Sandor, Dan H. Lutas, and **Adrian V. Colesa**. "Strongly isolated malware scanning using secure virtual containers." U.S. Patent No. 9,117,081. 25 Aug. 2015. <https://patents.google.com/patent/US9117081B2/en>

The offer addressed to the economic environment

Research & development	Our research fields are of direct interest to cybersecurity companies. In this area we have had successful cooperations with such companies. Our results are also important to any company that wants to protect its assets. They are also important to socio- economic stakeholders, including local community organizations, while contributing to a safe digital ecosystem is of critical importance to everyone.
Consulting	We could provide consultancy on different fields of cybersecurity, especially in malware analysis and OS security mechanisms.
Training	We used to keep cybersecurity trainings (awareness or technical focused) for SMEs in different projects we were members in.