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 ciberbetice	*N/A*
Acronym	**CYDAR**	
Logo	Not yet established	
Site	https://os.cs.utcluj.ro/cydar	
Address	Bariţiu 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 Suciu, Associate Professor Adrian Coleșa, Associate Professor Ciprian Oprișa, Assistant Professor Kinga Marton, Teaching Assistant, PhD Student, Istvan Csaszar

Representative projects

1. 2023 – 2025: CONSOLE, GA 101128070, owner: Bitdefender, role: Technical coordinator (Bitdefender) - Ciprian Oprișa, funder: European Union's Digital Europe Program
2. 2020 – 2022: GEIGER Cybersecurity Counter, UE, H2020-SU-DS03, Grant 883588/2020; Owner: ClujIT; Role: research member – Adrian Coleșa, Ciprian Oprișa
3. 2017 – 2020: SMESEC, GA 740787, owner: Atos, role: Technical coordinator (Bitdefender) – Ciprian Oprișa, funder European Union’s Horizon 2020 Program
4. 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)
5. 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
6. 2014 – 2015: Innovative project POSCCE/SMIS 49752 - “Feasibility study and design of a software subsystem for providing high-availability for Cloud software services”; Owner: Technical University of Cluj-Napoca; Role: work package (subproject) responsible – Adrian Coleșa; Funder: Romanian Ministry of Education and Scientific Research; Budget: about 30,000 Euro (assigned subproject)

Significant results

Articles in ISI rated journals, in the past 5 years

1. Portase, Radu-Marian, Adrian Coleşa, and Gheorghe Sebestyen. "Efficient Multi-Stage Detection of Malicious Windows Executable During Execution." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.

2. Şandor, Marian, Radu Marian Portase, and Adrian Coleşa. "Ember Feature Dataset Analysis For Malware Detection." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
3. Mihalca, Andrei Vasile, and Ciprian Pavel Oprişa. "Impact of Library Code in Binary Similarity Systems." *International Conference on Ubiquitous Security*. Singapore: Springer Nature Singapore, 2023.
4. Păcurar, Aralda, and Ciprian Oprişa. "Using Artificial Intelligence to Fight Clickbait in Romanian News Articles." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
5. Moşolea, Victor, and Ciprian Oprişa. "Detecting Domain Generation Algorithms in Malware Traffic Using Constrained Resources." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
6. Mărmureanu, Marius, and Ciprian Oprişa. "MITRE Tactics Inference from Splunk Queries." *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2023.
7. Váradi, Robert, Adrian Coleşa, and Gabriel Raț. "Infrastructure for Capturing and Persisting Virtualization-Specific Events Triggered by In-Guest Process Executions for Behavioral-Based Analysis." *2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet)*. IEEE, 2021.
8. Luţaş, Andrei, et al. "VE-VMI: high-performance virtual machine introspection based on virtualization exception." *2021 20th International Symposium on Parallel and Distributed Computing (ISPDC)*. IEEE, 2021.
9. Portase, Radu-Marian, and Adrian Coleşa. "Curator-A system for creating data sets for behavioral malware detection." *2021 20th International Symposium on Parallel and Distributed Computing (ISPDC)*. IEEE, 2021.
10. Rentea, Robert, and Ciprian Oprişa. "Fast clustering for massive collections of malicious URLs." *2021 IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2021.
11. Nagy, Imola, and Alin Suciu. "Randomness testing with neural networks." *2021 IEEE 17th international conference on intelligent computer communication and processing (ICCP)*. IEEE, 2021.
12. Fălămaş, 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.
13. Suciu, Alin, et al. "Parallel implementation of a PIC simulation algorithm using OpenMP." *2020 15th Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2020.
14. 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.
15. Valea, Ovidiu, and Ciprian Oprişa. "Towards pentesting automation using the metasploit framework." *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2020.
16. Crişan, Andrei, et al. "Detecting malicious URLs based on machine learning algorithms and word embeddings." *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2020.
17. Moldovan, Francisc, Paul Sătmărean, and Ciprian Oprişa. "An analysis of http attacks on home iot devices." *2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*. IEEE, 2020.
18. Mihalca, Andrei, Ciprian Oprişa, and Rodica Potolea. "Hunting for malware code in massive collections." *2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*. IEEE, 2020.
19. Sătmărean, Paul, and Ciprian Oprişa. "Web servers protection using anomaly detection for http requests." *Computer Security: ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26–27, 2019, Revised Selected Papers 2*. Springer International Publishing, 2020.
20. Joldoş, Marius, et al. "A Multi-threaded Particle-in-cell Approach for Kinetic Plasma Simulations." *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2020.
21. TRUŢA, Emanuel, and Alin Suciu. "Privacy Oriented Ecosystem Comparable to Google's Ecosystem." *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2020.
22. Szabo, Balint, and Adrian Colesa. "A Flexible Windows Workspace Saving and Restoring Utility." *2019 IEEE 15th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2019.
23. Ács, Dávid, and Adrian Coleşa. "Securely exposing machine learning models to web clients using intel sgx." *2019 IEEE 15th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2019.
24. Nagy, Lilla, and Adrian Coleşa. "Router-based IoT Security using Raspberry Pi." *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*. IEEE, 2019.
25. Széles, Gergő János, and Adrian Coleşa. "Malware clustering based on called API during runtime." *Information and Operational Technology Security Systems: First International Workshop, IOSec 2018, CIPSEC Project, Heraklion, Crete, Greece, September 13, 2018, Revised Selected Papers 1*. Springer International Publishing, 2019.
26. Mihalca, Andrei, and Ciprian Oprişa. "Full content search in malware collections." *Information and Operational Technology Security Systems: First International Workshop, IOSec 2018, CIPSEC Project, Heraklion, Crete, Greece, September 13, 2018, Revised Selected Papers 1*. Springer International Publishing, 2019.

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

Others:
N/A

The offer addressed to the economic environment

Research & development	Our research fields are of direct interest to cybersecurity companies. In this area we 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 (awarness or technical focused) for SMEs in different projects we were members in.