Allegato B

DANIELE CONO D’ELIA
Curriculum Vitae

Rome, 31/05/2023

Part I – General Information

Full Name	D’Elia, Daniele Cono
Spoken Languages	Italian, English

Part II – Education

Type	Year	Institution	Notes
B.Sc.	2010	Sapienza University of Rome	*Laurea triennale in Ingegneria Informatica* (B.Sc. in Engineering in Computer Science) Final mark: 110/110 cum laude. Thesis: “Hot Path Profiling”. Supervisor: Prof. Camil Demetrescu
M.Sc.	2012	Sapienza University of Rome	*Laurea magistrale in Ingegneria Informatica* (M.Sc. in Engineering in Computer Science), taught in English Final mark: 110/110 cum laude. Thesis: “Mining Hot Calling Contexts in Small Space”. Supervisor: Prof. Camil Demetrescu
Ph.D.	2016	Sapienza University of Rome	*Dottorato di Ricerca in Ingegneria Informatica* (Ph.D. in Engineering in Computer Science) Title: “New Techniques for Adaptive Program Optimization”. Supervisor: Prof. Camil Demetrescu. External reviewers: Prof. Steven Blackburn (ANU), Dr. David Grove (IBM)

Part III – Appointments

III.A – Academic Appointments

Start	End	Institution	Position
2022	--	Sapienza University of Rome	***Assistant professor*** (RTD-A) at Dipartimento di Ingegneria Informatica Automatica e Gestionale (DIAG) “Antonio Ruberti” (SSD ING-INF/05)
2016	2022	Sapienza University of Rome	***Research fellow*** (Assegnista di ricerca) at Dipartimento di Ingegneria Informatica Automatica e Gestionale (DIAG) “Antonio Ruberti” (SSD ING-INF/05). Research topics: - “Optimizing malware detection with dynamic analysis” (2016-18) - “Secure virtualization tools and techniques for distributed computing environments” (2018-19) - “Tool and techniques for malware analysis” (2019-20) - “Understanding adversarial behavior in malicious software” (2020-21) - “Analysis of transparency characteristics of dynamic analysis systems based on hypervisors and virtual machine introspection” (2021-22)
2014	2014	Purdue University	***Visiting researcher*** at the PL research group led by Prof. Jan Vitek (ACM SIGPLAN Chair at the time). 4 months

III.B – Other Appointments

- **Member of the selection board** for the Italian National Cybersecurity Agency (ACN) for hiring three highly qualified experts in computer security, call of February 2022

- *Free-lance consultant* for CINI (National Interuniversity Consortium for Informatics) on several projects involving security assessments of software solutions and cybersecurity training, since 2017

Part IV – Teaching Experience

IV.A –Bachelor and Master-level Courses

Year	Institution	Course
2022/23	Sapienza University of Rome	- Malware Analysis and Incident Forensics (3 CFU), M.Sc. program in Cybersecurity. Taught in English - Laboratorio di Architetture Software e Sicurezza Informatica (3 CFU), B.Sc. program in Engineering in Computer Science - Sistemi di Elaborazione delle Informazioni (1 CFU), B.Sc. program in "Tecniche di Neurofisiopatologia"
2021/22	Sapienza University of Rome	Malware Analysis and Incident Forensics (3 CFU), M.Sc. program in Cybersecurity. Taught in English
2020/21	Sapienza University of Rome	Malware Analysis and Incident Forensics (3 CFU), M.Sc. program in Cybersecurity. Taught in English
2019/20	Sapienza University of Rome	Malware Analysis and Incident Forensics (3 CFU), M.Sc. program in Cybersecurity. Taught in English
2018/19	Sapienza University of Rome	Malware Analysis and Incident Forensics (3 CFU), M.Sc. program in Cybersecurity. Taught in English
2017/18	Sapienza University of Rome	Sistemi di Calcolo II (Computer System Architecture II, 6 CFU). B.Sc. program in Engineering in Computer Science
2016/17	Sapienza University of Rome	Sistemi di Calcolo I (Computer System Architecture I, 6 CFU). B.Sc. program in Engineering in Computer Science
2014 to 2016	Sapienza University of Rome	Teaching Assistant for Sistemi di Calcolo I (Fall 2014, Fall 2015) and II (Spring 2015, Spring 2016), B.Sc. program in Engineering in Computer Science

IV.B – Other Teaching Service

- Organizer of the course *"Thinking outside the box: Adversarial behavior and unconventional attack vectors from security research"* on trending software and systems security research topics. The course has seen three editions (2021, 2022, 2023) and is formally held for students enrolled in the Ph.D. programs in Engineering in Computer Science and in Cybersecurity at Sapienza University of Rome
- Technical committee member and instructor for the *CyberChallenge.IT* training initiative, co-organized by CIS-Sapienza and CINI, for its 2017, 2018, and 2019 editions
- *System architect* for the automated install and maintenance of the IT teaching infrastructure of the Paolo Ercoli laboratory (~200 computers) in use to the School of Information Engineering, Informatics, and Statistics and to the Department of Physics of Sapienza University of Rome, 2018
- Developer of an *automated sandboxing and grading system* for exam papers written in the Python programming language, in use at DIAG Sapienza for introductory programming courses since 2014

IV.C – Student Supervision

- Dr. D'Elia has supervised 3 Ph.D. students (co-supervised another 5), 33 M.Sc. students (co-supervised another 7), 4 B.Sc. students (co-supervised another 4), and 10 honors program students.
- Among his former students, 9 have been co-authors of scientific articles on their thesis or honors program topics. Furthemore, another **9 won awards for their thesis**: Giorgia Di Pietro in 2023 with the Camil Demetrescu thesis award, Lorenzo Invidia and Antonella Gioia Rodio in 2022 from the CLUSIT association (2nd and 3rd prize, respectively), Riccardo Chiaretti in 2021 from the Italian intelligence agencies, Cristian Assaiante in 2020 from the CLUSIT association (1st prize), Andrea Salvati (co-supervised) in 2020 from the CLUSIT association (5th prize), Federico Palmaro (co-supervised) in 2018 from the Italian intelligence agencies and a second award from the CLUSIT association (5th prize), and Fabio Rosato (co-supervised) in 2017 from the CLUSIT association.

Part V – Society Memberships, Awards, and Honors

Year	Description
2021	**Distinguished Reviewer Award** for the service in the Shadow Program Committee of S&P 2021 (42nd IEEE Symposium on Security and Privacy). S&P is considered one of the most famous and well-established conference in computer security
2020	**Best Ph.D. Dissertation Award** from Sapienza University Press for the best research carried in the Engineering-Architecture macro area among the dissertations defended in 2015 and 2016
2020	*Traveling Fellowship* from the Italian Embassy in Seoul to visit South Korean research institution and set up collaborations on security research
2018	**Best Paper Award** at IEEE Symposium on Visualization for Cyber Security (VizSec 2018) for the work “ROPMate: Visually Assisting the Creation of ROP-based Exploits”
2013	*SIGPLAN PAC Award* from the Professional Activities Committee of the ACM Special Interest Group on Programming Languages as student author and presenter at OOPSLA 2013
2013	*Excellent Graduate Student Award* from the Alumni Noi Sapienza Association, accorded to students with outstanding academic performance
2011	*SIGPLAN PAC Award* from the Professional Activities Committee of the ACM Special Interest Group on Programming Languages as student author and presenter at PLDI 2011
2009	Enrolled in the *Honors Program* of the Bachelor program in Engineering in Computer Science at Sapienza University of Rome (from 2009 until graduation)
2007	Ranked first out of 382 students attending the admission test to the Bachelor program in Engineering in Computer Science at Sapienza University of Rome
2007	Merit Scholarship from the Italian Ministry of Education, Univerisities and Research (MIUR) for outstanding high school graduation

Part VI – Funding Information

Since January 2020, Dr. D’Elia is actively involved in the **SAFE** (Self-Attentive Function Embeddings for embedded systems) project sponsored by the Italian National Plan for Military Research (Piano Nazionale per la Ricerca Militare – PNRM) for a grant value of [redacted], contributing with his expertise in code analysis and reverse engineering to the study, design, and development of novel methods and techniques for the identification of failures and attacks in complex and critical IT systems.

Since May 2020, Dr. D’Elia has a leading technical role in a joint project between the Italian authorities and the CIS Sapienza research center, for a grant value of [redacted], contributing with his research expertise and vision to the design and development of novel testing methods to evaluate the security of ICT assets, systems, and services to be used within the National Security Perimeter of Italy. The activities are carried for the National Assessment and Certification Center (**CVCN**) of the Italian National Cybersecurity Agency (ACN).

In 2022, Dr. D’Elia received a **research gift** from Prisma Srl ([redacted]) to support his work on efficiency and transparency aspects of dynamic binary instrumentation systems when deployed in security scenarios, and an institutional gift from Regione Lazio ([redacted]) as part of a program to support early-career researchers.

Early in his career, Dr. D’Elia obtained from Sapienza University of Rome 3 Ph.D. Starting Grants (proposals: “Performance Engineering for Big Data Computing”, “Large-Scale Data Analytics in R”, and “Continuous Optimization for Large-Scale Data Analytics”) for ~[redacted] each and 3 Post-doctoral Starting Grants (“Return-Oriented Programming: the Good, the Bad and the Ugly”, “Analysis and Mitigation of Evasive Behavior in Malicious Software”, and “Understanding Evasive Behavior in Malicious Software”) for ~[redacted] each.

Part VII – Research Activities

Keywords	Brief description
Systems security	- Malware analysis and reverse engineering - Code reuse attacks and defenses - Transparency issues in dynamic program analysis

Software security	- Fuzzing - Side-channel analysis and removal - Software obfuscation and diversification - Adversarial attacks to ML-based software analysis systems - Sanitization schemes for silent memory corruption bugs
Program analysis and compilation	- Compiler testing and software debuggability - Static and dynamic program analysis techniques for source and binary code (e.g., symbolic execution, information flow tracking, binary instrumentation) - Optimizing compilers and managed runtimes - Performance engineering and profiling of programs

The work of Dr. D'Elia spans several fields of software and systems security. He mainly researches on program analysis techniques that can boost accuracy and performance aspects of security policies. The two pillars of his work are special-purpose techniques for adversarial code (as with malware and general transparency issues of the security domain) and the design of program analyses and transformations to make programs more secure. His programming language research background often helps him in the design of scalable solutions.

Dr. D'Elia has well-established research collaborations with renowned **international research groups**:

- S2Lab, led by Prof. Lorenzo Cavallaro (University College London) with 2 publications on malware;
- VUSec, led by Prof. Cristiano Giuffrida and Prof. Herbert Bos (Vrije Universiteit Amsterdam) with 2 publications on program hardening (side channels, Linux kernel bugs) and 1 paper under review;
- Software and System Security (S3) group, led by Prof. Davide Balzarotti (EURECOM) with 1 publication on fuzzing and 1 paper under review;
- HexHive, led by Prof. Mathias Payer (EPFL) with 2 ongoing projects on malware and fuzzing.

Part VIII – Summary of Scientific Achievements

VIII.A – Number of Publications by Type

Product type	Scopus	Google Scholar	Start year	End year
Journal	6	6	2016	2023
Conference	20	20	2011	2023
Book (full)	0	1	2020	2023

VIII.B – Bibliometrics

Metric	Scopus	Google Scholar	Start year	End year
h-index	11	15	2011	2023
Normalized h-index (h-index divided by 11 years since M.Sc. degree obtained in 2012)	1	1.36	2011	2023
i10-index	15	18	2011	2023
Total citations	596	1100	2011	2023
Mean citations per article	22.92	40.74	2011	2023
Total impact factor (5 journal articles indexed)	22.935 (WoS JCR Clarivate)		2016	2023
Mean impact factor per journal article	4.587		2016	2023

For the CORE21 ranking, 8 conference papers appeared in rank-A* venues, 6 in rank-A venues. For the GGS rating, 9 conference papers appeared in class-1 venues (5 A++, 4 A+), 6 in class-2 venues (5 A, 1 A-).

Part IX – Selected Publications

1. Where Did My Variable Go? Poking Holes in Incomplete Debug Information
Cristian Assaiante, Daniele Cono D'Elia, Giuseppe Antonio Di Luna, Leonardo Querzoni
2023, 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), Volume 2
Location: Vancouver, Canada. March 25-29
Pages 935-947, ISBN 9781450399166, ACM, New York, NY, USA
Acceptance rate: 16.67% (45 of 270 submissions for the round). CORE21 rank: A*. GGS rating: A+

Citations: 1 on Google Scholar, none on Scopus

2. Designing Robust API Monitoring Solutions
Daniele Cono D'Elia, Simone Nicchi, Matteo Mariani, Matteo Marini, Federico Palmaro
2023, IEEE Transactions on Dependable and Secure Computing (TDSC)
Volume 20, issue 1 (Jan-Feb 2023), pages 392-406
ISSN information: 1545-5971 (print), 1941-0018 (online), IEEE, Piscataway, NJ, USA
WoS JCR impact factor and SJR indicator (latest available): 6.791 - 1.828
Citations: 3 on Google Scholar, none on Scopus

3. Principled Composition of Function Variants for Dynamic Software Diversity and Program Protection
Giacomo Priamo, Daniele Cono D'Elia, Leonardo Querzoni
2022, 37th IEEE/ACM International Conference on Automated Software Engineering (ASE)
Location: Rochester, USA. October 10-14
Article 183, pages 1-5, ISBN 9781450394758, ACM, New York, NY, USA
Acceptance rate: 25.53% (156 of 611 technical paper submissions). CORE21 rank: A*. GGS rating: A
Citations: none yet

4. Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization
Pietro Borrello, Daniele Cono D'Elia, Leonardo Querzoni, Cristiano Giuffrida
2021, 28th ACM Conference on Computer and Communications Security (CCS)
Location: Seoul, South Korea (Virtual Event). November 15-19
Pages 715-733, ISBN 9781450384544, ACM, New York, NY, USA
Acceptance rate: 13.65% (43 of 315 submissions for the round). CORE21 rank: A*. GGS rating: A++
Citations: 26 on Google Scholar, 5 on Scopus

5. The Use of Likely Invariants as Feedback for Fuzzers
Andrea Fioraldi, Daniele Cono D'Elia, Davide Balzarotti
2021, 30th USENIX Security Symposium (USENIX Security)
Location: USA (Virtual Event). August 11-13
Pages 2829-2846, ISBN 978-1-939133-24-3, USENIX Association, Berkeley, CA, USA
Acceptance rate: 18.69% (246 of 1316 submissions). CORE21 rank: A*. GGS rating: A++
Citations: 26 on Google Scholar, 11 on Scopus

6. Rope: Covert Multi-Process Malware Execution with Return-Oriented Programming
Daniele Cono D'Elia, Lorenzo Invidia, Leonardo Querzoni
2021, 26th European Symposium on Research in Computer Security (ESORICS)
Location: Darmstadt, Germany (Virtual Event). October 4-8
Pages 197-217, ISBN 978-3-030-88417-8 (print), Springer, Cham, Switzerland
Acceptance rate: 20.23% (71 of 351 submissions). CORE21 rank: A. GGS rating: A+
Citations: 6 on Google Scholar, 2 on Scopus

7. On the Dissection of Evasive Malware
Daniele Cono D'Elia, Emilio Coppa, Federico Palmaro, Lorenzo Cavallaro
2020, IEEE Transactions on Information Forensics and Security (TIFS)
Volume 15, pages 2750-2765, February 2020
ISSN information: 1556-6013 (print), 1556-6021 (online), IEEE, Piscataway, NJ, USA
WoS JCR impact factor and SJR index (2020): 7.178 - 1.613
Citations: 40 on Google Scholar, 24 on Scopus

8. WEIZZ: Automated Grey-box Fuzzing for Structured Binary Formats
Andrea Fioraldi, Daniele Cono D'Elia, Emilio Coppa
2020, 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)
Location: Los Angeles, USA (Virtual Event). July 18-22
Pages 1-13, ISBN 9781450380089, ACM, New York, NY, USA
Acceptance rate: 26.34% (241 of 915 submissions). CORE21 rank: A. GGS rating: A+

Citations: 39 on Google Scholar, 25 on Scopus

9. SoK: Using Dynamic Binary Instrumentation for Security (And How You May Get Caught Red Handed)
Daniele Cono D'Elia, Emilio Coppa, Simone Nicchi, Federico Palmaro, Lorenzo Cavallaro
2019, 13th ACM Asia Conference on Computer and Communications Security (ASIA CCS)
Location: Auckland, New Zealand. July 7-12
Pages 15-27, ISBN 978-1-4503-6752-3, ACM, New York, NY, USA
Acceptance rate: 17.05% (44 of 258 submissions as full papers). CORE21 rank: A. GGS rating: A
Citations: 52 on Google Scholar, 33 on Scopus

10. A Survey of Symbolic Execution Techniques
Roberto Baldoni, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu, Irene Finocchi
2018, ACM Computing Surveys (CSUR)
Volume 51 Issue 3, July 2018 (39 pages)
ISSN 0360-0300, EISSN 1557-7341, ACM, New York, NY, USA
WoS JCR impact factor and SJR index (2018): 6.131 - 1.503
Citations: 618 on Google Scholar, 315 on Scopus

11. On-stack Replacement, Distilled
Daniele Cono D'Elia, Camil Demetrescu
2018, 39th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
Location: Philadelphia, PA, USA. June 18-22
Pages 166-180, ISBN 978-1-4503-5698-5, ACM, New York, NY, USA
Acceptance rate: 20.99% (55 of 262 submissions). CORE21 rank: A*. GGS rating: A++
Citations: 21 on Google Scholar, 13 on Scopus

12. Flexible On-Stack Replacement in LLVM
Daniele Cono D'Elia, Camil Demetrescu
2016, 14th International Symposium on Code Generation and Optimization (CGO)
Location: Barcelona, Spain. March 12-18
Pages 250-260, ISBN 9781450337786, ACM, New York, NY, USA
Acceptance rate: 23.15% (25 of 108 submissions). CORE21 rank: A. GGS rating: A
Citations: 25 on Google Scholar, 12 on Scopus

Part X – Other Activities

X.A – Organizing Roles in Scientific Events

- **Artifact Evaluation Chair** for the 31st Network and Distributed System Security Symposium (NDSS), 2024. NDSS is a top-tier conference in computer security (A* in CORE21, A+ in GGS) and started an Artifact Evaluation initiative with this edition. The process promotes the reproducibility of research results by means of a rigorous evaluation of a paper's experiments, repeated by anonymous peers from the Artifact Evaluation Committee (~80 members) of the conference.
- **Artifact Evaluation Co-chair** for the 18th European Conference on Computer Systems (EuroSys), 2023. EuroSys is a prominent conference (A in CORE21, A+ in GGS) in computer systems research
- **Associate editor** for the Digital Threats: Research and Practice journal (Q2 on Scimago) edited by ACM as of January 2023
- **Guest editor** for "Special Issue on Benefits and Outlook of Program Analysis for Systems Security" with the Computers & Security journal (Q1 on Scimago) edited by Elsevier, 2022-23. Dr. D'Elia managed the special issue (co-edited with Prof. Lorenzo Cavallaro, University College London). The special issue sought seeks technical and vision papers capitalizing on the cross-pollination among computer security, programming languages, and software engineering research
- **Publication co-chair** for the 7th IEEE European Symposium on Security and Privacy (EuroS&P), 2022. EuroS&P is the premier European venue for computer security research
- Poster co-chair, Web chair, and Housing chair for the 30th European Conference on Object-Oriented Programming (ECOOP), 2016

X.B – Peer Review

Dr. D'Elia has been a Program Committee member for the following international scientific conferences:

- CCS 2023 – The ACM Conference on Computer and Communications Security (A++ in GGS rating)
- NDSS 2023, 2024 – The Network and Distributed System Security Symposium (A+)
- USENIX Security 2023, 2024 – The USENIX Security Symposium (A++)
- S&P 2021 (Shadow PC) - 42nd IEEE Symposium on Security and Privacy (A++). ***Distinguished Reviewer Award***
- ASSS 2023 – 3rd International Symposium on Advanced Security on Software and Systems
- DIMVA 2023, 2022 – SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment
- EUROSEC 2023, 2022, 2021, 2020 - 13th-to-16th ACM European Workshop on Systems Security
- ICCQ 2023, 2022 - International Conference on Code Quality edited by IEEE
- EuroSys 2022 (Shadow PC) – 17th European Conference on Computer Systems (A+)
- CCS 2022 Posters (2-page peer-reviewed papers published in the main conference proceedings, A++)
- BAR 2021 - 4th Workshop on Binary Analysis Research
- MPLR 2019 - 16th International Conference on Managed Programming Languages & Runtimes.

Dr. D'Elia has also been an Artifact Evaluation Committee member for:

- PLDI 2019 - 40th ACM Conference on Programming Language Design and Implementation
- WOOT 2019 - 13th USENIX Workshop on Offensive Technologies
- ECOOP 2016 - 30th European Conference on Object-Oriented Programming

Finally, Dr. D'Elia has served as reviewer for the following journals over the years:

- Transactions on Privacy and Security (ACM)
- Digital Threats: Research and Practice (ACM)
- Computers & Security (Elsevier)
- Computer Science Review (Elsevier)
- Journal of Computer and System Sciences (Elsevier)
- Journal of Information Security and Applications (Elsevier)
- Journal of Systems and Software (Elsevier)
- Formal Aspects of Computing (Springer)
- Frontiers of Information Technology & Electronic Engineering (Springer)

X.C –Invited Talks and Seminars

- "Rope: Bypassing Behavioral Detection of Malware with Distributed ROP-Driven Execution". Invited talk, Malware and Exploit Development tracks, **Black Hat USA** 2021, August 4, Nevada, USA. Black Hat is the ***most prestigious industry conference*** series for professionals in information security
- "Too diluted to be seen: covert distribution of a malware payload with Rope". Invited talk, No Hat conference 2021, November 20, Bergamo, Italy
- "When Return-Oriented Programming Meets Program Obfuscation". Seminar at the CASTOR Software Research Centre, KTH Royal Institute of Technology, June 15, 2021 (online)
- "My Ticks Don't Lie: New Timing Attacks for Hypervisor Detection". Invited talk, **Black Hat Europe** 2020, December 10, Virtual Event
- "When program analyses may, or may not, solve your security problems". Seminar at the HexHive research group (led by ERC Starting Grant recipient Prof. Mathias Payer), EPFL, December 18, 2019, Lausanne, Switzerland
- "BluePill: Neutralizing Anti-Analysis Behavior in Malware Dissection". Invited talk, **Black Hat Europe** 2019, December 4, London, UK

X.D – Conference Presentations

- "Principled Composition of Function Variants for Dynamic Software Diversity and Program Protection", ASE 2022, Rochester, USA

- "Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization", ITASEC 2022, Rome, Italy
- "Rope: Covert Multi-Process Malware Execution with Return-Oriented Programming", ESORICS 2021, Virtual Event
- "SoK: Using Dynamic Binary Instrumentation for Security (And How You May Get Caught Red-Handed)". ASIA CCS 2019, Auckland, New Zealand
- "Static Analysis of ROP Code". EUROSEC 2019, Dresden, Germany
- "Reconciling Automatic and Manual Malware Analysis". ITASEC 2019, Pisa, Italy
- "On-Stack Replacement, Distilled". PLDI 2018, Philadelphia, USA
- "Rethinking Pointer Reasoning in Symbolic Execution". ASE 2017, Urbana-Champaign, USA
- "Securing Software Applications through Symbolic Execution: an Overview", ITASEC 2017, Venice, Italy
- "Flexible On-Stack Replacement in LLVM". CGO 2016, Barcelona, Spain
- "Ball-Larus Path Profiling Across Multiple Loop Iterations". OOPSLA 2013, Indianapolis, USA
- "Mining hot calling contexts in small space". PLDI 2011, San Jose, USA

X.E – Research Artifacts and Open Source Software

- BluePill: a dynamic analysis framework for handling evasive malware. Presented at Black Hat Europe 2019 and shortly after in a top-tier journal article (IEEE TIFS 2020, listed as J-4 later in Part XI)
- Flexible On-Stack Replacement in LLVM. Artifact published in the ACM Digital Library and endorsed by the joint Artifact Evaluation Process of CGO-PPoPP 2016. Later used in the high-performance R language runtime developed by a consortium led by Northeastern University (USA)
- k-BLPP: a k-Iteration Path Profiler. Available in the Jikes RVM Research Archive. Artifact endorsed by the ACM SIGPLAN OOPSLA 2013 Artifact Evaluation Committee

X.F – Technology Transfer

- Dr. D'Elia authored the research and and co-holds (30%) the economic rights of the patented invention *"Methods and systems for analyzing environment-sensitive malware with coverage-guided fuzzing"*. The **patent** was filed in Italy on July 28, 2022 (no. 102022000015966) and received a positive written opinion from the Italian Patent and Trademark Office (UIBM) on March 15, 2023. The documentation is publicly available as prescribed by the Italian law on intellectual property. Dr. D'Elia and the company that co-holds the economic rights of the invention consequently applied for extending the patent protection to the 39 countries part of the European Patent Convention and to the United States
- The BluePill research system (Part X.E) is the basis of a commercial sandboxing product for armored malware that Prisma Srl has been developing since 2019 under the name Dynamic Blue. Dr. D'Elia has provided scientific guidance to the company on how to develop and evolve the solution

Part XI – Full Publication List

XI.A – Books

[B-1] Daniele Cono D'Elia. "New Techniques for Adaptive Program Optimization". Book series: *Studi e Ricerche*. Edited by Sapienza Università Editrice (Sapienza University Press), ISBN 9788893771436, doi:10.13133/9788893771436, 204 pages, June 2020.

XI.B – Journals

[J-6] Daniele Cono D'Elia, Simone Nicchi, Matteo Mariani, Matteo Marini, Federico Palmaro. "Designing Robust API Monitoring Solutions". *IEEE Transactions on Dependable and Secure Computing* (TDSC), volume 20, issue 1 (Jan-Feb 2023), pages 392-406. [WoS JCR Impact Factor: **6.791** in 2021 for early-access version, Scimago Journal Rank 2022: 1.828 - most recent data was reported for both]

[J-5] Daniele Cono D'Elia, Lorenzo Invidia, Federico Palmaro, Leonardo Querzoni. "Evaluating Dynamic Binary Instrumentation Systems for Conspicuous Features and Artifacts". *ACM Digital Threats: Research and Practice* (DTRAP), volume 3, issue 2, article 10 (February 2022). [IF: journal not indexed yet, SJR 2022: 0.543]

[J-4] Daniele Cono D’Elia, Emilio Coppa, Federico Palmaro, Lorenzo Cavallaro. “On the Dissection of Evasive Malware”. *IEEE Transactions on Information Forensics and Security* (TIFS), volume 15 (February 2020), pages 2750–2765. [IF: **7.178**, SJR: 1.613]

[J-3] Luca Borzacchiello, Emilio Coppa, Daniele Cono D’Elia, Camil Demetrescu. “Memory Models in Symbolic Execution: Key Ideas and New Thoughts”. *Journal of Software Testing, Verification and Reliability*, 29(8), John Wiley & Sons (STVR), 2019. [IF: **1.226**, SJR: 0.309]

[J-2] Roberto Baldoni, Emilio Coppa, Daniele Cono D’Elia, Camil Demetrescu, and Irene Finocchi. “A Survey of Symbolic Execution Techniques”. *ACM Computing Surveys* (CSUR), volume 51, issue 3, article 50 (May 2018). [IF: **6.131**, SJR: 1.503]

[J-1] Daniele Cono D’Elia, Camil Demetrescu, and Irene Finocchi. “Mining Hot Calling Contexts in Small Space”. *Software: Practice and Experience*, 46(8), John Wiley & Sons (SPE), 2016. [IF: **1.609**, SJR: 0.412]

XI.C – Conference and Workshop Papers

[C-21] Jakob Koschel, Pietro Borrello, Daniele Cono D’Elia, Herbert Bos, Cristiano Giuffrida. “Uncontained: Uncovering Container Confusion in the Linux Kernel”. (To appear) in *Proceedings of the 2023 USENIX Security Symposium* (USENIX Security 2023), 2023. [CORE21: A*, GGS: A++]

[C-20] Cristian Assaiante, Daniele Cono D’Elia, Giuseppe Antonio Di Luna, Leonardo Querzoni. “Where Did My Variable Go? Poking Holes in Incomplete Debug Information”. In *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (ASPLOS 2023), 2023. [CORE21: A*, GGS: A+]

[C-19] Giacomo Priamo, Daniele Cono D’Elia, Leonardo Querzoni. “Principled Composition of Function Variants for Dynamic Software Diversity and Program Protection”. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering* (ASE 2022), 2022. [CORE21: A*, GGS: A]

[C-18] Pietro Borrello, Daniele Cono D’Elia, Leonardo Querzoni, Cristiano Giuffrida. “Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization”. In *Proceedings of the 28th ACM Conference on Computer and Communications Security* (CCS 2021), 2021. [CORE21: A*, GGS: A++]

[C-17] Daniele Cono D’Elia, Lorenzo Invidia, Leonardo Querzoni. “Rope: Covert Multi-Process Malware Execution with Return-Oriented Programming”. In *Proceedings of the 26th European Symposium on Research in Computer Security* (ESORICS 2021). [CORE21: A, GGS: A+]

[C-16] Andrea Fioraldi, Daniele Cono D’Elia, Davide Balzarotti. “The Use of Likely Invariants as Feedback for Fuzzers”. In *Proceedings of the 2021 USENIX Security Symposium* (USENIX Security 2021), 2021. [CORE21: A*, GGS: A++]

[C-15] Pietro Borrello, Emilio Coppa, Daniele Cono D’Elia. “Hiding in the Particles: When Return-Oriented Programming Meets Program Obfuscation”. In *Proceedings of the 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN 2021). [CORE21: A, GGS: A]

[C-14] Andrea Fioraldi, Daniele Cono D’Elia, Leonardo Querzoni. “Fuzzing Binary for Memory Safety Errors with QASan”. In *Proceedings of the 2020 IEEE Secure Development Conference* (SecDev 2020).

[C-13] Andrea Fioraldi, Daniele Cono D’Elia, Emilio Coppa. “WEIZZ: Automatic Grey-box Fuzzing for Structured Binary Formats”. In *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis* (ISSTA 2020). [CORE21: A, GGS: A+]

[C-12] Marco Angelini, Graziano Blasilli, Luca Borzacchiello, Emilio Coppa, Daniele Cono D’Elia, Camil Demetrescu, Simone Nicchi, Simone Lenti, Giuseppe Santucci. “SymNav: Visually Assisting Symbolic Execution”. In *Proceedings of the 16th IEEE Symposium on Visualization for Cyber Security* (VizSec 2019). [CORE21: C, GGS: B-]

[C-11] Daniele Cono D’Elia, Emilio Coppa, Simone Nicchi, Federico Palmaro, Lorenzo Cavallaro. “SoK: Using Dynamic Binary Instrumentation for Security (And How You May Get Caught Red Handed)”. In *Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security* (ASIA CCS 2019). [CORE21: A, GGS: A]

[C-10] Luca Borzacchiello, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu. "Reconstructing C2 Servers for Remote Access Trojans with Symbolic Execution". In *Proceedings of the 3rd International Symposium on Cyber Security Cryptography and Machine Learning* (CSCML 2019).

[C-9] Daniele Cono D'Elia, Emilio Coppa, Andrea Salvati, Camil Demetrescu. "Static Analysis of ROP Code". In *Proceedings of the 12th European Workshop on Systems Security* (EUROSEC 2019), ACM.

[C-8] Pietro Borrello, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu. "The ROP Needle: Hiding Trigger-based Injection Vectors via Code Reuse". In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing* (SAC 2019). [CORE21: B, GGS: A-]

[C-7] Daniele Cono D'Elia, Camil Demetrescu. "On-Stack Replacement, Distilled". In *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI 2018). [CORE21: A*, GGS: A++]

[C-6] Marco Angelini, Graziano Blasilli, Pietro Borrello, Emilio Coppa, Daniele Cono D'Elia, Serena Ferracci, Simone Lenti, Giuseppe Santucci. "ROPMate: Visually Assisting the Creation of ROP-based Exploits". In *Proceedings of the 15th IEEE Symposium on Visualization for Cyber Security* (VizSec 2018). **Best Paper Award**. [CORE21: C, GGS: B-]

[C-5] Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu. "Rethinking Pointer Reasoning in Symbolic Execution". In *Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering* (ASE 2017). [CORE21: A*, GGS: A]

[C-4] Roberto Baldoni, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu. "Assisting Malware Analysis with Symbolic Execution: A Case Study". In *Proceedings of the 1st International Symposium on Cyber Security Cryptography and Machine Learning* (CSCML 2017).

[C-3] Daniele Cono D'Elia, Camil Demetrescu. "Flexible On-Stack Replacement in LLVM". In *Proceedings of the 14th International Symposium on Code Generation and Optimization* (CGO 2016). [CORE21: A, GGS: A]

[C-2] Daniele Cono D'Elia, Camil Demetrescu. "Ball-Larus Path Profiling Across Multiple Loop Iterations". In *Proceedings of the 28th ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications* (OOPSLA 2013). [CORE21: A, GGS: A+]

[C-1] Daniele Cono D'Elia, Camil Demetrescu, Irene Finocchi. "Mining Hot Calling Contexts in Small Space". In *Proceedings of the 32nd ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI 2011). [CORE21: A*, GGS: A++]

Curriculum redatto ai fini della pubblicazione.
Autorizzo il trattamento dei dati personali contenuti nel mio curriculum vitae ai sensi dell'art. 13 del D. Lgs. 196/2003 e successive modificazioni