Daniele Cono D'Elia

Curriculum vitae

(last updated: August 7, 2020)

Employment

Jul 2016-Present Postdoctoral researcher
Sapienza University of Rome, Italy
CIS (Research Center of Cyber Intelligence and Information Security)

Fall 2016-Present Adjunct professor
Sapienza University of Rome, Italy
Current Subject: Malware Analysis and Incident Forensics

Education

Nov 2012-Jun 2016 Ph.D. in Computer Engineering
Sapienza University of Rome, Italy
Dissertation title: *New Techniques for Adaptive Program Optimization*
Advisor: Prof. Camil Demetrescu

Mar 2014-Jul 2014 Visiting Scholar at Purdue University
Research topic: novel techniques for program optimization
Supervisor: Prof. Jan Vitek

Oct 2010-Oct 2012 Master of Science in Computer Engineering (in English)
Sapienza University of Rome, Italy
Advisor: Prof. Camil Demetrescu
Final grade: 110/110 with honors (*summa cum laude*)

Sep 2007-Oct 2010 Bachelor degree in Computer Engineering
Sapienza University of Rome, Italy
Advisor: Prof. Camil Demetrescu
Final grade: 110/110 with honors (*summa cum laude*)

Sep 2002-Jun 2007 High school diploma
Liceo Scientifico Carlo Pisacane, Padula - Italy
Final grade: 100/100 with honors (*summa cum laude*)

Research interests

My work involves the fields of software and systems security research.

I research in malware analysis, code reuse attacks, code (de)obfuscation, bug finding, and robust monitoring solutions in presence of adversarial behavior. I'm passionate about program analyses that can cope with transparency issues from security domains. My programming language research background often helps in designing scalable solutions.

Teaching

2018-Present Adjunct Professor for *Malware Analysis and Incident Forensics* course (taught in English), M.Sc. in Cybersecurity (and M.Sc. in Engineering in Computer Science as *Software and Enterprise Security*), Sapienza University of Rome. Course editions: Fall 2018, Fall 2019.

Spring 2018 Adjunct Professor for *Sistemi di Calcolo II* course (Computer System Ar chitecture part 2), B.Sc. in Engineering in Computer Science and Control Engineering, Sapienza University of Rome.

Fall 2016 Adjunct Professor for *Sistemi di Calcolo I* course (Computer System Ar chitecture part 1), B.Sc. in Engineering in Computer Science and Control Engineering, Sapienza University of Rome.

2014-2016 Teaching Assistant for *Sistemi di Calcolo* course, part 1 (Fall 2014, Fall 2015) and part 2 (Spring 2015, Spring 2016), Sapienza University of Rome.

Spring 2013 Teaching Assistant for *Algorithm Engineering* course, Sapienza University of Rome.

Service

Research

2020 Program Committee member for EUROSEC 2020 – 13th European Workshop on Sys tems Security (ACM).

2019 Program Committee member for MPLR 2019 – 16th International Conference on Managed Programming Languages & Runtimes.

Artifact Evaluation Committee member for PLDI 2019 – 40th ACM SIGPLAN Confer ence on Programming Language Design and Implementation.

Artifact Evaluation Committee member for WOOT 2019 – 13th USENIX Workshop on Offensive Technologies.

2016 Artifact Evaluation Committee member, Web Technology & Housing Chair, and Posters Co-Chair for ECOOP 2016 – 30th European Conference on Object-Oriented Programming.

2015 Student Volunteer at ECOOP 2015 – 29th European Conference on Object-Oriented Programming.

Over time I have occasionally served as reviewer for *Computers & Security* (Elsevier), *Formal Aspects of Computing* (Springer), and *Journal of Systems and Software* (Elsevier).

Other

2017-2019 Technical Committee member and Instructor for CyberChallenge.IT (training program in cybersecurity for high-school and undergraduate students).

2018-2019 System architect for automated install and maintenance of the IT infrastruc ture (~200 machines) of the Paolo Ercoli laboratory of Sapienza University.

2014 Design of a fault-resistant, automated grading tool for Python exam papers, presently still used at DIAG Sapienza for introductory programming courses.

Honors and Awards

2020 **Best Ph.D. Dissertation Award** from Sapienza Università Editrice for the best research carried in the Engineering–Architecture macro area for graduation years 2015 and 2016.

2018 **Best Paper Award** at IEEE Symposium on Visualization for Cyber Security.

2013 **ACM SIGPLAN PAC Award**, granted by the SIGPLAN Professional Activities Committee to attend OOPSLA 2013 as student co-author of an accepted paper.

Selected for the final phase of *Best ICT Master's thesis* competition organized by AICA-CINI-CNIT.

Excellent graduate student award from the Alumni Noi Sapienza Association, accorded to students with outstanding performances in academic activities.

2011 **ACM SIGPLAN PAC Award**, granted by the SIGPLAN Professional Activities Committee to attend PLDI 2011 as a student co-author of an accepted paper.

Grant of Sapienza University of Rome for attending the 5th Bertinoro Work shop on Algorithms and Data Structures (ADS 2011), awarded to students with outstanding academic performance.

2009-2010 Enrolled in the *Honors Program* of the Bachelor Degree in Computer Engineer ing of Sapienza University of Rome for students with outstanding academic performance.

2007 Ranked first out of 382 students attending the admission test for the Bachelor program in Computer Engineering of Sapienza University of Rome.

Merit scholarship awarded by the Italian Ministry of Education, Universities and Research (MIUR) for outstanding high school graduation.

2006 Winner of the *Gerardo Ritorto* literary prize.

Publications

Books

2020 Daniele C. D'Elia. *New Techniques for Adaptive Program Optimization*. Book se ries: Studi e Ricerche. Edited by Sapienza Università Editrice, ISBN 9788893771436, doi:10.13133/9788893771436, 204 pages, June 2020.

Journals

2020 Daniele C. D'Elia, Emilio Coppa, Federico Palmaro, Lorenzo Cavallaro. *On the Dissec tion of Evasive Malware*. IEEE Transactions on Information Forensics and Security (TIFS), volume 15, pages 2750–2765. [Impact Factor: 6.211, Scimago Journal Rank: 1.364]

2019 Luca Borzacchiello, Emilio Coppa, Daniele C. 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 (SVTR). [IF: 1.171, SJR: 0.426]

2018 Roberto Baldoni, Emilio Coppa, Daniele C. D'Elia, Camil Demetrescu, and Irene Finocchi. *A Survey of Symbolic Execution Techniques*. ACM Computing Surveys (CSUR), 51, 3, Article 50 (May 2018). [IF: 6.131, SJR: 1.503]

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

Conferences and Workshops

2020 Andrea Fioraldi, Daniele C. D'Elia, Leonardo Querzoni. *Fuzzing Binary for Memory Safety Errors with QASan*. In Proceedings of the IEEE Secure Development Confer ence (SecDev 2020).

Andrea Fioraldi, Daniele C. 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). [GGS Rating: A+]

2019 Marco Angelini, Graziano Blasilli, Luca Borzacchiello, Emilio Coppa, Daniele C. D'Elia, Camil Demetrescu, Simone Nicchi, Simone Lenti, Giuseppe Santucci. *Sym Nav: Visually Assisting Symbolic Execution*. In Proceedings of the 16th IEEE Sympo sium on Visualization for Cyber Security (VizSec 2019). [GGS Rating: B-]

Daniele C. D'Elia, Emilio Coppa, Simone Nicchi, Federico Palmaro, Lorenzo Caval laro. *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). [GGS Rating: A-]

Luca Borzacchiello, Emilio Coppa, Daniele C. 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).

Daniele C. 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. [Microsoft Academic Rating: A-]

Pietro Borrello, Emilio Coppa, Daniele C. 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). [GGS Rating: A-]

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

Marco Angelini, Graziano Blasilli, Pietro Borrello, Emilio Coppa, Daniele C. 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 Visu alization for Cyber Security (VizSec 2018). **Best Paper Award**. [GGS Rating: B-]

2017 Emilio Coppa, Daniele C. 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). [GGS Rating: A]

Roberto Baldoni, Emilio Coppa, Daniele C. D'Elia, Camil Demetrescu. *Assisting Mal ware Analysis with Symbolic Execution: A Case Study*. In Proceedings of the 1st Interna tional Symposium on Cyber Security Cryptography and Machine Learning (CSCML 2017).

2016 Daniele C. D'Elia, Camil Demetrescu. *Flexible On-Stack Replacement in LLVM*. In Pro ceedings of the 2016 International Symposium on Code Generation and Optimiza tion (CGO 2016). [GGS Rating: A]

2013 Daniele C. 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). [GGS Rating: A+]

2011 Daniele C. 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). [GGS Rating: A++]

Research Artifacts and Software

2019 *BluePill*: a dynamic analysis framework for handling evasive malware. Presented at Black Hat Europe and later in a top-tier journal article.

2016 *Flexible On-Stack Replacement in LLVM*. Published in the *ACM Digital Library*. Artifact endorsed by the joint Artifact Evaluation Process of CGO-PPoPP 2016. Later used in the R language runtime developed by a consortium led by Northeastern University.

2013 *k-BLPP: a k-Iteration Path Profiler*. In *Jikes RVM Research Archive*. Artifact endorsed by the ACM SIGPLAN OOPSLA 2013 Artifact Evaluation Committee.

Funding

2018 Postdoctoral starting grant for the project: *Analysis and Mitigation of Evasive Behav ior in Malicious Software* from Sapienza University of Rome.

2017 Postdoctoral starting grant for the project: *Return-Oriented Programming: the Good, the Bad and the Ugly* from Sapienza University of Rome.

2015 Ph.D. starting grant for the project: *Continuous Optimization for Large-Scale Data*

Analytics from Sapienza University of Rome.

2014 Ph.D. starting grant for the project: *Large-scale data analytics in R* from Sapienza University of Rome.

2013 Ph.D. starting grant for the project: *Performance engineering for big data computing* from Sapienza University of Rome.

Talks and Seminars

Dec 2019 *When program analyses may, or may not, solve your security problems*. Invited seminar at the HexHive research group (led by ERC Starting Grant recipient Prof. Mathias Payer). EPFL, Lausanne, Switzerland.

BluePill: Neutralizing Anti-Analysis Behavior in Malware Dissection. Briefings ses sion (Malware track). Black Hat Europe 2019, London, United Kingdom.

Jul 2019 *SoK: Using Dynamic Binary Instrumentation for Security (And How You May Get Caught Red-Handed)*. Paper presentation, ASIA CCS 2019, Auckland, New Zealand.

Mar 2019 *Static Analysis of ROP Code*. Paper presentation, EUROSEC 2019, Dresden, Ger many.

Feb 2019 *Reconciling Automatic and Manual Malware Analysis*. Technical talk, ITASEC 2019, Pisa, Italy.

Jul 2018 *On-Stack Replacement, Distilled*. Paper presentation, PLDI 2018, Philadelphia, Pennsylvania.

Nov 2017 *Rethinking Pointer Reasoning in Symbolic Execution*. Paper presentation, ASE 2017, Urbana-Champaign, Illinois.

Jan 2017 *Securing Software Applications through Symbolic Execution: an Overview*. Tech nical talk, ITASEC 2017, Venice, Italy.

Mar 2016 *Flexible On-Stack Replacement in LLVM*. Paper presentation, CGO 2016, Barcelona, Spain.

Oct 2013 *Ball-Larus path profiling across multiple loop iterations*. Paper presentation, OOPSLA 2013, Indianapolis, Indiana.

Jun 2011 *Mining hot calling contexts in small space*. Paper presentation, PLDI 2011, San Jose Convention Center, California.

Mar 2010 *Finding frequent items in data streams*. Reading seminar, Department of Com puter and System Sciences, Sapienza University of Rome.

Student Supervision

I find working with students very rewarding, professionally and humanly.

At the moment I am supervising 9 master students, 1 bachelor student, and 3 honors program students as sole advisor, and co-supervising 2 doctoral students.

Since obtaining my Ph.D. I supervised 20 master (7 co-supervised), 6 bachelor (4 co supervised), and 4 honors program students, and co-supervised 3 doctoral students.

Among my former students, 2 won awards for their theses and 7 are co-authors of scien tific articles on their thesis topics.

Languages

English: Fluent

Italian: Native

Autorizzo la pubblicazione del presente curriculum vitae in ottemperanza agli obblighi di trasparenza di cui al d.lgs. 33/2013.