

# CURRICULUM VITÆ

*Mila Dalla Preda*

*Professore Associato*

---

## Address

Dipartimento di Informatica, Università di Verona, Strada Le Grazie 15, 37134 Verona, Italy

E-mail: [mila.dallapreda@univr.it](mailto:mila.dallapreda@univr.it) (professional)

e [m.dallapreda@gmail.com](mailto:m.dallapreda@gmail.com) (personal)

Web: [profs.sci.univr.it/dallapreda/](http://profs.sci.univr.it/dallapreda/)

**Data e luogo di nascita:** Novembre 1, 1977; Verona (Italy)

**Cittadinanza:** Italiana

**Lingue conosciute:** Italiano, Inglese

## Educazione

(2007) Dottorato di Ricerca in Informatica, Università di Verona

(2003) Laurea in Informatica. Università di Verona, con la valutazione di 110/110 e lode

(1996) Diploma di maturità scientifica, Liceo Scientifico Statale “G. Fracastoro”, Verona

(1995) High School Degree, anno scolastico 1994/95, Peekskill High School, NY, USA

## Posizioni pregresse e attuali:

(Ottobre 2025 – oggi) Professore Ordinario SSD INFO/01, 01/B1 INFORMATICA Dipartimento di Informatica, Università di Verona.

(Ottobre 2024 – oggi) Membro dell’International Scientific Advisory Board (ISAB) of the Flemish Cybersecurity Research Program (<https://cybersecurity-research.be/>).

(Febbraio 2021 – oggi) Componente del Consiglio Direttivo del Centro di Scienze della Sicurezza e della Criminalità, Università degli Studi di Trento - Università degli Studi di Verona.

(Gennaio 2022) Consegue l’Abilitazione Scientifica Nazionale alle funzioni di Professore Universitario di Prima Fascia per il SSD INF/01.

(Aprile 2020 – Settembre 2025) Professore Associato SSD INF/01, 01/B1 INFORMATICA Dipartimento di Informatica, Università di Verona.

(Novembre 2016 - Aprile 2020) Ricercatore a Tempo Determinato (RTDb), Dipartimento di Informatica, Università di Verona.

(Gennaio 2015) : Consegue l’Abilitazione Scientifica Nazionale alle funzioni di Professore Universitario di Seconda Fascia SSD INF/01.

(Marzo 2014 - Novembre 2016) Ricercatore a Tempo Determinato (RTDa) finanziato sul progetto FACE (Formal Avenue for Chasing malwarE) MIUR FIRB 2013, Dipartimento di Informatica, Università di Verona.

(Marzo 2013 - Febbraio 2014) Assegno di Ricerca, Dipartimento di Informatica, Università di Verona.

(Ottobre 2011 - Febbraio 2013) Assegno di Ricerca, Dipartimento di Scienze dell’Informazione dell’Università di Bologna.

(Giugno 2011 - Settembre 2011) post-doc a INRIA Sophia Antipolis - Mediterranee.

(Agosto 2010 - Marzo 2011) borsa di ricerca finanziata dal progetto SMART AGGREGATION - Spinner 2013.

**(Gennaio 2008 - Agosto 2008)** Contratto di collaborazione coordinata e continuativa con il Department of Information and Communication Technology, Università di Trento, nell'ambito del progetto Europeo FET Re-Trust (2006-2009).

**(Maggio 2007 - Luglio 2010)** Assegno di Ricerca, Dipartimento di Informatica, Università di Verona.

**(Gennaio 2007 - Aprile 2007)** borsa post-Doc presso il Department of Information and Communication Technology, Università di Trento. La borsa è finanziata sui fondi del progetto europeo FET Re-Trust (2006-2009).

**(Gennaio 2004 - Dicembre 2006)** borsa di Dottorato, Dipartimento di Informatica, Università di Verona.

### **Principali interessi di ricerca**

Interpretazione astratta, analisi di programmi e semantica di programmi.

Trasformazione del codice, protezione del codice, offuscamento, watermarking, sicurezza.

### **Responsabilità Istituzionali**

**(2024 – oggi)** Membro del gruppo docenti-tutor per le lauree triennali del Dipartimento di Informatica, Università di Verona.

**(2024 – oggi)** Referente per la Ricerca per il Dipartimento di Informatica, Università di Verona.

**(2023 – oggi)** Componente del Gruppo AQ Dottorato in Informatica - Collegio dei Docenti del Dottorato in Informatica - Dipartimento Informatica

**(2023 – oggi)** Componente della Commissione AQ Laurea magistrale in Ingegneria e Scienze Informatiche - LM18-32 - Collegio Didattico di Informatica - Dipartimento Informatica.

**(2022 – 2024)** Referente per la Comunicazione per il Dipartimento di Informatica, Università di Verona.

**(2019 – oggi)** Responsabile per l'Ateneo di Verona del programma CyberChallenge per la formazione di giovani talenti in cyber security ([www.cyberchallenge.it](http://www.cyberchallenge.it)).

**(2020 – oggi)** Componente del Collegio Didattico del Corso di Laurea Magistrale di Data Science, Dipartimento di Informatica - Università di Verona.

**(2019 – oggi)** Componente del Collegio dei Docenti del Dottorato in Informatica - Università di Verona.

**(2014 – oggi)** Componente del Collegio Didattico di Informatica, Dipartimento di Informatica - Università di Verona.

**(2014 – oggi)** Componente del Consiglio di Dipartimento del Dipartimento di Informatica, Università di Verona.

**(2014 - 2020)** Componente del Collegio Didattico di Corso di Cultura e Civiltà - Università di Verona.

**(2016 - 2018)** Componente della commissione AQ per la stesura del Rapporto di Riesame per il Corso di Laurea in Informatica - L31.

### **Congedi per Maternità**

22 Maggio 2018 - 22 Ottobre 2018 Congedo Maternità - Legge 30/12/71 N. 1204

16 Novembre 2011 - 16 Aprile 2012 Congedo Maternità - Legge 30/12/71 N. 1204

3 Novembre 2009 - 3 Aprile 2010 Congedo Maternità - Legge 30/12/71 N. 1204

## **Descrizione della Ricerca**

I miei interessi di ricerca comprendono l'interpretazione astratta e i metodi formali applicati a diversi aspetti dell'informatica tra cui l'analisi dei programmi, la semantica dei programmi, la trasformazione di programmi, la protezione dell'integrità del codice, la protezione della proprietà intellettuale del codice, l'analisi e identificazione automatica di malware, il model checking.

Sono autrice di più di 50 articoli in riviste e convegni internazionali. In [Google Scholar](https://scholar.google.com/citations?user=...): più di 1400 citazioni, H-index 19, i10-index 28. L'articolo che ha maggiormente segnato la mia carriera è stato:

M. Dalla Preda, M. Christodorescu, S. Jha e S. Debray. A semantics-based approach to malware detection. *34th ACM Symposium on Principles of Programming Languages POPL 2007* [58].

Questo articolo è il risultato del lavoro di ricerca svolto durante la mia visita al prof. Saymua Debray all'Università dell'Arizona durante il mio ultimo anno di dottorato. Le mie conoscenze di metodi formali e interpretazione astratta applicate alla semantica del codice unite all'esperienza degli altri autori nell'ambito dell'analisi dei malware hanno portato alla definizione di un framework formale per la modellazione e verifica di robustezza degli antivirus rispetto alle tecniche di evasione usate dagli scrittori di malware. Questo lavoro ha contribuito a consolidare la mia visibilità internazionale ed ha caratterizzato la mia attività di ricerca negli anni successivi.

## Principali risultati ottenuti

**Formalizzazione dell'offuscamento mediante interpretazione astratta e semantica formale:** Con il termine offuscamento del codice si identificano trasformazioni di programmi che preservano la funzionalità del codice rendendolo più complicato da analizzare da parte di tool automatici. L'offuscamento viene utilizzato dagli sviluppatori di codice per proteggere la proprietà intellettuale del codice rendendo il programma più difficile da comprendere e quindi da violare, e dagli scrittori di malware per aggirare le tecniche di riconoscimento automatico. Abbiamo utilizzato la teoria formale dell'interpretazione astratta per modellare le tecniche di offuscamento al fine di comprenderne limiti e potenzialità, evidenziando gli effetti che gli offuscamenti hanno sulla precisione dei risultati dell'analisi statica [18, 61, 60, 59]. Abbiamo poi usato i risultati ottenuti per definire un framework generale per la modellazione e verifica di robustezza degli antivirus rispetto alle tecniche di offuscamento comunemente usate dai malware [20, 58]. Abbiamo poi approfondito la relazione tra l'incompletezza dei tool di analisi statica e la potenza dell'offuscamento, ovvero la capacità dell'offuscamento di confondere un attaccante interessato nei risultati di quella specifica analisi, al fine di suggerire strategie per sviluppare offuscameti in grado di sconfiggere un dato attaccante [12, 46, 15]. Abbiamo poi formalizzato gli effetti delle tecniche di offuscamento sulla precisione dell'analisi dinamica [29, 30].

Nel contesto del remote entrusting, abbiamo proposto tecniche per la protezione della proprietà intellettuale del codice basate sullo slicing dei programmi e sull'offuscamento. Lo scopo è quello di poter garantire al server, che ha solo accesso remoto al client, l'affidabilità delle applicazioni in esecuzione sul client [19, 57, 55].

**Malware detection and program similarity:** Abbiamo mostrato come gli identificatori automatici di malware (per Android) non siano in grado di riconoscere malware offuscati [14]. Per poter identificare varianti offuscate dei malware è necessario definire metodi di riconoscimento che si basino su caratteristiche semantiche del codice o che siano in grado di riconoscere programmi semanticamente simili anche se sintatticamente diversi [50]. Abbiamo quindi sviluppato strumenti automatici in grado di riconoscere programmi simili basandosi su proprietà semantiche [47, 37, 35, 31], oppure applicando algoritmi di deep learning alla rappresentazione di programmi come immagini [10, 34]. Abbiamo poi studiato il problema della similarità del codice nell'ambito dell'attribuzione del codice ad autori [7, 33].

Molti metodi di analisi similarità del codice binario possono essere visti come particolari interpretazioni astratte del codice modellato come automi a stati finiti simbolici (SFA). Abbiamo quindi introdotto la nozione abstract-SFA e studiato la relazione tra le astrazioni sintattiche, topologiche e semantiche degli SFA e gli effetti di queste astrazioni sul linguaggio riconosciuto dall'SFA [42, 43, 40] e come tutto questo possa essere applicato al riconoscimento di malware [45].

**Formalizzazione del watermarking mediante interpretazione astratta e semantica formale:** Il termine software watermarking si riferisce a trasformazioni di codice in grado di nascondere una firma all'interno dei programmi per dimostrarne la proprietà. Abbiamo proposto un framework formale, basato sulla semantica dei programmi e l'interpretazione astratta, per la modellazione delle tecniche di software watermarking e delle relative proprietà di segretezza, resilienza, trasparenza e accuratezza. In particolare, si osserva che la capacità di un attaccante di identificare il watermark può essere espressa come una proprietà di completezza dell'analisi [11, 36]. Abbiamo proposto un algoritmo di software watermarking che sfrutta la relazione tra semantica e sintassi [56].

**Interpretazione astratta e analisi di programmi:** Abbiamo introdotto la nozione di semantica delle fasi per formalizzare il comportamento di codice che si auto-modifica (come alcuni malware) e ne abbiamo dimostrato la correttezza mostrando che si tratta di un'interpretazione astratta della semantica delle tracce [17, 54]. Abbiamo introdotto il concetto di firme metamorfiche: rappresentazioni astratte del codice in grado di riconoscere tutte le varianti generate da un malware che si auto-modifica e le abbiamo specificate in termini di grammatiche indicizzate [9]. Abbiamo quindi studiato le proprietà dei linguaggi riconosciuti dalle grammatiche indicizzate e approfondito la loro relazione con gli altri linguaggi nella gerarchia di Chomsky [32].

La completezza è una proprietà desiderabile dell'interpretazione astratta in quanto rappresenta l'assenza di falsi positivi nell'analisi. La completezza è raramente soddisfatta e di fatto abbiamo a che fare con analisi incomplete e quindi con falsi positivi. Abbiamo quindi proposto un'indebolimento del concetto di completezza, che chiamiamo completezza parziale, dove viene fissato un limite alla quantità di falsi positivi dell'analisi. In questo modo è possibile distinguere e misurare i diversi livelli di imprecisione delle analisi aprendo nuovi orizzonti nell'analisi del codice [8, 27].

Data la natura immutabile della blockchain è importante poter rilevare problemi di sicurezza prima della distribuzione degli smart contract. Sfortunatamente, l'analisi degli smart contract è resa complicata dall'assenza del codice sorgente. Per supportare l'analisi del codice compilato abbiamo proposto un nuovo approccio basato sull'esecuzione simbolica per l'estrazione di un control flow graph preciso da bytecode generato dall'Ethereum Virtual Machine [6, 28].

**Sistemi distribuiti:** Lo sviluppo di applicazioni distribuite libere da deadlock e race-condition è complesso soprattutto in presenza di aggiornamenti dinamici. Abbiamo introdotto approccio basato su choreographic programming che permette di specificare quali parti dell'applicazione possono essere aggiornate e di generare a tempo di esecuzione applicazioni senza deadlock e race conditions [13, 41, 44, 16]. Abbiamo studiato il problema dell'integrazione di servizi nel contesto delle architetture orientate ai servizi [48, 49, 52].

## Premi e riconoscimenti

**(Agosto 2006)** Vincitrice del QinetiQ ([www.qinetiq.com](http://www.qinetiq.com)) Award for research contributions with strong practical applications al Doctoral Symposium associato alla conferenza Formal Methods 2006, Hamilton, Canada, Agosto 2006.

**(Ottobre 2007)** Riceve una menzione speciale da parte della commissione del capitolo italiano della EATCS (European Association for Theoretical Computer Science) che assegna il premio annuale per la miglior tesi di dottorato in informatica teorica.

## Relazioni invitate

**(2024)** Seminario per ultimo anno magistrale e dottorato di ricerca in informatica presso il Dipartimento di Informatica dell'Università di Pisa dal titolo "Measuring the (im)precision of program analysis".

**(2022)** Webinar su tema Cybersecurity, organizzato da Unioncamere del Veneto che, nell'ambito del "Programma Infrastrutture - Fondo di perequazione 2019-2020", ha programmando attività di "Sensibilizzazione delle PMI sui temi della BUL, del 5G e del digitale a favore di una crescita della cultura digitale". 13 Luglio 2022.

**(2021)** Intervento al convegno CyberSecurity: l'importanza delle difese informatiche nel post-pandemia all'interno di mcT Cyber Security - Mostra Fiera Cyber Security, Milano. 26 Novembre 2021.

**(2021)** Technology as a Social Fact Prof. Ryan Calo Lane Powell & D. Wayne Gittinger Professor of Law, University of Washington, Presenta e introduce Prof. Lorenzo Picotti - Ordinario di diritto penale, Università di Verona, Discussants: Prof.ssa Mila Dalla Preda - Associato di Informatica, Università di Verona, Prof. Massimiliano Badino - Associato di filosofia della scienza, Università di Verona, Prof. Roberto Flor - Associato di diritto penale, Università di Verona. 20 Ottobre 2021.

(2021) Intervento al convegno Sicurezza informatica: come difendersi dai cyber criminali. Organizzato dal Dipartimento di Informatica dell'Università di Verona in collaborazione con lo studio legale "4 chiacchiere" e con il patrocinio del comune di Verona. 21 Aprile 2021.

(2019) Dagstuhl Seminar 19331, Title: Software Protection Decision Support and Evaluation Methodologies. Organizzatori Mila Dalla Preda (University of Verona, Italy), Bjorn De Sutter (Ghent University, Belgium), Christina Collberg (University of Arizona - Tucson, US) and Brecht Wyseur (NAGRA Kudelski Group SA – Cheseaux, CH). 11-16 Agosto 2019.

(2017) Dagstuhl Seminar Seminar 17281, Title: Malware Analysis: From Large-Scale Data Triage to Targeted Attack Recognition. Organizzatori: Saumya K. Debray (University of Arizona - Tucson, US), Thomas Dullien (Zürich, CH), Arun Lakhotia (University of Louisiana - Lafayette, US), Sarah Zennou (Airbus Group - Suresnes, FR). 9-14 Luglio 2017.

(2014) Invitata ad intervenire all'ARO Workshop on Continuously Upgradeable Software Security and Protection, Phoenix, AZ, USA. 17 Novembre 2014.

(2014) Invitata ad intervenire al Cyber Security Day in Verona, evento all'interno del Cyber Security Month organizzato da ENISA. 6 Ottobre 2014.

(2014) Dagstuhl Seminar 14241 - Challenges in Analysing Executables: Scalability, Self-modifying Code and Synergy. Organizzatori: Roberto Giacobazzi (University of Verona, IT), Axel Simon (TU Munchen, DE), Sarah Zennou (EADS-Suresnes, FR). 9-13 Giugno 2014.

(2013) Invita ad intervenire al 27th CREST open workshop - Malware CREST27, UCL, London. 29 Maggio 2013.

(2011) Seminario dal titolo "Modeling Metamorphism by Abstract Interpretation", presso il Center for Advanced Computer Studies, University of Louisiana at Lafayette. 24 Maggio 2011.

(2008) Seminario dal titolo "Advances in Code Obfuscation and Malware Detection by Abstract Interpretation", presso il Dipartimento di Scienze dell'Informazione, Università di Bologna. 18 Novembre 2008.

(2007) Seminario dal titolo "Code Obfuscation and Malware Detection by Abstract Interpretation", presso il Computer Science Department, University of Madison, Wisconsin, USA. 18 Luglio 2007.

(2006) Seminario dal titolo "Code Obfuscation and Malware Detection by Abstract Interpretation", presso il Department of Information and Communication Technology, Università di Trento. 9 Novembre 2006.

(2004) Seminario dal titolo "Completeness Refinement in Abstract Symbolic Trajectory Evaluation", presso il Dipartimento di Informatica, Università di Verona. Luglio 2004.

## **Relatrice a Convegni internazionali tra cui**

M. Dalla Preda, R. Giacobazzi, N. Marastoni. Formal Framework for reasoning about the precision of dynamic analysis. 27th Static Analysis Symposium, SAS 2020.

M. Dalla Preda, I. Mastroni e R. Giacobazzi. Formal Framework for property-driven obfuscation. 19th International Symposium of Fundamentals of Computer Theory FCT 2013.

M. Dalla Preda, R. Giacobazzi, S. Debray, K. Coogan, G. Townsedn. Modelling Metamorphism by Abstract Interpretation. 17th International Static Analysis Symposium SAS 2010.

M. Dalla Preda, M. Christodorescu, S. Jha e S. Debray. A semantics-based approach to malware detection. 34th ACM Symposium on Principles of Programming Languages POPL 2007.

M. Dalla Preda, M. Madou, R. Giacobazzi e K. De Bosschere. Opaque Predicate Detection by Abstract Interpretation. 11th International Conference on Algebraic Methodology and Software Technology AMAST 2006.

M. Dalla Preda e R. Giacobazzi. Control Code Obfuscation by Abstract Interpretation. IEEE International Conference on Software Engineering and Formal Methods SEFM 2005.

M. Dalla Preda e R. Giacobazzi. Semantics-based Code Obfuscation by Abstract Interpretation. 32th International Colloquium on Automata, Languages and Programming ICALP 2005.

M. Dalla Preda. Completeness Refinement in Abstract Symbolic Trajectory Evaluation. 11th Static Analysis

Symposium SAS 2004.

## Formazione di Giovani Ricercatori

- Responsabile scientifico della dottoranda Veronica Paternolli, Dottorato in Informatica - 39° ciclo (Ottobre 2023 - Dicembre 2026).
- Responsabile scientifico del Ricercatore a Tempo Determinato (RTDa) SSD INF/01 finanziato dal PON (DM 1062 del 2021) vinto dalla Dott.ssa Vittoria Cozza. Tema della ricerca: software security and smart cities (Febbraio 2022 - Gennaio 2025).
- Responsabile scientifico dell'assegno di ricerca SSD INF/01 vinto dal Dott. Marco Campion. Tema della ricerca: precisione dell'analisi di programmi (Aprile 2021 - Marzo 2023).
- Responsabile scientifico dell'assegno di ricerca SSD INF/01 vinto dal Dott. Michele Ianni. Tema della ricerca: analisi del codice binario (Ottobre 2019 - Ottobre 2021).
- Responsabile scientifico del dottorando Niccolò Marastoni, Dottorato in Informatica - 33° ciclo (Ottobre 2017 - Dicembre 2020).
- Responsabile dell'assegno di ricerca SSD INF/01 vinto dal Dott. Niccolò Marastoni, Tema della ricerca: Analisi e classificazione di applicazioni Android (Dicembre 2016 - Settembre 2017).

## Servizi alla Comunità Scientifica

**(2025)** Program co-chair della 20th International Conference on Availability, Reliability and Security, ARES 2025, Ghent, Belgium, August 2025.

**(2024)** Organizzatrice del Dagstuhl Seminar 24112, dal titolo: EU Cyber Resilience Act: Socio-Technical and Research Challenges. Organizzatori Mila Dalla Preda (University of Verona, IT), Serge Egelman (ICSI - Berkeley, US), Anna Maria Mandalari (University College London, GB), Narseo Vallina-Rodriguez (IMDEA Networks Institute - Madrid, ES), March 10 - March 13, 2024.

**(2023)** General Chair del Workshop on Attacks and Software Protection WASP 2023, co-located con ESORICS 2023, The Hague, The Netherlands, Settembre 2023.

**(2020)** General Chair del Workshop on Software Attacks and Defenses SAD 2020, co-located con Euro S&P 2020, 19 Giugno 2020, Genova, Italia.

**(2020)** General Chair del PhD Forum @ITASEC 2020, Annual Italian Conference on Cybersecurity. 6 Febbraio 2020, Ancona, Italy.

**(2019)** Organizzatrice del Dagstuhl Seminar 19331, dal titolo: Software Protection Decision Support and Evaluation Methodologies. Organizzatori Mila Dalla Preda (University of Verona, Italy), Bjorn De Sutter (Ghent University, Belgium), Christian Collberg (University of Arizona - Tucson, US) and Brecht Wyseur (NAGRA Kudelski Group SA – Cheseaux, CH). Agosto 11th - 16th 2019.

**(2018-2019)** Steering Committee di ACM Software Security, Protection and Reverse Engineering Workshop 2018-2019.

**(2013-2017)** Co-chair di ACM Software Security, Protection and Reverse Engineering Workshop, SSPREW 2017-2016-2015-2014-2013.

## Progetti di Ricerca

ODIN: Abstract Interpretation Driven Programming Languages. Funded 800K by AIR FORCE OFFICE OF SCIENTIFIC RESEARCH. September 2023 - September 2028. Ruolo: **Principal Investigator**

COVERT: In search of evidence of stealth cyber threats. Funded 200K by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. June 2024 - December 2025. Ruolo: **Principal Investigator for UniVR**

SOP: Securing sOftware Platforms Funded 130K by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. April 2024 - December 2025. Ruolo: **Principal Investigator for UniVR**

BINTRACE: Binary Similarity Analysis based on Execution Traces. Joint Project dell'Università di Verona con Relatech SPA. Finanziamento: 45K Euro. Gennaio 2020 - Gennaio 2022. Ruolo: **Principal Investigator**

SMALAWI: Smart Label Wine Funded by Regione Veneto. Partners: Vignaioli Veneti (PI), Dipartimento di Economia Aziendale, Dipartimento di Informatica - Università degli studi di Verona. Marzo 2019 - Marzo 2022. Ruolo: **Researcher**

Cyber Risk Management e Resilienza nelle Operations: modelli di analisi di rischio, strategie di gestione e copertura assicurativa. Finanziato da Fondazione Cariverona. Partners: Dipartimento di Economia Aziendale (PI), Dipartimento di Informatica - Università degli studi di Verona. Ottobre 2019 - Ottobre 2021. Ruolo: **Researcher**

ASPIS: Early threat detection by approximate similarity analysis. Joint Project dell'Università di Verona con Poste Italiane. Finanziamento: 47K Euro. Gennaio 2017 - Gennaio 2019. Ruolo: **Principal Investigator**

FACE: Sconfiggere i malware in modo formale (2014-2018). Progetto MIUR "Futuro in ricerca 2013" coordinato tra le università di Milano e Verona (PI). (acceptance rate 5,10%). Finanziamento 522K Euro. Marzo 2014 - Marzo 2018. Ruolo: **Principal Investigator**

SMART AGGREGATION: Sovvenzione Globale Spinner 2013 – Programma Operativo Regione Emilia-Romagna. Ruolo: **Principal Investigator** 2010 -2011.

Shadowcode: code protection in .net by abstract and dynamic steganography. Joint Project dell'Università di Verona con Consorzio Veneto dell'Informatica e del Tecnologico Avanzato (VITA). Marzo 2009 - Marzo 2011. Ruolo: **Researcher**

PRIN2007: Analisi e protezione del software mediante interpretazione astratta. PRIN 2007, Progetto MIUR COFIN coordinato tra le Università di Padova, Parma e Verona. Settembre 2008 - Settembre 2010. Ruolo: **Researcher**

RE-TRUST: Remote EnTrusting by RUn-time Software auThentication (2007-2010), progetto europeo FET coordinato tra l'Università di Trento, Politecnico di Torino, Gemalto (France), Katholieke Universiteit (Leuven-Belgium) and SPIIRAS St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (Russia). Ruolo: **Researcher**

## Trasferimento tecnologico

(2021) socia fondatrice dello Spin-off dell'Università di Verona, costituito a Settembre 2021: Vero4Chain per lo sviluppo di soluzioni blockchain per la tracciabilità e NFT.

(2021 – oggi) membro Consiglio Direttivo del Centro di Scienze della Sicurezza e della Criminalità, Università degli Studi di Trento - Università degli Studi di Verona. Il centro inter-universitario vuole promuovere la formazione e la ricerca sulla sicurezza, intesa sia come security sia come safety.

(2018 – 2019) Tetra Pak Packaging Solutions S.p.A., Via Delfini, 1, Modena. Attività di consulenza per lo studio di specifiche soluzioni per problemi di sicurezza posti da Tetra Pak.

(2019 - 2020) DANIELI AUTOMATION è parte del Gruppo Danieli, azienda multinazionale che opera nel capo della siderurgia. Abbiamo collaborato con la sede di DANIELI AUTOMATION di Udine. Attività di consulenza per lo studio di soluzioni specifiche per la protezione della proprietà intellettuale del codice.

## Collaborazioni scientifiche

Dr. Narseo Vallina-Rodriguez - Research Associate Professor (Ramon y Cajal Fellow). IMDEA Networks Institute, Madrid, Spain.

Prof. Natalia Stakhanova, University of Saskatchewan, Canada. (dal 2013). Pubblicazioni rilevanti [7, 33].

Prof. Arun Lakhotia, University of Louisiana at Lafayette - Center for Advanced Computers Studies, Lafayette, Louisiana USA (dal 2011). Pubblicazioni rilevanti [43, 47, 50].

Prof. Stefano Zanero, Politecnico di Milano, Italia (dal 2014). Gestione del progetto FIRB, attività della Cyberchallenge e una pubblicazione [39].

Prof. Saumya Debray, University of Arizona - Department of Computer Science, Tucson, Arizona USA (dal 2006). Pubblicazioni rilevanti [17, 20, 54, 58].

Prof. Christian Collberg, University of Arizona - Department of Computer Science, Tucson, Arizona USA (dal 2006). Organizzazione del Dagstuhl Seminar 19331 e pubblicazioni rilevanti [19, 57].

Prof. Somesh Jha, University of Wisconsin - Department of Computer Science, Madison, Wisconsin USA (dal 2006). Pubblicazioni rilevanti [20, 58].

Prof. Bjorn De Sutter, Department of Electronics and Information Systems, Ghent University, Belgium (dal 2006). Organizzazione del Dagstuhl Seminar 19331.

Prof. Koen De Bosschere, Universiteit Ghent - Department of Computer Science, cv-Ghent, Belgio (in 2005-2006). Pubblicazioni rilevanti [59].

## Attività di Revisione per Progetti Internazionali

**(2024)** Valutatore di due proposte per la YOUNG INTERNATIONAL ACADEMICS call per la selezione di ricercatori per la University of Luxemburg.

**(2024)** Componente della commissione valutatrice per le proposte ricevute in ambito AUTOMOTIVE, relativamente ai bandi di ricerca e innovazione banditi dall'associazione Cyber4.0 e finanziati dal MIMIT (Ministero delle Imprese e del Made in Italy)

**(2020)** Valutatore di quattro proposte per la Young Academics research proposal per la University of Luxembourg's Institute of Advanced Studies. Per la selezione di candidati per PhD interdisciplinari (Agosto 2020)

**(2019)** Valutatore di un progetto di ricerca per Austrian Science Fund (FWF) dal titolo "Inference of Optimal Cyber Defense Strategies" (Maggio 2019)

**(2016)** Valutatore di un progetto di ricerca per Internal Research Projects Call 2016 per l'University of Luxembourg (UL) dal titolo "HitDroid: Hinting at Malicious Code in Android Apps Identifying Malicious Payloads in Malware at Market Scale with Graph and Data Clustering Techniques" (Giugno 2016)

## Commissioni di Concorso

**(Luglio/Agosto 2025)** Componente della commissione per il conferimento Premio giovane ricercatore italiano in Informatica Teorica bandito dal Capitolo Italiano dell'EATCS per un giovane ricercatore o una giovane ricercatrice che abbia svolto la propria recente attività di ricerca primariamente in Italia e che abbia apportato un contributo significativo all'Informatica Teorica.

**(Luglio/Agosto 2024)** Componente della commissione per il conferimento Premio giovane ricercatore italiano in Informatica Teorica bandito dal Capitolo Italiano dell'EATCS per un giovane ricercatore o una giovane ricercatrice che abbia svolto la propria recente attività di ricerca primariamente in Italia e che abbia apportato un contributo significativo all'Informatica Teorica.

**(Maggio/Luglio 2024)** Componente della commissione di concorso per un posto da Assistant Professors (Tenure-track) in Computer Science with focus on Programming Languages or Concurrency, University of Southern Denmark (SDU), Danimarca.

**(Ottobre/Novembre 2023)** Componente della commissione di concorso per un posto da assistant professor in informatica, University of Southern Denmark (SDU), Danimarca.



**(Luglio/Agosto 2023)** Componente della commissione di concorso per un posto RTDb INF/01, Dipartimento di Matematica e Informatica, Università degli studi di Catania.

**(Ottobre/Novembre 2022)** Componente della commissione di concorso per un posto da professore associato in informatica, University of Southern Denmark (SDU), Danimarca.

**(Maggio/Giugno 2022)** Componente della commissione di concorso per un posto RTDb INF/01, Dipartimento di Informatica, Sapienza, Roma.

**(Luglio 2020)** Componente della commissione giudicatrice per l'ammissione al XXXVI ciclo di Dottorato in Informatica XXXVI (2020), Dipartimento di Informatica - Università di Verona.

### **Commissione Esame Finale di Dottorato**

**(Maggio 2025)** Componente della commissione giudicatrice per l'esame finale di dottorato in Global Studies. Justice, Rights, Politics della dott.ssa Ludovica Ilari. PhD all'Università degli Studi di Macerata. Titolo della tesi: Navigating Ethical Challenges in Cybersecurity: From Risk Assessment to Quantum-AI Applications.

### **Comitati Editoriali e di Programma per Conferenze Internazionali**

**(WeRobot 2026)**, Berlin.

**(POPL 2026, 2023, 2018, 2017)** ACM SIGPLAN Symposium on Principles of Programming Languages.

**(OOPSLA 2026)** ACM Conf on Object Oriented Programming Systems Languages and Applicatins.

**(TACAS 2024, 2025)** International Conf. on Tools and Algorithms for the Construction and Analysis of Systems.

**(DPM 2023, 2024)** Workshop on Data Privacy Management DPM @ ESORICS.

**(ESORICS 2024)** 29th European Symposium on Research in Computer Security.

**(ITASEC 2023, 2022)** Italian Conference on Cybersecurity .

**(FPS 2013-2016, 2019 - 2021)** International Symposium on Foundations & Practice of Security .

**(FORTE 2019)** International Conf. on Formal Techniques for Distributed Objects, Components, and Systems.

**(CRISIS 2020 )** International Conference on Risks and Security of Internet and Systems.

**(APLAS 2020)** Asian Symposium on Principles of Programming Languages and Systems.

**(CC 2020)** International Conference on Compiler Construction.

**(SPRO 2015, 2016, 2019)** IEEE International Workshop on Software PROtection.

**(ForSE 2017 - 2019)** International Workshop on FORMal methods for Security Engineering.

**(SECURWARE 2017, 2018)** Internat. Conf. on Emerging Security Information, Systems and Technologies.

**(NSAD 2016)** Numerical and Symbolic Abstract Domain Workshop, .

**(CGO 2016)** IEEE/ACM International Symposium on Code Generation and Optimization.

**(PLDI 2015)** ACM SIGPLAN conference on Programming Language Design and Implementation.

**(SOFSEM 2014, 2015)** International conference on Current Trends in Theory and Practice of Computer Science - Cryptography, Security & Verification track.

**(SAS 2025, SAS 2013)** Static Analysis Symposium.

**(MALWARE 2012, 2012)** IEEE international conference MALWARE.

### **Attività di Revisione per Riviste Internazionali**

**(2023)** Journal of Software: Evolution and Process - John Wiley and Sons Ltd.

**(2018 –2022)** Journal of Computer Virology and Hacking Techniques - Springer.

**(2021)** Information Science - Elsevier.

**(2020, 2022)** IEEE Transactions of Software Engineering.

**(2020)** IEEE Transactions on Dependable and Secure Computing.

**(2019)** Journal of Computer Security - IOS Press.

(2019, 2016, 2011) Journal of Systems and Software - Elsevier.  
(2019, 2017, 2015, 2011) Journal of Information Security - Springer.  
(2017) Recent Patents on Engineering - Benthamscience.  
(2015) International Journal of Computers in Healthcare (IJCIH) - InderScience.  
(2015) Discrete and Applied Mathematics - Elsevier.  
(2011) Higher-Order and Symbolic Computation - Springer.  
(2010) IEEE Software Journal.

## Didattica

**Compilatori (6 crediti)** Laurea in Informatica. Dipartimento di Informatica. AA 2024/2025, AA 2023/2024, AA 2022/2023, AA 2021/2022, AA 2020/2021.

**Sicurezza del Software (6 crediti)** Laurea Magistrale in Ingegneria e Scienze Informatiche. Dipartimento di Informatica. AA 2024/2025, AA 2023/2024, AA 2022/2023, AA 2021/2022, AA 2020/2021, AA 2019/2020, AA 2018/2019, AA 2017/2018, AA 2016/2017.

**Nuove tecnologie e gestione dei dati (6 crediti)** Laurea Magistrale in Diritto per le Tecnologie e l'Innovazione Sostenibile. Dipartimento di Scienze Giuridiche. AA 2024/2025, AA 2023/2024.

**Fondamenti di Linguaggi di Programmazione e Specifica (3 crediti su 12).** Laurea Magistrale in Ingegneria e Scienze Informatiche. Dipartimento di Informatica. AA 2024/2025, AA 2023/2024, AA 2022/2023, AA 2021/2022.

**Data Security & Privacy (2 crediti su 6)** Laurea Magistrale in Data Science. Dipartimento di Informatica. AA 2024/2025, AA 2023/2024, AA 2022/2023, AA 2021/2022, AA 2020/2021.

**Informatica (4 crediti)** modulo del corso Scienze comportamentali e metodologia scientifica nel corso di Laurea magistrale a ciclo unico in Odontoiatria e protesi dentaria. Scuola di Medicina e Chirurgia. AA 2019/2020, AA 2017/2018, AA 2016/2017.

**Informatica di base (6 crediti)** Corso di Laurea in Scienze della Comunicazione. Dipartimento di Cultura e Civiltà. AA 2019/2020, AA 2018/2019, AA 2017/2018, AA 2016/2017.

**Analisi Statica e Protezione (6 crediti)** corso caratterizzante del Curriculum in Ingegneria del Software e Sicurezza del Corso di Laurea Magistrale in Ingegneria e Scienze Informatiche. Dipartimento di Informatica. AA 2015/2016, AA 2014/2015.

## Relatore tesi di Laurea

### Relatrice delle seguenti Tesi di Laurea Magistrale in Ingegneria e Scienze Informatiche

Dott. Alessio Tonelli "Minacce cyber nell'automotive Simulazione di un replay attack" AA 2023/2024. Valutazione: 109/110

Dott.ssa Laura Canaia "The role of cognizance in responsibility" A.A. 2023/2024. Valutazione: 110/110

Dott. Simone Baldi "Development and Evaluation of a Secure Gateway for Industry 4.0 Applications" A.A. 2022/2023. Valutazione: 102/110

Dott. Andrea Caliarì "Analisi di Sicurezza dei Protocolli RF Sub-Gigahertz in Dispositivi IoT per il Controllo Termico" A.A. 2022/2023. Valutazione: 109/110

Dott. Federico Bertelli "Conversazioni invisibili: il sensore di luminosità per comunicare con gli smart phone" A.A. 2022/2023. Valutazione 90/110.

Dott. Massimo Diviggiano "Watermarking e NFT" A.A. 2021/2022. Valutazione 97/110.

Dott. Cittadini Massimiliano "Un metodo pseudocasuale di offuscamento dell'attribuzione di codice sorgente." A.A. 2020/2021. Valutazione 107/110.

Dott. Giovanni Schiavone "anonsw: un approccio alternativo per l'author obfuscation" A.A. 2020/2021. Valutazione 107/110.

Dott. Padovani Alan Michael "Heap spraying attacks and countermeasures" AA 2020/2021. Valutazione 110/110 e lode.

Dott. Marco Fattorelli “Analysis of Covid-19 related cyber attacks: a focus on international enterprises and reverse engineering of Maze ransomware” AA 2019/2020. Valutazione 110/110 e lode.

Dott. Michele Martini “Analysis of Covid-19 related cyber attacks: a focus on international enterprises and reverse engineering of Ekans ransomware” AA 2019/2020. Valutazione 110/110 e lode.

Dott. Paolo D’Arienzo “Classification of programs as binary files with LSTM” AA 2019/2020. Valutazione 107/110.

Dott. Michele Pasetto “A statistical similarity approach to Android malware” AA 2018/2019.

Dott. Tommaso Bonetti “Malware classification based on risky data flow” AA 2018/2019. Valutazione 110/110 e lode.

Dott. Davide Rocco “Anomaly detection of malicious consumer behaviours” AA 2018/2019. Valutazione 100/110.

Dott. Riccardo Pret “Andorid Malware Classification: an approach based on resource similarity through fuzzy hashing” AA 2016/2017. Valutazione 110/110 e lode.

Dott. ssa Elisa Pellegrini “ITA: an Instrumentation Tool for dynamic analysis of Android applications” AA. 2016/2017. Valutazione 110/110 e lode.

Dott. Marco Campion “Learning di regole di riscrittura da widening di automi” AA 2015/2016. Valutazione 110/110 e lode.

Dott. Giacomo Annaloro “Tecniche di evasione dall’analisi dei malware: anti-emulation e anti-instrumentation” AA 2015/2016. Valutazione 105/110.

Dott. Niccolò Marastoni “R.E.H.A. Reverse Engineering Helper for Android” AA 2015/2016. Valutazione 110/110 e lode.

Dott. Luca Barile “Telephone mobile malware for Android” AA 2015/2016. Valutazione 110/110.

Dott. Alberto Albiero: “Identificazione automatica della manomissione tramite hashing” AA 2014/2015. Valutazione 106/110.

Dott.ssa Vanessa Vidali: “Abstract Similarity Analysis For Python” AA 2014/2015. Valutazione 110/100 e Lode.

Dott. Filippo Vivaldi: “Taint Analysis per PHP usando il K-Framework” AA 2014/2015. Valutazione 100/110.

Dott. Alberto Fanini: “Alias Analysis per PHP basata sul K-Framework” AA 2014/2015. Valutazione 108/110.

Dott. Michele Pasqua: “Approccio semantico al Software Watermarking: Un modello generale basato su Interpretazione Astratta” AA 2014/2015. Valutazione 110/110 e lode.

#### **Relatrice delle seguenti Tesi di Laurea in Informatica**

Dott. Matteo Menegatti “Analisi Comparativa di Tool di Analisi Statica” 2024/2025

Dott. Matteo Baucé “Buffer Overflow: Vulnerabilità e Tecniche di Mitigazione” 2023/2024

Dott. Roman Cicolin “Comparazione tra regole di correlazione statiche e dinamiche per la rilevazione di falsi positivi di attacchi informatici brute force” 2023/2024.

Dott. Davide Cordioli. “Sicurezza sistemi IoT implementati con AWS: analisi vulnerabilità e mitigazione attraverso uso di strumenti diagnostici messi a disposizione dal Cloud” 2022/2023.

Dott. Altamura Nicolò “Microscope: un software per l’analisi statica di ransomware basata sulla costruzione di diagrammi di controllo di flusso.” AA 2022/2023.

Dott. Ancute Alin Gheorghe “Programmare in Reach.” AA 2022/2023.

Dott. Bragastini Enrico. “Investigating partial-completeness.” AA 2022/2023.

Dott. Riccardo Felisi “Tecnologie emergenti in ambito blockchain.” AA 2022/2023.

Dott. Alvisè Bacco “Active Directory: attacco e difesa in cybersicurezza.” AA 2022/2023.

Dott. Pietro Pedrina “Utilizzo dei DAG nei compilatori” AA 2022/2023.

Dott. Luca Lovato “Buffer Overflow e mitigazioni” AA 2021/2022.

Dott. Luca Ziliani “ROPfinder, un tool per attacchi ROP ” AA 2020/2021.

Dott. Denis Rudes “Analisi dinamica di malware in ambiente virtualizzato controllato ” AA 2020/2021.

Dott. Enrico Cavicchini “flagWarehouse: tool per la gestione degli exploit in competizioni Capture the Flag ”

AA 2020/2021.

Dott. Francesco Tubini “Analisi di binari tramite Angr” AA 2020/2021.

Dott. Riccardo Peruffo “Analisi di comportamenti anomali e malevoli. ” AA 2018/2019.

Dott. Cristian Turetta “Clustering techniques applied on Android malware analysis” AA 2016/2017.

**Relatrice delle seguenti Tesi di Laurea Magistrale in Diritto per le Tecnologie e l’Innovazione Sostenibile**

Dott. Elia Giacon.”AI-Act Sfide e Impatti per le imprese” AA 2024/2025. Valutazione 103/110

Dott.ssa Martina Papiccio. AA 2024/2025. ”La Cybersecurity nell’Unione Europea tra obblighi normativi e applicazione operativa: il modello della direttiva NIS2” Valutazione 104/110

Dott.Marco Bressan “Smart Contract ed Enforceable Business Processes: una soluzione tecnologica all’incompletezza contrattuale” AA 2024/2025. Valutazione 110/110 e Lode.

**Relatrice delle seguenti Tesi di Laurea Scienze della Comunicazione**

Dott.ssa Chiara Piana “Nuove forme di narrazione digitale: il caso Scratch” AA 2021/2022.

## Lista delle Pubblicazioni

### Riviste

- [1] G. Gaggero, R. Caviglia, D. Aliaskharov, A. Aceti, M. dalla Preda and P. Girdinio. A Security Operation and Event Management (SOEM) Platform for Critical Infrastructures Protection. To appear in CMC-Computers, Materials & Continua
- [2] M. Dalla Preda, C. Greco, M. Ianni, F. Lupia, A. Pugliese. Light Sensor Based Covert Channels on Mobile Devices. To appear in Information Science.
- [3] V. Cozza, M. Dalla Preda, R. Lanotte, M. Lucchese, M. Merro, N. Zannone. Obfuscation Strategies for Industrial Control. To appear in International Journal of Critical Infrastructure Protection.
- [4] M. Champion, M. Dalla Preda, R. Giacobazzi and Caterina Urban. Monotonicity and the Precision of Program Analysis. *51st ACM SIGPLAN Symposium on Principles of Programming Languages*. volume 8, number POPL, pag. 1629–1662, 2024, [DOI](#)
- [5] M. Dalla Preda and M. Ianni. Exploiting Number Theory for Dynamic Software Watermarking. *Journal of Computer Virology and Hacking Techniques*. 20(1) pag.41–51, [DOI](#)
- [6] M. Pasqua, A. Benini, F. Contro, M. Crosara, M. Dalla Preda, M. Ceccato. Enhancing Ethereum Smart-Contracts Static Analysis by Computing a Precise Control-Flow Graph of Ethereum Bytecode. *Journal of Systems & Software*, Elsevier. volume 200, pag.111653, 2023 [DOI](#).
- [7] F. Abazari, E. Branca, N. Ridley, N. Stakhanova, M. Dalla Preda. Dataset characteristics for reliable code authorship attribution. *IEEE Transactions on Dependable and Secure Computing* 20(1): 506-521, 2023. ISSN 1545-5971. [DOI](#).
- [8] M. Champion, M. Dalla Preda, and R. Giacobazzi. Partial (In)Completeness in Abstract Interpretation. The 49th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2022), *PACMPL (POPL)* 6, POPL, Article 59 (January 2022), 31 pages. 2022.ISSN 2475-1421. [DOI](#).
- [9] M. Champion, M. Dalla Preda, and R. Giacobazzi. Learning Metamorphic Malware Signatures from Samples. *Journal of Computer Virology and Hacking Techniques*. February 2021. ISSN 2263-8733. [DOI](#).
- [10] N. Marastoni, R. Giacobazzi, and M. Dalla Preda. Data Augmentation and Transfer Learning to Classify Malware Images in a Deep Learning Context. *Journal of Computer Virology and Hacking Techniques*. April 2021. ISSN 2263-8733. [DOI](#).
- [11] M. Dalla Preda and M. Pasqua. Semantics-based Software Watermarking by Abstract Interpretation. *Mathematical Structures in Computer Science* 29(2), pages 339-388, 2019. ISSN 09601295. [DOI](#).
- [12] M. Dalla Preda e I. Mastroeni. Characterizing a Property Driven Obfuscation Strategy. *Journal of Computer Security* 26(1), pages 31-69, 2018. ISSN 0926-227X [DOI](#).
- [13] M. Dalla Preda, M. Gabbrielli, S. Giallorenzo, I. Lanese, J. Mauro. Dynamic Choreographies: from theory to practice. *Logical Methods in Computer Science* 13(2) 2017. ISSN 1860-5974. [DOI](#).
- [14] M. Dalla Preda e F. Maggi. Testing Android Malware Detectors Against Code Obfuscation: A Systematization of Knowledge and Unified Methodology. *Journal of Computer Virology and Hacking Techniques* 13(3) pages 209 - 232, 2017. ISSN 2274-2042. [DOI](#).
- [15] R. Giacobazzi, I. Mastroeni, and M. Dalla Preda. Maximal incompleteness as obfuscation potency. *Formal Aspects of Computing* 29(1):3-31, Springer Verlag, 2017. ISSN: 0934-5043. [DOI](#).

- [16] M. Dalla Preda, M. Gabbrielli, S. Giallorenzo, I. Lanese e J. Mauro. Developing correct, distributed, adaptive software. *Science of Computer Programming (SCP)* vol. 97, pages 41-46, 2015. ISSN: 0167-6423. [DOI](#).
- [17] M. Dalla Preda, R. Giacobazzi, and S. Debray. Unveiling Metamorphism by Abstract Interpretation of Code Properties. *Theoretical Computer Science*. Volume 577(27):74-97 2015. [DOI](#).
- [18] M. Dalla Preda and R. Giacobazzi. Semantic-based Code Obfuscation by Abstract Interpretation. *Journal of Computer Security*, 17(6):855-908, 2009. [DOI](#).
- [19] M. Ceccato, M. Dalla Preda, J. Nagra, C. Collberg e P. Tonella. Trading off security and performance in barrier slicing for remote software trusting. *Special Issue of Journal of Automated Software Engineering* 16(2), pages 235-261, 2009. ISSN: 0928-8910. [DOI](#).
- [20] M. Dalla Preda, M. Christodorescu, S. Jha e S. Debray. A Semantics-based approach to Malware Detection. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 30(5), pages 1-54. 2008. ISSN: 0164-0925. [DOI](#).

### **Congressi Internazionali**

- [21] N. Altamura, E. Bragantini, M. Campion, M. Dalla Preda. Assessing the Effectiveness of the Tigress Obfuscator Against MOPSA and BinaryNinja *To appear at the Workshop on research on offensive and defensive techniques in the context of Man At The End (MATE) attacks, CheckMATE at ACM CCS 2025*
- [22] V. Paternolli, M. Dalla Preda, R. Giacobazzi. Fairness of AI Systems in the Legal Context *To appear at the Workshop on Fairness and ethics towards transparent AI: facing the chalLEnge through model Debiasing (FAILED), Workshop at ECCV 2024, Milano, Italy.*
- [23] L. Canaia and M. Dalla Preda. On the Role of Cognizance in Responsibility *To appear 31st Static Analysis Symposium SAS 2024.*
- [24] M. Campion, C. Urban, M. Dalla Preda, R. Giacobazzi. A Formal Framework to Measure the Incompleteness of Abstract Interpretation. *To appear 30th Static Analysis Symposium SAS 2023.*
- [25] V. Cozza, M. Dalla Preda, M. Lucchese, M. Merro, N. Zannone. Towards Obfuscation of Programmable Logic Controllers. *To appear SecIndustry@ARES 2023.*
- [26] M. Dalla Preda and F. Masaia. Exploring NFT Validation through Digital Watermarking (short paper). *To appear IWSECC@ARES 2023.*
- [27] M. Campion, M. Dalla Preda, R. Giacobazzi. On the Properties of Partial Completeness in Abstract Interpretation. *23rd Italian Conference on Theoretical Computer Science ICTCS 2022*, pages 79-85. [DOI](#).
- [28] F. Contro, M. Crosara, M. Ceccato, M. Dalla Preda. EtherSolve: Computing an Accurate Control-Flow Graph from Ethereum Bytecode. *29th IEEE/ACM International Conference on Program Comprehension ICPC 2021*, pages 127-137. [DOI](#).
- [29] M. Dalla Preda, R. Giacobazzi, and N. Marastoni. Formal Framework for Reasoning About the Precision of Dynamic Analysis. *The 27th Static Analysis Symposium (SAS2020)*. Lecture Notes in Computer Science, vol 12389, pages 178-199. 2020. [DOI](#).
- [30] M. Dalla Preda. Towards a unifying framework for tuning analysis precision by program transformation. *Recent Developments in the Design and Implementation of Programming Languages, Gabbrielli's Festschrift 2020*. OASICS 86, Schloss Dagstuhl - Leibniz-Zentrum für Informatik 2020, pages 4:1 - 4:22. ISBN 978-3-95977-171-9

- [31] M. Pasetto, N. Marastoni e M. Dalla Preda Revealing Similarities in Android Malware by Dissecting their Methods. *Workshop on Software Attacks and Defenses SAD@Euro S&P* 2020, pages 625-634. [DOI](#).
- [32] M. Campion, M. Dalla Preda, and R. Giacobazzi. Abstract Interpretation of Indexed Grammars. *The 26th Static Analysis Symposium (SAS2019)*. Lecture Notes in Computer Science, vol 11822, pages 121–139. Springer 2019. [DOI](#).
- [33] A. Matyukhina, N. Stakhanova, M. Dalla Preda, C. Perley. Adversarial author attribution on open-source projects. *9th ACM Conference on Data Application Security and Privacy, CODASPY* 2019, pages 291-302. [DOI](#).
- [34] N. Marastoni, R. Giacobazzi, and M. Dalla Preda. A Deep Learning Approach to Program Similarity. *The 1st International Workshop on Machine Learning and Software Engineering in Symbiosis* 2018. pages 26-35. ACM Press. [DOI](#).
- [35] N. Marastoni, A. Continella, D. Quarta, S. Zanero, M. Dalla Preda. GroupDroid: Automatically classifying mobile malware by extracting code similarity. *7th ACM Workshop on Software Security, Protection and Reverse Engineering SSPREW@ACSAC* 2017, pages 1:1 - 1:12. [DOI](#).
- [36] M. Dalla Preda e M. Pasqua. Software watermarking: a semantics based approach. *6th Numerical and Symbolic Abstract Domain Workshop NSAD* 2016. ENTCS volume 331, pp 71 - 85, 2016. [DOI](#).
- [37] M. Dalla Preda e V. Vidali. Abstract similarity analysis. *6th Numerical and Symbolic Abstract Domain Workshop NSAD* 2016. ENTCS volume 331, pp 87-99, 2016. [DOI](#).
- [38] R. Sarte, M. Dalla Preda, A. Farinelli, R. Giacobazzi, and I. Mastroeni. Active Android malware analysis: an approach based on stochastic games. *6th ACM Workshop on Software Security, Protection and Reverse Engineering SSPREW @ ACSAC* 2016: 5:1-5:10. 2016. [DOI](#).
- [39] C. Zheng, M. Dalla Preda, J. Granula, S. Zanero e F. Maggi. On-chip system call tracing: feasibility study and open prototype for Linux/ARM. *IEEE Conference on Communication and Network System CNS* 2016, pages 73 - 81. [DOI](#).
- [40] M. Dalla Preda, R. Giacobazzi, and I. Mastroeni. Completeness in Approximate Transduction. *The 23th International Static Analysis Symposium SAS'16*, Lecture Notes in Computer Science, pages 129-145, Springer Verlag. September 2016, Edinburgh, UK. [DOI](#).
- [41] M. Dalla Preda, M. Gabbrielli, S. Giallorenzo, I. Lanese e J. Mauro. Dynamic Choreographies Safe Runtime Updates of Distributed Applications. *17th IFIP International Conference on Coordination Models and Languages COORDINATION* 2015, Volume 9037 of Lecture Notes in Computer Science, page 67-82. [DOI](#).
- [42] M. Dalla Preda e I. Mastroeni. Infections as Abstract Symbolic Finite Automata: Formal Model and Applications. *1st IEEE International Workshop on Software PRO-tecton (SPRO)* 2015, page 59-65. [DOI](#).
- [43] M. Dalla Preda, R. Giacobazzi, A. Lakhotia, and I. Mastroeni. Abstract Symbolic Automata. *42th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'15)*, pages 329–341, ACM 2015. [DOI](#).
- [44] M. Dalla Preda, S. Giallorenzo, I. Lanese, J. Mauro e M. Gabbrielli. AIOCI: A Choreography Framework for SafeAdaptive Distributed Applications. *7th International Conference on Software Language Engineering (SLE'14)*. [DOI](#).
- [45] M. Dalla Preda, I. Mastroeni, and R Giacobazzi. Analyzing program dependencies for malware detection. *3rd ACM SIGPLAN Program Protection and Reverse Engineering Workshop 2014, PPREW* 2014, pages 6:1–6:7, ACM. [DOI](#).

- [46] M. Dalla Preda, I. Mastroeni, and R. Giacobazzi. Formal Framework for Property-driven Obfuscations. *19th Int. Symp. on Fundamentals of Computer Theory*, FCT 2013, Volume 8070 of Lecture Notes in Computer Science, pages 133-144, Springer Verlag. 2013. [DOI](#).
- [47] A. Lakhotia, M. Dalla Preda, and R. Giacobazzi. Fast location of similar code fragments using semantic 'juice'. *2nd ACM SIGPLAN Program Protection and Reverse Engineering (PPREW)*. ACM, Article No.: 5, pages 1–6, 2013. [DOI](#).
- [48] M. Dalla Preda, M. Gabbrielli, C. Guidi, J. Mauro e F. Montesi. Service Integration via Target-Transparent Mediation. *IEEE International Conference on Service-Oriented Computing and Applications*, SOCA 2012, pages 1- 5, IEEE Computer Society Press. [DOI](#).
- [49] M. Dalla Preda, M. Gabbrielli, C. Guidi, J. Mauro e F. Montesi. Interface-based service composition with aggregation. *European Conference on Service-Oriented and Cloud Computing (ESOCC'12)*, Volume 7592 of Lecture Notes in Computer Science, pages 48 - 63. 2012. [DOI](#).
- [50] M. Dalla Preda. The Grand Challenge in Metamorphic Analysis. (Position Paper). *International Conference on Information Systems, Technology and Management*, ICISTM 2012. Volume 285 of Communications in Computer and Information Science, pages 439-444. 2012. [DOI](#).
- [51] M. Dalla Preda, W. Feng, R. Giacobazzi, R. Greechie, and A. Lakhotia. Twisting Additivity in Program Obfuscation. In *Program Protection and Reverse Engineering (PPREW12)*. Communications in Computer and Information Science, 285, pages 336-347, 2012. [DOI](#).
- [52] M. Dalla Preda, M. Gabbrielli, I. Lanese, J. Mauro e G. Zavattaro. Graceful Interruption of Request response Service Interactions. *9th International Conference on Service Oriented Computing (ICSOC11)*. Volume 7084 of Lecture Notes in Computer Science, pages 590-600. Springer-Verlag, 2011. [DOI](#).
- [53] M. Dalla Preda e C. Di Giusto. Hunting distributed malware with the k-calculus. *18th International Symposium on Fundamentals of Computation Theory (FCT11)*, volume 6914 of Lecture Notes in Computer Science, pages 102-113. 2011 [DOI](#).
- [54] M. Dalla Preda, R. Giacobazzi, S. Debray, K. Coogan, and G. Townsend. Modelling Metamorphism by Abstract Interpretation. *The 17th International Static Analysis Symposium SAS'10*, volume 6337 of Lecture Notes in Computer Science, pages 218-235, Springer Verlag. 2010. [DOI](#).
- [55] M. Ceccato, M. Dalla Preda, A. Majumdar and P. Tonella. Remote software protection by orthogonal client replacement. *24th Annual ACM Symposium on Applied Computing (SAC'09-SE track)*, pagine 448-455, ACM SIGAPP press. [DOI](#).
- [56] M. Dalla Preda, R. Giacobazzi, and E. Visentini. Hiding software watermarks in loop structures. *The 15th International Static Analysis Symposium SAS'08*, volume 5079 of Lecture Notes in Computer Science, pages 174-188, Springer Verlag. 2008. [DOI](#).
- [57] M. Ceccato, M. Dalla Preda, J. Nagra, C. Collberg e P. Tonella. Barrier Slicing for Remote Software Trusting. *7th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM'07)*, pagine 27-36, Computer Society IEEE Press. 2007 [DOI](#).
- [58] M. Dalla Preda, M. Christodorescu, S. Jha e S. Debray. A semantics-based approach to malware detection. *34th ACM Symposium on Principles of Programming Languages (POPL'07)*, pagine 377-388. 2007. [DOI](#).
- [59] M. Dalla Preda, M. Madou, K. De Bosschere, and R. Giacobazzi. Opaque Predicate Detection by Abstract Interpretation. *11th International Conference on Algebraic Methodology and Software Technology (AMAST'06)*. Volume 4019 of Lecture Notes in Computer Science, pages 81-95, Springer Verlag. [DOI](#).
- [60] M. Dalla Preda and R. Giacobazzi. Control Code Obfuscation by Abstract Interpretation. *Proceedings of the 3rd IEEE International Conference on Software Engineering and Formal Methods (SEFM'05)*. IEEE Computer Society Press, pages 301-310. 2005 [DOI](#).



- [61] M. Dalla Preda and R. Giacobazzi. Semantic-based Code Obfuscation by Abstract Interpretation. *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05 - Track B)*. Volume 350 of Lecture Notes in Computer Science, pages 1325-1336, Springer Verlag. 2005. [DOI](#).
- [62] M. Dalla Preda. Completeness Refinement in Abstract Symbolic Trajectory Evaluation. *11th Static Analysis Symposium (SAS'04)*, Volume 3148 of Lecture Notes in Computer Science, pagine 38-52, Springer-Verlag. 2004. [DOI](#).

## Other Publications

- [63] M. Dalla Preda, N. Marastoni and F. Paci. Next Generation Vulnerability Detection with LLMs *To appear in the ERCIM news Special Theme: Software Security*
- [64] M. Dalla Preda. Code Obfuscation and Malware Detection by Abstract Interpretation. Tesi di Dottorato del Dipartimento di Informatica, Università di Verona, 2007

## Sottomessi

- [65] M. Campion, M. Dalla Preda, R. Giacobazzi, C. Urban. A Logic for the Imprecision of Abstract Interpretations Submitted July 2025.
- [66] M. Dalla Preda, M. Gambini, S. Migliorini, V. Paternolli, F. Zerbato. Modeling Incomplete Procedural Contracts with Blockchain-based Enforceable Business Processes

In [17, 18, 20, 29, 51, 54, 58, 59, 60, 61] il mio contributo è stato prevalente. Nei lavori dove non ho dichiarato contributo prevalente e dove si è seguito l'ordine alfabetico il contributo è stato paritetico. In alcuni lavori come [10, 28, 31, 33, 34, 35] il mio nome appare alla fine come supervisore dello studente che è primo autore.

Settembre 2024

La sottoscritta, MILA DALLA PREDA nata a Verona il 01/11/1977, residente a Rimini, in Via Beltramelli 11/B, consapevole delle sanzioni penali a cui può andare incontro in caso di dichiarazioni mendaci, di produzione o uso di atti falsi, ai sensi degli artt. 19, 46 e 47 del D.P.R. 445 del 28/12/2000, dichiara di essere in possesso di tutti i titoli contenuti nel presente curriculum e che tutto quanto dichiarato corrisponde a verità.