Matteo Busi

Curriculum Vitæ

Personal information

Citizenship Italian
Birthday Jul. 11, 1993
Address Via San Gallo 119/F, 25082 Botticino BS, Italy

Contacts

(+39) 3204026174
matteo.busi42@gmail.com
https://scholar.google.com/citations?user=0aOyNBIAAAAJ
https://github.com/matteobusi
http://matteobusi.github.io

Education

Ph.D. in Computer Science [Nov. 1, 2017 — Apr. 26, 2021]

Institution Department of Computer Science, University of Pisa
Thesis *Secure Compilation all the Way Down*
Defense Apr. 26, 2021
Supervisors Prof. Pierpaolo Degano & Dr. Letterio Galletta
External reviewers Prof. Dominique Devriese & Prof. Cătălin Hriţcu

M.Sc. in Computer Science [Oct. 12, 2015 — Oct. 06, 2017]

Institution University of Pisa
Thesis *Four Semantics for a Disciplined Concurrency in COP*
Grade *110/110 (hons.)*
Supervisors Prof. Pierpaolo Degano & Dr. Letterio Galletta

B.Sc. in Computer Science [Sep. 06, 2012 — Oct. 09, 2015]

Institution University of Pisa
Thesis *Type Systems to Realize Domain-specific Languages (in italian)*
Grade *110/110 (hons.)*
Supervisors Prof. Pierpaolo Degano & Dr. Letterio Galletta

Visits and seminars

Seminar participant [Nov. 28, 2021 — Dec. 3, 2021]

Event name Dagstuhl Seminar 21481 (Secure Compilation)
Details https://www.dagstuhl.de/en/program/calendar/semhp/?semnr=21481

Visiting scholar [Nov. 15, 2021 — Nov. 26, 2021]

Institution *DistriNet*, KU Leuven
Host Prof. Dominique Devriese

Visiting scholar [Feb. 25, 2019 — May 24, 2019]

Institution *DistriNet*, KU Leuven
Host Prof. Frank Piessens

Ph.D. Schools

BISS'19 [Mar. 10 — 15, 2019]

Extended name Bertinoro International Spring School 2019
Location Bertinoro, Italy

Courses
- *Multitask learning and learning-to-learn: a statistical learning perspective* (Prof. Massimiliano Pontil)
- *Software security across abstraction layers* (Prof. Frank Piessens)
- *Internet of things: a data oriented approach* (Prof. Luciano Bononi)

FOSAD'18 [Aug. 28 — 31, 2018]

Extended name 18th International School on Foundations of Security Analysis and Design
Location Bertinoro, Italy
Courses
- *Data protection in cloud scenarios* (Prof. Sabrina De Capitani di Vimercati)
- *Formally secure compilation* (Prof. Cătălin Hriţcu)
- *Secure Internet architectures* (Prof. Adrian Perrig)
- *Secure multi party computation* (Prof. Nigel Smart)
- *Differential privacy* (Prof. Kunal Talwar)

BISS'18 [Mar. 11 — 16, 2018]

Extended name Bertinoro International Spring School 2018
Location Bertinoro, Italy
Courses
- *Provable security for low level execution platforms* (Prof. Mads Dam)
- *Distributed models, MapReduce and large scale algorithms* (Dr. Silvio Lattanzi)
- *Elements of Quantum Computation* (Prof. Herbert Wiklicky)

WORKING EXPERIENCE

Junior Assistant Professor [Feb. 20, 2023 — ongoing]

Institution Ca' Foscari University of Venice
Official role *RTD-A*

(Postdoctoral) research fellow [Feb. 01, 2022 — Feb. 20, 2023]

Project title *Securing the digital transformation, from the ground up*
Institution Ca' Foscari University of Venice
Supervisor Prof. Riccardo Focardi
Official role *Assegnista di ricerca*

(Postdoctoral) research fellow [Jul. 1, 2021 — Jan. 30, 2022]

Project title *Formal Methods and Techniques for Secure Compilation*
Institution University of Pisa
Supervisor Prof. Gian-Luigi Ferrari
Official role *Assegnista di ricerca*

Research fellow [Jan. 1, 2021 — Jun. 30, 2021]

Project title *Incremental Type Systems for Secure Compilation*
Institution University of Pisa
Supervisor Prof. Roberto Bruni
Official role *Borsista di ricerca*

TEACHING EXPERIENCE

Speaker at the *Hot topics in language-based security 2023* seminar series [Mar. 21, 2023]

Details `https://web.archive.org/web/20230315073037/http://pages.di.unipi.it/bodei/HTLBS.html`

Guest lecturer for the lessons about *side-channels* of the *System Security* course [Dec. 16 and 20, 2022]

Institution Ca' Foscari University of Venice
Main teacher Prof. Riccardo Focardi
Details `https://web.archive.org/web/20230204140611/https://secgroup.dais.unive.it/teaching/system-security/`

Co-organizer of and speaker at the *Hot topics in language-based security 2022* seminar series [Spring 2022]

Details https://web.archive.org/web/20230331121459/http://pages.di.unipi.it/bodei/HTLBS2022.html

Tutor for the *Turing Machine Programming National & International Contest* [14 — 17 Sep 2021]

Details https://www.turingcontest.com/

T.A. for *Laboratory of Innovative Software* [Mar. 2021 — May 2021]

Degree M.Sc. in Computer Science at the University of Pisa
Main teachers Prof. Chiara Bodei & Prof. Gian-Luigi Ferrari
Log https://unimap.unipi.it/registri/dettregistriNEW.php?re=3311405::::&ri=9408

T.A. for *Foundations of Computer Science* [Oct. 2020 — Dec. 2020]

Degree B.Sc. in Computer Science at the University of Pisa
Main teacher Prof. Andrea Corradini
Log https://unimap.unipi.it/registri/dettregistriNEW.php?re=3310600::::&ri=8054

T.A. for *Advanced Programming* [Oct. 2019 — Dec. 2019]

Degree M.Sc. in Computer Science and Networking at the University of Pisa
Main teacher Prof. Andrea Corradini
Log https://unimap.unipi.it/registri/dettregistriNEW.php?re=3297002::::&ri=8054

Teacher for the laboratory *Introduction to Turing Machines* [Feb. 2019]

Institution "U. Dini" high school
Location Pisa, Italy

T.A. for *Advanced Programming* [Oct. 2018 — Dec. 2018]

Degree M.Sc. in Computer Science and Networking at the University of Pisa
Main teacher Prof. Andrea Corradini
Log https://unimap.unipi.it/registri/dettregistriNEW.php?re=3286601::::&ri=8054

T.A. for *Algorithms and Laboratory* [Feb. 2018 — May 2018]

Degree B.Sc. in Computer Science at the University of Pisa
Main teachers Prof. Anna Bernasconi & Prof. Alina Sîrbu
Log https://unimap.unipi.it/registri/dettregistriNEW.php?re=2086516::::&ri=9431

SKILLS

Programming and markup languages

- Good knowledge of OCaml, C, Java, C++, LaTeX, Python
- Basic knowledge of Javascript, Haskell, Coq, Isabelle/HOL

Languages

	Comprehension		Spoken		Written
	Listening	Reading	Interaction	Oral production	
Italian	Mother tongue				
English†	C1	C1	C1	C1	C1

† Self-evaluation w.r.t. the "Common European Framework of Reference for Languages"

Other activities

PC member
- Principles of Secure Compilation (PriSC) 2022, IEEE Secure Development Conference (SecDev) 2022, Workshop on Foundations of Computer Security (FCS) 2022, IEEE Cyber Security and Resilience (CSR) 2023, IEEE Secure Development Conference (SecDev) 2023, Workshop on Foundations of Computer Security (FCS) 2023

Reviewer
- Elsevier "Blockchain: Research and Applications" (BCRA)

External reviewer
- Principles of Security and Trust (POST) 2019, ITASEC 2020, Hot Issues in Security Principles and Trust (HotSpot) 2020

Student volunteer
- ACM SIGPLAN Symposium on Principles of Programming Languages (POPL) 2020, ITASEC 2020

Participation in research projects

SERICS foundation, Spoke 6: Platform and Software Security, Project *SWOPS* [Mar. 2023 — ongoing]

Title Securing softWare frOm first PrincipleS
PI Gabriele Costa, IMT
Details Part of the Next Generation EU programme, Italy's NRRP.
Website `https://serics.eu/services/spoke-6-sicurezza-software-piattaforme/`

Project *DECLWARE* [Jul. 2018 — Jul. 2020]

Title Declarative methodologies for designing and deploying applications
Financed by University of Pisa
Ref. number PRA_2016_64
Website `http://pages.di.unipi.it/declware/`

Event organization

Co-organizer of *THESES'19* [05/12/2019]

Extended name THeses presentation Event for StudEntS
Supervisor Prof. Paolo Ferragina
Website `http://theses.di.unipi.it/`

Thesis co-supervision

Co-supervision of Marco Antonio Corallo's B.Sc. thesis [A.Y. 2020/2021]

Institution University of Pisa
Thesis (in italian) *An F# Framework for Value-Set Analysis*
Co-Supervisors Prof. Pierpaolo Degano & Dr. Letterio Galletta

Co-supervision of Federico Pennino's B.Sc. thesis [A.Y. 2019/2020]

Institution University of Pisa
Thesis (in italian) *CADL: Generating a Type Checking Module from Datalog to OCaml*
Co-Supervisors Prof. Pierpaolo Degano & Dr. Letterio Galletta

Publications

For **conferences and workshops**:

- [✈] indicates that I (physically or remotely) **participated** at the event during which the work was presented;
- [🎙] indicates that I **presented** the work during the corresponding event;
- [**i**] indicates the **lack of formal proceedings** for the corresponding work.

JOURNALS

1. Matteo Busi, Job Noorman, Jo Van Bulck, Letterio Galletta, Pierpaolo Degano, Jan Tobias Mühlberg, and Frank Piessens. "Securing Interruptible Enclaved Execution on Small Microprocessors". *ACM Trans. Program. Lang. Syst.* 43 (2021)
2. Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "Mechanical incrementalization of typing algorithms". *Science of Computer Programming* 208 (2021). ISSN: 0167-6423. DOI: https://doi.org/10.1016/j.scico.2021.102657

CONFERENCES

1. Emiel Lanckriet, Matteo Busi, and Dominique Devriese. "pi_RA: A pi-calculus for verifying protocols that use remote attestation". *36th IEEE Computer Security Foundations Symposium, CSF 2023, Dubrovnik, Croatia, July 9-13, 2023*
2. [🎤, 🎙] Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "Towards effective preservation of robust safety properties". *SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, April 25 - 29, 2022*. Ed. by Jiman Hong, Miroslav Bures, Juw Won Park, and Tomás Cerný. ACM, 2022, pp. 1674–1683. DOI: 10.1145/3477314.3507084
3. [🎤, 🎙] Carmine Abate, Matteo Busi, and Stelios Tsampas. "Fully Abstract and Robust Compilation and How to Reconcile the Two, Abstractly". *19th Asian Symposium on Programming Languages and Systems, APLAS 2021, Chicago, IL, USA, October 17-22, 2021*. 2021
4. [🎤, 🎙] Matteo Busi, Job Noorman, Jo Van Bulck, Letterio Galletta, Pierpaolo Degano, Jan Tobias Mühlberg, and Frank Piessens. "Provably Secure Isolation for Interruptible Enclaved Execution on Small Microprocessors". *33rd IEEE Computer Security Foundations Symposium, CSF 2020, Boston, MA, USA, June 22-26, 2020*. 2020, pp. 262–276. DOI: 10.1109/CSF49147.2020.00026
5. [🎤, 🎙] Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "Control-flow Flattening Preserves the Constant-Time Policy". *Proceedings of the Fourth Italian Conference on Cyber Security, Ancona, Italy, February 4th to 7th, 2020*. Ed. by Michele Loreti and Luca Spalazzi. Vol. 2597. 2020, pp. 82–92. URL: http://ceur-ws.org/Vol-2597/paper-08.pdf
6. Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "Robust Declassification by Incremental Typing". *Foundations of Security, Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows*. Ed. by Joshua D. Guttman, Carl E. Landwehr, José Meseguer, and Dusko Pavlovic. Vol. 11565. Lecture Notes in Computer Science. Springer, 2019, pp. 54–69. DOI: 10.1007/978-3-030-19052-1_6
7. [🎤, 🎙] Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "Using Standard Typing Algorithms Incrementally". *NASA Formal Methods - 11th International Symposium, NFM 2019, Houston, TX, USA, May 7-9, 2019, Proceedings*. 2019, pp. 106–122. DOI: 10.1007/978-3-030-20652-9_7
8. [🎤, 🎙] Matteo Busi and Letterio Galletta. "A Brief Tour of Formally Secure Compilation". *Proceedings of the Third Italian Conference on Cyber Security, Pisa, Italy, February 13-15, 2019*. Ed. by Pierpaolo Degano and Roberto Zunino. Vol. 2315. 2019. URL: http://ceur-ws.org/Vol-2315/paper03.pdf
9. Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "A Semantics for Disciplined Concurrency in COP". *Proceedings of the 17th Italian Conference on Theoretical Computer Science, Lecce, Italy, September 7-9, 2016*. 2016, pp. 177–189. URL: http://ceur-ws.org/Vol-1720/full13.pdf

WORKSHOP

1. [ℹ] Matteo Busi, Riccardo Focardi, and Flaminia Luccio. "Automated Learning and Verification of Embedded Security Architectures". *7th Workshop on Principles of Secure Compilation, PriSC 2023, Boston, Massachusetts, United States, January 21, 2023*. 2023
2. [ℹ] Emiel Lanckriet, Matteo Busi, and Dominique Devriese. "pi_RA: A pi-calculus for verifying protocols that use remote attestation". *7th Workshop on Principles of Secure Compilation, PriSC 2023, Boston, Massachusetts, United States, January 21, 2023*. 2023
3. [ℹ] Emiel Lanckriet, Matteo Busi, and Dominique Devriese. "pi_RA: A pi-calculus for verifying protocols that use remote attestation". *Workshop on Foundations of Computer Security 2022, FCS 2022, Haifa, Israel, August 11, 2022*. 2022
4. [🎤, 🎙, ℹ] Carmine Abate, Matteo Busi, and Stelios Tsampas. "The Fox and the Hound (Episode 2): Fully Abstract, Robust Compilation and How to Reconcile the Two, Abstractly". *6th Workshop on Principles of Secure Compilation, PriSC 2022, Philadelphia, Pennsylvania, United States, January 22, 2022*. 2022. URL: https://arxiv.org/abs/2006.14969

5. [✈, 🎙, ℹ] Carmine Abate and Matteo Busi. "The Fox and the Hound: Comparing Fully Abstract and Robust Compilation". *5th Workshop on Principles of Secure Compilation, PriSC 2021, Virtual event, January 17, 2021*. 2021. URL: https://arxiv.org/abs/2006.14969v2
6. [✈, ℹ] Carmine Abate and Matteo Busi. "The Fox and the Hound: Comparing Fully Abstract and Robust Compilation". *Workshop on Foundations of Computer Security 2020, FCS 2020, Virtual event*. 2020
7. [✈, 🎙, ℹ] Matteo Busi, Job Noorman, Jo Van Bulck, Letterio Galletta, Pierpaolo Degano, Jan Tobias Mühlberg, and Frank Piessens. "Securing Interruptible Enclaves". *4th Workshop on Principles of Secure Compilation, PriSC 2020, New Orleans, Louisiana, United States, January 19, 2020*. 2020
8. [✈, 🎙, ℹ] Matteo Busi, Pierpaolo Degano, and Letterio Galletta. "Translation Validation for Security Properties". *3rd Workshop on Principles of Secure Compilation, PriSC 2019, Cascais, Portugal, January 13, 2019*. 2019. URL: https://arxiv.org/abs/1901.05082

PAPERS UNDER REVISION

1. Matteo Busi, Riccardo Focardi, and Flaminia Luccio. "Bridging the Gap: Automated Analysis of Secure Embedded Architectures". *Under review*