Matteo Busi

(+39)3204026174 | matteo.busi42@gmail.com | Verona, Italy
https://www.linkedin.com/in/mbusi/ | https://github.com/matteobusi
http://matteobusi.github.io

Skills

- **Programming languages:** OCaml | Coq | Java | C | C++ | Python | Haskell (basics) | Verilog (basics) | Isabelle/HOL (basics)
- **Languages:** English (fluent) | Italian (native)

Work experience

Ca' Foscari University of Venice, Venice, Italy | Researcher | 02/2023 — Present

- **Mechanization of security protocols:** Mechanized proofs about security protocols within the Strand space framework using Coq (with colleagues at Ca' Foscari University).
- **Automated analysis of embedded systems:** Continued from previous postdoc position.

Ca' Foscari University of Venice, Venice, Italy | Postdoctoral researcher | 02/2022 — 02/2023

- **Automated analysis of embedded systems:** Developed a tool in OCaml that uses automata learning and model checking to analyze embedded security architectures, finding known and new side-channel attacks or (probabilistically) proving their absence (with colleagues at Ca' Foscari University).
- **Remote attestation:** Studied how to formalize the concept of remote attestation as a cryptographic primitive and how to leverage such formalization to prove remote attestation-based protocols correct (with colleagues at KU Leuven).

University of Pisa, Pisa, Italy | Postdoctoral researcher | 05/2021 — 01/2022

- **Translation validation for secure compilers:** Built a framework that leverages program analysis to decide whether a program is compiled securely and mechanized its correctness proof in Coq (with colleagues at University of Pisa).

Education

Ph.D. in Computer Science, 11/2017 — 04/2021

University of Pisa, Pisa, Italy

M.Sc. in Computer Science, 10/2015 — 10/2017

University of Pisa, Pisa, Italy
Graduated with honors

B.Sc. in Computer Science, 10/2012 — 10/2015

University of Pisa, Pisa, Italy
Graduated with honors

Professional activities

- **Program Committee member:** PriSC'22 | IEEE SecDev'22 | FCS'22 | IEEE CSR'23 | IEEE SecDev' 23 | FCS'23 | PriSC'24
- **Participant and presenter** at Dagstuhl Seminar 21481 on Secure Compilation, 2021
- **Artifact Evaluation Committee member:** ACM POPL'24
- **Session chair:** PriSC'23 | FCS'23
- **Reviewer:** Elsevier "Blockchain: Research and Applications" (BCRA)
- **External reviewer:** POST'19 | ITASEC'20 | HotSpot'20
- **Student volunteer:** ACM POPL'20 | ITASEC'20

PUBLICATIONS

PAPERS UNDER REVISION

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

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. Francesco Palmarini, Leonardo Veronese, Matteo Busi, Riccardo Focardi, and Flaminia Luccio. "A Recipe for Cost-Effective Secure IoT: the Safe Place Project Case Study". *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2023, pp. 99–104. DOI: 10.1109/CSR57506.2023.10225007
3. 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
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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. Matteo Busi, Riccardo Focardi, Flaminia Luccio, et al. "Don't Get Stranded: Secure and Dynamic Key Management Policies with Strand Spaces". *Workshop on Foundations of Computer Security (FCS23)*. 2023
2. 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

3. 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
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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