

The logo for SPÜMA features the letters 'S', 'P', 'M', and 'A' in a bold, dark red sans-serif font. The letter 'Ü' is replaced by a red shield icon with two small circles above it. The entire logo is enclosed within a dark red L-shaped frame consisting of a vertical line on the left and a horizontal line at the bottom.

SPÜMA

Security and Privacy
language-based
Methods At work

<http://spuma.di.unipi.it/>

SPUMA & close collaborators



Pierpaolo
Degano

Full Professor



Gian-Luigi
Ferrari

Full Professor



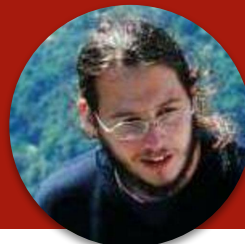
Chiara
Bodei

Associate Professor



Matteo
Busi

PhD Student



Lorenzo
Ceragioli

PhD Student



Gabriele
Costa

Assistant Professor



Letterio
Galletta

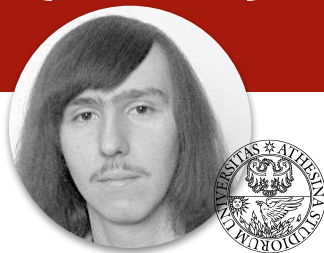
Assistant Professor



(Some) Collaborators



David Basin
ETH Zurich



Roberto Zunino
Università di Trento



Frank Piessens
KU Leuven



Emilio Tuosto
Gran Sasso Science Institute



Massimo Bartoletti
Università di Cagliari



Riccardo Focardi
Ca' Foscari Venezia



Joshua Guttman
Worcester Polytechnic Institute



Rosario Pugliese
Università di Firenze



VS



That's why formal methods

... in particular we work on language-based security

Language-based Security

Studies

how to prevent vulnerabilities and attacks

using

formal semantics, program analysis, formal verification...



Our slogan: PLT marries Cyber-security!

Modelling and Analysing Networks of devices

Communication across components

- IoT Systems
- Multi-party interactions

Prove security properties considering

- Tampered sources & untrusted nodes
- Provenance of Data

- IoT-LySa with static analysis
 - Link calculus
- with Roberto Bruni & Linda Brodo

Access Control

Selectively restrict access to resources in

- Operating system
- Web services
- ...

Goals:

- Design of high-level languages
- Specifications VS implementation
- Targeting challenging domains

- Distributed collaborative environment
- Analysis & synthesis of policies
- Cyber-physical spaces & firewalls

Secure Compilation

Security in source code is **NOT** security in compiled code!

Goal: preserving security properties during compilation

- Full abstraction
- Language-based & HW mechanisms

- Incremental type analysis
 - Against micro-architectural attacks
 - Secure Translation Validation
-

Security in the Fog

with SOCC group - Antonio Brogi & Stefano Forti

Fog: resources and services along the continuum from Cloud to Things

Goal: assess security of app deployments

- Security threats from the Cloud & IoT
- Many stakeholders & trust relations
- Need for explainability

- Application security requirements VS infrastructure security capabilities
 - Declarative & explainable methodology
 - Automated and secure deployment
-

Others

Past Projects

- Context oriented programming languages
- Service oriented computing
- Contracts in service oriented computing
- Nominal automata for verification

IT/OT and Mobile Security

- Security assessment IT/OT infrastructures - fast virtualization of scenarios
- Automatic security verification of Android apps



Blockchain

- A Ethereum-based platform for fair bug bounty programs
- Formal semantics of smart contract languages



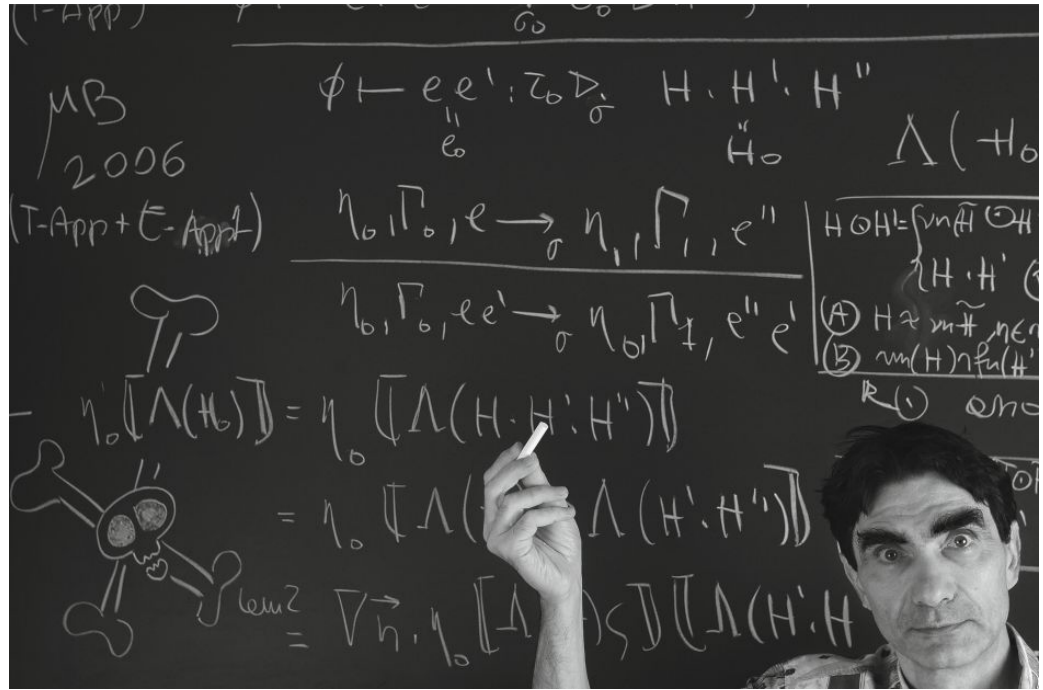
Bibliography

1. **Protocol Verification:** Chiara Bodei, Pierpaolo Degano, Gian-Luigi Ferrari, Letterio Galletta. "Tracing where IoT data are collected and aggregated." *LMCS 13(3) 2017*. [\[paper\]](#)
2. **Access Control:** Chiara Bodei, et al. "Language-independent synthesis of firewall policies." *IEEE EuroS&P 2018*. [\[paper\]](#)
3. **Secure Compilation:** Matteo Busi and Letterio Galletta. "A Brief Tour of Formally Secure Compilation." *ITASEC 2019*. [\[paper\]](#)
4. **Security in the Fog:** Stefano Forti, Gian-Luigi Ferrari, Antonio Brogi. "Secure Cloud-Edge Deployments, with Trust" *To appear in Future Generation Computer Systems*. [\[paper\]](#)
5. **Blockchain:** Massimo Bartoletti, Letterio Galletta, Maurizio Murgia. "A Minimal Core Calculus for Solidity Contracts." *DPM/CBT@ESORICS 2019*. [\[paper\]](#)



Find us @

<http://spuma.di.unipi.it/>



WE WANT YOU!