Gustavo Zambonin

gustavo.zambonin@posgrad.ufsc.br · +55 48 999 973 940 · github.com/zambonin rev. 20190112
925 Francisco Roberto da Silva Av. · 88160-284 · Biguaçu, Santa Catarina · Brazil

Education (lattes.cnpq.br/8192345791741876)

Today / **Aug/2018** — **M.Sc. in Computer Science** (PPGCC/UFSC)

- Post-quantum cryptography researcher, in particular digital signature schemes
  - Multivariate cryptography with focus on the Rainbow family
- Teaching assistant for Mathematical Foundations of Informatics
  - Order theory, lattice theory, algebraic structures, group theory

Jul/2018 / **Mar/2013** — **B.Sc. in Computer Science** (UFSC)

- Thesis named "Performance optimization for the Winternitz digital signature scheme"
  - Tuning the Winternitz hash-based digital signature scheme (10.1109/ISCC.2018.8538642)
- Tutor for Probability and Statistics and Introduction to Computer Science
  - Discrete and continuous probability distributions and their applications
  - Building blocks of programming languages and GNU/Linux operating systems

Professional experience

Today / **May/2016** — **Computer Security Laboratory** (LabSEC/UFSC)

- Senior developer of the Conformance Verifier for digital signatures in the Brazilian PKI
  - Implementation of CMS and PDF signatures verification, and creation of a generic heuristic to classify digital signatures. Migration of the code base from Ant to Maven, unifying the package generation for Windows, macOS and Debian, and production of WAR files. Creation of the Web Verifier, developing Java servlets from scratch, with focus on maintainable code and ease of use. Employment of continuous integration and deployment practices using Docker, automating unit testing and package builds. Establishment of a validation environment updated frequently, using Apache HTTP Server and Tomcat. Migration of the code base history from Subversion to Git. Supervision of general development progress for CAdES, XAdES and PAdES signature verification. Administration of all related virtual infrastructure.
- Researcher of software requirements needed to support digital signatures in certain applications
  - Description of a library model used to configure and instantiate a public-key infrastructure, with the intent of testing targeted software. Generated artifacts include multi-level certificate authorities, user certificates, certificate revocation lists and OCSP responses.
  - Analysis of the effort needed to add digital signatures support on PDF.js, with the intent of enabling verification directly inside the browser. Creation of fork that verifies a small set of digital signatures. Description of a software model that allows modularization and decoupling of the digital signature verification component from PDF.js.
- Various roles in other projects related to information security
  - Researcher of a protocol to quantum-proof a blockchain, with secure substitution of wallets, replacement of cryptographic algorithms and zero downtime for the platform.
  - Operator of security ceremonies, in which secure servers were provisioned to run verifiable online elections through Helios, itself based on frameworks such as Celery and Django.
  - Forensic computer examiner of images generated by speed enforcement cameras, handling large amounts of heterogeneous data with tools such as `coreutils`, with the intent of proving accuracy and integrity of such files.

Qualifications

Coding — AWK, Bash, C, C++, Java (JSE, JEE), LaTeX, sed
Python (Flask, gspread, Helios, IPython, Matplotlib, NumPy, PyQt, Requests, robobrowser, Scrapy)

- Brief experience: CSS, gnuplot, Haskell, JavaScript, Julia, Octave, Pascal, Prolog, SageMath

Environs — GNU/Linux, Vim, IntelliJ Idea, PyCharm, Eclipse, Visual Studio Code

- Management: Ant, Git, GitLab CI/CD, Make, Maven, Subversion

Software — Clang Static Analyzer, Docker, GDB, QEMU, PostgreSQL, SQLite, Valgrind

- Middleware: Apache HTTP Server, Archiva, Tomcat, WildFly

Languages — Portuguese (native), English (fluent), French (beginner)