

# Nicolas Badoux

 n.badoux@hotmail.com

 +41 79 914 00 47

 nbadoux

Rue de la Gare 21  
1030 Bussigny  
CH—Switzerland  
Swiss citizen—married  
Born in 1994



**STATEMENT** - Passionate about cybersecurity, its ever evolving nature, and the adaptations it requires.

**OF PURPOSE** - Curious by nature, I love to understand architectures and their security implications.

- With automated defenses and monitoring, I hope to reduce the repercussion of cyber incidents.
- Can-do attitude, committed, and strong ability to adapt to changing requirements.

---

## EXPERIENCE **PhD Researcher** - HexHive @ EPFL - Lausanne, CH

*Mar' 2020–May 2025*

- Lead the development and evaluation of different security-themed projects reducing the attack surface of low-level code (C/C++). With novel secure dialects, compiler passes (SAST) and automated testing (DAST), we ease secure development across large code bases.
- As part of our research, we extensively tested low-level APIs and dutifully followed the vulnerability lifecycle, from responsible disclosure to contribution of fixes.
- Facing continuously evolving requirements, I strategically scoped our projects and effectively communicated their outcomes to a global audience.
- In a diverse team, I lead projects with senior professors and designed and mentored research projects for junior students. We contributed to open source projects and reported CVEs.

## **Software Engineer** - Fondation Digger, NGO - Tavannes, CH

*Aug' 2019–Mar' 2020*

- Quantified the feasibility of low-latency VR in C++ for an industrial demining machinery.

## **Software Engineer** - Compassion Suisse, NGO - Yverdon, CH

*Mar'–May 2018*

- Contributed in an Agile environment to open source modules for the Python Odoo ERP.

## **Security Engineer Intern** - Ergon Informatik - Zürich, CH

*60%—Sept' 2017–Mar' 2018*

- Designed and developed a blackbox fuzzer for testing a Web Application Firewall (WAF).

## **Technology Summer Analyst** - Morgan Stanley - London, UK

*Jun'–Aug' 2016*

- Developed a webview for metrics tracked by the Architecture Security team of the bank.

---

## EDUCATION **Doctorate of Sciences (PhD)**

*2020–2025*

*École Polytechnique Fédérale de Lausanne (EPFL)* - Switzerland

- Advisor: Prof. Mathias Payer in the HexHive laboratory.
- Thesis: Securing low-level code with minimal developer efforts.
- Keywords: System security, software testing, compiler-based defenses, fuzzing.

## **Master of Science ETH in Computer Science**

*2016–2019*

*Eidgenössische Technische Hochschule Zürich (ETHZ)* - Switzerland

- Specialization in Information Security, GPA: 5.39/6.

## **Bachelor in Communication Sciences**

*2013–2016*

*École Polytechnique Fédérale de Lausanne (EPFL)* - Switzerland

- **Exchange program** @ Carnegie Mellon University - USA, GPA: 5.26/6.

*2015–2016*

## **Bilingual Matura (German/French)**

*2010–2013*

*Kantonschule Frauenfeld & Gymnase d'Yverdon* - Switzerland

- Specialization in Mathematics and Physics, GPA: 5.19/6, Best 3%.

---

**SKILLS Programming Languages:** Python, C++, L<sup>A</sup>T<sub>E</sub>X, Bash.

**Software:** LLVM, Docker, GDB, Linux, Make, afl++, libfuzzer.

**Spoken Languages:** French (native), English (C2), Swiss-German (C2), German (C1).

---

**TALKS BlackAlps:** No App? No Problem: Automatic Library Fuzzing

*Upcoming, Nov' 2025*

---

**RESEARCH***NDSS'25***PROJECTS Authors:** Nicolas Badoux, Flavio Toffalini, Yuseok Jeon, & Mathias Payer.

- *Distinguished Paper Award* (top 1% of submissions).
- In C++, incorrect downcasts are a severe vulnerability often exploited in the wild.
- By inlining the type in each C++ object, we create a compiler-based mitigation against type confusion attacks allowing downcast to be checked at runtime while requiring minimal code adaptations. We evaluate our prototype against the state-of-the-art and achieve less than 1% runtime overhead while protecting 90B casts. We deploy our prototype on Chromium.
- Built on top of LLVM, `type++` is available on [GitHub](#) and its artifact evaluated.
- During this multi-year project, I learned some intricacies of compilers, developed my writing skills, and strategic planning to face a constantly evolving project.

**LIBERATOR: Balancing library fuzzing without consumer code***FSE'25***Authors:** Flavio Toffalini, Nicolas Badoux, Zurab Tsinadze, & Mathias Payer.

- Drivers, a sequence of API calls building state, allows for dynamic testing like fuzzing, to execute a library's code. Manually written drivers are rare and exhaustively tested.
- LIBERATOR automates the generation of fuzzing drivers without consumer code and allows for balancing resources between driver generation and fuzzing.
- From insights gathered through LLVM passes, we build valid C drivers calling the API.
- We report and fix 24 bugs, including CVE-2024-8006. We release our prototype on [Github](#).
- Through the design and multifaceted evaluation of LIBERATOR, I improved my cross-cutting understanding of complex systems.

**Sourcerer: channeling the void***DIMVA '25***Authors:** Nicolas Badoux, Flavio Toffalini, & Mathias Payer.

- In C++, conversions from `void*` to typed pointers are ubiquitous but, if the type is not the original one, leads to type confusions and possibly further memory corruption.
- By extending the protection of `type++` to all the types used in casts, we design Sourcerer, a complete type confusions sanitizer. With a low-overhead of 5% on average, we conduct the first fuzzing campaign targeting specifically type confusions.
- We find type confusions in Blender and OpenCV and release our prototype on [GitHub](#).
- As the main author, I designed and evaluated our system as well as wrote the paper.

---

**TEACHING** *Operating System (2021)* *Software Security (2021 & 2023)* *Information, Calcul & ASSISTANT Communication (2022 & 2024)* *Information Security & Privacy (2023)*

---

**ACTIVITIES** **Board Member, Treasurer** - Groupes Bibliques des Écoles et Universités *2023–ongoing*

- Define the vision, hiring, and budget planning ( $\simeq 500\text{kCHF}$ ).

**Camp Leader** - Interjeunes & Ligue pour la Lecture de la Bible *2014, 2017, 2021, 2022*

- Lead week-long camps with up to 110 kids/young adults. Built a team, prepared the event, managed the team and had final authority.

---

**REFERENCES** **Prof. Dr. Mathias Payer***mathias.payer@nebelwelt.net*

- Associate Professor at EPFL in Lausanne (CH) and head of HexHive.
- Advised me during my PhD between 2020 and 2025.

**Prof. Dr. Flavio Toffalini***flavio.toffalini@rub.de*

- Assistant Professor at Ruhr-Universität in Bochum (DE).
- Close collaborator and advising post-doc during my PhD (2021–2025).

**Benoît Pfister***benoit.pfister@gbeu.ch*

- Chairman of the Board at Groupes Bibliques des Écoles et Universités.
- We worked together for hiring committees, budgeting, and general strategy.