Rue de la Gare 21
1030 Bussigny
CH—Switzerland
Swiss citizen—married
Born 06.11.1994

Nicolas Badoux

n.badoux@hotmail.com +41 79 914 00 47 nbadoux

Education

Doctor 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.
- Topics: 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*

Billingual Matura (German/French) *2010–2013*
Kantonschule Frauenfeld & Gymnase d'Yverdon - Switzerland
- Specialization in Mathematics and Physics, GPA: 5.19/6, Best 3%.

Research Experience

`type++`: prohibiting type confusion with inline type information *NDSS'25*
Authors: **Nicolas Badoux**, Flavio Toffalini, Yuseok Jeon, & Mathias Payer.
- *Distinguished Paper Award* (top 5%).
- In C++, incorrect downcast 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.

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 allow 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.

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, lead 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.

Bypassing LLVM-CFI cast protection *Ongoing*
Authors: Nicolas Almerge, **Nicolas Badoux**, & Mathias Payer.
- We present a novel attack against LLVM-CFI, bypassing the cast protection for C++.
- As the main advisor for this Master project, I laid out the research plan, provided guidance, and reviewed the results.

Industry Experience

Software Engineer - Fondation Digger, NGO - Tavannes, CH *Aug' 2019–March 2020*
- Developed a virtual overlay for remotely removing explosives with the help of OpenCV and Unity in an Agile environment as part of my civil service.

Software Engineer - Compassion Suisse, NGO - Yverdon, CH *Mar'–May 2018*
- As part of my civil Service, contributed to open source Python modules for the Odoo ERP.

Security Engineer Intern - Ergon Informatik - Zürich, CH *60%—Sept' 2017–Mar' 2018*
- Developed a blackbox fuzzer in Python to find bugs in Ergon's Web Application Firewall.

Technology Summer Analyst - Morgan Stanley - London, UK *June–Aug' 2016*
- Developed charts in AngularJS for statistics of the Architecture Security team.

Skills

Programming Languages: Python, C++, LaTeX, Bash.

Software: LLVM, Docker, GDB, Linux, libfuzzer.

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

Teaching Assistant

CS-119 Information, Calcul & Communication *2022 & 2024*

CS-323 Operating System *2021*

CS-412 Software Security *2021 & 2023*

COM-402 Information Security & Privacy *2023*

Activities

Board Member, Treasurer - Groupes Bibliques des Écoles et Universités *2023–present*
- Define the vision, hiring of the general secretary, and budget planning ($\simeq$ 500kCHF).

Camp Leader - Interjeunes & Ligue pour la Lecture de la Bible *2014, 2017, 2021, 2022*
- Lead camps with up 110 kids/young adults for a week. Built a team, prepared the event, managed the team and was in charge of the authority during the week.

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.