M2 internship on e-voting security

Second semester 2022-2023

Enka Blanchard
CNRS researcher at LAMIH (UMR 8201) and associate researcher at CIS (UPR 2000)

E-mail: enka.blanchard@cnrs.fr Web: **https://koliaza.com**

---

1 Objectives

The goal of this internship is to lay the basis for a longer project aimed at providing a regular analysis of the main e-voting systems used in France. Our recent work on the Neovote system — used in 2022 for the French presidential primaries — proved the existence of multiple major vulnerabilities. We suspect that similar vulnerabilities would be present in other competing systems and plan to study them one by one. The main goal of the internship would be to analyse the code of at least one competing software to detect vulnerabilities, inconsistencies, and departures from best practices in e-voting. The data would be either obtained by soliciting a trial or by using evidence from ongoing elections (e.g. on systems used by other universities).

2 Candidate profile

We are not expecting any strong expertise in cybersecurity, however the ideal candidate should be at least somewhat proficient and interested by :

- code analysis (especially obfuscated code),
- cybersecurity in general,
- cryptographic protocols,
- knowledge about verifiable voting would be a plus but can easily be learned during the internship.

If the intern would like to go further, an interest in legal infrastructure and administration would be welcome as we also plan to investigate the mechanisms by which defective cybersecurity solutions get selected and used by French institutions.

3 Supervision

The internship will be supervised within the Laboratory of Automation, Mechanics and Industrial and Human Computer Science in Valenciennes. The laboratory is staffed by around 110 permanent researchers, 30 permanent engineers, technicians and administrative personel, a dozen postdoctoral researchers and 80 PhD students (including two who recently started their theses co-supervised by Enka Blanchard). The LAMIH is a mixed research unit between the French National Centre for Scientific Research (CNRS UMR 8201) and the Polytechnic University Hauts-de-France. It has four main departments (Automatics, Mechanics, Human and Life sciences, and Computer Science) and is in the process of creating a team in cybersecurity led by Antoine Gallais.

4 References

To have an idea of the kind of technique we plan to use, one can look at our main paper on Neovote, which was selected as the best paper in the technical track at EVOTE-ID 2022. It can be found in open access at :
https://link.springer.com/chapter/10.1007/978-3-031-15911-4_1.

A French short paper can be found here :
https://hal.archives-ouvertes.fr/hal-03656951

An analysis of Neovote from a different team can be found here :
https://hal.inria.fr/hal-03580506/document