Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol

Alexandre Debant*[1]

[1]Inria – Inria Nancy - Grand Est – France

Résumé

In this talk I will discuss the security of the evoting protocol used by citizens overseas during the 2022 French legislative elections. During our analysis, we uncovered two design-level and implementation-level vulnerabilities which allow a standard voting server attacker and even more so a channel attacker to defeat the election integrity and ballot privacy due to 5 attack variants, all acknowledged by the relevant stakeholders during our responsible disclosure. Finally, I will discuss recent news about the security requirements of evoting systems in France.

*Intervenant