Jalon 4A : Rapport technique présentant les études de cas sur le vote électronique

SVP

Date: 27/06/2024
Doc. Version: <1>

Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre du Plan France 2030 portant la référence ANR-22-PECY-0006

Document Control Information

Settings	Value
Document Title:	Rapport technique présentant les études de cas sur le vote électronique
Project Title:	SVP
Document Author:	Véronique Cortier
Scientific Coordinator:	<Stéphanie Delaune>
Project Manager (PM):	<Benoît Josset (PM)>
Doc. Version:	<1>
Sensitivity:	<Public >
Date:	01/07/2023

Rapport technique présentant les études de cas sur le vote électronique

Véronique Cortier[1], Alexandre Debant[1], Pierrick Gaudry[2], Stéphane Glondu[3], and Lucca Hirschi[1]

[1]PESTO team, CNRS, Université de Lorraine, Inria
[2]CARAMBA team, CNRS, Université de Lorraine, Inria
[3]Inria

1er juillet 2024

L'objectif de la tâche 4.3 est d'appliquer nos techniques pour analyser la sécurité des protocoles de vote électronique, les améliorer et mieux comprendre comment formaliser les propriétés souhaitées. Une tâche préliminaire pour cette tâche est d'identifier les études de cas qui seront considérées. Nous avons choisi des protocoles de vote correspondants à des systèmes déployés :

- protocole de SwissPost, utilisée pour des élections nationales et cantonales en Suisse
- protocole FLEP, utilisé lors des élections législatives en France en 2022 et 2023
- Belenios, protocole conçu et développé par des équipes impliquées dans le projet. La plateforme de vote libre `https://vote.belenios.org/admin` est utilisée chaque année dans plus de 1000 élections.

L'objet de ce document est de présenter succinctement les réalisations effectuées pour chaque protocole, l'ensemble de ces réalisations consituant la partie technique du livrable 4A.

1 Protocole de SwissPost

Ce protocole est développé par l'entreprise SwissPost qui, conformément à la législation suisse, rend son code public, accompagné d'une spécification publique détaillée [1].

Contribution : Sur la base de cette spécification, nous avons mis au point des modèles ProVerif pour prouver à la fois le secret du vote et la vérifiabilité, dans le modèle de confiance établi par la Chancellerie Suisse. Ces modèles ont été publiés par SwissPost [2].

2 Protocole FLEP

Le système utilisé lors des élections législatives en France en 2022 et 2023 a été développé par un prestataire. Cette entreprise a rendu public une spécification partielle du système.

1. Swiss Post Voting System Specification
2. Symbolic Analysis of the Swiss Post Voting System

Cette spécification ne permettait cependant pas de savoir quel était l'échange de messages entre le client de vote et le serveur.

Contribution : En partant de cette première spécification et en étudiant le client de vote de l'élection, nous avons pu établir une spécification complète du protocole, mettant ainsi à jour des faiblesses sur la vérifiabilité et le secret du vote [3]. Ces problèmes ont essentiellement été corrigés dans la version utilisée en 2023 pour le rejeu partiel des élections. Suite à notre travail, il est désormais possible d'établir des modèles du protocole FLEP, pour la suite du projet.

3 Belenios

Le logiciel Belenios, implémentant le protocole éponyme, est un logiciel open-source, fourni avec une spécification détaillée [4].

Contribution : Nous tenons à jour la spécification à chaque nouvelle version du logiciel. Les modèles ProVerif que nous prévoyons de construire permettront également de tester de futures pistes de développement du protocole, avant leur déploiement.

4 Rappel des contributions techniques du livrable 4A

— Modèles ProVerif du protocole SwissPost
Symbolic Analysis of the Swiss Post Voting System
— Spécification détaillée du protocole FLEP
Alexandre Debant, Lucca Hirschi. Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol. Usenix Security, 2023
— Mise à jour de la spécification du protocole Belenios
`https://www.belenios.org/specification.pdf`

3. Alexandre Debant, Lucca Hirschi. Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol. Usenix Security, 2023
4. `https://www.belenios.org/specification.pdf`