Haute école spécialisée bernoise
Technique et informatique

SwissiVi Proof-of-Concept for a Novel E-Voting Platform

Défense de thèse de bachelor

Andrea Pellegrini, Philémon von Bergen
25.06.2012

Table des matières

Introduction

Le problème de la plateforme sécurisée

- **Règles de sécurité pour une votation**
  - Possibilité de voter qu'une seule fois
  - Personne ne doit pouvoir voter au nom de quelqu'un d'autre
  - Personne ne doit pouvoir savoir ce que je vote
  - Personne ne doit pouvoir modifier mon vote
- **Problème avec une plateforme de vote par internet**
  - Malware installé sur le poste du votant
    - ➔ Plus d'intégrité du vote
    - ➔ Plus de confidentialité du vote
  - Connexion avec le compte d'une autre personne
- **Comment résoudre le problème de la plateforme sécurisée ?**

Le concept de la BFH/HESB

R. Haenni, R. Koenig, and E. Dubuis,"Secure internet voting with a trusted voting device,"EVOTE12 Bregenz, 2012.

Le concept de la BFH/HESB

- **Problèmes résolus:**
  - Possibilité de voter qu'une seule fois ✗
  - Personne ne doit pouvoir voter au nom de quelqu'un d'autre ✓
  - Personne ne doit pouvoir savoir ce que je vote ✓
  - Personne ne doit pouvoir modifier mon vote ✓

Vue d’ensemble du travail

Notre partie du travail

- **Simulation de la carte de vote**
- **Simulation de l'appareil de vote**
- **La plateforme de vote**
  - Partie d'administration
  - Upload des fichiers de vote

Simulation de la carte de vote

La carte de vote

- **Données présentes sur la carte de vote**
  - Langue de l'utilisateur
  - Code PIN évitant son utilisation par une tierce personne
  - Clé privée pour signer le vote
  - Fichiers de vote créés par l'appareil de vote
- **La simulation de la carte**
  - permet de choisir la langue
  - affiche le code PIN
  - permet de récupérer les fichiers de vote en la connectant à un ordinateur
  - supporte le changement du code PIN par l'appareil de vote

La carte de vote

- **La carte simulée communique avec l'appareil de vote par NFC**
  - Elle envoie la langue, le code PIN et les fichiers déjà présents sur la carte à l'appareil
  - Le premier message NFC enclenche l'appareil de vote
  - Ensuite, la carte attend de recevoir des fichiers de vote à signer ou un changement du PIN

Simulation de l’appareil de vote

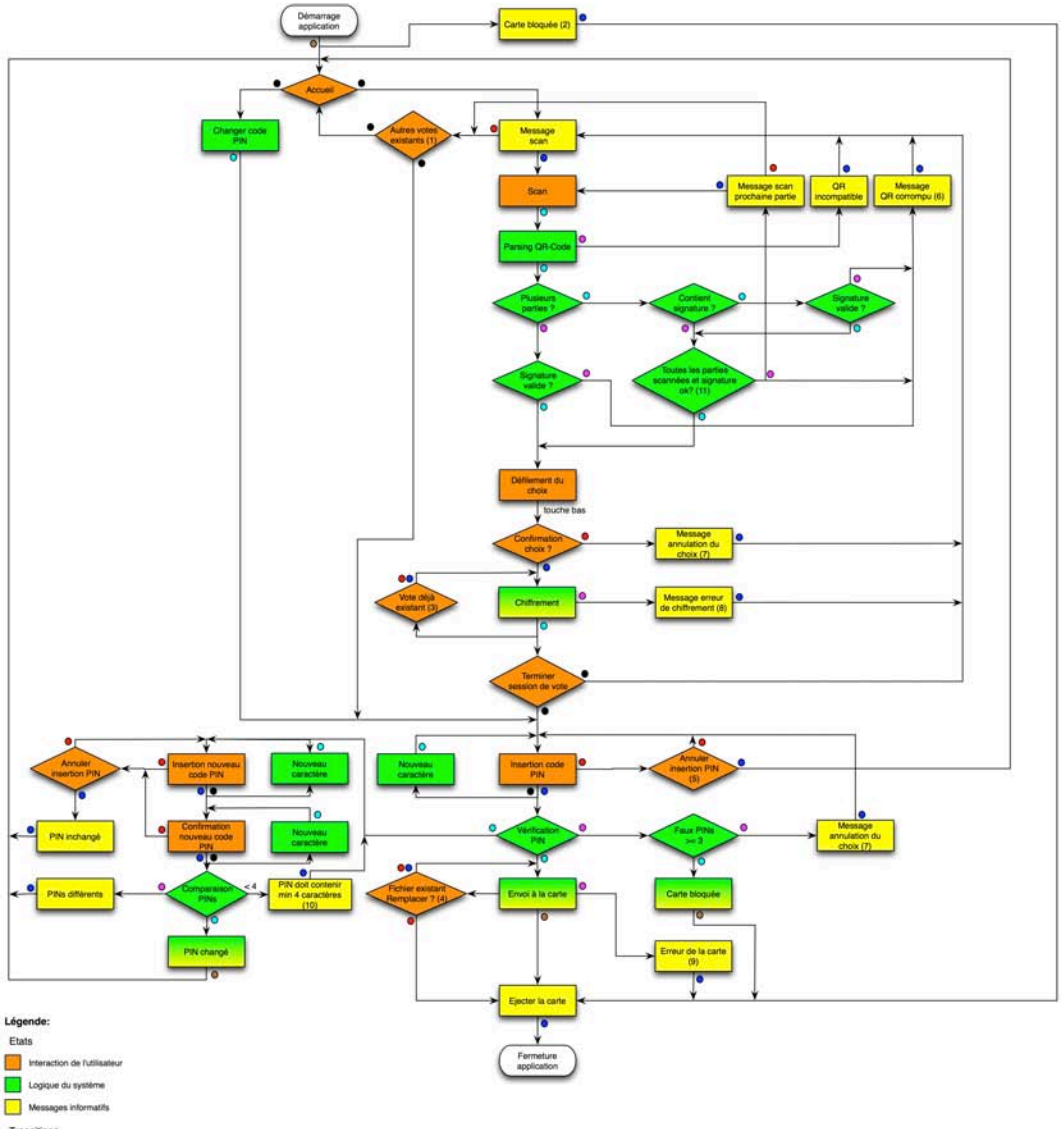
L’appareil de vote

- **Cycle de vote**
  - Accueil
  - Scan du code-barres
  - Confirmation du choix
  - Introduction du PIN
  - Finalisation du vote
- **Cycle de changement du PIN**
  - Accueil
  - Introduction du PIN
  - Introduction du nouveau PIN
  - Confirmation du nouveau PIN
  - Ecriture du nouveau PIN sur la carte

Cycle de vote

- **Scan du code-barres**
  - Code-barres en plusieurs parties
  - Vérification de la signature de la question
- **Confirmation du choix**
  - Défilement de tout le vote scanné
  - Valider ou annuler
  - Contrôle d'existence du vote
  - Chiffrage du vote (cryptographie pas implémentée)
- **Introduction du PIN**
  - Blocage de la carte après 3 faux PINs
- **Finalisation du vote**
  - Contrôle d'existence du vote sur la carte
  - Envoi à la carte pour signature (cryptographie pas implémentée)

Architecture de l’application de l’appareil de vote



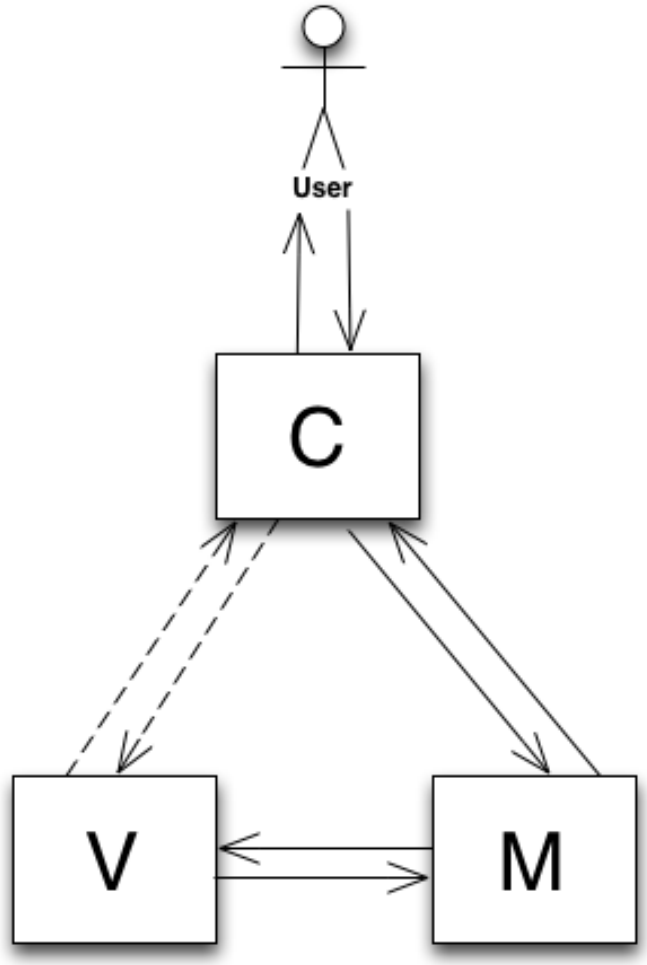
Caractéristiques de l'appareil de vote

- **Scanner de codes-barres**
- **Internationalisation**
- **Format du fichier de réponse**
- **Convivialité d'utilisation**
  - Design
  - Vibration à l'appui des touches
  - Défilement à l'écran
  - Textes

La plateforme de vote

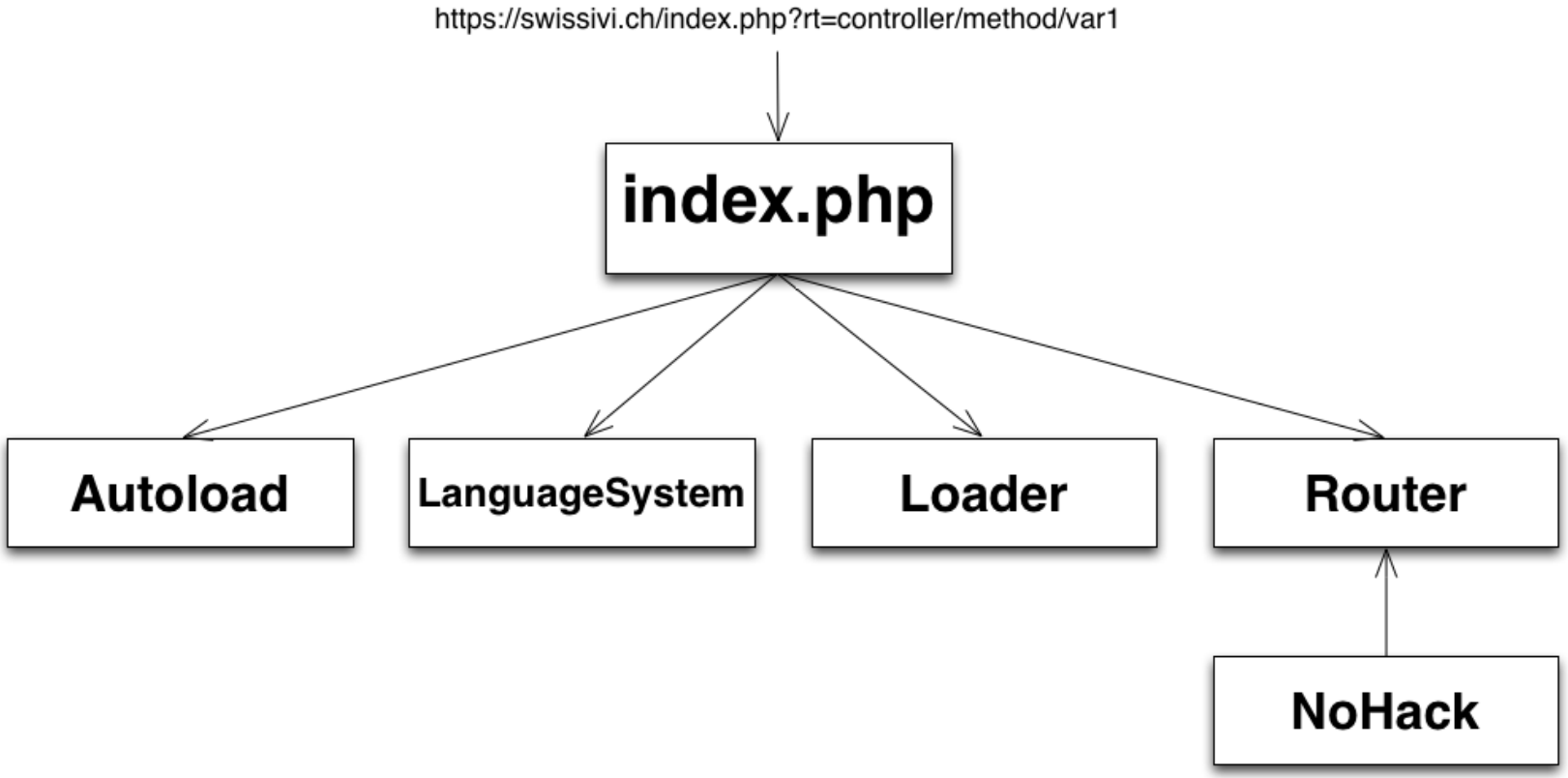
La structure de la plateforme de vote

- **Modèle de conception MVC (Model View Controller)**



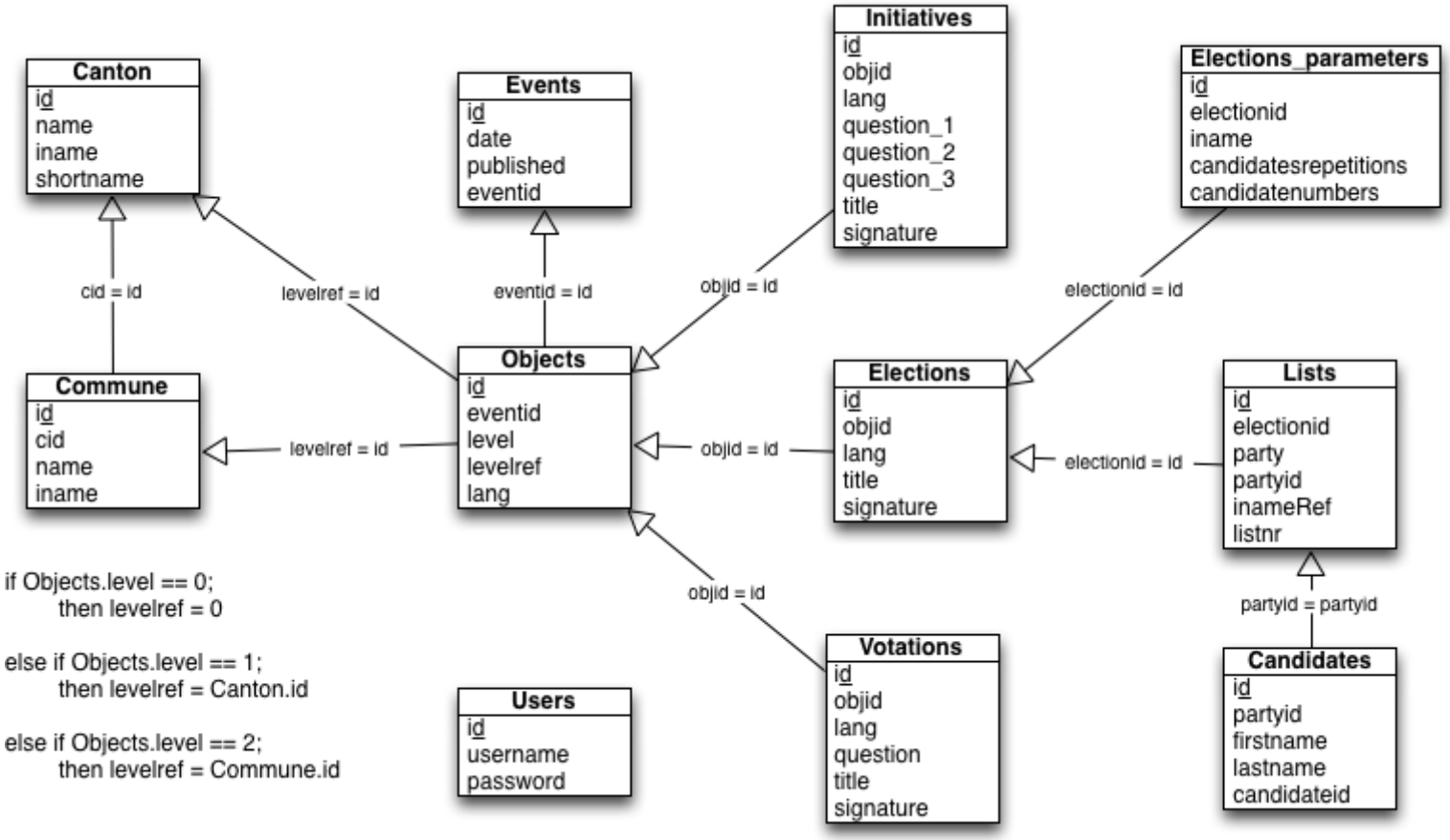
La structure de la plateforme de vote

- **Centralisation des requêtes via la page index.php**



La structure de la plateforme de vote

- **La base des données**



La structure de la plateforme de vote

- **Les QR-Codes (Quick-Response)**
  - Ils sont disponibles en 40 versions
  - A partir de la version 18 et plus haut, ils sont difficiles à scanner avec une caméra de smartphone
  - Limitation 5768 bits de données par QR-code
  - Trop petit pour de grandes élections, il faut donc générer plusieurs codes-barres
  - Compression des données pour minimiser l'espace utilisé

- **Contenu de QR-codes**
  - Numéro et nombre de parties
  - Identifiant de l'événement et de l'objet de vote
  - Type de votations (votation, élection, initiative)
  - Signature numérique de la question
  - Question
  - Réponse

Interfaces de la plateforme de vote

Démonstration dans le navigateur web

Démonstration du cycle de vote

Conclusion

Tâches restantes et potentiel d'amélioration

- **Tâches restantes:**
  - Implémentation de la cryptographie
  - Une vraie urne électronique (Bulletin Board)
- **Potentiel d'amélioration:**
  - Le panneau d'administration
  - Améliorations code jQuery et code Android
  - Interfaces graphiques

Connaissances acquises

- **Programmation web (jQuery)**
- **Développement Android**
- **NFC**
- **QR-Code**

Discussion

Haute école spécialisée bernoise
Technique et informatique

Merci pour votre attention.