

Epoll

Vote en ligne

Olivier Thauvin

26 mars 2009

- 1 Vote électronique
- 2 Epoll ?
- 3 Epoll 1.0 (aujourd'hui)
- 4 L'avenir
- 5 Test
- 6 A vous

Plan

- 1 Vote électronique
- 2 Epoll ?
- 3 Epoll 1.0 (aujourd'hui)
- 4 L'avenir
- 5 Test
- 6 A vous

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
 - techniquement compliqué

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
 - techniquement compliqué
 - logiciel souvent opaque

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
 - techniquement compliqué
 - logiciel souvent opaque
 - contrôle visuel impossible

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
 - techniquement compliqué
 - logiciel souvent opaque
 - contrôle visuel impossible
- le syndrome "L'ordinateur ne se trompe jamais"

Généralités

http://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
 - techniquement compliqué
 - logiciel souvent opaque
 - contrôle visuel impossible
- le syndrome "L'ordinateur ne se trompe jamais"

Références

- <http://www.ordinateurs-de-vote.org/>
- <http://www.cnil.fr/>

Plan

- 1 Vote électronique
- 2 Epoll ?**
- 3 Epoll 1.0 (aujourd'hui)
- 4 L'avenir
- 5 Test
- 6 A vous

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Logiciel libre

Rien de bien satisfaisant

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Logiciel libre

Rien de bien satisfaisant

solutions payantes

Entre 1500 et 5000 euros

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Logiciel libre

Rien de bien satisfaisant

solutions payantes

Entre 1500 et 5000 euros

Sujet intéressant

Surtout quand il me donne des arguments contre

Résumé

Application web

Résumé

Application web

- accessible avec un simple navigateur

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail
- pas d'intervention de l'administrateur

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail
- pas d'intervention de l'administrateur

Les fondations

- Perl (<http://www.perl.org/>)
- Catalyst (<http://www.catalystframework.org/>)

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail
- pas d'intervention de l'administrateur

Les fondations

- Perl (<http://www.perl.org/>)
- Catalyst (<http://www.catalystframework.org/>)
- PostgreSQL (<http://www.postgresql.org>)

Plan

- 1 Vote électronique
- 2 Epoll ?
- 3 Epoll 1.0 (aujourd'hui)**
 - Utilisation
 - Respect des règles
- 4 L'avenir
- 5 Test
- 6 A vous

Création du vote

La commission électorale

- 1 demande de création

Création du vote

La commission électorale

- 1 demande de création
- 2 confirmation de la demande (par mail)

Création du vote

La commission électorale

- 1 demande de création
- 2 confirmation de la demande (par mail)
- 3 configuration du vote (dont date)

Création du vote

La commission électorale

- 1 demande de création
- 2 confirmation de la demande (par mail)
- 3 configuration du vote (dont date)
- 4 inscription des électeurs

Création du vote

La commission électorale

- 1 demande de création
- 2 confirmation de la demande (par mail)
- 3 configuration du vote (dont date)
- 4 inscription des électeurs
- 5 envois des identifiants au électeurs

Le vote

Les électeurs

- 1 réception du mail avec url, login et mot de passe

Le vote

Les électeurs

- 1 réception du mail avec url, login et mot de passe
- 2 authentification sur le site

Le vote

Les électeurs

- 1 réception du mail avec url, login et mot de passe
- 2 authentification sur le site
- 3 choix

Le vote

Les électeurs

- 1 réception du mail avec url, login et mot de passe
- 2 authentification sur le site
- 3 choix
- 4 confirmation des choix

Le vote

Les électeurs

- 1 réception du mail avec url, login et mot de passe
- 2 authentification sur le site
- 3 choix
- 4 confirmation des choix
- 5 affichage du numéro du bulletin

Le vote

Les électeurs

- 1 réception du mail avec url, login et mot de passe
- 2 authentification sur le site
- 3 choix
- 4 confirmation des choix
- 5 affichage du numéro du bulletin
- 6 réception d'un accusé de réception par mail

Le dépouillement

La commission électorale

- 1 consolidation des choix libres si besoin

Le dépouillement

La commission électorale

- 1 consolidation des choix libres si besoin
- 2 marquage des bulletins invalides

Le dépouillement

La commission électorale

- 1 consolidation des choix libres si besoin
- 2 marquage des bulletins invalides

Dès la fin du vote

- Les résultats (provisoires) sont disponibles
- La liste de bulletins est disponible

Anonymat

stockage

Pas de relation entre l'électeur et le bulletin

Anonymat

stockage

Pas de relation entre l'électeur et le bulletin

Émargement

Mail	IP	heure de vote
thauvin@latmos.ipsl.fr	134.157.16.151	2009-03-19 15:31:56

Anonymat

stockage

Pas de relation entre l'électeur et le bulletin

Émargement

Mail	IP	heure de vote
thauvin@latmos.ipsl.fr	134.157.16.151	2009-03-19 15:31:56

Le bulletin

Id	Contenu
f4f667c78a2178095c3bae4d	oui

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5
- mot de passe aléatoire (électeurs)

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5
- mot de passe aléatoire (électeurs)
- *salt* aléatoire

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5
- mot de passe aléatoire (électeurs)
- *salt* aléatoire

Stockage des mots de passe

En clair :

```
password
```

Version chiffrée :

```
$1$aqsedfirt$sxdgVr1CwHx6VdBpRAx6m1
```

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- ne peut être retrouvé

Stockage des mots de passe

En clair :

```
password
```

Version chiffrée :

```
$1$aqsedfrt$xdgVr1CwHx6VdBpRAx6m1
```

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- ne peut être retrouvé
- méthode fiable

Stockage des mots de passe

En clair :

```
password
```

Version chiffrée :

```
$1$aqsedf$rt$ sxdgVr1CwHx6VdBpRAx6m1
```

Éviter les tricheries

Côté base de données

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Contrôle par l'utilisateur

- nombre de votants et nombre de bulletins disponibles

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Contrôle par l'utilisateur

- nombre de votants et nombre de bulletins disponibles
- liste d'émargement disponible

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Contrôle par l'utilisateur

- nombre de votants et nombre de bulletins disponibles
- liste d'émargement disponible
- liste des bulletins disponible dès la fin du vote

Les problèmes

Les problèmes

Le Mail

- n'est pas chiffré

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

- lecture : accès aux résultats avant la fin du vote

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

- lecture : accès aux résultats avant la fin du vote
- écriture : modification des résultats (mais cela devrait se voir)

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

- lecture : accès aux résultats avant la fin du vote
- écriture : modification des résultats (mais cela devrait se voir)

L'application elle même

S'assurer de l'intégrité du code

Bilan

Est-ce parfait ?

Bilan

Est-ce parfait ?

Bien sûr

Bilan

Est-ce parfait ?

Bien sûr

des bogues ?

Bilan

Est-ce parfait ?

Bien sûr

des bogues ?

Aucun !

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote

des bogues ?

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes

des bogues ?

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes
- des validations des données à ajouter
- ...

des bogues ?

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes
- des validations des données à ajouter
- ...

des bogues ?

Pas de connu à ce jour pour cette version.

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes
- des validations des données à ajouter
- ...

des bogues ?

Pas de connu à ce jour pour cette version.

Promesse :

Avoir quelque chose à proposer pour le vote du CL (en 15 jours)

Plan

- 1 Vote électronique
- 2 Epoll ?
- 3 Epoll 1.0 (aujourd'hui)
- 4 L'avenir**
 - Questions
- 5 Test
- 6 A vous

Epoll 2.0

Idées

Epoll 2.0

Idées

- pouvoir changer son vote (demande réflexion)

Epoll 2.0

Idées

- pouvoir changer son vote (demande réflexion)
- support de plusieurs langues (i18n)

Epoll 2.0

Idées

- pouvoir changer son vote (demande réflexion)
- support de plusieurs langues (i18n)
- rendre un vote privé

Epoll 2.0

Idées

- pouvoir changer son vote (demande réflexion)
- support de plusieurs langues (i18n)
- rendre un vote privé
- pouvoir redemander un mot de passe (électeurs)
- ...

Epoll 2.0

Idées

- pouvoir changer son vote (demande réflexion)
- support de plusieurs langues (i18n)
- rendre un vote privé
- pouvoir redemander un mot de passe (électeurs)
- ...

et la CNIL ?

Appliquer la *Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.*

<http://www.cnil.fr/index.php?id=1356>

Questions

Des questions rapides avant de passer au test ?

Plan

- 1 Vote électronique
- 2 Epoll ?
- 3 Epoll 1.0 (aujourd'hui)
- 4 L'avenir
- 5 Test**
- 6 A vous

Le test

La demo

<http://forge.ipsl.jussieu.fr/epoll/demo>

Plan

- 1 Vote électronique
- 2 Epoll ?
- 3 Epoll 1.0 (aujourd'hui)
- 4 L'avenir
- 5 Test
- 6 A vous**

Questions et remarques

Le projet

[http://forge.ipsl.jussieu.fr/epoll:](http://forge.ipsl.jussieu.fr/epoll)

- le code
- la documentation

Questions et remarques

Le projet

[http://forge.ipsl.jussieu.fr/epoll:](http://forge.ipsl.jussieu.fr/epoll)

- le code
- la documentation

Avez-vous :

- des questions
- des remarques
- des critiques