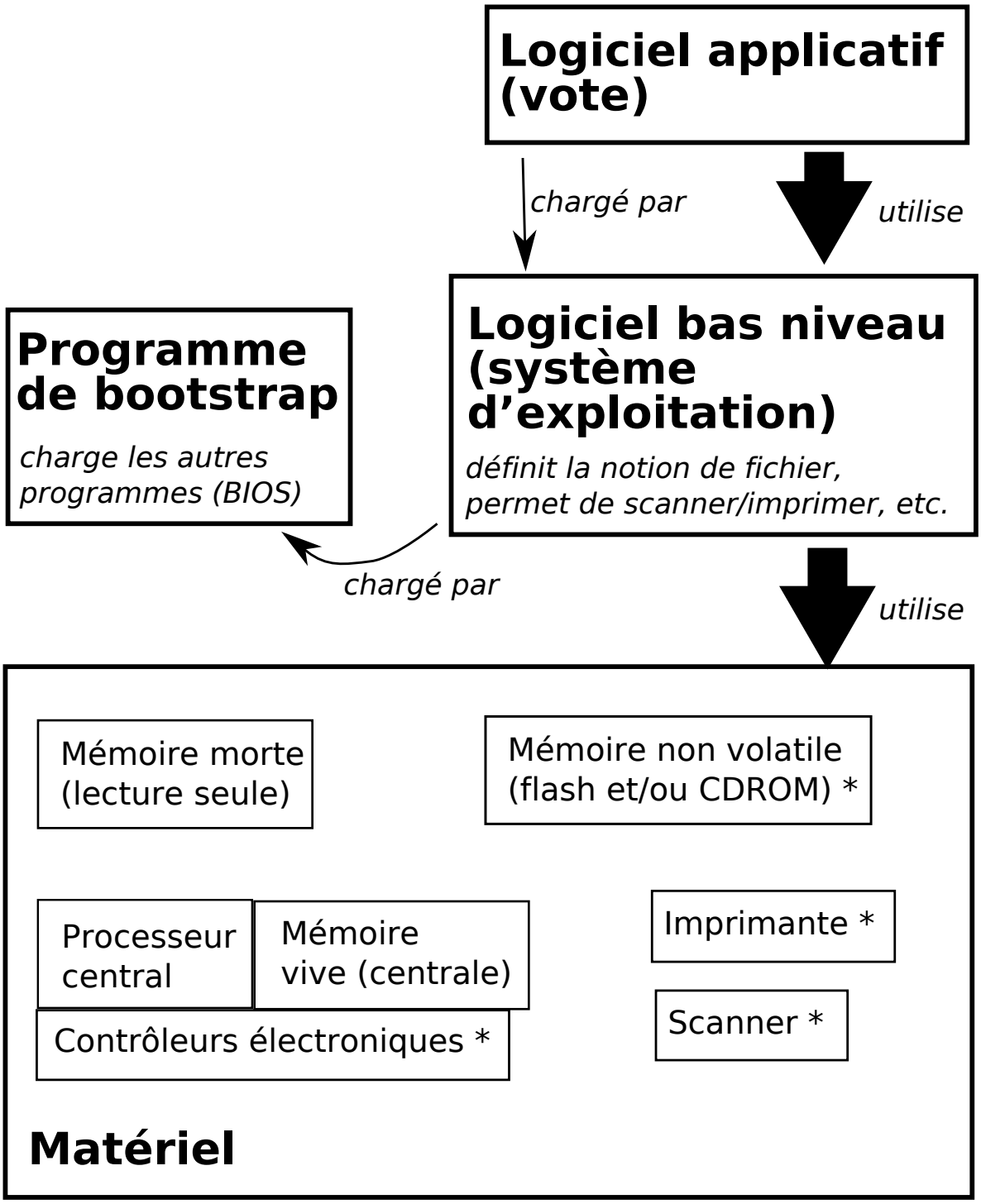
VOTE ELECTRONIQUE :

ASPECTS TECHNIQUES DE LA SECURITÉ

MARCIN SKUBISZEWSKI

- Composants d’une machine à voter
- Quelques problèmes potentiels
  - où ces problèmes peuvent résider
  - solutions possibles

ORDINATEUR DE VOTE — PRINCIPAUX COMPOSANTS



* *L'astérisque désigne les composants comportant leur propre logiciel bas niveau*

Les composants matériels sont listés à titre d'exemple

PROBLEMES POTENTIELS

Logiciel frauduleux

- décompte de voix délibérément faux

Bug logiciel, erreur matérielle

- difficulté de détection dans certains cas
- intérêt à ne pas révéler les bugs
  - pour sauvegarder la réputation des fournisseurs

Violations de secret de vote

- Ecriture d'informations en mémoire non-volatile
  - problème éventuel du logiciel
- Rayonnement électromagnétique
  - problème matériel
  - les espions soviétiques n'écrivaient qu'à la main
  - aux USA une norme de rayonnement (TEMPEST) existe pour les équipements militaires

Utilisabilité (fonctionnement non-intuitif de la machine)

- problème non couvert ici

TRACE PAPIER

La méthode de vérification la plus reconnue : trace papier

– Vénézuéla
– Majorité d'Etats américains

Position américaine décrite dans un rapport NIST : *Four Approaches to SI and Accessibility*

`http://vote.nist.gov/meeting-03222007/SI-n-access-031207.pdf`

Thus, in the future, only software-independent (SI) voting systems will be eligible for certification. An SI system is defined as one in which "a previously undetected change or error in its software cannot cause an undetectable change or error in an election outcome." That is, even if the software fails or is incorrect, there is still a mechanism which would allow such detection. Examples of such systems include DRE + voter-verifiable paper audit trail (DRE/VVPAT) systems and systems with paper ballots.

COMMENT VERIFIER LE LOGICIEL

- Est-ce que le logiciel fonctionne correctement ?
  - audit logiciel
  - publication du logiciel

- Le logiciel présent est-il celui qui a été audité ?
  - signature électronique

- Le matériel présent est-il celui qui a été audité ?
  - le matériel charge-t-il un autre logiciel en cachette ?
  - c’est la partie difficile
    - plombages ?

PUBLICATION DU LOGICIEL

Logiciel ***libre*** ou ***open source***

- publié en forme lisible et modifiable par un humain
- tout le monde peut lire, tester, modifier, adapter
- mais aussi : tout le monde peut copier
  - logiciel gratuit
  - modèles économiques spécifiques à *open source*

Problème apparent : peut-on trouver le logiciel libre adéquat ?

- tous les logiciels ne sont pas libres
- **Exemple :** systèmes d'exploitation : Windows non libre, Linux libre

PUBLICATION DU LOGICIEL, suite

Peut-on utiliser le logiciel libre pour le vote ?

Ce qui est coûteux :

- logiciel bas niveau
  - tout est disponible, gratuitement
- déploiement et maintenance
  - aucun désavantage économique à utiliser le logiciel libre
  - au contraire : on peut mettre en concurence plusieurs fournisseurs

Logiciel de vote : coût minime

- Problème potentiel : refus de certains fournisseurs, absence de mutualisation de coût
- Avantage : l'Etat n'est pas dépendant d'un fournisseur

=> inconvénients économiques faibles, avantages évidents

SIGNATURE DU LOGICIEL

Techniques mathématiquement avancées, mais

- connues depuis des années
- utilisées tous les jours en commerce électronique
  - accès HTTPS : vérification de l'authenticité du serveur
  - sécurisation de logiciels distribués

Fonctionnement :

- Seul celui qui connait la clef privée peut signer un texte
- Celui qui connait la clef publique peut vérifier la signature
- La clef publique est générée à partir de la clef privée
- On ne sait pas générer la clef privée à partir de la clef publique

Qui peut signer (s'assurer personnellement de l'identité du logiciel) :

- L'organisateur de l'élection
- Les partis politiques
- Les groupes d'observateurs

CE QU'ON PEUT VERIFIER

Supports portant un logiciel : CDROM ou mémoire flash

- vérification facile par tout ordinateur
- vérification par l'ordinateur de vote
  - le matériel + bootstrap vérifie le reste du logiciel

Supports portant le bootstrap

- par matériel spécialisé

Matériel, logiciel caché dans l'ordinateur de vote :

- vérification difficile

CONCLUSION

Trace papier :

- Méthode plébiscitée au niveau mondial
- Bonne protection
  - mais pas contre les violations du secret de vote

Publication du logiciel :

- Facile à réaliser
- Les problèmes sont culturels/organisationnels
- Résout la moitié du problème

Signature du logiciel

- Certifie le logiciel (facilement) et le bootstrap (difficilement)
- Ne protège pas contre les manipulations complexes du matériel

PLANONS UN PEU...

Code électoral, art. 64 : Dans les bureaux de vote dotés d'une machine à voter, le bureau de vote s'assure publiquement, avant le commencement du scrutin, que la machine fonctionne normalement [...]