scytl
Secure Electronic Voting

scytl
Secure Electronic Voting

Pnyx.DRE

Redundancy, Enhanced Auditability and Voter-Verifiability for DREs

Annapolis (Maryland), March 18 2005

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- Our solution: Pnyx.DRE
- Conclusions

Contents

scytl
Secure Electronic Voting

- **Presenting Scytl**
- DREs: Benefits and Drawbacks
- Our solution: Pnyx.DRE
- Conclusions

About Scytl

- Scytl is a European software company specialized in application-level cryptography and in the development of secure electronic voting solutions
- Scytl was formed as a spin-off from a University research group that holds the first two European PhD thesis on e-voting security (with over 25 scientific papers) and that participated in the first Internet binding elections in Europe in 1997
- Scytl commercializes Pnyx, a unique family of products that derives from its more than 10 years of research and development and is protected by international patents
- The objective of Pnyx is to provide electronic voting platforms with the same levels of trust, privacy and security as the conventional paper-based electoral systems
- Pnyx has been successfully used in numerous projects, including one of the only two permanent Internet voting platforms in the world (Switzerland)
- Scytl focuses its efforts on developing and maintaining unique security technology and distributes its solutions through partners such as Hewlett-Packard, Accenture, Oracle and Telefonica
- Scytl has received numerous international awards including the 2005 IST Prize granted by the European Commission to the best technology companies in Europe

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- **DREs: Benefits and Drawbacks**
- Our solution: Pnyx.DRE
- Conclusions

DREs - Benefits

scytl
Secure Electronic Voting

- **User-friendly** – Easy-to-use voter interface that facilitates the voting process
- **Speed and accuracy** in the vote counting process – Votes are counted electronically in digital format
- **Accessibility** – People with disabilities (e.g., visually impaired) can vote without the assistance from a third party
- **Flexibility** – Allows last-minute changes in the ballots, supports multiple languages, etc.
- **Prevention of unintentional errors** – Reduces “under-voting” and “over-voting” errors

DREs - Drawbacks

scytl
Secure Electronic Voting

- DREs may be perceived as **“black boxes”**
  - DREs are generally based on proprietary software
  - High-level of complexity in the software
  - Difficult to audit and certify by election authorities
  - Need to re-audit the software after any change in the election
- DREs **do not provide voters with verification mechanisms** to check that their votes have been correctly cast and recorded
- DREs **do not provide election authorities and third-parties with sufficient independent audit mechanisms** (e.g., DREs do not allow a meaningful parallel recount of the votes independent from the results from the DRE)

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- **Our solution: Pnyx.DRE**
- Conclusions

Objectives of Pnyx.DRE

scytl
Secure Electronic Voting

1. **Allow the voter to individually verify the correct treatment of his/her vote**
   - Verification that his/her vote is cast and recorded as he/she intended
   - Assurance that the recorded vote will be counted as cast
   - Make this verification process accessible to everyone, including the blind and visually impaired
2. **Provide redundancy through a double-register of the votes**
   - Reduction in the risk of loss of votes
   - Possibility of an independent parallel recount of the votes
3. **Facilitate the audit and certification process by the election authorities**
   - Simplification of the audit and certification of the voting system by concentrating the critical security features in a simple and easy-to-audit device
   - Enhancement of the auditability of the election through the use of cryptographic tools

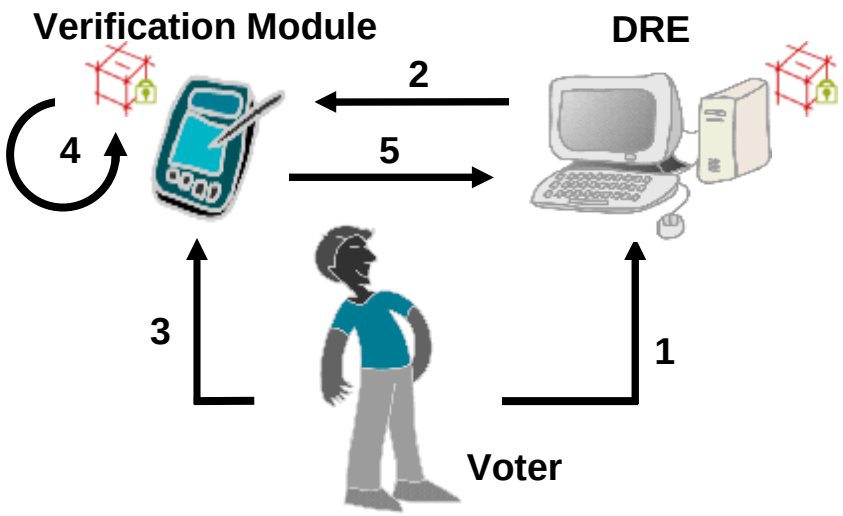
Pnyx.DRE Components

scytl
Secure Electronic Voting

- Pnyx.DRE is based on an independent module (called **Verification Module**) connected to the DRE
- The Verification Module has **two components:**
  - A **hardware device** with a screen, an audio port and two buttons
  - **Cryptographic software** that runs in this hardware device to protect the votes
- The Verification Module represents a **secure and reliable environment** because:
  - It is independent from the manufacturer of the DRE
  - It is based on open-source software and on software that is open to audits
  - It is very simple since it only performs a limited number of functions
  - It is very easy to audit and certify by election authorities
- Additionally, our solution provides **election authorities with cryptographic tools** (e.g., one-way accumulators) **to check the integrity of every single vote**

How is the voting process?

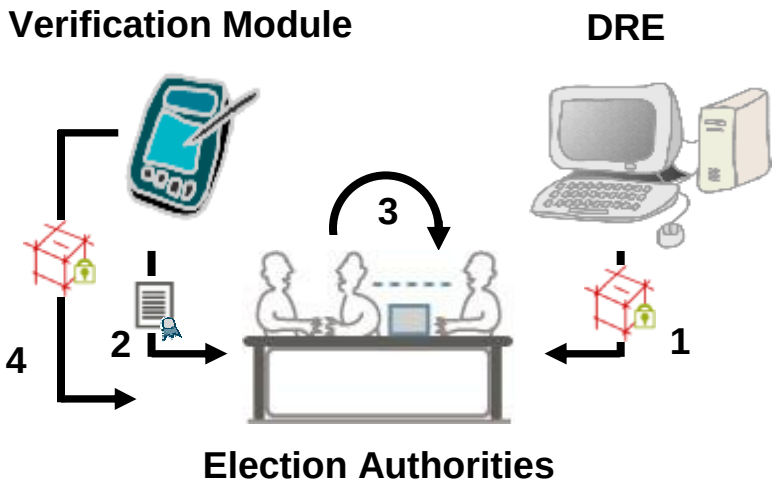
scytl
Secure Electronic Voting



1. The voter makes the selection of the desired voting options for all the races in the DRE
2. The selected options are transferred to the Verification Module
3. The voter verifies (via screen and/or audio) the selected options and accepts them
4. The verified voting options are encrypted and digitally signed in the Verification Module in order to protect every single ballot from internal and external attacks
5. The protected ballot is stored in the Verification Module and a positive verification message is sent to the DRE where the ballot is stored in the usual format

How is the audit process?

scytl
Secure Electronic Voting



1. The election authorities retrieve the votes from the DRE
2. The election authorities retrieve the Integrity Record from the Verification Module. This Integrity Record was generated in a secure environment based on every single voter-verified vote
3. The election authorities check that the set of votes retrieved from the DRE matches the value of the Integrity Record from the Verification Module
4. If the check fails, the election authorities can retrieve the back-up votes (which are the cryptographically-protected voter-verified votes) from the Verification Module and implement a parallel recount

Cost of Pnyx.DRE

scytl
Secure Electronic Voting

- The **cost** of Pnyx.DRE is **approximately $500** per DRE and includes the following:
  - The **hardware** device with a color screen, audio port and computing and cryptographic capabilities
  - The **software** implemented in this hardware device to cryptographically protect every single vote
  - The **software** used by electoral authorities or independent auditors to audit the election accuracy and integrity

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- Our solution: Pnyx.DRE
- **Conclusions**

Conclusions

scytl
Secure Electronic Voting

- Pnyx.DRE can **enhance the security** of your existing voting equipment and contribute to **increase public confidence** in this voting equipment by:
  - Allowing voters to verify that their votes were cast and recorded as they intended
  - Simplifying the audit and certification processes since the auditing efforts need to focus only on the simple and easy-to-audit Verification Module
  - Protecting the integrity and anonymity of every single vote
  - Reducing the risk of losing votes by providing the voting system with redundancy
  - Allowing an independent parallel vote recount
- Pnyx.DRE can be **easily integrated with your current Diebold equipment**
- Pnyx.DRE is a **cost effective** solution to provide redundancy, enhanced auditability and voter-verifiability to your current voting equipment

scytl
Secure Electronic Voting

Secured by scytl