scytl
Secure Electronic Voting

scytl
Secure Electronic Voting

Scytl's voter-verifiability solutions

Pnyx.DRE and Pnyx.VVPAT

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- Pnyx.DRE: Voter-verifiability through electronic verification modules
- Pnyx.VVPAT: Providing security and accessibility to VVPAT solutions
- Conclusions

Contents

scytl
Secure Electronic Voting

- **Presenting Scytl**
- DREs: Benefits and Drawbacks
- Pnyx.DRE: Voter-verifiability through electronic verification modules
- Pnyx.VVPAT: Providing security and accessibility to VVPAT solutions
- Conclusions

About Scytl

- Scytl is a European software company specializing in **application-level e-voting 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**
- The objective of Pnyx is to provide electronic voting platforms with the same levels of **trust, privacy and security** that exist in conventional paper-based electoral systems
- Pnyx has been successfully used in **numerous projects**, including one of the only two permanent Internet voting platforms for binding elections 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, Intel, 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**
- Pnyx.DRE: Voter-verifiability through electronic verification modules
- Pnyx.VVPAT: Providing security and accessibility to VVPAT solutions
- 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 of the DRE)

Types of voter-verifiability solutions

scytl
Secure Electronic Voting

- The current debate on the security of DREs has resulted in the development of a number of innovative solutions to allow voters to individually verify that their votes are cast and recorded as they intended
- These voter-verifiability solutions for DREs can be classified in two categories:
  - **Voter-Verified Paper Audit Trail (VVPAT) solutions**: Solutions that rely on printed paper ballots to provide DREs with voter-verifiability
  - **Electronic voter-verifiability solutions**: Solutions that rely on electronic means (e.g., cryptography, independent electronic verification modules, etc.) to provide DREs with voter-verifiability

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- **Pnyx.DRE: Voter-verifiability through electronic verification modules**
- Pnyx.VVPAT: Providing security and accessibility to VVPAT solutions
- 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

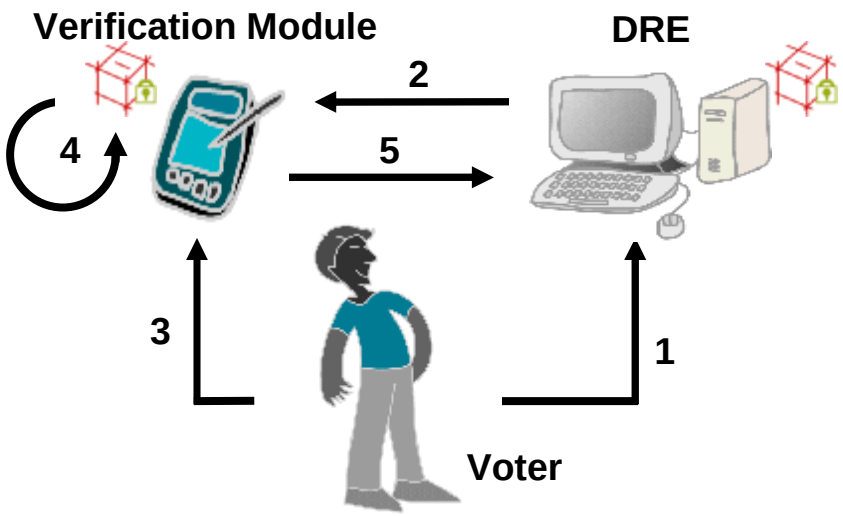
Pnyx.DRE components

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 with Pnyx.DRE?

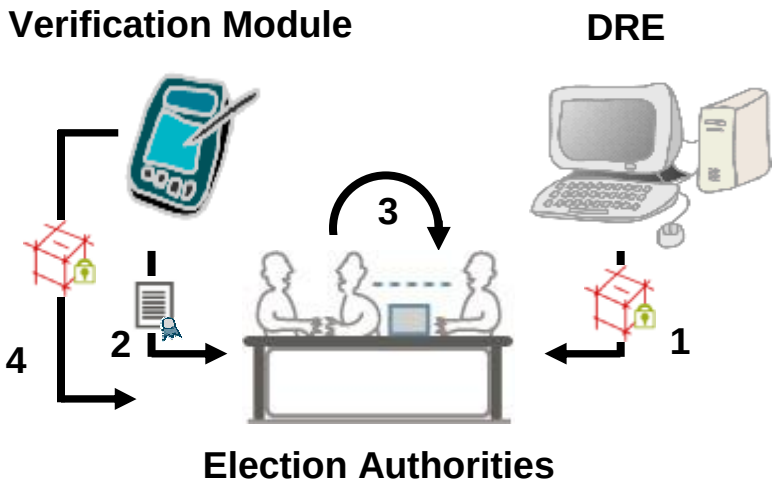
scytl
Secure Electronic Voting



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 with Pnyx.DRE?

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

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- Pnyx.DRE: Voter-verifiability through electronic verification modules
- **Pnyx.VVPAT: Providing security and accessibility to VVPAT solutions**
- Conclusions

VVPAT - Advantages

scytl
Secure Electronic Voting

- The main advantages of VVPAT solutions for DREs are as follows:
  - VVPAT solutions can be an **effective method to guarantee that votes are cast as the voters intended**
  - VVPAT solutions are **based on tangible elements** (i.e., paper) and, therefore, have great capability to generate voter confidence
  - VVPAT solutions are **simple** and, therefore, are easy to understand by average voters
  - VVPAT solutions provide election authorities with a physical record that can be used to carry out a **parallel recount** independent from the results of the DRE
- As a result of these advantages, many groups favour the adoption of VVPAT solutions and a number of states have initiated legislative reforms to implement VVPAT solutions with their current DRE equipment

VVPAT - Drawbacks

scytl
Secure Electronic Voting

- VVPAT solutions present the following drawbacks:
  - VVPAT solutions allow voters to verify that votes are cast as they intended but **do not provide sufficient assurance that the votes will be counted as they were cast**:
    - VVPAT solutions do not prevent the addition of bogus ballots (ballot stuffing)
    - VVPAT solutions do not prevent the elimination of valid votes
    - VVPAT solutions do not prevent the alteration of valid votes
  - VVPAT solutions **do not provide election authorities with accurate mechanisms to determine the correct result** in case of discrepancies between the results provided by the count of electronic votes in the DRE and the count of paper ballots
  - VVPAT solutions are based on paper and, therefore, they **are not accessible for blind or visually impaired voters**
- These disadvantages can represent a serious roadblock to the adoption of VVPAT solutions by many states

VVPAT with digital signature

scytl
Secure Electronic Voting

- A number of partial solutions have been proposed to mitigate some of the drawbacks of VVPAT solutions described in the previous slide
- Some experts propose to have the DRE digitally sign the paper ballots that are printed in order to guarantee their authenticity and prevent the addition of bogus ballots
- This solution does not solve most of the other problems:
  - **It is still possible to eliminate valid votes** (e.g., by physically eliminating the paper ballots) since there is not an accurate recovery mechanism
  - Election authorities **do not have accurate mechanisms to determine the correct results** in case of discrepancies between the results of the DRE and the count of the paper ballots
  - The verification system is still **not accessible for blind** and visually impaired voters
- Additionally, the digital signing of the paper ballots by the DRE adds a **new risk: the DRE could generate an incorrect digital signature to invalidate votes**
  - The voter may verify and cast his/her vote without realizing that the printed paper ballot has an invalid digital signature
  - It would be possible to carry out a “selective” attack by invalidating votes only for a particular candidate

Objectives of Pnyx.VVPAT

scytl
Secure Electronic Voting

1. **Provide VVPAT solutions with mechanisms to assure that votes will be counted as they were cast**
   - Prevent the addition of bogus ballots but without running the risk of invalidating valid votes as a result of the accidental or voluntary generation of incorrect digital signatures
   - Prevent the elimination of valid votes (e.g., by physically eliminating the printed paper ballots) by providing an accurate recovery mechanism
   - Prevent the alteration of valid votes
2. **Provide election authorities with accurate mechanism to determine the correct results in case of discrepancies between the results from the DRE and the count of paper ballots**
3. **Improve the accessibility of the VVPAT solutions**
   - Provide blind and visually impaired voters with the possibility to individually verify that their votes are cast and recorded as they intended without the assistance from a third party

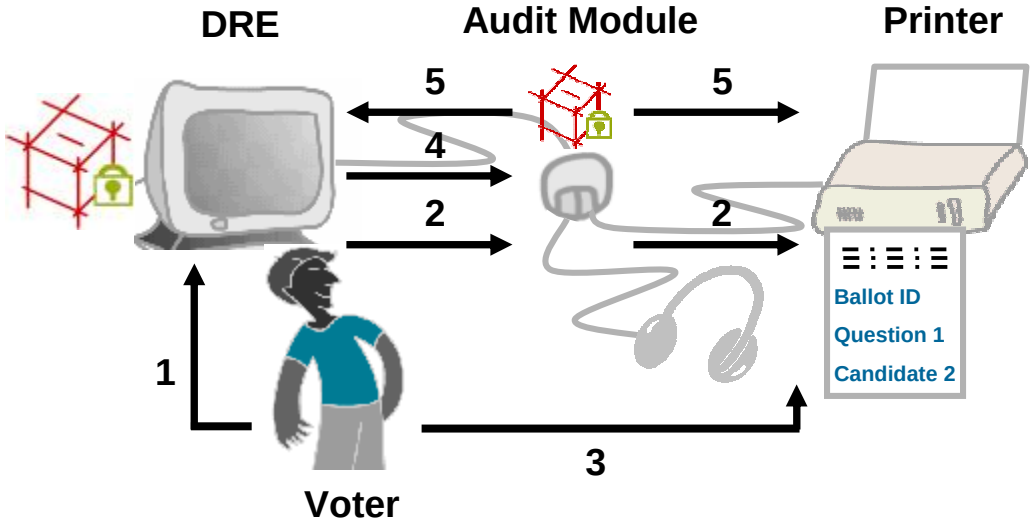
Pnyx.VVPAT basic concept

scytl
Secure Electronic Voting

- Pnyx.VVPAT is based on an independent module (called **Audit Module**) connected to both the DRE and the printer
- This Audit Module has **two components:**
  - A **hardware device** with minimum computing capabilities
  - **Cryptographic software** that runs in this hardware device to protect the votes
- The Audit 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
- The main function of the Audit Module is to **provide cryptographic protection to printed paper ballots and digital votes**, avoiding having to rely on the DRE and on the physical handling of the printed ballots. This prevents the elimination of valid votes as a result of the accidental or voluntary generation of incorrect digital signatures

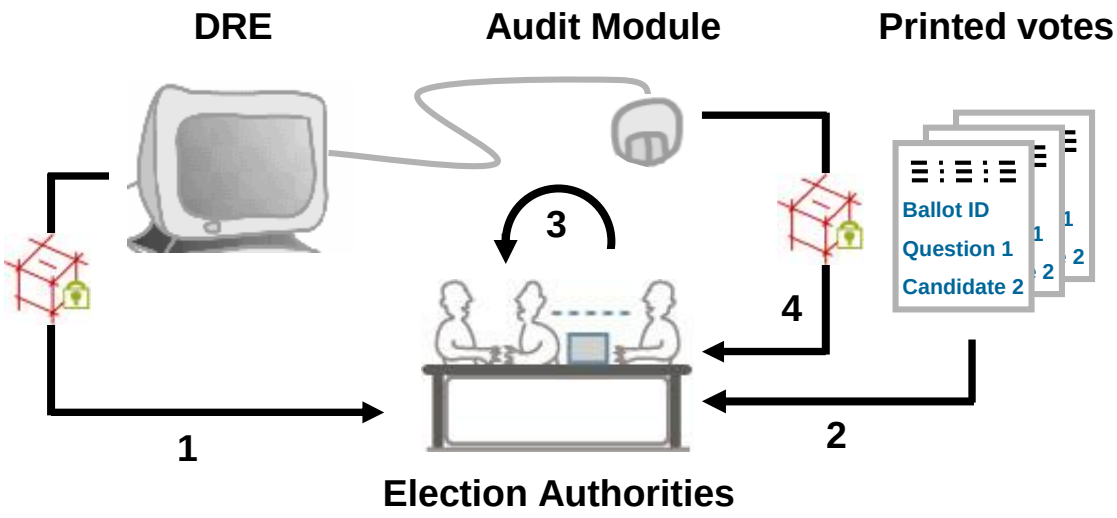
How is the voting process with Pnyx.VVPAT?

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 from the DRE to the printer through the Audit Module. A paper record containing the selected options is printed (and/or reproduced through headphones)
3. The voter verifies (via the paper record and/or audio) the selected options and accepts them
4. The verified voting options are digitally signed in the DRE and are sent to the Audit Module. The Audit Module checks the validity of the digital signature. Any problem that could invalidate the signature of the verified options would be detected at this point
5. The Audit Module digitally signs the digitally signed voting options received from the DRE. The resulting digital signature is sent from the Audit Module to the printer (e.g., the digital signature is printed on the paper record as a bar code) and to the DRE. The DRE verifies the validity of this signature and stores it with the electronic vote. The Audit Module can also store the digitally signed vote to enhance the redundancy of the voting system

How is the audit process with Pnyx.VVPAT?



1. The election authorities retrieve the electronic votes from the DRE and check their validity by verifying their digital signatures (generated by the DRE and the Audit Module) before counting them
2. The election authorities also check the validity of the printed votes by verifying their digital signatures (generated by the DRE and the Audit Module) before counting them
3. Printed votes and electronic votes can be cross-checked using the ballot identifiers and digital signatures. This allows to:
    - Recover lost electronic or paper votes
    - Recover valid votes that have been invalidated due to printing or electronic errors
4. The Audit Module contents can also be used to check the election accuracy and solve disputes

Contents

scytl
Secure Electronic Voting

- Presenting Scytl
- DREs: Benefits and Drawbacks
- Pnyx.DRE: Voter-verifiability through electronic verification modules
- Pnyx.VVPAT: Providing security and accessibility to VVPAT solutions
- **Conclusions**

Conclusions

scytl
Secure Electronic Voting

- Voter-verifiability through independent electronic verification modules represents a valid alternative to VVPAT solutions
- The use of electronic verification modules allows voters (even blind voters) to individually verify their votes in a secure and reliable environment independent from the DRE
- Current VVPAT solutions can be an effective method to guarantee that votes are cast as voters intended but do not provide sufficient assurance that those votes will be counted as they were cast
- The use of an Audit Module (between the DRE and the printer) to digitally sign both the paper ballots and the digital votes can solve some of the security deficiencies of current VVPAT solutions while making them accessible to blind voters

scytl
Secure Electronic Voting

Secured by scytl