Privacy of E-Voting (Internet Voting)

Asst. Prof. Sinem Sav

Some slides taken from Prof. Philippe Oechslin and Prof. Erman Ayday

Background

Some background

- We vote in standard/traditional way in Turkey
  - *Voting in person at poll booths*
- Some countries, e.g., Switzerland, vote in mail
  - *Voting by mail (over 90% of votes)*
  - *Voting over Internet (called e-voting, in Switzerland) is possible experimentally since 2004*
  - *The laws are being adapted to make it an official 3rd channel*

Security Objectives

- Accuracy:
  - the result reflects the choice of the voters
- Secrecy:
  - The vote of each voter remains secret
- Absence of provisional results:
  - There is no information about provisional results during the election

Across all channels (booth, mail, Internet)

Typical risks for (e)voting

- Accuracy:
  - Double votes (e.g. over two channels)
  - Manipulation of votes (e.g. on the voters machine while voting, during transmission over Internet, by hacking the servers)
  - Fake votes, given without authorization (voting card)
- Secrecy
  - Interception of votes (e.g. on the voters machine while voting, during transmission over Internet, by hacking the servers)
- No provisional results:
  - Interception of votes (e.g. on the voters machine while voting, during transmission over Internet, by hacking the servers)

Verifiable e-voting protocols

- To limit the risks, the use of verifiable e-voting protocols is mandated.
  - they allow to verify that the results have not been manipulated
- Individual verifiability
  - An individual has proof that their vote has been correctly taken into account
    - protects against a man-in-the-browser that changes outgoing votes and incoming confirmation (you think you voted ‘yes’ but you voted ‘no’)
- Universal verifiability
  - We have proof that all votes have been correctly counted
    - protects against attacks on the server, that delete, add or modify some votes

Let’s dive more into this…

Internet Voting

- **Internet voting:** Actions that are used by voters to obtain and return ballots using the Internet
- Convenient, efficient and secure facility for recording and tallying votes in an election
- Should be explained as simply as possible to be understandable for voters
  - Preferably, no zero-knowledge proofs, blind signatures, etc.

"We don't have the technology yet to do [Internet voting] in a secure way, and we may not for a decade or more."

Ron Rivest (2010)

A “Perfect” Internet Voting System Guarantees:

- **Privacy**
  - Votes cannot be linked to voters
  - Voters can vote anonymously
- **Receipt-freeness**
  - Voter cannot gain any information (a receipt) which can be used to prove to a coercer that he voted in a certain way
- **Coercion-Resistance**
  - Voter cannot *cooperate* with a coercer to prove to him that he voted in a certain way
  - No vote buying
- Correctness
  - Only eligible voters can vote
  - Nobody can vote more than once
  - Submitted votes cannot be altered
  - All valid votes are counted
- Fairness
  - No partial results are revealed
- Verifiability
  - Correctness can be publicly verified (by anyone)

Internet Voting - Privacy Requirements

- **Vote-privacy**
  - *The attacker cannot discern how a voter votes from any information that the voter necessarily reveals during the course of the election*
- **Receipt-freeness**
  - Can be intentional or unintentional
  - Unintentional receipts include nonces or keys the voter gives during the protocol
  - Stronger than privacy
  - *The attacker cannot discern how a voter votes even if the voter voluntarily reveals additional information*
- **Coercion-resistance**
  - Strongest of the three
  - *The attacker cannot discern how a voter votes even if the voter cooperates with the attacker during the election process*
    - Giving the attacker any data
    - Using data which the attacker provides in return
- Note: voter can tell an attacker how he voted, but unless he provides convincing evidence the attacker has no reason to believe him

Main Challenges

- Internet voting should offer the same level of security and confidence as traditional voting
- When there's no physical ballot, it becomes impossible to determine whether there has been tampering in a close election
- Privacy when casting ballots
- Privacy of returned ballots

Privacy Challenges

- Privacy when casting ballots
  - Software bugs or malicious software in the voter's computer
    - Modify the candidates selection before the ballot is returned
  - Employers can monitor the online activity of their employees
    - By monitoring logs or using "key loggers"
- Privacy of returned ballots
  - Voter needs to sends some identifying information along with his ballot
  - Vote can be linked to the voter

Internet Voting in Research

- More than 6 specialized international conferences
  - VoteID
  - EVT/WOTE
  - EVOTE
  - REVOTE
  - SecVote
  - Swiss E-Voting Workshop

Internet Voting – Potential Directions

- Standard cryptography
  - Encryption
  - Digital signatures
- Advanced cryptography
  - Homomorphic tallying
  - Blind signatures
  - Secret sharing
  - Threshold cryptosystems
  - Mix networks
  - Zero-knowledge proofs

CRYPTOGRAPHIC SOLUTIONS FOR INTERNET VOTING

Existing Techniques

- *Blind signature schemes*
  - Message blindly signed by the administrator
  - Signature of the administrator confirms the voter's eligibility to vote
- *Homomorphic encryption*
  - Compute the encrypted tally directly from the encrypted votes
- *Randomization*
  - E.g., by mix-nets
  - Mix up the votes so that the link between voter and vote is lost

Verifying Privacy-Type Properties of Electronic Voting Protocols [1]

- Formalized the privacy-related properties
- Used applied pi calculus
  - Language for describing concurrent processes and their interactions
  - Used to study a variety of security protocols
- Evaluated three schemes based on
  - Privacy
  - Receipt-freeness
  - Coercion-resistance

[1] S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security, July 2009

Formalizing the Properties

- **Privacy:** attacker cannot distinguish a situation in which Alice votes *a* and Bob votes *b*, from another one in which they vote the other way
- **Receipt-freeness:** attacker cannot detect a difference between Alice voting in the way he instructed, and her voting in some other way, provided Bob votes in the complementary way each time
- **Coercion-resistance:** attacker is assumed to communicate with Alice during the protocol, and can prepare messages which she should send during the election process

Main Findings

- *If a voting protocol is receipt-free then it also respects privacy*

- *If a voting protocol is coercion-resistant then it also respects receipt-freeness*

1st protocol [1] - Overview

- *Secure bit-commitment*: voter computes a commitment on his vote
  - Noone can see the vote before the voter releases the key for the commitment
- *Blind signatures*: administrator digitally signs the voter's (blinded) commitment without learning the commitment or the vote
  - Administrator is not allowed to see the commitment
    - Administrator knows the ID of the voter
    - It can link the voter to the vote once the voter reveals the commitment key

[1] Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A practical secret voting scheme for large scale elections. In Advances in Cryptology AUSCRYPT '92, 1992

Simplified Protocol

ADMINISTRATOR

3) Verify voter's eligibility

2) Blinded commitment

4) Sign the (blinded) commitment using blind signature

5) Signed commitment

VOTER

1) Compute commitment on vote *v* using a random key *r*

6) Signed commitment

COLLECTOR

7) Verify the signature

8) Post the commitment to a list and publish the list

9) Random key *r*

10) Publish the votes

1st protocol - Analysis

- Privacy: respects privacy
- Receipt-freeness: scheme is not receipt-free
  - If the voter gives away the key for commitment, the coercer can verify that the committed vote corresponds to the coercer's wish
- Coercion-resistance: scheme is not coercion-resistant

2nd Protocol [1] - Overview

- *Trap-door bit commitment* scheme to have receipt-freeness
  - Allows the voter who has performed the commitment to open it in many ways
  - Voter says how he wants to open his commitment during the voting stage
- Introduced an extra party to the 1st protocol:
  - *Timeliness member*: voter says how to open the commitment through an *untappable anonymous* channel

[1] Tatsuaki Okamoto. An electronic voting scheme. In *Proc. IFIP World Conference on IT Tools*, pages 21–30, 1996

Simplified Protocol

VOTER

2) Blinded commitment

ADMINISTRATOR

5) Signed commitment

3) Verify voter's eligibility

4) Sign the (blinded) commitment using blind signature

1) Compute commitment on vote *v* using a random key *r*

9) How to open the commitment, including random key *r*

6) Signed commitment

COLLECTOR

7) Verify the signature

8) Post the commitment to a list and publish the list

TIMELINESS MEMBER

10) Publish the votes

2nd Protocol - Analysis

- Privacy: respects privacy
- Receipt-freeness: scheme is receipt-free
  - Info given by the voter to the timeliness member (T) can be different from the one he provides to the coercer
  - Voter who forged the commitment, provides to the coercer the one allowing the coercer to retrieve the vote *c*, whereas she sends to T the one allowing him to cast the vote *a*
- Coercion-resistance: scheme is not coercion-resistant
  - If the coercer provides the voter with the commitment that he has to use (without revealing the trap-door), the voter cannot cast her own vote *a*
    - Voter cannot produce fake outputs as she did for receipt-freeness
    - Similar to providing a public key to sign but not providing the private key

3rd Protocol [1] - Overview

- Relies on *re-encryption* and *designated verifier proofs (DVP)* of re-encryption
  - DVP of the re-encryption proves that the two ciphertexts contain indeed the same plaintext
  - *Gives the designated verifier the ability to simulate the transcripts of the proof*
  - Only convinces one intended person
    - Here only convinces the voter, that the re-encrypted ciphertext contains the original plaintext
  - Cannot be used to convince the coercer

[1] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *Proc. Information Security and Cryptology*, 2004

Simplified Protocol

ADMINISTRATOR

3) Encrypted vote and signature

4) Verify voter's eligibility

5) Re-encrypt the ciphertext

6) Sign the re-encrypted vote

VOTER

7) Re-encrypted vote, signature, DVP

1) Encrypt vote with the collector's public key

2) Sign the encrypted vote

8) Re-encrypted vote, signature

COLLECTOR

9) Verify the signature

10) Decrypt the votes

11) Publish the result

3rd Protocol - Analysis

- Privacy: respects privacy
- Receipt-freeness: scheme is receipt-free
  - Remember: DVP gives the designated verifier the ability to simulate the transcripts of the proof
  - Using his private key, the voter provides a fake DVP stating that the actual re-encryption of the encryption of vote *a* is a re-encryption of the encryption of vote *c*
- Coercion-resistance: scheme is coercion-resistant
  - Similar reasoning as receipt-freeness

Zero Knowledge Proofs (ZKPs)

- ZKPs are/can be used for:
  - prove we know the content of an encrypted vote without revealing it,
  - that we use the correct key for decryption, without revealing it,
  - that we did not modify the votes when mixing them, without revealing the votes.

INTERNET VOTING IN REAL LIFE

Internet Voting in Real-Life

- Netherlands
  - Vulnerability of system exposed in public (2006)
  - Council of ministers decided to fully return to paper-based elections (2008)
- Germany
  - Computers used for Bundestag election (2005)
- Norway
  - Communal and regional elections in 2011
- Switzerland, Estonia, Spain, Brazil, Australia, India, Canada

Internet Voting - Estonia

Internet Voting - Estonia

- **Goal:** increase voter participation

Type of elections	Date	Internet votes (% of all votes)	Turnout (% of electorate)	Internet voting turnout (% of electorate)	First time users of ID card online (%)
Municipal elections	Oct 2005	1.9	47.4	0.9	61
Parliamentary elections	April 2007	5.5	61.9	3.4	39
European Parliament	June 2009	14.7	43.9	6.5	19
Municipalel ections	Oct 2009	15.8	60.6	9.5	18.5
Parliamentary elections	March 2011	24.3	63.5	15.4	N/A

  - Allowed voting through chip-secure mobile phones

Legislative Demands

- Voters should hold a certificate and be able to generate a digital signature
- Voters may vote electronically on the web page of the National Electoral Committee
- A voter shall identify himself or herself by giving a digital signature
- **E-voting shall be an additional voting option**

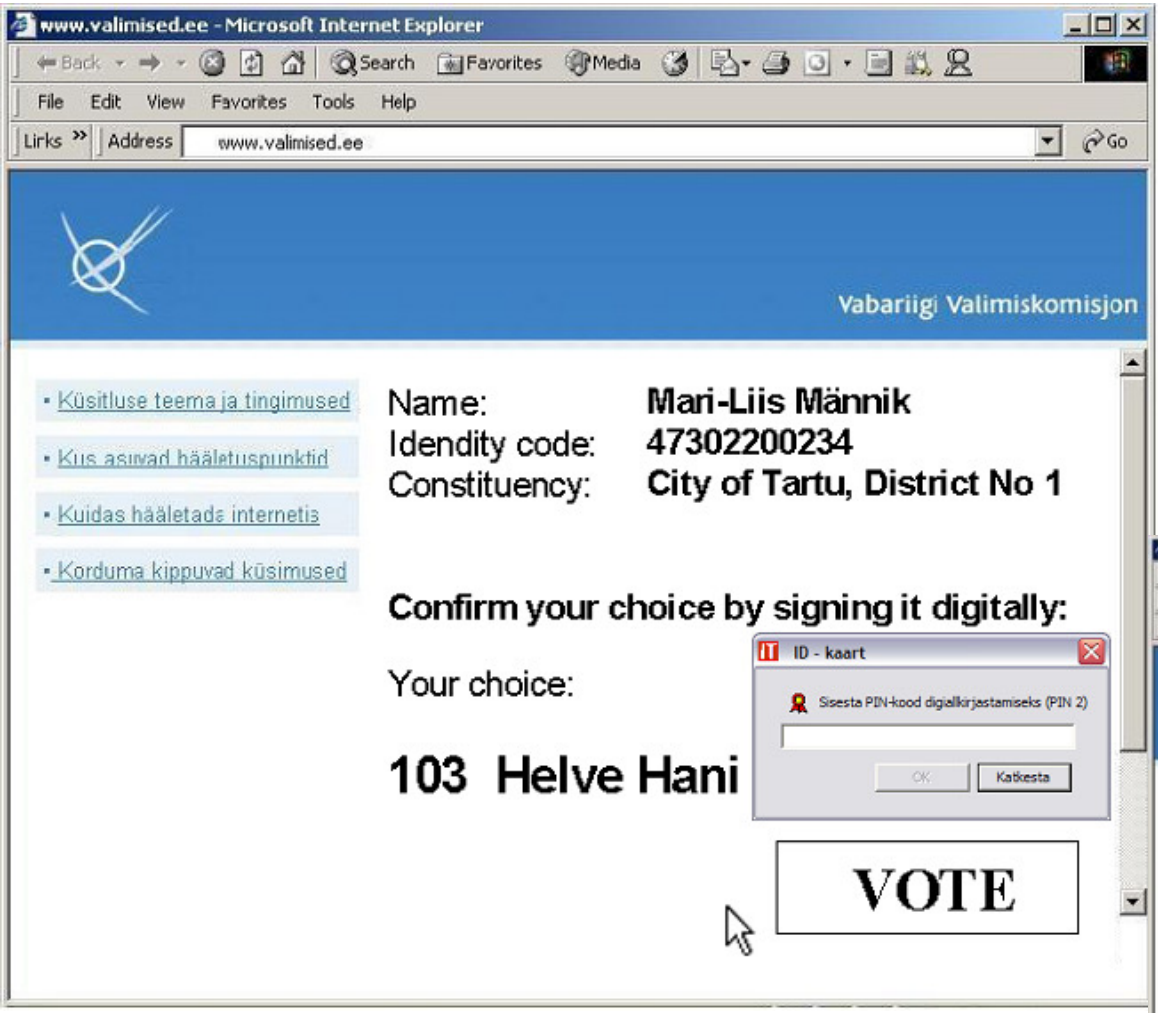
Highlights

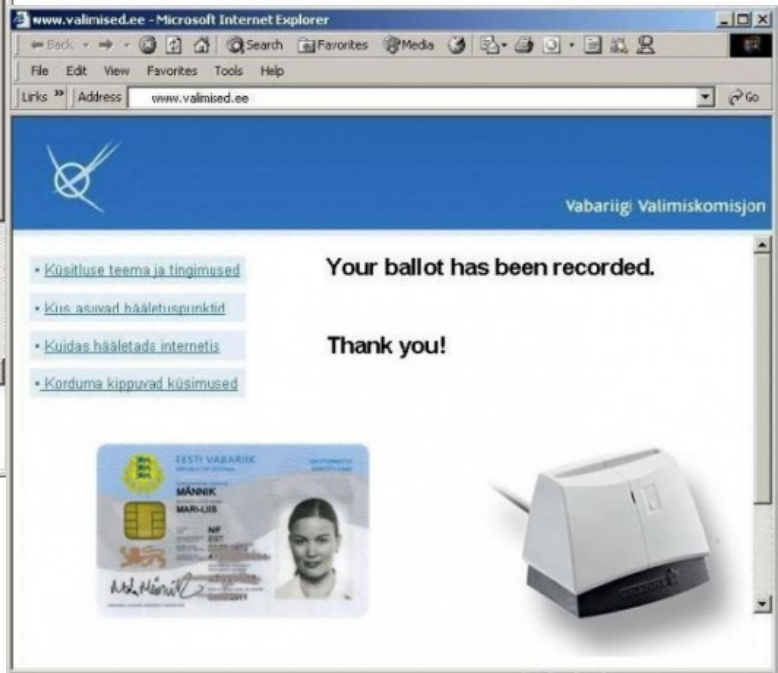
- ID-cards are used for voter identification
  - Open-source public key-private key encryption software (upgraded to 2048-bits in 2011)
- Possibility of electronic re-vote
  - **Voter can cast his vote again and the previous vote will be deleted**
  - Measure against vote-buying and voting under *coercion*
- The priority of traditional voting
  - **Should the voter go to polling station on voting day and cast a vote, his e-vote shall be deleted**
- Published e-voting source code on GitHub – 2013
  - https://github.com/vvk-ehk/evalimine

Voter Authentication

- Via the ID card
- Cards are equipped with a chip containing electronic data, certificates and their associated private keys protected with PIN-codes
- In some countries, identification codes are sent to the voters often by post
  - But, many citizens have not been interested to disclose their real home address to the national population register

Voter Authentication





To Vote Remotely You Need:

- **The ID-card**
  - Issued by Citizenship and Migration Board
- **PIN-codes**
  - Issued together with the ID-card
- **Valid certificates**
  - Once your certificates are expired, you can renew them on your own
- A **computer** with an active Internet connection
- A **smartcard reader**
  - From a computer store or your local bank office
- **ID-card software**

Overview of the Protocol

- Voter inserts the ID-card into a card reader and opens the homepage of the National Electoral Committee
- Relevant candidate list is displayed according to the voters personal identification number
- Voter makes his voting decision
  - **Encrypted (via the public key of the system) and can be defined as *inner envelope***
- **Voter confirms his choice with a digital signature**
  - Can be defined as *outer envelope*
  - Voter gets a confirmation that his vote has been recorded
- During the count:
  - Voter's digital signature (outer envelope) is removed
  - Members of the National Electoral Committee can only open the anonymous e-votes and count them

Overview of the Protocol

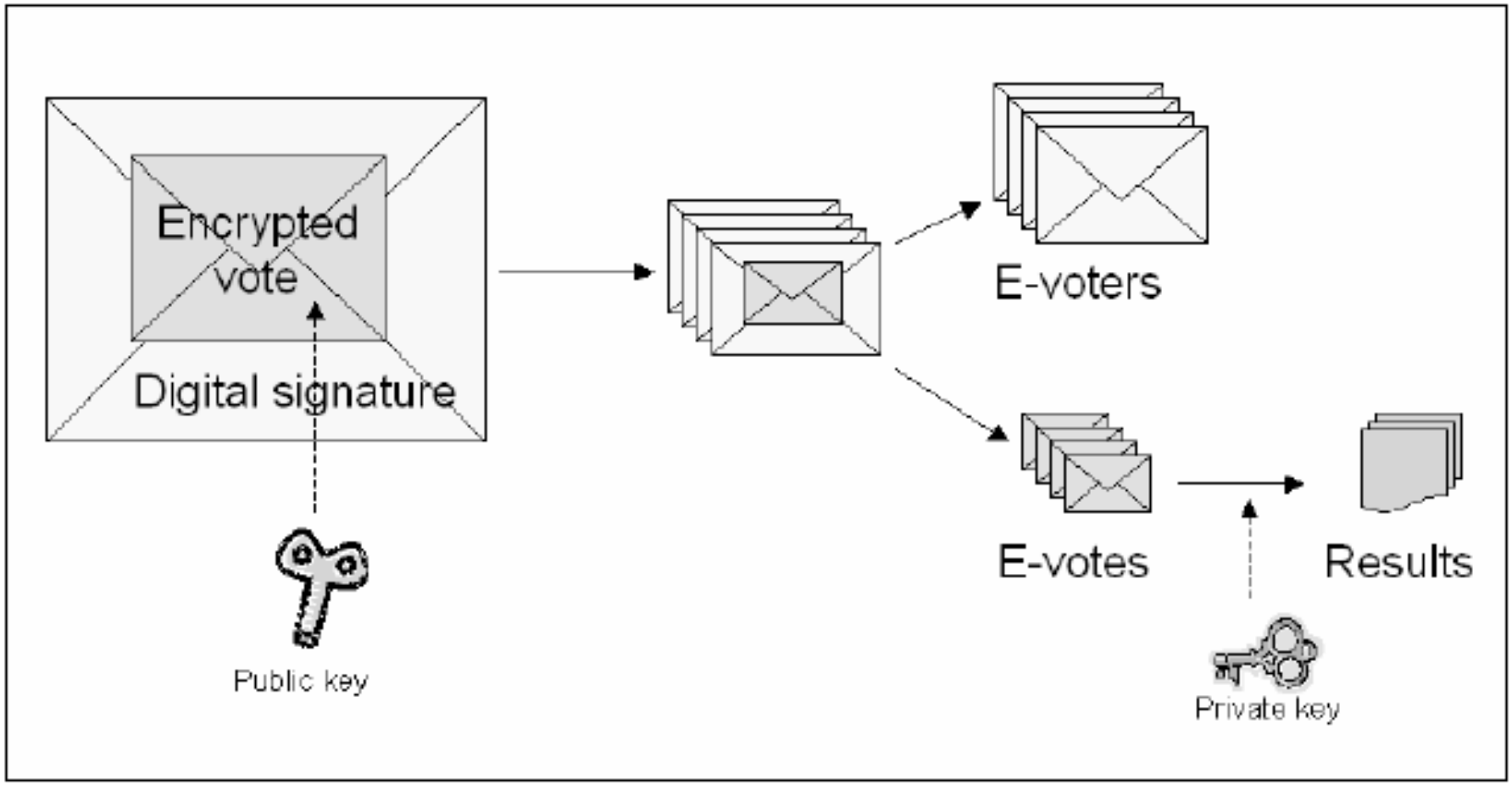


Figure: The Estonian National Electoral Committee

Privacy

- To ensure the voter's privacy:
  - At no point any part of the system should be in possession of both the digitally signed e-vote and the private key of the system
- To count e-votes, the system's private key is activated by key-managers according to the established key management procedures
- Counting of votes takes place in the vote counting application, separated from the network

Drawbacks

- Application encrypts voter's choice with the system's public key
  - 1 public key for all inner envelopes
  - Single point of failure
- Threats due to viruses, malware, etc. not considered
- Have not been used in other countries
  - Require storing information about the voter identity with the votes
  - Increasing the risk that voter privacy will be compromised

over an example: Switzerland

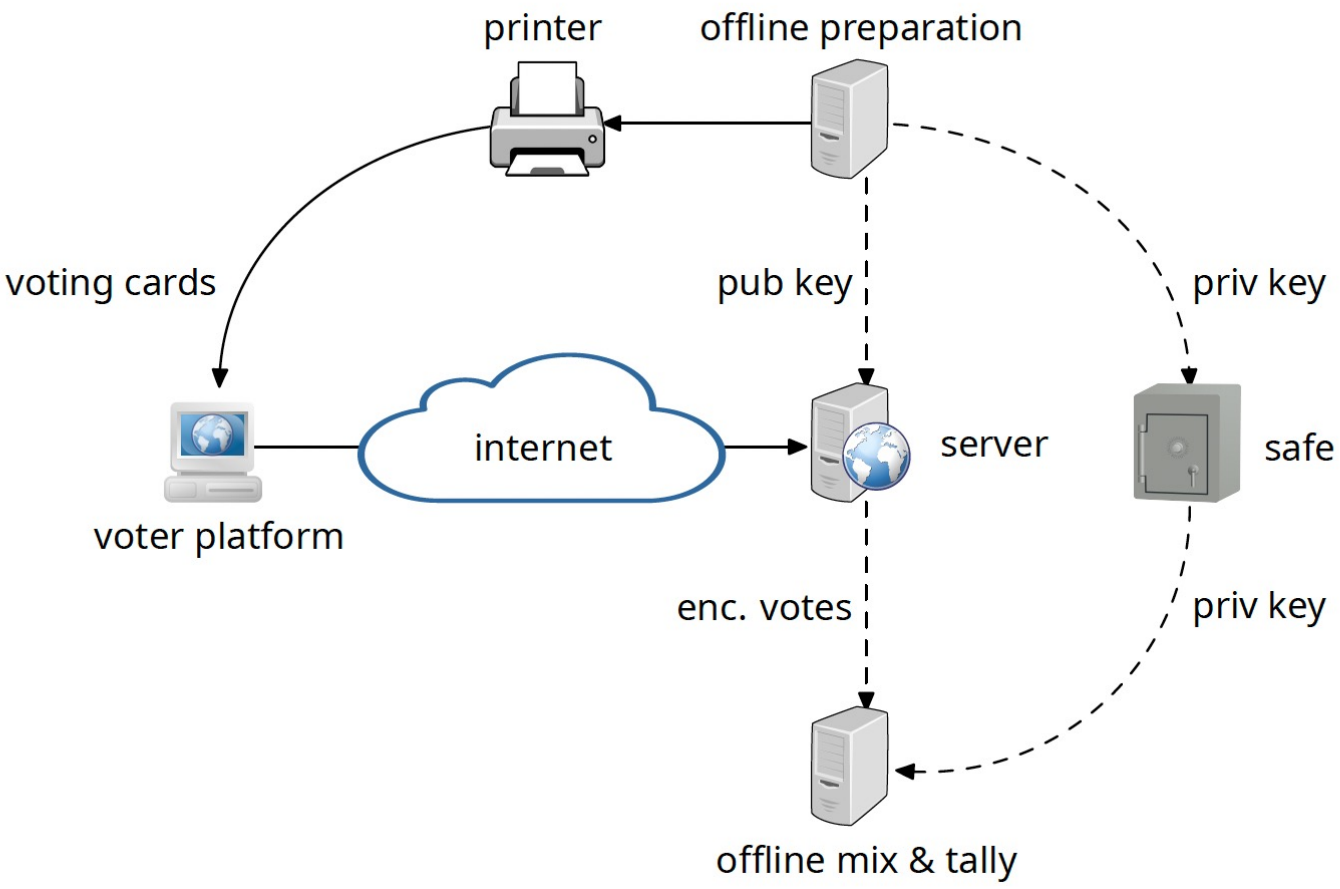
Security levels and trust models (over an example: Switzerland)

- Over the years, Switzerland has gradually increased the security levels required for e-voting systems

- Currently the requirements include the following
  - The system must offer complete verifiability (individual & universal)
  - The system must be independently reviewed
  - The code must be published
  - There is a limit on the percentage of the electorate that can use the system

The actual details of the requirements are being discussed right now by the government.

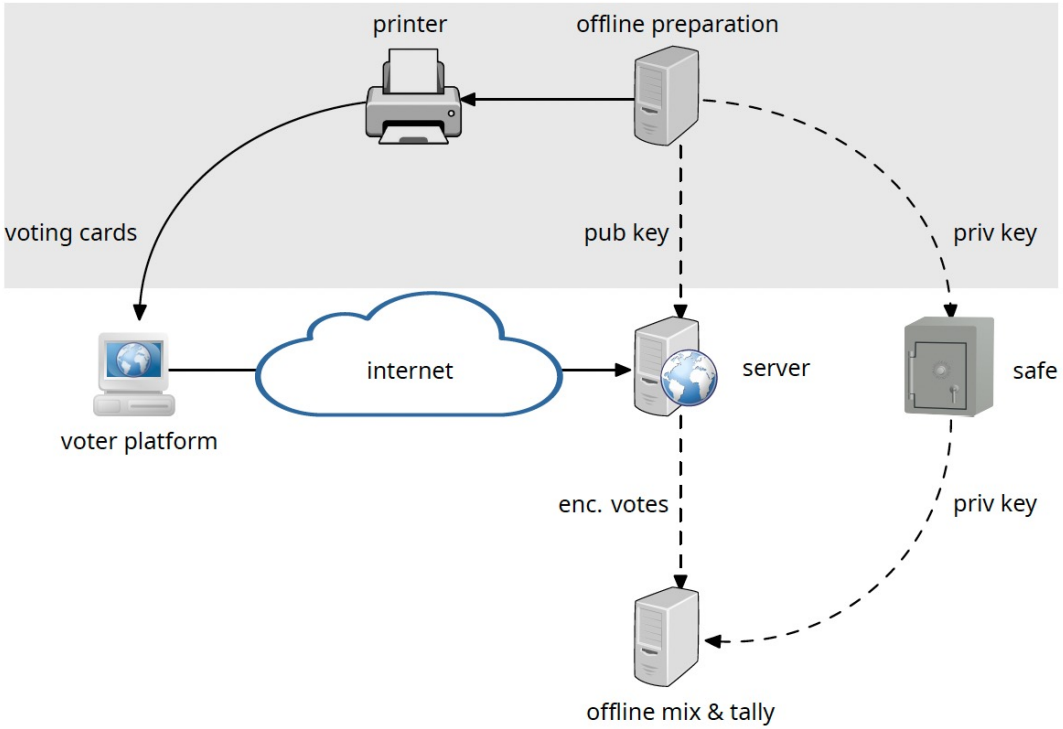
Elements of the e-voting systems



3 phases

1. Preparation

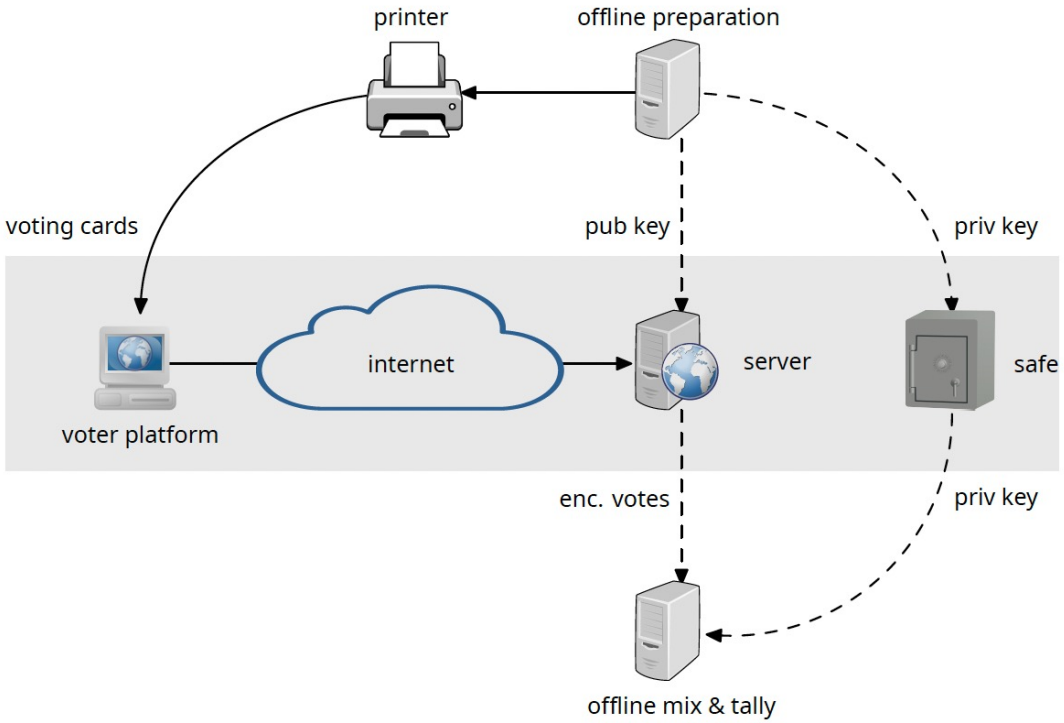
- Key pairs are generated
- Printer gets data to print on voting card
- Cards are sent to voters
- Server gets public key
  - with USB stick
- Private key is stored in police safe



3 phases

2. Voting

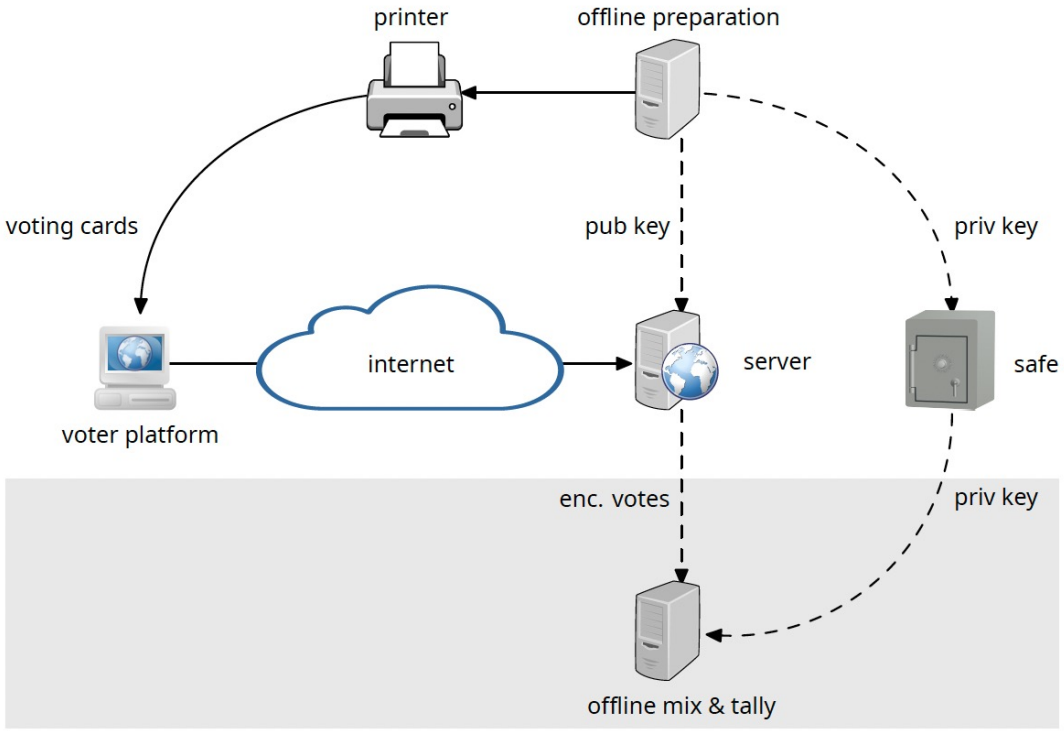
- Voter use voting card to cast vote
- Server encrypts vote



3 phases

3. Tallying

- Encrypted votes are transferred to offline server
  - with USB stick
- Private key is taken from police safe
- Votes are mixed
  - to guarantee anonymity
- Votes are decrypted and tallied

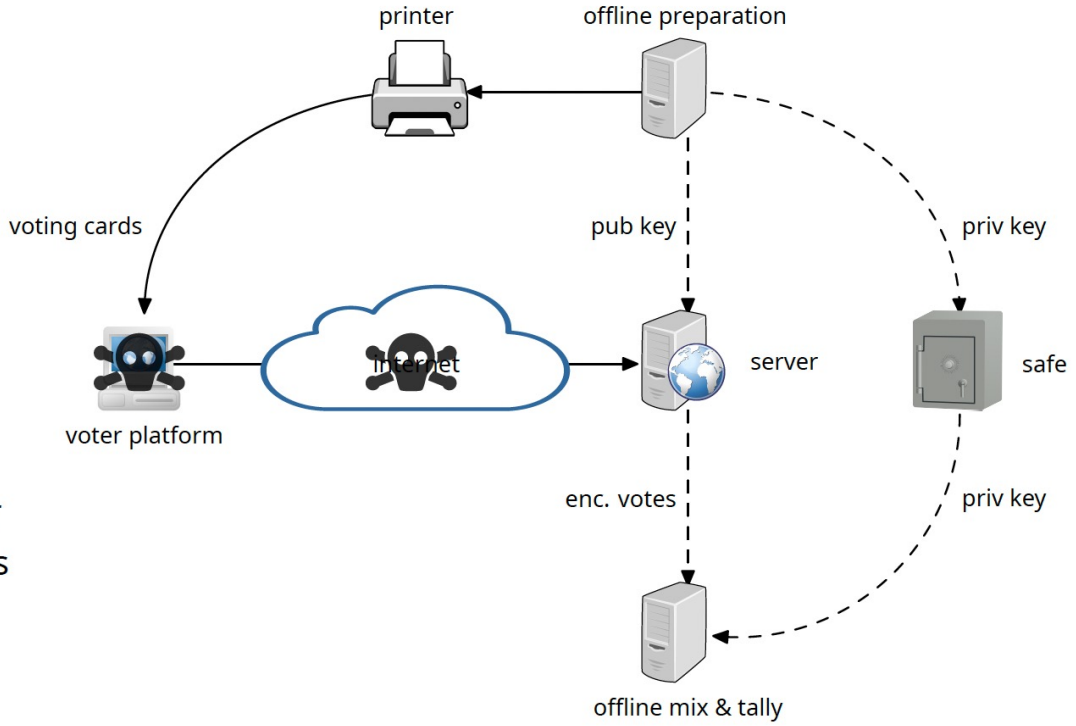


Trust model

- A basic security level is achieved through very good security controls
  - machine hardening
  - physical, network and user access control
  - segregated teams for different jobs (e.g. dev $\neq$ ops $\neq$ monitor)
  - four-eyes principle for critical operations
    - e.g. two people are needed retrieve the priv. key from safe
  - everything is monitored and logged
  - test votes are given before and during the voting phase
    - results of tests are verified
  - e-vote results are compared statistically to votes from other channels

Trust model for individual verifiability

- The platform is not trusted
- The network is not trusted
- The protocol must guarantee individual verif. even if the platform or the network are hacked
  - voting cards contain verification codes
  - when vote is received, server sends back verification codes
  - voter compares codes on screen, with codes on voting card



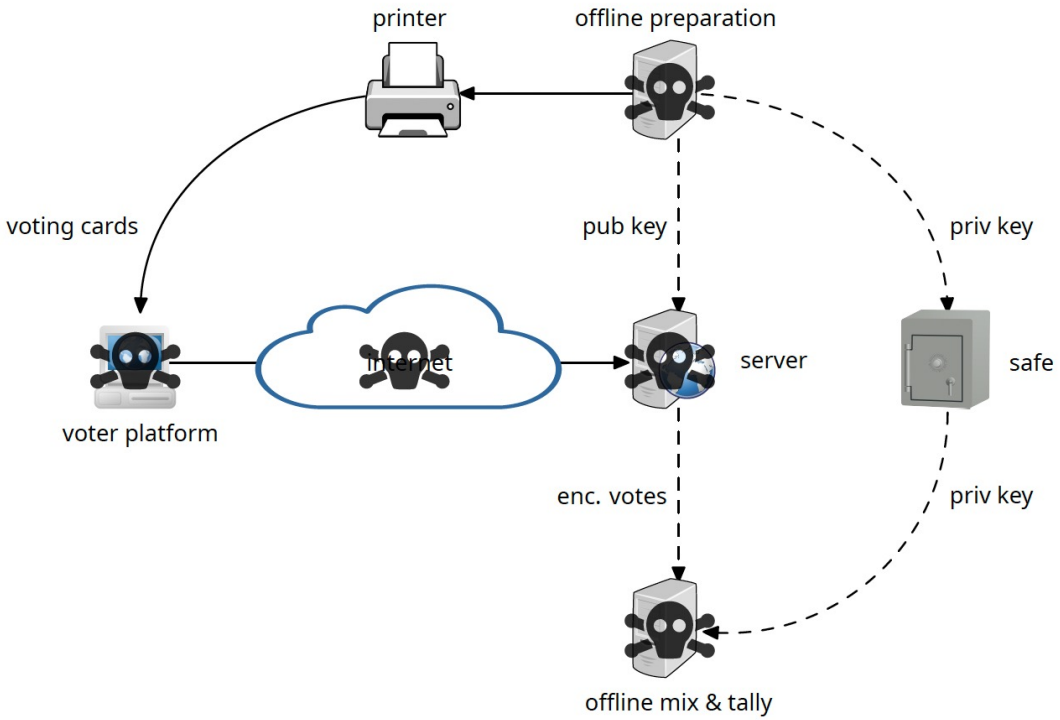
- hacker can't see the code on the card, they can not change the vote and still display the correct code!
- the platform is trusted for keeping the vote secret !

Example (**Svote** from Swiss Post)

- Receive voting card by postal mail
- Log in e-voting portal with Initialization code
- Make your selection and transmit the vote
- Receive the verification codes
- If codes are correct, confirm vote with confirmation code
- Receive finalization code as confirmation.

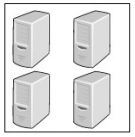
Trust model for universal verifiability

- The platform is not trusted
- The network is not trusted
- The servers are not trusted
- The printer is trusted
- The safe is trusted

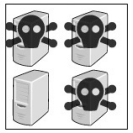


- the platform is trusted for keeping the vote secret !
  - It is the voter's responsibility to make sure that no malware observes their vote

Control Components

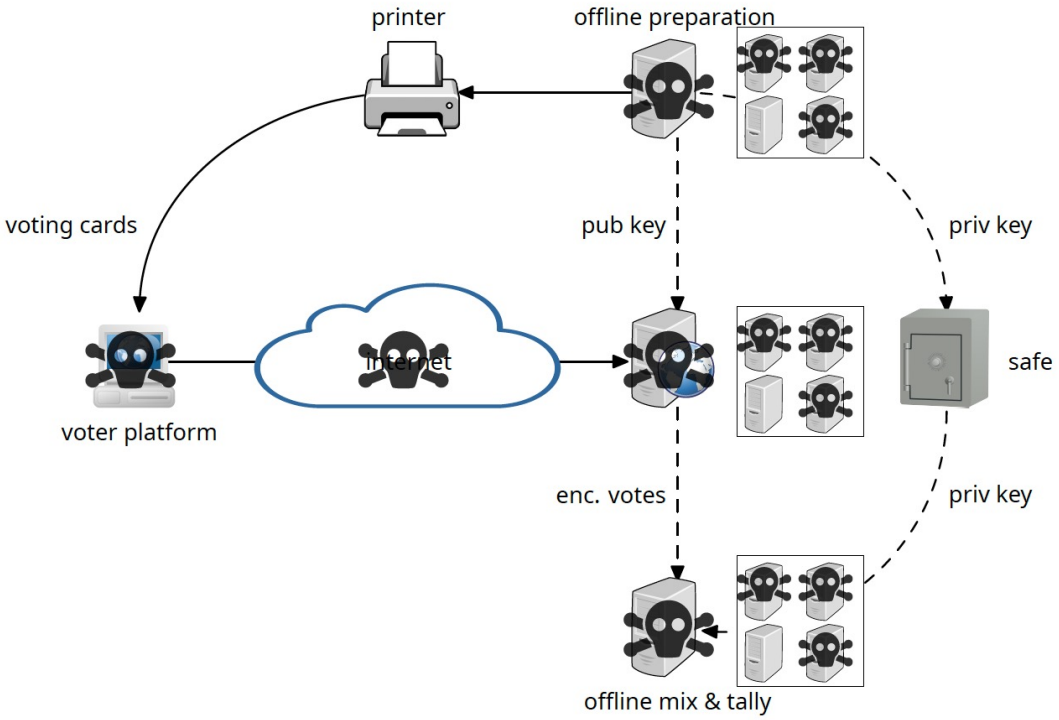
- Since the servers are not trusted, cryptographic operations are executed on specialized control components (CC) 
  - generation of keys
    - each CC generates a part of the keys
    - nobody knows the full private keys
  - mixing
    - each CC mixes and anonymizes the votes
  - decryption
    - each CC participates to the decryption
  - they log all of these operations
- there are four CCs: 

Control Components Trust model

- We trust that at least 1 in four CC operates correctly 
- The cypto protocol is built such that, as long as one CC operates correctly, any manipulation can be prevented or detected
- To justify the trust into the CCs (or at least in one of them), they are highly secured and diverse:
  - different machines
  - different operating systems
  - different teams
  - different code?

Trust model: complete picture

- The platform is not trusted
- The servers are not trusted
- Only 1 in 4 CCs is trusted
- The protocol must still guarantee vote correctness, secrecy and no provisional results
  - keys are generated by the CCs
  - return codes are calculated by CCs
  - mixing and decryption is done by CCs



- the platform is still trusted for keeping the vote secret !

Internet Voting - Conclusion

- The “perfect” system is still missing
- Open problems
  - Secure platform
  - Vote buying and coercion
  - Long-time privacy
  - Usability of complex cryptography
- Many cryptographers are against Internet voting

References

- Epp Maaten. Towards remote e-voting: Estonian case. In Electronic Voting in Europe - Technology, Law, Politics and Society, 2004
- Rolf Haenni. Privacy and Integrity in Internet Voting. March, 2012
- Jeremy Epstein. Internet Voting, Security, and Privacy. William & Mary Bill of Rights Journal, 2011
- S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security, July 2009
- Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A practical secret voting scheme for large scale elections. In Advances in Cryptology AUSCRYPT ’92, 1992
- Tatsuaki Okamoto. An electronic voting scheme. In *Proc. IFIP World Conference on IT Tools*, pages 21–30, 1996
- Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *Proc. Information Security and Cryptology*, 2004