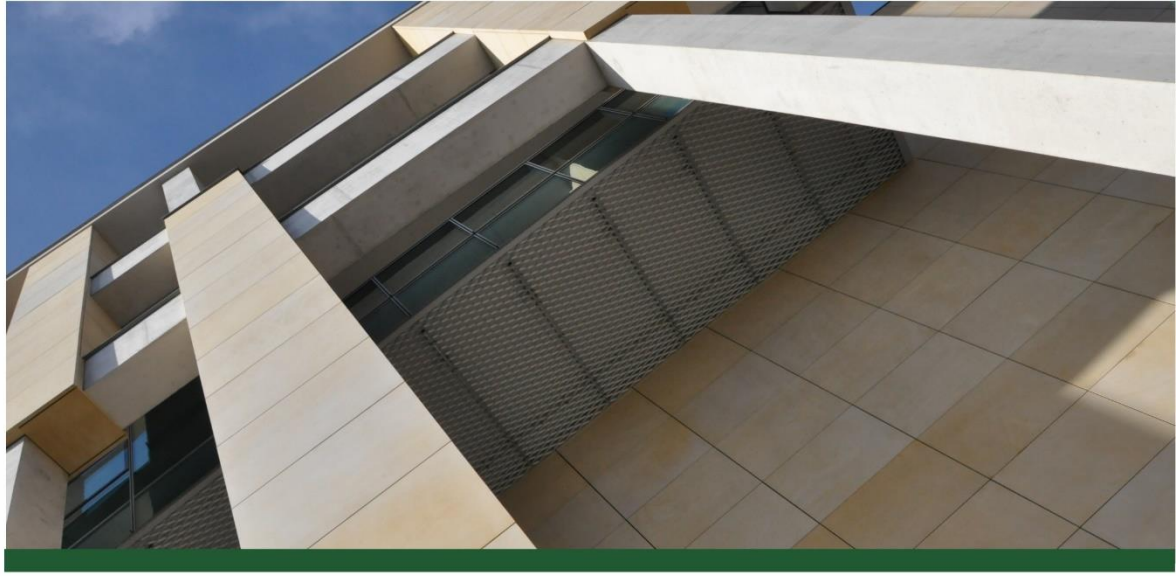

POZNAŃ UNIVERSITY OF ECONOMICS AND BUSINESS

Should We Deploy Electronic Remote Voting Systems Now?

Adam Wójtowicz

Department of Information Technology

Poznań University of Economics and Business

III INTERNATIONAL CONFERENCE

CHALLENGES AND REALITY OF THE IT-SPACE: SOFTWARE ENGINEERING AND CYBERSECURITY

Electronic remote voting

- Voting **online** via **electronic means**
- Using **user devices**, **internet** connections and **dedicated systems** collecting and counting votes
  - instead of traditional procedures and infrastructure: physical presence, paper ballots, booths and ballot boxes.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Motivation

- **Debate** regarding the migration from on-site voting towards remote voting via electronic means.
- Under peacetime circumstances:
  - next phase in the development of **electronic government services**
  - motivated by the convenience of the voters, cost and time reduction, possibly higher turnout.
- Under wartime circumstances:
  - stronger motivations: enabler of voting in the areas where traditional voting cannot be safely conducted at all.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Security requirements for remote voting system

- However, **security** is a key requirement
- **Security requirement** has a number of different, to some extent **contradictory**, attributes:
  - authenticity (SR1),
  - correctness (SR2),
  - anonymity (SR3),
  - verifiability (SR4),
  - receipt-freeness (SR5),
  - availability (SR6),
- …which are **vulnerable to various security risks**.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(SR1) Authenticity of votes cast

- System ensures that **only registered voters can vote – each voter once**
- Some systems allow multiple votes and include only the last vote of a given voter in the results
  - to make it difficult to force a specific vote by the physical presence of an attacker
  - voter can vote again without the knowledge of the attacker, thus invalidating the previous, forced vote.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(SR2) Correctness of set of votes cast

- System **prevents modification, replacement, removal and addition ("stuffing") of votes**
- Before, during and after the voting period
- It should be impossible:
  - to carry out such attacks **from the outside**,
  - **for the voting operator or system administrator**, even if they have full access to all system modules and the data stored in them.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(SR3) Anonymity of voters

- Voter's **identity** or other identifying data cannot be **linked** at any stage of the process to the **choice made** in the vote cast.
- Link cannot be made
  - by **external attacker**,
  - by **voting operator** with full access to all modules of the system.
- Anonymity of voters must be maintained
  - in the system itself,
  - in the communication channels.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(SR4) Verifiability of voting results

- System enables **cryptographic verification** by an external party, e.g. voter (not only the voting operator)…
- …whether the vote of a given voter was
  - **registered** in the system,
  - correctly **counted**: included in published results.
- It should also be possible to **globally verify** (audit) the correctness of the system operation and the results
  - compliance with SR1 and SR2

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(SR5) Receipt-freeness

- System **does not provide voters with cryptographic receipts of vote cast containing the choice**,
  - e.g. in order to provide SR4.
- Otherwise, it would enable conducting **vote selling or coercion**
- Receipt would provide vote buyer with certainty that voter actually cast a vote in accordance with buyer's intention.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(SR6) Availability and verifiability of voting system

- System is **accessible to voters** during the voting period
  - it is resistant to various types of failures and DoS attacks
- Also the **authenticity of the system is verifiable by voters**
  - in order to minimize the risk of substitution of a false system for voters, e.g. by phishing.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

"if we make online money transfers securely, why can't we vote online?"

- In online banking: **no SR3, SR4, SR5**
- Also some errors are reversible
- Security achievements of electronic banking apply to the field of e-voting only to a limited extent

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Naive approach

- **Secret voting in an ordinary IT system: would not meet at least SR2**
  - voting operator or system administrator could freely modify the voting results…
  - …without any reliable trace, there would be no possibility of "recounting the votes".
  - even if the announced voting result is correct, the loser has no reason to believe it.
  - such systems are offered on the market and are advertised as "secure".
- Other unacceptable approach: public voting systems, where open votes are registered in public registers: maintain SR2, violate SR3.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Cryptography-based voting systems

- **Protocols and systems that combine somewhat contradictory**: SR2 and SR3, or SR4 and SR5,
- based on cryptographic formalisms
  - e.g., homomorphic encryption (HE), zero-knowledge proofs (ZKP), or mix networks
- in line with the E2E verifiability

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Cryptography-based voting systems

- Systems (such as Helios Voting) ensure that:
  - vote is **cast** in accordance with the intention of the anonymous voter,
  - **collected** by the system in accordance with how it was cast,
  - **counted** in accordance with how it was collected.
- There are **no trusted parties**
  - each of the parties in the process (voter, voting operator, server administrator, software provider/sub-provider, hardware provider) can be the source of an attack
- In the case of servers, this property is achieved by distributing them among independent entities.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Cryptography-based voting systems

- **Cryptographic verification** of published results:
  - voter can verify whether his vote was included in the results without revealing it
  - anyone can verify the total of counted votes without knowing who voted how

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Cryptography-based voting systems

• Code implementing cryptographic operations is **open source**,

  – its quality and security can be **externally assessed**.

• Significant part of the code – e.g., encrypting the vote - is executed on **client side**, i.e. on device under voter's control.

• Voter knows what code is actually used in the process and can theoretically verify its correctness or choose an alternative implementation.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Cryptography-based voting systems

- Consistency with the ***open design*** principle
  - security of a solution **cannot depend on the secrecy of its design or implementation**.
  - secrecy of the design or implementation ("security by obscurity") introduces a false sense of security (easy to breach) and impedes "thousand-eye review" by cryptographers and programmers

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Challenges

- (C1) Voter inability to verify process
- (C2) Lack of trust
- (C3) Voting server vulnerabilities
- (C4) Client software vulnerabilities
- (C5) Selling votes or voting coercion

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(C1) Voter inability to verify process

- Average voter inability to consciously verify
  - **correctness of the tool** they are using,
  - **authenticity of the system**,
  - **counting of their vote** by the system,
  - or **be certain of their anonymity**.
- Regardless of whether the cryptographic tools use simple UIs or not
- HE, where it is possible to perform operations on encrypted data (e.g. adding votes) without knowing this data (who voted how) **- difficult to accept for voters without a technical education**.
  - also ZKP, where one party is able to prove to the other that they have some information, without revealing it.
- Difficulties with understanding the system's operation and verifying its correctness - at the **conceptual** level, the **implementation** level.

(C2) Lack of trust

- **Lack of trust of losing party** and neutral observers in the published results.
- **Acceptance** of the will of voters **by all parties regardless of its verdict**: foundation of democratic voting.
  - electoral process which do not inspire trust will additionally fuel social conflicts.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(C3) Voting server vulnerabilities

- **Servers** providing remote voting are **exposed to Internet traffic**,
  - **target of anonymous automated/manual attacks** from various geographical locations
  - e.g., by using 0-day malware can be loaded onto voting server.
- It is **difficult** to develop software that is **100% free of errors** at the design, implementation and deployment levels.
- For voting – ***software independence*** requirement: "undetected change or error in its software cannot cause an undetectable change or error in an election outcome".
- Servers can also become the target of network attacks or spoofing attempts, e.g. MitM or DDoS attacks.
  - DDoS can be carried out not only against the entire system, but also against selected voters or voting groups.
- **C3 challenge concerns: SR1, SR2, SR6**

(C4) Client software vulnerabilities

- **Security of client terminals**, i.e. devices and systems used by voters.
- May be under **control of a third party** or **infected with malware**.
- Security assurance of devices at the disposal of end users **is difficult, if not impossible, to 100% implement in practice**.
- Malware (e.g. MitB) can modify the vote without the user's knowledge - already on the user's device, before it is sent to the secure system.
- Similarly, feedback provided to the user by the system can be modified by malware on the client device just before it is displayed, keeping the user in the false belief – e.g. that he cast a valid vote.
- Attacker can obtain paid access to ready-made attack tools in the as-a-service model (darknet).

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(C5) Selling votes or voting coercion

- Possible on larger scale due to **cryptographic receipts** of cast votes
  - **if receipts contain information about the choice made**
  - these can be **requested by buyer**, voter cannot secretly vote against the will of the buyer
  - can be used also in **coercion** attacks
- These risks can be reduced by receipt-free systems (SR5)
  - makes system more difficult to secure against C1 and C2.
- Another approach: to guarantee cryptographic ***plausible deniability***
  - providing voter with **alternative receipts** that they can present to party buying votes, who can then verify them

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

(C5) Selling votes or voting coercion

• Party buying votes can obtain **access to the entire client software for the entire voting period** (including authenticators),

- buying the ability to remotely **impersonate** the voter's identity,
- eliminates the need to provide receipts of the vote cast,
- risk could be reduced by using biometrics, but it decrease the level of voter anonymity and create other technical and organizational problems.

• Coercion can also be done simply by **physical presence** of the coercer near the voter during the voting (smaller scale)

- risk can be reduced by **enabling multiple voting** and counting only the last vote cast,
- voter can vote again later without the coercer and invalidate the previous vote.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Do not fix it if it works

- In traditional procedures, **level of risks is lower**.
- Voting and counting takes place in a space controlled by representatives of different candidates or supporters of different positions and neutral observers.
- They do not trust each other and control the electoral process and each other.
- At the same time, in this public space, it is possible to designate private areas (booths) where the voter marks a secret choice on the ballot paper.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Do not fix it if it works

- Anonymity of voting is also ensured by separating the process of issuing cards preceded by identity verification from the process of making a choice on the card and putting the card in the ballot box.
- No official receipts of the choice made are issued, so the procedure of selling votes is difficult.
- The entire process is understandable to all members of the commission, as well as to individual voters.
- In the event of suspicions of irregularities or protests, it is possible to recount the votes cast on paper, which are safely stored (also understandable procedure).

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Impact

- Impact factor: determines here difference in risks
- Successful attack on the e-voting system (from outside or inside) will most often **allow for a difficult to detect and decisive influence on the final result of the voting**
- Successful attack on traditional scheme usually will result in the falsification (e.g. invalidation) of **small percentage of votes**
  - e.g. single committee member not effectively checked by the others.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Probability

- Estimating the probability of an incident is more difficult,
- Factors that can increase the probability of a successful attack in the remote model:
  - infrastructure is open to anonymous automated attacks from all over the world,
  - it is difficult to guarantee the absence of software vulnerabilities,
  - it is easier to trade votes than the traditional model.
- The traditional model is disadvantaged by the need of advanced IT expertise required to carry out an attack.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Hybrid approaches

• Hybrid approaches: **local voting using electronic devices maintained by the voting operator and paper cards at the same time**.

• If they are based on proven protocols, they reduce the level of certain risks, ensuring better verifiability and audit.

• But they do not eliminate all risks (DoS),

• They add new problems (failure rate, costs),

• They do not increase voter convenience – voters still have to physically go to a specific room where cards are issued and voting takes place.

• If the machines for on-site electronic voting are not based on proven protocols, the list of risks is even longer (problems with trust in devices, hacking into the system, internal attacks).

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Blockchain?

- Blockchain technology: **insufficient to secure remote voting**
- **It does not solve any of the security problems**
  - voters still dependent on untrusted end devices
  - network infrastructure still susceptible to attacks and failures
  - could be used as a trusted results board, but even here the technologies used so far are more suitable.
  - blockchain consensus by blockchain nodes or "voting" on the results of smart contracts – do not apply to voting SRs
- **It introduces new problems related to complexity of decentralized systems maintained by many parties**
  - protocol updates, patching security holes require more resources and time, which can be critical

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Conclusions

- Mere fact that solution is surrounded by **aura of "technology"**
  - **does not mean that this solution is more secure than the one used so far**
- Using Internet voting with proven cryptographic solutions **within organizations** could be good idea in some cases
  - where the weight of decisions is low,
  - voters understand how the protocol works,
  - they do not have a strong motivation to force others to vote in a specific way,
  - they maintain above-average awareness of security rules,
  - risk of an external attack is low.

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Conclusions

- **Authorities are unanimous in skepticism about the application of online voting where vote buying or coercion may occur**
  - until we develop better solutions, which does not seem likely at the moment
- Consensus of American cybersecurity specialists should cool the enthusiasm for ill-considered deployments

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en

Thank you

Al. Niepodległości 10
61-875 Poznań, Poland
phone +48 61 856 90 00
www.ue.poznan.pl/en