Trusted3Ballot: Improving Security and Usability of ThreeBallot Voting System using Trusted Computing

Yusuf Uzunay
Informatics Institute
Middle East Technical University
Ankara, 06800, TURKEY
yuzunay@gmail.com

Kemal Bicakci
Department of Computer Engineering
TOBB University of Economics and Technology
Ankara, 06560, TURKEY
bicakci@etu.edu.tr

Abstract—The main goal in the design of ThreeBallot system was to provide an end-to-end auditable voting system in a simple way without use of cryptography to bolster voter confidence in the system. However, later it was shown that this system has significant security and usability problems. To solve these problems, in this work we propose Trusted3Ballot; an electronic ThreeBallot based voting system which uses trusted computing technology. One notable feature of the proposed system is the use of TPM remote attestation property to address a number of trust and security problems. The analysis of our proposal reveals that significant improvements to the ThreeBallot system are provided in terms of both security and usability.

Keywords—trusted computing; e-voting; ThreeBallot; TPM;

I. INTRODUCTION

E-voting is deemed as the technological opportunity to reduce vote counting time, provide evidence that a vote has been correctly accounted, reduce fraud, remove errors in filling out ballots and improve system usability especially for people with special needs [1,2]. However, it also poses several serious security concerns [1]. Beside many and sometimes conflicting technical requirements, social concerns like citizens' trust on e-voting systems emerge as a critical factor that acts as a barrier preventing these systems being widely deployed and used.

ThreeBallot voting system was proposed by Rivest [3, 4] as a paper-based voting system which improves standard ballot based voting by adding several important functionalities (e.g., providing individual and universal verifiability) without using cryptography. In ThreeBallot voting, each voter gets a “receipt” that she can take home to be used later to verify that her vote is actually included in the final tally. The voter is also able to check all the ballots in a bulletin board and verify the tally results. However, voter’s receipt does not allow her to prove to anyone how she has voted. By this way, vote trade is not of concern.

To provide the security properties of ThreeBallot, more advanced protocols based on cryptography can also be designed [5-13]. However, ThreeBallot has the virtue of not depending on the use of cryptography [3, 4].

On the other hand, ThreeBallot suffers from the following issues: (1) ThreeBallot puts an extra burden on user to understand and use the system in the right way when compared to the conventional voting systems [14]. (2) ThreeBallot has been subject to a number of attacks (see Section 3).

In this paper, we propose Trusted3Ballot, an electronic e-voting system based on ThreeBallot voting system and trusted computing technology. In our proposed system, we implement a trusted electronic system to mitigate usability issues with paper based ThreeBallot system. Our proposal addresses not only the voting step but all the components of the voting system. By adopting a systems view, our work provides a secure and trusted environment for each step of an election using trusted computing. The software used in Trusted3Ballot is open-source and publicly available. Anyone can inspect the source code before the election and carry out remote attestation to understand whether the software used is the one already inspected. The steps of the election is transparently designed enabling different entities to take part and contribute.

We note that our work is on electronic on site voting and does not address remote voting. The rest of the paper is organized as follows. Section 2 provides more information on paper based ThreeBallot voting system. Section 3 overviews its security weaknesses. Section 4 gives brief information on trusted computing with an emphasis on TPM and its core functionalities used in our work. Related work is examined in Section 5. We describe our proposed system, Trusted3Ballot in detail in Section 6. The prototype implementation is introduced in Section 7. Section 8 is for security and usability analysis. We sum up our paper in Section 9.

II. THREEBALLOT VOTING SYSTEM

ThreeBallot has a multi-ballot structure having three columns each of which is a complete ballot on its own (see Figure 1). Each ballot is identical except the ballot ID number printed at the bottom and uniquely identifies the ballot among its own multi-ballot and the others. In order to vote, voter randomly checks off two bubbles on the same row for the candidate she wants to vote and just one random bubble for the other candidates. Figure 1 illustrates an example for a filled ThreeBallot on which candidate 2 is selected. After marking is completed, the voter puts its multi-ballot into a checker machine which ensures the validity of the vote by checking the constraints. If the constraints hold, checker machine cuts it into three separate ballots. Voter can then cast each ballot separately. Voter can take copy of one of the ballots as receipt before the casting operation. One convenient way for the receipt operation is to do it in checker.
At the end of the Election Day, all ballots are scanned and published on a bulletin board. Scan operation is a representation of the ballot with the selected bubbles and the ballot ID. The names of the voters who participated in the election are also listed on the bulletin board.

For individual verification, each voter can look for the ballot that is identical with the receipt on bulletin board. If the voter cannot find a match, she can file a protest to the election office to declare that her vote has not been displayed in bulletin board. After checking the validity of the receipt, election office can decide to make a rescan of the cast ballots. Since each ballot is published as cleartext on bulletin board, tallying can be done by anyone by basically summing up the marks on each ballot. The only difference from the conventional one ballot system is that the total value of each candidate has been inflated by the numbers of voters. So that the real number of votes can easily be found by subtracting the number of voters from the total number of marks for that candidate. Therefore, universal verification is satisfied if the voter verifies that the total number of marks is three times the number of voters and the result of the individual tally operation is as same as the announced one on bulletin board.

III. SECURITY OF THREEBALLOT

In this section, we overview ThreeBallot's security weaknesses:

1. In three pattern attack [3, 4], the voter is asked for marking a pre-specified pattern in each of her three ballots so that attacker can check this pattern on bulletin board. If he finds a match, voter is awarded or otherwise voter might be punished.

2. The security of checker machine is crucial for the security of the whole system. If the checker machine is compromised, various attacks can be mounted [3, 4]. For example, if an adversary finds a way to eliminate the checker machines' control, he can triple the number of votes he has given to his favorite candidate as each voter can cast three ballots. It is very difficult to detect this attack later as it is impossible to check the constraints once the multi ballot has been split into separate ballots. A malicious checker can also note the ballot IDs of the receipts and gives the attacker an ability to make modification on the other non-receipt ballots. Since the ballots selected as receipts are not changed, it is impossible for the voters to recognize this fraud.

3. In the "Paying for receipt" attack, adversary pays the voter to buy her receipt. After that, since the voter loses her ability to carry out individual verification, adversary can hack the bulletin board and modify the corresponding ballot. In this attack, the more receipt the adversary obtains, the more he can affect the election results. This is a complex attack as the adversary both needs to obtain a high amount of receipts and hack the bulletin board.

4. In order to start chain voting attack [15], the adversary needs to obtain an initial ballot somehow e.g., by stealing a ballot before election. After obtaining the initial ballot, the adversary marks the ballots for his candidate and hands in to a subverted voter who will then go to the polling booth, exchange the prefilled ballot with the blank ballot and return it back to the adversary. The same cycle is followed until the adversary cannot take the process further. The voters are paid if they agree to take place in the chain and follow the process.

5. Voter can memorize ballot IDs and prove to a third party how she voted. This brings the problem of vote trading.

6. After the approval of the checker machine, voter can make modification on the ballots such as marking extra bubbles on the ballots before she casts them into the ballot box. Since constraints cannot be checked once the checker machine approves the ballot, it will not be possible to detect the modification.

7. In ThreeBallot, Rivest makes Short Ballot Assumption which means that there are many voters in an election than the ways to fill out an individual ballot [3, 4]. However, if this assumption does not hold, then reconstruction attack can be of concern. Strauss showed through simulations [16] that the three ballots of the voter can be reconstructed by using her receipt and the ballots published in bulletin board. This is basically done by comparing the receipt with every possible pair ballots on the bulletin board. At the end, the attacker expects to find two other ballots that can form a unique three ballot with the receipt. If the ballot is lengthy, then the number of possible patterns may be more than the number of voters, which increases the probability of having a unique three ballot pattern.

IV. TRUSTED COMPUTING

Trusted Platform Module (TPM), the core component of Trusted Computing [17], is a chip attached directly to the motherboard of the computer. It has cryptographic capabilities such as RSA key generation, encryption, signing and verification, secure random number generation and SHA1 hashing. TPM has special registers called PCR (Platform Configuration Registers) which are used to store 160 bit SHA1 hash values. PCRs cannot be directly written. Instead, they are extended. "TPM Extend" is a special operation which calculates the new value of the PCR by hashing the concatenation of the old value and a new SHA1 hash value.

One of the important functionalities of TPM is remote attestation. Attestation stands for proving the trustworthy status of a machine to a third party, which means that the machine has an original and enabled TPM and the requested hash values are correctly retrieved from the PCRs of the TPM chip. Basically, an attestation request includes a nonce.
and some PCR numbers. The attested machine then performs a TPM quote operation and produces a quote as a reply. This quote includes the signed values of nonce and the contents of the requested PCRs. The attested machine also sends an untrusted event log including the hash values of each entity that forms the trust chain in the relevant PCRs. The attester can then verify the untrusted event log by computing the aggregate hashes expected to be in the PCRs and compare the final value with the one in the quote signed by TPM [18]. Sign operation is performed via the private portion of a special key, called Attestation Identity key (AIK). AIK key is certified to be generated by a legitimate TPM [19].

V. RELATED WORK

ThreeBallot system was first proposed by Rivest in 2006 [3]. The system was extended with some other paper based systems and discussions on possible problems and potential solutions [4]. Cryptographic techniques can also provide the security properties of ThreeBallot [5-13].

The problems of ThreeBallot voting has been examined in detail. Appel presents a combined attack [20]. Henry et al. provide a detailed analysis of known receipt-based attacks against ThreeBallot focusing on two-candidate races in [21]. Storer examines three pattern attack [22] and proposes a randomization device to mitigate. Strauss has pointed out usability problems and potential receipt buying attacks against ThreeBallot [23]. Strauss [16] and Jones et al. [14, 24] examine reconstruction attack and provide some empirical results that prove the effectiveness of the attack. In order to mitigate the reconstruction attack, Rivest proposes to replace the receipts [4] in a way similar to Farnel’s idea [25, 26]. i.e., each voter replaces their receipt with some other’s receipt. Rivest also presents some other mitigation techniques against reconstruction attack [4].

Araujo et al. draw attention that the receipt may expose some statistical information about the vote [27]. Some enhancements to mitigate reconstruction attack and information leakage problem has been proposed in [29]. Clark et al. examine and compare the security of ballot receipts in three end-to-end auditable voting systems Pret a Voter [6, 7], Punchscan [30, 31] and Three Ballot [3, 4] [30]. They find that Pret a Voter and Punchscan have similar security properties with respect to ballot receipts and provide no non-negligible information on the receipt itself that could compromise privacy and security. However, ThreeBallot receipts leak partial information useful for compromising voter privacy and the integrity of the tally.

A ThreeBallot based secure electronic voting system has been proposed by Costa et al. [1]. The proposed system is based on classic cryptography techniques and addresses vote receipts, voter privacy and anonymity. One important drawback of the system is that the trustworthiness and the security of the software and the keys have not been taken into account.

Smart et al. present a remote, coercion-resistant electronic voting protocol using trusted computing [32]. With the proposed protocol, system verifies the state of the voter’s (remote) machine and permits revocable anonymity. Fink et al. propose using TPMs in direct recording electronic voting machines [33]. They try to ensure election data integrity by binding voter’s choices with the presented ballot. Paul and Tenenbaum propose a simple and easy-to-understand voting system [34]. They take into consideration each step in the election process and try to strengthen the security and trustworthiness of the scheme by utilizing trusted computing technologies like we do for Trusted3Ballot. However, there are some important problems of this work; the system is open to vote trade problems as it gives a receipt to the voter which clearly shows the selected candidate. The work also does not support universal verifiability.

VI. PROPOSED SYSTEM

A. Voting Machine

Voting machine used in our proposed system is depicted in Figure 2.

![Voting Machine Diagram](image)

Figure 2. Trusted3Ballot voting machine.

It has a diskless embedded computer system with a touch screen panel. The ThreeBallot voting software is bundled in a bootable and secured operating system written on a CD. The kernel of the operating system is specifically designed to execute only the e-voting software, required modules and the relevant drivers to run DVD-ROM, optical storage (DVD RW) and printer. Other software are eliminated in order to keep the system as minimal as possible for security reasons. During the election period, the boot CD is used to load the operating system and the voting software. DVD-ROM is used to load the CD including the operating system and the trusted voting software. Token Reader is used to read chips or barcodes on cards. An optical storage (DVD RW) is used to store the vote database. Vote token is a ticket including a barcode given by poll worker to the voter to let her identify herself to the system. The barcode on the token is read by the token reader.

B. Preparation Phase

The security of the voting system highly depends on the security of the software and the operating system burned into the bootable CD. Therefore we should ensure that the operating system and the voting software are trusted and establish their integrity till the end of the election. With this goal in mind, similar to the steps in the work by Paul and Tanenbaum [34], we propose the following steps for preparation (we note that unlike original ThreeBallot system, we use cryptography for the security of preparation but these cryptographic operations are simple and standardized unlike other crypto-based e-voting systems):
(a) Preparation Meeting: For each precinct, an open meeting is organized for the CD preparation. Different actors that have critical role in the elections are invited (members from different political parties, voting registrar, police department, etc.). We assume that each actor sends at least one technical person to follow the cryptographic operations.

(b) Training: Each participant is informed about the procedures to be followed, the design of operating system kernel and the functioning of the voting software.

(c) TPM Verification: During the meeting, technical members of each participant actor verify the certificates of TPM endorsement keys produced by the vendors to ensure that each machine has an original and enabled TPM.

(d) AIK Certificate Generation: During the meeting, AIK key for each TPM is generated and the AIK certificates are created.

(e) Attestation of Key Generation Software: Key generation software is executed on a diskless PC. An attestation operation is executed via a portable device and the results are checked by all technical experts.

(f) Election Key Generation: A public and private key generation for each precinct is carried out in front of the participants and private part has been split into different parts which are then delivered to different actors.

(g) Preparation of Voting Software: The same procedures as key generation software are carried out for the Trusted3Ballot voting software and if attestation is successfully performed, the bootable CD is encrypted with the election public key and kept secure until the Election Day.

(h) Preparation of Barcode Box: Before the Election Day, election registrar prepares unique barcode ID pairs for each voter. However these pairs are not linked to a specific voter. These barcode IDs are delivered randomly to the voter during the voting process as a proof indicating that the user has cast his vote.

C. Election Day

Booting Voting Machines and Initial Attestation: In Election Day, before election starts, each holder of the election private key part comes to the polling site. We assume that heavy legal sanctions are in place for those who do not bring the part of the private key on time and try to disrupt the election. Poll workers execute a decryption software via a bootable CD after attestation of this software. The software forms the original private key by assembling each part, decrypts the voting software and writes it in a new CD. Then, poll workers boots each voting machine in the poll. After each machine has been started, attestation operation has been performed for each voting machine in front of the stakeholders.

Individual Attestation: In normal conditions, voters are not allowed to go into polling booth with a device in order to prevent any recording facility which may cause vote trading later on. However if voter informs the poll worker that she is going to use the device for the attestation purposes, a special poll worker accompanies the voter during the attestation operation. In order to perform attestation operation, attestation button is touched on the voting software. System asks the voter to input a challenge into the given input text field. Voter enters the challenge in the system, performs attestation and receives a signed result. Then she enters the received result into an application on her portable device. This can be basically done by taking photo of the screen and automatically input it into the application having OCR capabilities. The application can then verify that the attestation with the given challenge is correct and the AIK certificate is verified. We assume that voter has already loaded the correct AIK certificate published for her precinct by connecting the election web site before she comes to the polling site. We note that there is a camera on top of the voting machine recording the user activities (see figure 2) but is not able to display the screen of the voting software. After the attestation button is clicked the software can switch on a warning lamp located on the polling booth where camera can see and after the operation is finished this lamp can be switched off. By this way, the camera can follow whether the poll worker gets out of polling booth after the attestation operation. So any other process except the attestation operation cannot be done with a corrupted poll worker.

Voting Process: Voting process is depicted in Figure 3. After a security check, voters come to identification desk. Here, there are poll workers who have the list of all the voters assigned for this precinct. Poll worker requests an identity card from the voter, checks whether her identity number is in the list or not. Then, poll worker asks the voter to select one of the closed envelopes from the barcode box. Voter opens the envelope, takes out the paper including two identical barcodes. Then, she removes the first barcode which is glued to the paper and sticks it on the voting form. After that, she writes her identity number and signs it. She performs the same operation for a second voting form and gives them to the poll worker.

Poll worker also puts his signature on the forms and gives back one of them to the voter and puts the other one into a file. This form is kept as a record on both sides indicating that the voter has casted his vote and prevents anyone to cast a vote without having this uniquely prepared barcode. User enters the polling booth with this form and starts voting process by touching the vote button on the voting software. Onscreen directions tell the voter to put her barcode in the token reader. User completes the voting by following the instructions. During the voting, software holds two separate tables; one of them includes only the identity numbers and the associated barcodes. The other includes the electronic ballots. All the records are also located in random order in the table. By this way, associating the ballots with the voters.
are prevented. After finishing the voting process, voter selects one of the three ballots as the receipt and touches the print button. System prints the selected ballot as a receipt in a different paper and the other three ballots separately as the original ballots. Voter completes the voting process by casting all three ballots in the ballot box, and taking the receipt one with him.

Tabulating the Votes and Publishing Results: At the end of the voting period, poll workers enter a CD into the optical storage of voting machines and enter a special code in the software to indicate that the election is finished. The software encrypts the vote database with the election public key and writes them into the CD and also prints the total scores of the candidates in plaintext. Then, the poll workers inform the election registrar about the results by phone and take all CDs and the ballot box to the headquarters with an escort. All these facilities are carried out in front of the observers of different stakeholders. The first preliminary results obtained by phone calls are announced by the election registrar and the encrypted vote database including the ballots and the list of identity numbers and barcodes indicating who has participated the election are decrypted with the precinct’s private keys created again by assembling each part from the different part holders. The decrypted ballots are stored in a common election database and each ballot and the identity numbers are published on the election bulletin board with the results. So that each voter having a receipt can check whether her own vote has been taken into account in the election and also can perform universal verifiability. At the headquarters all the software running go through attestation process as it has happened in the poll site. We note that paper based voting forms and the electronic forms of barcodes and implemented in a way so that only seen in figure 4.

B. Usability Analysis

A. Security Analysis

Three Pattern Attack: In Trusted3Ballot system, the ballots are prefilled randomly and cannot be changed by the voter. So that it is impossible for the voter to select a pre-specified pattern in each ballot.

Security of Checker Machine: Voting machine does all the checker machine functionalities. The software of the voting machine is open source and by using TPM based remote attestation, the code can be verified by anyone (voters, observers, poll workers etc.). All the security critical software in the election process go through attestation process and the secret data are stored as encrypted. The private key used in decryption is separated into different parts and each of them are delivered to different holders. So that unless all the part holders come together and assemble the key, the decryption becomes impossible.

Paying for Receipt: The trustworthiness of bulletin board is also provided by TPM remote attestation, hence the modification of bulletin board is not possible.

Chain Voting: Paper based ballots are only used at the time of casting after electronic voting. Therefore the system does not permit to acquire an empty paper ballot to establish the chain before the voting. System also gives a specific ID for each ballot during the voting which makes it impossible to insert a paper ballot with the correct ballot ID.

Memorizing Ballot IDs: Ballot IDs are displayed in the form of barcodes and implemented in a way so that only seen after printing the receipt.

Modification of the Ballot: Since both electronic and paper based ballots are used, any modification on the paper ballot can easily be detected.

Reconstruction Attack: This is the only attack the design of Trusted3Ballot does not directly address. On the other hand, for this attack, our proposal can be extended with mitigation methods proposed by Rivest [4].

B. Usability Analysis

Usability improvements of Trusted3ballot can be listed as follows:

1. Trusted3Ballot displays randomly pre-filled ballots. Therefore voters do not need to mark 4 bubbles for a 3 candidate election. She only marks one bubble as in a standard voting.
2. In order to prevent confusion, pre-filled bubbles are marked as red and the bubble voted by voter is marked green.
3. Three ballot constraints have been embedded in the system. Voters cannot change prefilled bubbles and cannot mark more than one bubble. When she tries to mark another bubble, previously marked bubble returns to unmarked.
4. There is an information screen at
top of the window in order to show the voted candidate. (5) There is also a one ballot interface for the voters who have difficulty in voting with three ballots. (6) The system can be easily supported by audio and video technologies to aid people with disabilities.

IX. CONCLUSION

In this paper, we revisit ThreeBallot voting system and by taking into account each step of an election we propose an electronic on site voting system called Trusted3Ballot. Integrating ThreeBallot into an electronic voting system secured by trusted computing gives everyone the ability to attest the voting software. Our prototype implementation shows how various security and usability problems of original ThreeBallot system could be solved in the proposed approach. Some recent incidents fueled doubts about the security of e-voting systems and raised concerns about voter confidence. We believe confidence in electronic voting systems could be regained (i) by incorporating human verifiable paper ballots into the system, (ii) with a simple and easy-to-understand operation, (iii) by use of trusted open-source software, (iv) by providing extra functionalities (such as individual and universal verifiability) absent in traditional paper based voting. Trusted3Ballot system is proposed to achieve these fundamental objectives.

REFERENCES