Security Analysis on an Elementary E-Voting System

Xiangdong Li,

Computer Systems Technology, NYC College of Technology, CUNY, Brooklyn, New York, USA

Summary
E-voting using RFID has many advantages over the current voting systems, like a paper ballot. It separates the ballots from the voting software and hardware, thus making the voting system verifiable the re-count easy. In this paper we analyze the procedure of an elementary e-voting system using RFID technology, which we proposed early, and its security issues are discussed.

Key words:
E-Voting, RFID, Security.

1. Introduction

Radio Frequency Identification (RFID) technology is becoming pervasive in our daily life. It is commonly used in the manufacturing, supply chain management, inventory control, highway toll, also in the customer/object identification fields, such as the credit cards and passport systems. Optical barcodes for commercial products are used dominantly, but the low-cost RFID systems are made using the advanced silicon industry technology, we will see more and more RFID technology applications.
This paper discusses the security issues based on the framework of an elementary electronic voting protocol using RFID, which we proposed in [1]. Here we briefly describe the protocol of the voting system.

1.1 Assumptions and requirements

The basic working prototype applies an inexpensive RFID-tag (several Kbytes) ballot in the remote voting which replaces problematic absentee ballots as suggested. The required changes to the election law discussed in [2] may be minimal, so electronic voting technology could be deployed easily. Four idealized assumptions are suggested in the elementary electronic voting protocol [1]:

- An electronic storage medium capable of reading and writing is available;
- Reliable software capable of reading and/or writing to the media or public bulletin board is available.
- A poll station, i.e. completely contained inside a building, and all entrances and exits are watched, is available.
- Voters are capable of using computer equipments or its assistances.

The voting system and procedure using RFID should satisfy five requirements, described in [3, 4]:

- Correctness: Votes are counted and tallied correctly.
- Privacy (Anonymity): No way to trace a voter from his/her vote.
- Receipt-freeness: Voters have no evidence to show others what they vote.
- Verifiability: Votes are double-checked during their voting. Specifically, it requires (individual) voter verification and universal (precinct, federal, and any individual) verification.
- Robustness: The voting system can withstand some technical failures.

This e-voting system reconciles verification and receipt-freeness with an asymmetric homomorphic encryption scheme [5] and a bulletin board [6] vote posting system as in [7].
The e-voting system publishes all (encrypted) votes and the "receipt" numbers associated to the votes on the Internet, the voters can verify whether their votes have been casted. But a "receipt" number may not be associated with an actual ballot (the two must be published separately in time and visual space). The protocols in [7, 8] allows the write-ins, the voting system in [1] utilizes the aggregate counting techniques typical of homomorphic encryption schemes to avoid write-in ballot coercion issues.

1.2 Hardware Equipments

Several specifications of the e-voting using RFID are described in [1]:

- Physical Ballot, an active RFID tag, which can be read and written with encryption keys to be locked/unlocked. Such a ballot contains an encrypted GUID (global unique ID). Each voter is given a ballot randomly before he starts to vote.
- Verifier, a device which can display the contents of a Physical Ballot.
- Voting Device, a device which can read from and write to a Physical Ballot. It connects to the

Manuscript received October 5, 2010
Manuscript revised October 20, 2010

database server and sends the voting content and the ballot information to the server.

- Ballot Box, a radio-shielded receptacle to store and protect the Physical Ballot after they have been casted, keeps "locked" until the tally process begins.
- Public Bulletin Board, a distributed and load-balanced, to display the result of the Ballots during the tallying process.
- Centralized database to store information about valid Physical Ballot.
- Poll workers validate Physical Ballots using the encryption key for voters to use.
- Eraser, placed at all the entrances or exits of the poll station, to detect and erase the Physical Ballots which are brought in or away.

We assume that we trust the software which has been tested and verified without any security issues, and we try to isolate any issue inherent from this architecture. The hardware and software setup is contingent on the election law. During the voting process, the voters are able to assure that their votes are counted correctly and casted anonymously.

1.3 Voting, Tallying and Verification Procedure

The voting, tallying, and verification procedure is described in [1]:
Preparation: The poll workers have done the physical preparation before the voting starts, such as the equipment set-up, public and private keys for asymmetric homomorphic encryption scheme (not specified in this architecture) are available; after the private keys are randomly placed on Voting Devices and Verifiers (e.g. smart card or the like), they are deleted from the generating system and the smart cards are collected and locked for the remainder of the voting; poll workers use the public key to validate the Physical Ballots (unlock them) and a Physical Ballot is handled to each registered voter.

Voting:

- A voter is verified as a registered voter by poll workers and given a randomly selected, validated, unlocked Physical Ballot.
- In the voting booth, the voter can verify the Physical Ballot by using the Verifier.
- The Voting Device also verifies the Physical Ballot if it is unused and valid before the voting. After the voter casts his vote, the Voting Device writes encrypted ballot to Database server and "locks" the Physical Ballot. The Database server locks that Physical Ballot's GUID from its database, decrypts the vote and sends the update result to the bulletin board at a given period of time.
- The voter drops the Physical Ballot into the Ballot Box before he/she leaves the voting booth.

Tallying, verification, and re-count
At the end of election, the poll workers use the smart card which contains the private key to decrypt the ballots. All ballots have been collected and combined into one value on the Bulletin Board, the sum of the votes will be displayed, but individual vote remains unseen. The poll workers verify the number of the ballots casted and the number received from the Bulletin Board, these two numbers should match up. For the case of the re-count, poll workers need to check the vote on each Physical Ballot and compare the result received by the Database server and the results displayed on the Bulletin Board.
In this paper we do not consider the security issues arisen from the encryption or decryption protocols. The voting is shown in Fig. 1 [1].

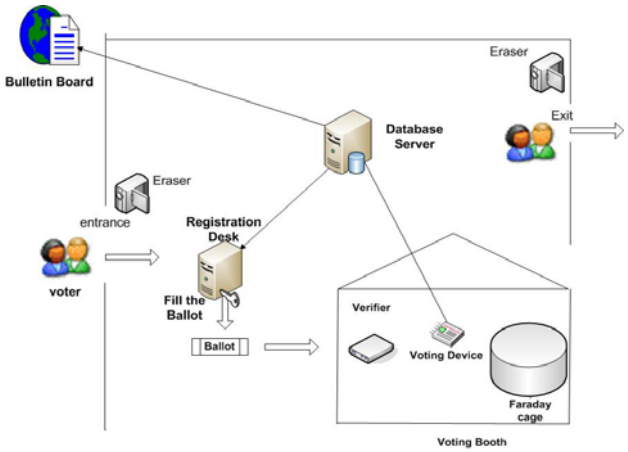

Fig. 1. Voting Process

2. Security analysis

2.1 Security on Requirement

We analyze how strong the e-voting system satisfies the five requirements (in the section 1.1) in reality.

- Correctness:

Votes are counted and tallied correctly Each vote can be only casted, counted and tallied once. The Physical Ballot is locked by the Voting Device after the voter casts it. There are four security concerns we need to address. – We are supposed to trust the election registration system that no one can register twice or more. – The Eraser is supposed to detect any fake RFIDs which is brought by a

voter to the voting. However, if the RFID is put in a metal Faraday cage (which could be with a small size) brought in the poll station, the eraser is not able to detect it. Should an x-ray machine is used for the scan like the airport entrance exam? If such, the election law would be involved. – There will be two levels to lock the Physical Ballot after it is casted in the proposed voting protocol: It is locked by Voting Device and the database server. The design of the Physical Ballot is shown in Fig. 2. The GUID (Global unique ID) is a several K-byte part in the ballot. The private/public key can unlock/ lock it. Even a voter finds out the key which can be used to unlock the ballot to do the double votes on the Voting Device, but the Database server cannot allow this to be happened since after the a ballot is casted, its GUID is locked in the Database server. (The GUID should be a number built in the tag, the same as the MAC address built on the NIC). If it sees a ballot tries to be casted twice, the server should give an alarm. – A ballot should be dropped in the Ballot Box after it is casted in order for the re-count. The same issue exists here if a voter brings away his/her ballot, the Easer should detect it. If not, it causes problem for re-count. All voters should know that if their ballots missing in the Ballot Box, their votes will be invalid and be removed from the final voting result at the end of election.

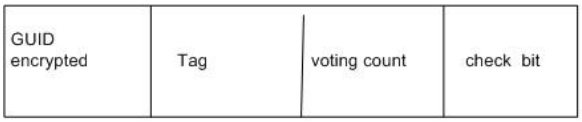

Fig. 2. Physical Ballot
GUID: Each ballot is assigned a unique ID. This GUID is registered in the Database server.

- Privacy:

An individual voter cannot be determined from his/her vote. There should be no relation between the voter and the assigned Physical Ballot, which is randomly distributed to the voters. Two ways can be used to trace a voter: one is to write down the number of the Physical Ballot for a voter, one is to check the timestamps of the voting and the result displayed on the Bulletin Board. However, they can be easily avoided. First, when a voter walks in the poll station, the poll workers check his/her registration and give him/her a Physical Ballot randomly. The poll workers are forbidden to write any number of the Physical Ballot. Next, the Bulletin Board should be updated with the new result at regular time intervals. One minor security issue is that the design of the Voting Device keeps a record of the voting with the Physical Ballot.

- Receipt-freeness:

A voter has no evidence to show others what they vote. When a voter finishes his voting, his Physical Ballot should be left in a Faraday cage before he leaves the voting room. It is not proper to give the ballot to a poll worker since the voter's record (even encrypted) would be traced. The voters should be notified that they should not take their Physical Ballots away after their voting, the missing Physical Ballots will cause their votes denied and not counted. (Even their voting is collected by the bulletin board, but it will be modified at the end of the election.) Clarification in the tallying process is needed to account for this situation – depending on election laws, if write-ins are allowed, then a random write-in string, an RFID reader and the now-public private keys allow a stolen PB to become a true receipt after the election is complete. Therefore, a conscious or unconscious attempt to keep a receipt is foiled. A minor issue is that a voter is not allowed to bring any device which can record the process or result of his voting, as a cell phone, camera, etc.

- **Verifiability:**

A voter has a way to verify his/her vote casted, and the re-count can be conducted easily and correctly.

Before the voting, a voter is able to check his/her ballot by the verifier to confirm the ballot is valid. The content of the vote is verified during the voting process on the Voting Device. The sum of votes can be verified by checking the content of each ballot at the end of the election. The total number of valid Ballot casted should match the total votes displayed on the Bulletin Board. Otherwise, some voters attempted to walk away with their cards; then the poll workers have to manually compare the ballots casted, those recorded by the Database server, and those left in the Faraday cage. For this situation, if the Physical Ballots have been casted and recorded by Database server, but missed in the Faraday cage, those votes should be treated as invalid and the result on the Bulletin needs to be modified. One feature of this voting protocol is that a piece of paper with a unique number is printed for each vote by the Voting Device after he/she casts the vote. This number has no relation with the content of the vote; it is only used to prove this vote is casted without showing any other information, such as the ballot number and the voter information. The voter then can check whether his/her vote has been casted from the internet.

- **Robustness:**

Several minor system problems should not shut down the election.

The common problems are from the hardware and software. – The private and public key could not be generated. The poll station needs several backup key generators. – The voting device/verifier could not work. Several back up devices are needed. – Physical Ballots are broken before or during the voting. If someone casts his vote, but he claims his ballot is damaged and asks for another vote with a new ballot, the poll workers need to check from the database server to find whether this damaged ballot has been casted. – Database server is down. An additional backup server is needed. – Public bulletin is down. The mechanic workers are needed to maintain the whole system.

2.2 Other Security Concerns

One major concern is that an attacker could bring a RFID writer in the poll station. This RFID writer can be with a small size and carried in the pocket. It can write content on the blank RFID tags. Today, this kind of RFID writer can be powered with batteries. When the attacker walks in the poll station, his writer is power off and the Eraser is not able to detect it. After he enters in, then he switches his writer on, which able to write content to the RFID of the ballots. So we need additional requirement for verifier and voting device that a ballot is valid only it is blank. If such saturation happens, the attack could get the election into a mess. To avoid this to happen, we may need a powerful detector for those metal devices, or to detect any un-recognized frequency within the poll station.

From the outside, near the poll station, any powerful radio frequencies could interfere with the RFID used in the poll station. The poll station should locate in an open place where the environment is not complicated. If any radio frequency found during the Election Day, it is easy to find the source of that signal.

A voter may drop a RF transmitting device into the Faraday cage (the Box used for the Ballots after their cast) to blank all the ballots in the box (used for recount). To avoid this to happen, the sealed Faraday cage may be matched by a poll worker.

3. Conclusion

In this paper, we analyze the security issue of a framework of hybrid e-voting system based on standard hardware and software using RFID technology as e-ballot, which was proposed early. We discuss the security concerns on the five requirement and possible attacks. This e-voting using RFID could be applied for the remote voting, since the result can be transmitted through the internet and collected/counted by the database server. The system of elementary voting protocol could be considered as an alternative physical implementation only needs minor modification.

Acknowledgments

Many thanks to M. Carlisle, A.C. Kwan, L. Leung, A. Enemuo and M. Anshel on our framework of hybrid e-voting system based on standard hardware and software using RFID technology as e-ballot. Special thanks to Mr. Kwan, who was the most diligent graduate student I have met.

This work was partially supported by PSC-CUNY grant 2009.

Reference

[1] X. Li, M. Carlisle, A.C. Kwan, L. Leung, A. Enemuo and M. Anshel, “An Elementary Electronic Voting Protocol Using RFID”, Proc of 2007 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, 20-22 June 2007.

[2] R. Benbunan-Fich and C. Springstead, “From levers to clicks: A voting technology decision,” Case Research Journal, vol. 23 (1), pp. 87-108, Winter 2003.

[3] T. Okamoto, and K. Suzuki, and Y. Tokunaga, “Quantum Voting Cryptosystems (Invited Lecture)”, DIMACS Workshop on Electronic Voting -- Theory and Practice, 2004.

[4] A. Kwan and M. Carlisle, “Privacy-preserving RFID-based Protocol for Electronic Voting”, Technical Report, November 2004.

[5] R. Cramer, R. Gennero, and B. Schoenmakers, “A secure and optimally efficient multi-party election scheme,” Eurocrypt’96, LNCS 1070, pp. 72-83, Springer-Verlag, 1997.

[6] D. Chaum, “Secret-ballot receipts: true voter-verifiable elections,” IEEE Security and Privacy 2(1), pp. 38-47, 2004.

[7] A. Acquisti, “Receipt-free Homomorphic Elections and Write-in Ballots,”Technical Report 2004/105, IACR, May 2004.

[8] A. Kiayas and M. Yung, “The vector-ballot E-voting Approach”, Financial Cryptography 2004, LNCS 2110, pp. 72-89, Springer, 2004.

Xiangdong Li received M.S. in Computer Information Science from CUNY Brooklyn College in 1997, and Ph.D. in physics from the CUNY Graduate School in 2000. Professor Li has five years working experience in the IT industry. He is an associate professor at the Department of Computer Systems Technology in New York City College of Technology, CUNY. He is a faculty member of both Ph.D. programs in Computer Science and Physics at the CUNY Graduate School. His research fields include information security, quantum information and nuclear physics. Professor Li is a member of APS.