Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 14-17

http://www.krishisanskriti.org/acsit.html

Computer Science and Information Technology E-NOTE with Public Key Kerberos: An E-Voting Protocol

Alka Swami[1] and Sarvesh Tanwar[2]

[1]Student, Mody University of Science and Technology, Sikar
[2]Mody University of Science and Technology, Sikar
E-mail: [1]swami.alka212@gmail.com, [2]s.tanwar1521@gmail.com

Abstract—*Electronic voting includes both electronic means of casting the vote and electronic means of counting the votes. In the paper we implemented a protocol for e-voting using E-NOTE (Enhanced Name and Voter Separated E-voting), where candidate's and the voter's choice are kept separately, technique with public key Kerberos. Public key Kerberos is another form of traditional Kerberos that uses public key cryptography. In proposed protocol responsibilities are distributed to four voting authorities that are Key Distribution Authority (KDC), Election Committee (EC), Ballot Distribution Centre (BDC) and Vote counting Committee (VCC). We also used Blind Signature technique in the protocol. It is a form of digital signature in which the content of a message is blinded before it is signed. The proposed protocol address the issues related to voter authentication, voter uniqueness and confidentiality, vote confidentiality, voting accuracy and receipt freeness and fraud detection.*

Keywords: *Confidentiality, voting accuracy, public key Kerberos.*

1. INTRODUCTION

Electronic voting reduces the time and efforts of voting authorities, but it should maintain the voting security and accuracy. To address a fair voting along with the issued like voting security, confidentiality, accuracy etc. we proposed a protocol for electronic voting and implemented it. E-NOTE used in the protocol refers Enhanced Name and Voter Separated E-Voting [1]. In E-NOTE ballots contains two fields one is type of ballot and second is list of candidates. Each type of ballot will have a different sequence of candidates in the list. Let us consider 3 candidates say 'Alice, Bob, Charlie', then there will be 3! =6 different types of ballots. For example, if there are three types of ballots with the sequences of candidates "Alice, Bob, Charlie", "Alice, Charlie, Bob" and "Charlie, Alice, Bob". Proposed E-NOTE [1] used a certificate that is given to the voter using three-pass protocol. There may be a case where an intruder pretends to be the voter and gets the certificate, like this man in middle attack is possible in protocol.

To remove this attack and make the voter authentication more secure and verifiable, we are using Public Key Kerberos. Although Kerberos provides both public key cryptography (asymmetric) and secret key (symmetric) encryption for authentication, but in symmetric cryptography all authentications are controlled by a centralized Key Distribution Centre (KDC) any attack on KDC causes to compromise the privacy. Where in Public key cryptography i.e. asymmetric encryption provides distributed trust i.e. distribution of keys is conducted from a publicly accessible certificate repository. Public key cryptography with Kerberos yields the system that increases the security, verifiability and efficiency and overcomes the administering and maintaining disadvantage of Kerberos and the risk of compromise of the private key in public key cryptography. Public key Kerberos is another form of traditional. In public key Kerberos not only in initial steps, public key is used in all steps of it.

2. PROPOSED PROTOCOL

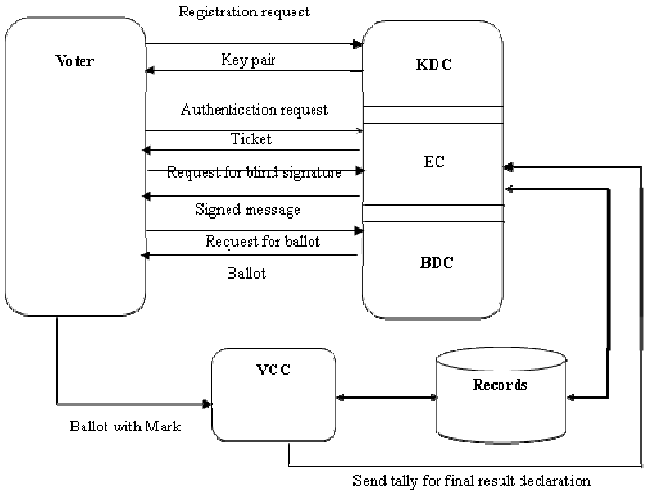

Fig. 1: Block diagram of proposed e-voting process

We used four voting authorities as components of the protocol. The proposed protocol is summarized in the Fig. 1. For this protocol we pre supposed that voter gets its voter id and password physically for login at KDC. Public keys of all the authorities saved in public keys directory. In the election database voter's identity particulars and other details are saved.

Step 1: Voter login at KDC by submitting its id and password. This request also contains the hash of the voter id. For registered voter KDC generate public/private key pair and send to the voter.

$$Voter \rightarrow KDC$$
$$E_{KDC^{pub}}[V_i, T_p, hash(V_i)]$$
$$KDC \rightarrow Voter$$
$$E_{Tp}[V^{pub}, Cert_v, TimeStamp, LifeTime]$$

$$Cert_v : E_{KDC^{pri}}[V^{pri}]$$
$$V^{pri} : Voter's\,\mathrm{Pr}ivateKey$$
$$V^{pub} : Voter'sPublicKey$$

Step 2: Voter requests to the EC for ticket. EC ensures that voter is registered with KDC and gets the public key from it .After verification of voter EC generates the ticket and send it to the voter confidentiality i.e. in encrypted form. EC keeps track of the voters that have got the tickets, to ensure one vote can take the ticket once.

$$Voter \rightarrow EC$$
$$E_{EC^{pub}}[Name, Age, hash(V_i), IP, TS]$$
$$EC \rightarrow Voter$$
$$P = [E_{EC^{prv}}[TicketNo, E_d[M], TS_1]$$
$$E_{V^{pri}}[P, hash(P)]$$

$$E_d[M] = E_d[IP, V_{pub}, TS_1, LifeTime]$$

Step 3: Voter prepares the mark for and send it to EC for bind signature. Mark signed with voter's private key is called as salted voter mark. EC decrypts it and put the signature on it and sends it back to the voter. Here 'r' is the blind factor. Voter removes the blind factor and gets the mark signed by EC.

$$m' = m(r^{EC_{pub}}) \bmod n$$
$$Voter \rightarrow EC$$
$$E_{EC^{pub}}[E_{V^{pri}}[m]']$$
$$R' = (m')^{EC^{pri}} \bmod n$$
$$EC \rightarrow Voter$$
$$E_{V^{pub}}[R']$$

Step 4: Voter submits the ticket to the BDC to get the ballot. BDC records the used tickets in order to prevent the reuse of the ticket. Other than the ticket voter need not to show any of its identity to the BDC. This ensures voter confidentiality in the protocol.

Step 5: For the request with valid ticket BDC issues a ballot. Each ballot contains two fields. The fields of the ballot {C, T} are T that denotes the type of the ballot and c[i] that denotes the i^{th} name of the candidate in the list. BDC encrypts both data sets with different keys.

Let h be the shares key which is used to encrypt the type of ballot and v is the keys used to encrypt the list of candidates. Ballot type (t) and list (C[i]) are encrypted as:

$$T = E_h(t) \quad \text{and} \quad C[i] = E_v(c[i])$$

Step 6: Voter can decrypts the list. It marks it choice and sends the choice 'D', type 'T' and signed mark 'R' to the VCC for counting.

$$Voter \rightarrow VCC$$
$$E_{VCC^{pub}}[D, T, R]$$

Step 7: VCC cannot open the exact type of the ballots; to count the casted votes VCC enlists all the votes as per their types. It decrypts the mark by EC's public key and stores the marks too corresponding to the vote.

$$m = Decryption_{EC^{pub}}[R]$$
$$d[i] = Decryption_{VCC^{prv}}(D)$$
$$TALLY_T = (\sum (d[1], d[2], ..., d[w]), T)$$

After counting it publishes the list in public domain and sends it to the EC.

Step 8: EC decrypt the types of the ballots with the key shared with BDC and declare the final results. It cannot modify the results as they are already among public.

$$t = E_h(T)$$

3. IMPLEMENTATION AND RESULTS

We deploy the moduls on systems, where each server was running on different system. In this four servers are running on four different systems and voters are interacting with these servers from their systsems. For this implementation we took 3 candidates this results 6 types of ballots. Ballot type is randomly generated at BDC to issue to the voter.When the process is started votes need to login shown in Fig. 2.

After successful login at KDC, voters send the details to the EC. EC issues the ticket and signs the mark blindly. Then voter send this ticket to the BDC and gets the ballot.

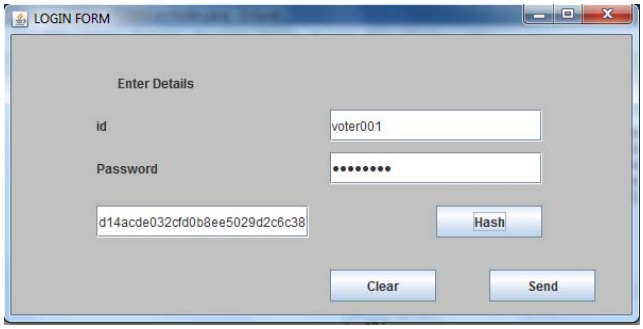

Fig. 2: Login form

Fig. 3 and 4 shows the interaction of KDC and EC servers with the voters respectively. They work in same manner until voting time overs.

```
KDC (1) [Java Application] C:\Program Files\Java\jdk1.8.0_31\l
Waiting to connect
Connected to voter
KDC activated and has been connected to voter
Voter ip address /10.20.131.15 at port 6666
voter id voter001
Authorized Voter
 Generating keys for voter
Keys Send to voter
Waiting to connect
```

Fig. 3: Running KDC server

```
EC (1) [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (May 5, 20
getting keys from directory
Recevied client's public key
Checking the credentials
name correct
age correct
VALID USER
generating ticket
hash of ticket 979e8a976625eb6371497184eddbb004cbca0b45
Ticket send
mark signed with EC private key 715594492100724019239945 4
signed mark send
Waiting to connect
```

Fig. 4: Running EC server

After receiving the ballot voter gets the list of candidates and marks the choice, Refer to Fig. 5(a). This choice is send to the VCC, Fig. 5(b).

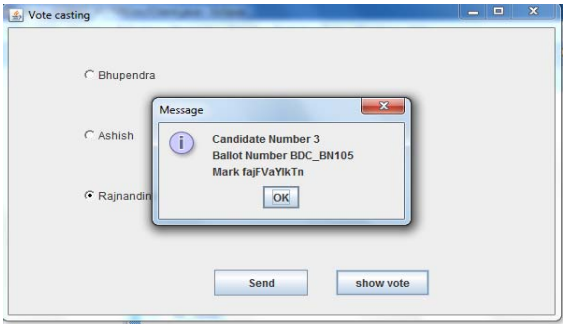

Fig. 5(a): List of candidates

```
<terminated> Voter (1) [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (May 5, 2015,
11:02:03
Voter activated and has been connected to KDC
KDC ip address /10.20.131.5 at port 6666
Keys from KDC recevied
Voter activated and has been connected to EC
EC  ip address /10.20.131.6 at port 6667
Send to EC
ticket hash e07b5c177c91d617025a0f07c510abc1ed63af49
generate hash of ticket e07b5c177c91d617025a0f07c510abc1ed63af49
Message integrity checked
time stamp of ticket is 11:02:41
The mark bpdoEPGoozx
Salted valter mark send
Blid signature completed
Voter activated and has been connected to BDC
BDC  ip address /10.20.131.7 at port 7447
Connected to BDC
send to BDC
ballot noBDC_BN101
Voter activated and has been connected to VCC
VCC  ip address /10.20.131.8 at port 6669
Thanx for participating in voting, your vote has caste successfully
```

Fig. 5(b) : Voter display

When election time overs BDC prints the total ballots issued along with the types of the ballots. Fig. 6 shows how BDC interacts with BDC during election time, and the list of issued ballots after elecition time.

```
Waiting to connect
Connected to voter
BDC activated and has been connected to voter
Voter ip address /10.20.131.15 at port 7446
voter ip address : 10.20.131.15
Time with  ticket : 11:14:01
Ticket is not used before
Inside Ticket
voter ipaddress10.20.131.15
generation time11:13:58
life time11:23:58
IP address is matched
Ticket is valid generate the ballot
ballot number BDC_BN115
ballot type 0IzesDk5jmX7BC33rKCOIg==
ballot has generated
Waiting to connect
Election time has over, no more voter now
Press 1 to get the information of issued ballots
1
type    number of ballots
3       1
5       3
4       4
1       2
6       3
2       2
total ballots issued 15
```

Fig. 6: BDC server

As VCC do not know the actual type of the ballot it cannot declare the result. It only can differentiate the types and prepares the list. Fig. 7 (a) shows that prepares list of votes. VCC publishes this list in public before sending it to the EC for final results.

Fig. 7 (b) shows the respective marks of the votes, counted by the VCC. This list is also on public domain. By looking at this voters can check weather their votes are counted or not. This also helps in preventing the fraud in voting.

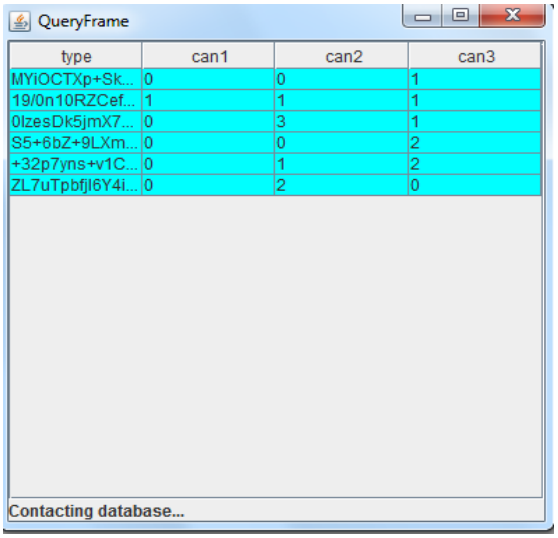

Fig. 7(a): List of counted votes as per their types

```
counted marks are
bpdoEPGoozx
cGRHpudjElI
duGRIaVRYow
ekObnUPkdaJ
fajFVaYIkTn
ggUbLFsSqlR
huXQUiiaWPB
inwsdccEFmh
jCcMHNvXCMp
kyPGYKpcQba
lalsBTXaGdN
mVtGoMRDodj
nNBlPFePakf
olAxOxcqSbS
pWyTsLdchxF

Total recevied marks are 15
```

Fig. 7(b): Received marks with votes

BDC shares the secret key of ballot type with EC. EC decrypts the type of the ballots and count total votes of the candidates and announces winner of the voting. It publishes this result on public domain. Refer Fig. 8(a), decrypted types of the ballots and total votes of individual candidates and Fig. 8(b) shows winner of the voting.

```
Waiting for tally
connected to vcc
decrypted type is 3
decrypted type is 5
decrypted type is 4
decrypted type is 1
decrypted type is 6
decrypted type is 2
votes of Ashish 3
votes of Bhupendra 4
votes of rajnandini 8
```

Fig. 8 : Results at EC

4. CONCLUSION

We have implemented the protocol for an e voting process. This protocol ensures voter confidentiality using the ticket to get the ballot, vote accuracy by seperating the name and vote in the ballot and provides a secure and verifiable voter authentication using public key Kerberos. Use of blind signature makes the protocol receipt free. By following the list publishes by the authorities any fraud in the voting can also be detected ie.e if total number of issued ballots are not equal to total number of marks published by VCC, then there must be a fraud attempted by any of the two authotities collectively. We can conclude that the proposed protocol meets all the security requirements of an e-voting process and ahs achevend all its objective.

REFERENCES

[1] Haijiun Pan, Edwin Hou and Nirwan Ansari, “E-NOTE: An E-voting System That Ensures Voter Confidentiality and Voting Accuracy”, *IEEE ICC*, pp. 825-829, 2012.

[2] Hussein Khalid Abd-alrazzq, Mohammad S. Ibrahim and Omar AbdulrahmanDawood, “Secure Internet Voting System based on Public Key Kerberos”, *International Journal of Computer Science Issues*, vol. 9, issue 2, no. 3,pp. 428-432, March 2012

[3] López-García, Lourdes, Luis J. Dominguez Perez, and Francisco Rodríguez-Henríquez. "A pairing-based blind signature e-voting scheme." *The Computer Journal* , bxt069, 2013.

[4] Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. "Security analysis of India's electronic voting machines." In *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 1-14. ACM, 2010.

[5] Kucharczyk, Marcin. "Blind signatures in electronic voting systems." *In Computer Networks, Springer Berlin Heidelberg.* pp. 349-358, 2010.

[6] Xia, Zhe, and Steve Schneider. "A new receipt-free e-voting scheme based on blind signature." *WOTE*, pp. 127-135, 2006.

[7] Ray, Indrajit, and NatarajanNarasimhamurthi. "An anonymous electronic voting protocol for voting over the internet," In *Advanced Issues of E-Commerce and Web-Based Information Systems, WECWIS 2001, Third International Workshop on.*, pp. 188-190. IEEE, 2001.

[8] Virendra Kumar Yadav, SaumyaBatham and Amit Kumar Malik, “Kerberos based Electronic Voting System”, *International Journal of Computer Applications*, pp.21-23,November 2012

[9] Ms.Tanzila Afrin and Prof K.J.Satao, “E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept”, *International Journal of Advanced Research in Computer Engineering &Techology*, vol. 2, issue 7,pp. 2258-2261, July 2013.

[10] RobertKofler, Robert Krimmer, Alexander Prosser, “Electronig Voting: Algorithmic and Implementation Issues”, *the 36th Hawaii International Conference on System Sciences, IEEE* , 2002