Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 2, July-2017, ISSN 2230-7540

Analysis of the Security of Two E-Voting Systems

Neeru Kamboj[1]*Dr. Omprakash[2]

[1]Research Scholar

[2]Associate Professor, OPJS University, Churu, Rajasthan

Abstract – In this paper, we analyse the security of the two e-voting systems. We show that the Estonian e–voting system is practically secure and the SERVE system is not secure. To declare that an e-voting system is secure, it must be as secure as the traditional voting system. The reason is that traditional voting methods are considered to be practically secure and do not allow large-scale misbehaviour. This means that e-voting must be secure against large- scale voting-specific attacks and the security properties of e-voting must be justified.

----------X----------

INTRODUCTION

We use the activity model of adversary and analyse whether the e-voting systems are secure against the following voting-specific attacks:

- large-scale votes' theft;
- large-scale disfranchisement of votes;
- large-scale votes' buying and selling;
- large-scale privacy violation.

If an e-voting system is secure against these voting-specific attacks, then the following properties are justified:

- Eligible voters are capable to cast ballots that participate in the computation of the final tally.
- Non-eligible voters are disfranchised.
- Eligible voters are not capable to cast two ballots that both participate in the computation of the final tally.
- Votes are secret.

Additionally, we give also the informal justification for other security properties of e-voting:

- It is possible for auditors to check if all correct cast ballots participated in the computation of the final tally.
- The result of election must be secret before the end of election.
- It must be possible to repeat the computation of the final tally.
- All valid votes are counted correctly and a system outputs the final tally.

If all the security properties of e-voting are justified then e-voting system is secure.

To give the justified analysis of e-voting security we use security assumptions (Section 4. 4.) and the attack game risk analysis (Subsection 4.6.3.). The attack game risk analysis is based on the defined environment model (Subsections 4.6.1. and 4.6.2.).

THE SECURITY ANALYSIS OF THE ESTONIAN E-VOTING SYSTEM

In this subsection, we analyse the security of the Estonian e-voting system. We study the security of the Estonian e-voting system based on the security assumptions and the model of environment. We go through all the voting-specific attacks and show that they are unlikely to happen. More precisely, they are unprofitable for rational attackers. Therefore, we conclude that all the security properties of e-voting are justified. In the following, we give the security analysis against the voting-specific attacks.

LARGE-SCALE VOTES' THEFT

If the Estonian e-voting system is secure against a large-scale votes' theft then following two security

properties must be justified: *Non -eligible voters are disfranchised* and *Eligible voters are not capable to cast two ballots that both participate in the computation of the final tally*.

A. large-scale votes' theft has three possibilities:

- votes are forged;
- non-eligible voters are able to vote;
- eligible voters vote more than once. In this paragraph, we study a large-scale votes' theft e.g. the votes are forged.

A voter generates a vote *v* and before it is encrypted an adversary changes without voter's knowledge the vote to *v'*, *v v'* (without voter's knowledge) . For successful attack, the attacker needs a large-scale control over voters' processes for achieving the attack. Assumption IX states that adversaries are unable to take a large-scale control over voters' processes. Therefore, a large-scale forgery of votes by getting control over Voter Application processes is unlikely.

In Network Server, Votes Storing Server and in the connections between Voter Application, Network Server and Votes Storing Server a large-scale votes' theft is possible when non-eligible voters are able to cast votes or when eligible voters are able to vote more than once.

In the following, we study the threat that non-eligible voters are able to cast votes. This means that an adversary is able to create at least 1,000 new correctly verifying signed encrypted ballots for a vote in the name of voters. For creating a large amount of signedand encrypted ballots in the name of voters, an adversary needs access to a large number of voters' private signature keys. Assumption IV states that adversaries do not have a large-scale access to the private keys of voters. Additionally, if the adversary is able (without having access to voters' private keys) to cast a vote then it is possible to construct an adversary that breaks the signature scheme. It is impossible by Assumption I. Therefore, under the assumptions we made, non-eligible voters are not able to cast large numbers of correct ballots.

Large scale votes' theft is also possible if a large number of eligible voters are able to vote twice or if eligible voters are able to cast large numbers of votes. In the Estonian e-voting system, voters are able to cast more than one ballot, but only the last one is counted. Votes Storing Server cancels multiple votes. In case an adversary has access to the server and modifies the multiple votes' cancelling process, then eligible voters would be able to vote many times. We analyze this attack by using attack game risk analysis in Subsection 4.6.3.5. Risk analysis shows that this attack is not profitable.

A large-scale votes' theft against Votes Counting Server or the connection between Votes Storing Server and Votes Counting Server is an inside attack. The connection between servers is a data transfer by using data carriers i.e. data transfer is offline. Votes Counting Server of the Estonian e-voting system is not connected to the Internet. The phase of votes' counting is secure by using Assumption VI. Let us assume that before the phase of votes' counting an attack against Votes Counting Server or data carriers is possible. The encrypted ballots are transferred to Votes Counting Server. Therefore, for adding votes to Votes Counting Server, an adversary does not need voters' private signature keys. The attack needs a program for creating encrypted ballots and a possibility to add votes into the data carrier or to Votes Counting Server. In Votes Storing Server there is a log file LOG3 which consist of all encrypted ballots and voters' personal data. Assumption VII declares that the independent log file system in the Estonian e-voting system is secure. For successful attack against Votes Counting Server or data carriers, the attacker should attack also Votes Storing Server for adding encrypted ballots and voters' personal data to LOG3. This means that the attack consists of affecting the two e-voting servers. In Subsection 4.6.3.7 there is an attack tree analysis for this attack. The probability to succeed the attack is 0.01 and it is unprofitable. Moreover, to change the log file in Votes Storing Server, attackers should affect the log file also in Network Server. Obviously, an attack against three e-voting servers is unprofitable. Therefore, even when the attacker is able to get access to offline Votes Counting Server or data carriers, a large-scale votes' theft is unlikely.

Conclusions, in the Estonian e- voting system: (1) *Non-eligible voters are disfranchised* and (2) *Eligible voters are not capable to cast two ballots that both participate in the computation of the final tally* are completed.

LARGE-SCALE DISFRANCHISEMENT OF VOTES

If the Estonian e-voting system is secure against a large- scale disfranchisement of votes then the security property *Eligible voters are capable to cast ballots that participate in the computation of the final tally* holds.

The aim of disfranchisement of votes is to eliminate undesired votes. The first possibility is to attack the phase of voters' registration. In Estonia the e-voting's certificates of authentication and digital signatures are distributed among voters by using the national Public Key Infrastructure. Assumption V says that the Estonian national Public Key Infrastructure is secure. Therefore, the attack against the phase of voters' registration is impossible by Assumption V.

There are the following possibilities to achieve a large-scale disfranchisement by attacks on e-voting system components:

- undesired votes are eliminated so that voters do not get a positive response from e-voting system;
- undesired votes are eliminated so that voters get a positive response from e-voting system;
- undesired voters' votes are eliminated and voters get a positive response from the e-voting system. In the following, we consider the cases when attacks are performed against Voter Application, Network Server or the connection between them. For example, a denial of service attack against Network Servers disfranchises voters so that signed encrypted ballots from eligible voters never reach Back-office. In the case when voters are not able to cast votes they will inform Electoral Committee. Therefore, by using Assumption VIII the attack is unlikely.

The second possibility is that a vote is eliminated, but the voter gets still a confirmation about accepted vote. In this case, Voter Application is injured for converting the error message from Network Server. We analyse this threat in Subsection 4.6.3.6 by using attack game risk analysis. The attack tree analysis shows proofs that this attack is not profitable.

Thirdly, if the attack is against Network Server or the connection between Network Server and Votes Storing Server, then voters are able to cast votes but they will get error messages. Voters inform Electoral Committee about misbehaviours and Electoral Committee terminates the e-voting process by using Assumption VIII.

A dedicated attack against Votes Storing Server is an attack against the pairs of voters' data and signed encrypted ballots, because the attacker needs information about voters or votes in order to eliminate undesired votes. If attackers want to eliminate votes based on values of votes then they should be able to decrypt ballots. Assumption II says that adversaries do not have access to the private decryption key *SK*. Therefore, adversaries could not eliminate undesired votes this way. To deduce the values of votes without having private keys, the adversary needs to know the random numbers inside the ballots. Therefore, attackers need a control over voters' voting processes. Assumption IX states that adversaries are not able to take a large-scale control over the voters' processes. Hence, the attack to eliminate undesired encrypted ballots is not possible.

Another possibility to achieve the aim of attack is to use undesired voters' list and delete their votes in Votes Storing Server. The Estonian e-voting system has an independent log files system, which guarantees the integrity of the e-voting. In case some votes are just deleted without modifying the log files, the sum of logs is not verifiable. Hence, the reliability of e-voting is damaged and the e-voting is terminated and will be cancelled by Assumption VIII.

Let us assume that the adversary eliminates voters' votes in Votes Storing Server so that deleted ballots never reach to the log file system. If adversary attacks Votes Storing Server in order to eliminate votes, then adversary should also attack Network Server for catching the vote's data written in LOG1. We will analyse the threat in Subsection 4.6.3.7. The result of the attack tree analysis confirms that this attack is unlikely.

Finally, we analyse an attack against Votes Counting Server or against the data carriers which are used to transfer encrypted ballots to Votes Counting Server at the end of voting. To delete votes in purpose, adversaries must know the value of votes; therefore they need an access to the private key of e- voting. Assumption III states that adversaries do not have access to the private keys of e-voting. If adversaries know the encrypted ballots of undesired votes', they may compare these with the encrypted ballots in Votes Counting Server and deduce, which votes are undesired. In order to decide which ballot is undesired, an adversary needs a large-scale control over voters' e-voting processes and we have a contradiction with Assumption IX. Moreover, adversaries need to get control over the log file system and therefore they have to attack Network Server and Votes Storing Server. As shown in the previous paragraphs and Assumptions III and IX the attack against Votes Counting Server or data carrier is not successful.

To conclude, the verification of log files is highly important for achieving the completeness of security property *Eligible voters are capable to cast ballots that participate in the computation of the final tally*. If independent auditors do not verify the integrity of the independent log file system then the Estonian e-voting system would not be secure enough.

REFERENCES

A Ansper, A. Buldas, M. Oruaas, J. Piirsalu, A. Veldre, J. Willemson, K. Kivinurm (2003). The Security of Conception of E-voting: Analysis and Measures. E-hääletamise kontseptsiooni turve: analüüs ja meetmed. 2003.

http://www.vvk.ee/elektr/docs/Analyys-01.pdf. 21.01.2007.

A. Buldas, P. Laud, J. Piirsalu, M. Saarepera, J. Willemson (2006). Rational Choice of Security Measures via Multi-Parameter Attack Trees. In Critical Information Infrasturctured Security First International Workshop - CRITIS 2006, LNCS 4347, pp. 235-248.

D. Jefferson, A.D. Rubin, B. Simons, D. Wagner (2004). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). 2004. http://www.servesecurityreport.org/. 21.01.2007.

Estonian National Electoral Committee home page, www.vvk.ee. 21.01.2007.

Estonian National Electoral Committee. General Description of the E-voting

http://www.vvk.ee/elektr/docs/Yldkirjeldus-02.pdf. 21.01.2007.

System. E-hääletamise süsteemi üldkirjeldus. 2004.

Corresponding Author

Neeru Kamboj*

Research Scholar

E-Mail –