Security Analysis of the Geneva e-voting system

Daniel Franke
TU Darmstadt
franke_d@rbg.informatik.tu-darmstadt.de

Abstract: The Swiss democracy, which is a direct democracy, carries out up to five referenda a year. This causes that 95 % of the Geneva voters use postal voting instead of going to the polling station. In 2001 the Cantons of Geneva, Neuchâtel and Zurich decided to start pilot projects in electronic voting (e-voting). Although the Canton of Geneva published more and more information about their system, an independent security analysis about it has neither been conducted nor published. This paper analyzes the system based on the available information and identifies vulnerable points at the components and on the communication channel between them. At each vulnerable point, we analyze whether the security requirements from the Swiss state chancellery which are based on the requirements of free, equal and secret elections, are violated. If an obvious solution for a security problem exists, it will also be illustrated. Two main problems are the security of the client-PC and the Internet connection of this PC. The system does not try to solve the trusted platform problem and it is not possible to solve it without introducing additional components.

1 Introduction

The Swiss democracy is a so-called direct democracy. This means that any citizen who is allowed to vote can propose a new law or demand change in an existing one[1]. As a result of this, referenda [2] are held four to five times a year. This fact causes very high use of postal voting, which is more comfortable than voting at the polling station. For example in Geneva on average 95 % of the voters use postal voting (see [TMK03, page 183]). In addition, the Swiss living abroad are allowed to vote at most federal and some cantonal elections [DMSTW12]. But in some states there are problems with the delivery time of the postal service (see [DMSTW12, page 174]). These two reasons are the main arguments for introducing electronic voting or more precisely Internet voting in Switzerland. In 2001 the Cantons of Geneva, Neuchâtel and Zurich decided to start pilot projects for introducing e-voting. They signed a contract with the Federal Chancellery which allowed them to launch the pilot projects and constitutes that the Swiss Confederation pays up to 80 % of the costs. The results of the projects had to be made public to the other cantons.
On the 8. February 2009, the pilot project ended at cantonal level with the inscription of the e-voting system in the Geneva constitution. On October 2011 the Geneva system was used at a federal election for the first time and more information about the system was

[1] More about the possibilities of direct democracy in the Switzerland are described in [Swi].

[2] Here the word referendum is used as a synonym for referenda, elections or initiatives (see [Swi] for more information about these possibilities).

published. Geneva also offers other cantons use of the e-voting system for their elections and referenda.

Although more and more documents about the functionality of the system appeared no independent security analysis was released. The lack of an analysis is the reason for this paper which is based on the information - published until March 2013 - and E-Mail correspondence. At first, the system is described (Section 2). Then the security requirements for the e-voting system which are defined in the Ordinance of political rights are cited (Section 3) before possible attacks on the components of the system and their complexity will be analyzed in Section 4. The analysis will show that the client-PC and the Internet connection of this PC are vulnerable points which the security measures of the e-voting system cannot protect.

2 Components, Voting Protocol, and Procedures

Most of the information in this section is taken from [Sta], [Sch06], [Sta13], [Gen07] and E-Mail correspondence with Michel Chevallier, the deputy general secretary in the canton of Geneva.

2.1 Components and entities

There are several components and entities which are involved in the electronic voting system: The components are the register of inhabitants, the printing office, the postal service, the voting card, the voter, the client-PC, the Java-voting-applet also called Java-applet, firewalls, the e-voting server, the electronic ballot box, the electoral register, the Central Electoral Commission (CEC), the admin-PC, one administrator of the e-voting system and a random number generator. An image with the components and their relationship can be seen in figure 1.

In the following paragraphs each component and its functionality is described. No information can be found about the **firewalls** which protects the e-voting network with the three servers. Thus it will not be described in this section. The voter can use any computer with a browser and installed Java plugin as a **client-PC**. The security problems of this computer are discussed in Section 4.4.

2.1.1 The voting card

The voting card existed before e-voting was introduces in Geneva. It is the legitimation for the voter to vote at the polling station or to use postal voting. In the e-voting system the voting card has the same function. It contains information about the referendum including the election day as well as the voters name, her address and the name of the polling station. For the electronic voting system, the information on the voting card is extended by a 16

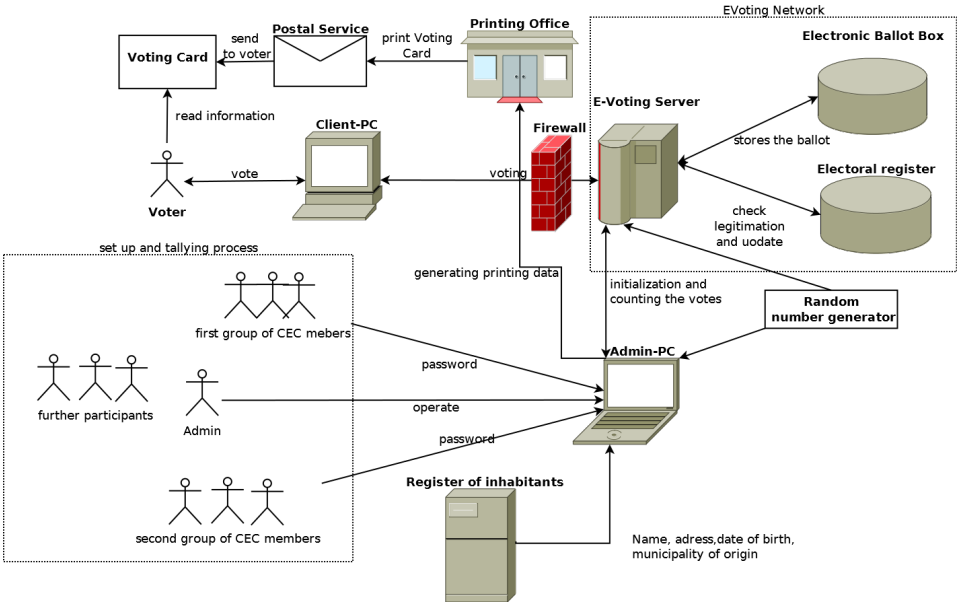

Figure 1: Components and their interaction

digits long voting card number (VCN), a password, a control-code, the URL of the e-voting server and the fingerprint of the SSL certificate, the server serves to the client-PC. The password is covered with a field which must be scratched off. To simplify handling of the voting card at the polling station, the VCN is also printed as a bar code on the voting card. The VCN and password are generated with a **quantum random number generator** at the admin-PC which is used for the set up and tallying process.
The data for generating the voting card is taken six weeks before every election from the **register of inhabitants** of the"Cantonal Population Office" and the register containing the registered Swiss living abroad. The date of birth and the municipality of origin of every voter are also transmitted to the admin-PC. These two values, the VCN, the location of the polling station, the control-code and the password are stored in the electoral register. The voter has to type in the date of birth and the municipality of origin during the voting process. This prevents somebody who steals the voting card or the printing data from voting without knowing this additional data. After the generation of the printing data, two random values (also called salt) are generated. The first salt is appended to each VCN and a HASH value of the result is generated. The second salt and and a correspondence table containing the generated HASH values with the corresponding voting card numbers are stored on the e-voting server. Both salt values are also stored in the Java-applet. More information about the correspondence table and the salt values can be found in Section 2.3.

The printing data for the voting card are transmitted to a **printing office** which prints the voting card and uses the **postal service** to send them to the voter. For both postal and voting at the polling station the card must be filled out with the voters date of birth and has

to be signed (see picture in [Sta13, page 4]). For postal voting the card has to be sent back together with an envelope containing the ballot paper. If the cover of the password was scratched off, the personnel at the polling station knows that a person could have voted online. In this case a query to the electoral register (Section 2.1.3) has to be performed.

2.1.2 E-voting server and Java-applet

The e-voting server represents a group of servers with two different applications. One application is an *Apache* web server which serves the web page and manages the communication with the client-PC. The other application is an *Apache Tomcat* server which is also a web server that enables the server to execute java code [3]. The e-voting server does not store any data of the voters. The connection to the Internet is established for the duration of the referendum, after that the connection is physically disconnected. To generate random numbers for cryptographic keys at set up and for the voting procedure, a quantum random number generator is connected to the e-voting server. The server serves an extended validation (EV) certificate to the web browser whose fingerprint can be checked by the user with the information on the voting card. Furthermore, most browsers show a green address bar when they receive a valid EV-certificate. The e-voting server also serves the Java-applet, processes the vote, stores the electronic ballot in the electronic ballot box and updates the electoral register and the integrity meter (see 2.1.3).
The Java-applet authenticates the user, establishes a symmetric encrypted connection to the e-voting server and leads the user through the whole voting process. It is digitally signed with a valid code signing certificate, but the corresponding fingerprint is neither printed on the voting card nor available online.

2.1.3 Servers for electronic ballot box and electoral register

The servers are cloned, located at two different places and managed by different administrators by the four eyes principle. The data is stored on Oracle databases which store log files containing the changes of the database (see [Gen07, page 22]). These log files help to recover the database if both copies are defective.
The electronic ballot box stores an encrypted data set containing the electronic ballot, a salt and the voters polling station. It also contains the stored ballots with a counter and an integrity meter which is an encrypted value that represents the number of votes the e-voting server has stored in the ballot box. The value is encrypted with a symmetric key which is stored at the e-voting server, so only this server can increment it.

Except the correspondence table, all data of the voters needed for the voting process are stored in the electoral register. It contains the voting card number, the password and the control-code from the voting card, the date of birth, the municipality of origin and the time when a VCN has voted. The register also contains a counter which counts the electronic votes. This counter and the voting time are updated when the e-voting server announces that a VCN has voted. All servers and their connection including the e-voting server, the electronic ballot box and the electoral register are continuously monitored.

[3] The only available information about the construction can be found in [Gen07, page 22].

2.1.4 Central Electoral Commission

The Central Electoral Commission (CEC) was founded in January 2010 at the same time that electronic voting was added to the cantonal constitution of Geneva. To guarantee a democratic control of the e-voting process, some members are representatives from the different parties. The CEC is allowed to audit the whole e-voting system by itself or hire experts for this task. It has access to all documents concerning the e-voting system. Two groups of CEC members have to be present during the set up and tallying process. They choose two passwords which encrypts the private key that decrypts the electronic ballots.

2.2 Set up procedure

As described in [Sta], during the set up procedure, the following people are present: A representative of the State Chancellery as chairman of the session, the president of the CEC, the Chairman of the CEC [4], two groups of two CEC members, a representative of the Voting and Elections Department [5] ("VED"), a notary, a Police information systems security officer ("security officer") and an administrator of the Internet voting system.
At first the administrator connects the Admin-PC with the e-voting network and starts the generation of a symmetric key and an asymmetric public-private key pair. The symmetric key is stored at the e-voting server where it is responsible to decrypt and encrypt the integrity counter of the ballot box. The public key responsible for encrypting the electronic ballot is stored on the e-voting server. Before the copy of the key pair (public and private key) is deleted from the admin-PC, it is encrypted with a two-part password and stored on a CD and an USB stick. The two-part password is chosen by the two groups of the CEC. Each group chooses their part of the password independently, enters it in the admin-PC and notes it on a sheet of paper which is put in an envelope. The envelopes are sealed and handed to the notary. The data media are given to the "security officer". After this, the e-voting server sets the integrity counter to zero. The admin-PC will be put in a sealed bag and handed over to the VED representative. This takes place 30 days before the election day. Three days later the ballot for every registered voter is opened. To test the integrity of the system, the representatives of the CEC have to make test votes and document their choice. These votes are done with special VCNs which are associated with a virtual polling station. This makes it possible to separate these votes during the tallying process.

2.3 Voting protocol

The communication between the client-PC and the e-voting server is described in Figure 2. The voter starts the Internet voting process when she calls the website of the cantonal e-voting system which establishes a SSL/TLS connection. She should check the fingerprint of the transmitted certificate (compare Section 2.1.1) to determine whether she is con-

[4] Leading the set up and tallying procedure. She is responsible for organization of the ballot.
[5] The Voting and Elections Department is responsible for the organization of the referenda.

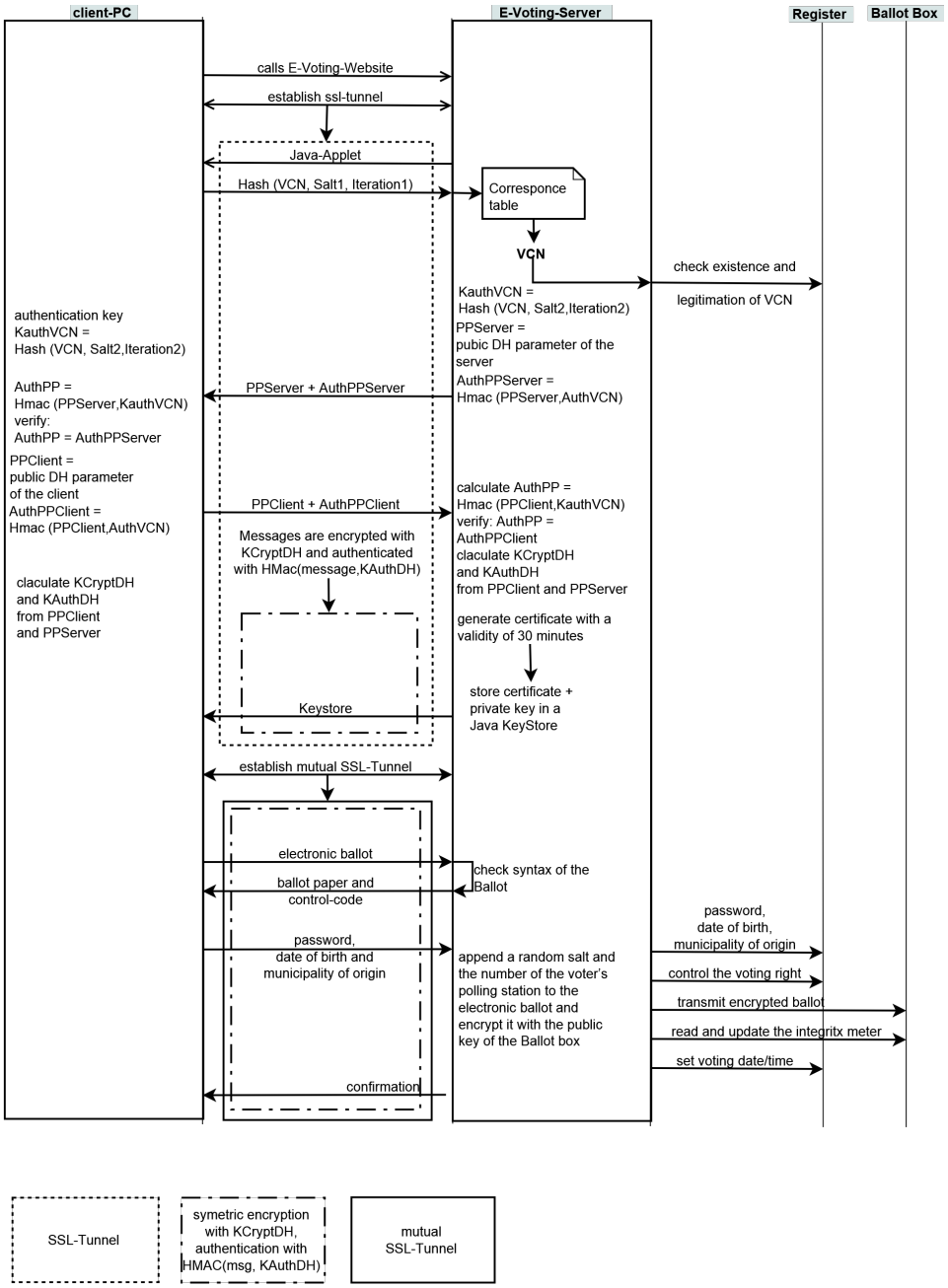

Figure 2: Voting protocol

nected to the correct server. The e-voting server transmits the Java-applet, which manages the rest of the voting process, to the PC. Before the applet is executed, a message will be shown. This message contains the information that a signed Java-applet will be executed if the user chooses "execute" [6]. After the voter has typed in his VCN, a Hash value of it extended with "Salt1" is generated and transmitted to the server. The e-voting server uses the correspondence table to determine the VCN and sends it to the electoral register. If the number exists and has not voted yet, *KCryptDH* and *KAuthDH* are generated with a Diffie-Hellman key exchange [7]. The messages for the key exchange are authenticated with a HMAC [8] which is generated from the message and the voting card number. *KCryptDH* is used to establish a symmetrical encrypted connection in which the messages are authenticated with *HMAC(Message,KAuthDH)*.
The server creates a public/private key pair, generates a user certificate for the public key and sends it, together with the private key to the applet. Based on this certificate, a mutual SSL connection will be established. In this connection the symmetric encrypted connection with the HMAC will also be established to repair some weakness in SSL connections(see [Sta, p. 8-9]). After this process the voter places her vote and the applet sends it to the server which makes a syntactic check of the ballot and when this succeeds, it generates pictures for every question of the referendum, containing the choice of the voter, her control code and the number of the question (see Figure 3). This enables the voter to

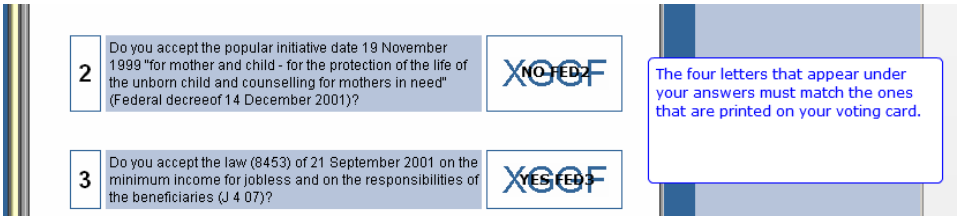

Figure 3: Picture of the Geneva e-voting system demo web site showing the purpose of the control-code (control-code:XGGF). Retrieved 07.12.2012 from http://www.ge.ch/evoting/english/welcome.asp

determine if her vote has been transmitted correctly. If she has examined these images, she has to enter the password from the voting card, her date of birth and her municipality of origin. Then the applet transmits the data to the server which validates this information. If the electoral register verifies the validity of the parameters, the e-voting server encrypts the Ballot including the number of the polling station [9] with the public key generated at the initialization process and updates the data in the voting register. To update the integrity meter, the server reads and decrypts it with the symmetric key, increments it and writes

[6] An applet which is not signed with a valid code signing certificate of a well known issuer will generate a warning instead of a simple message.

[7] Diffie Hellman key exchange allows two parties to establish a shared secret key over an insecure communication channel.

[8] HMAC offers the possibility to generate an identifier for a message with the help of a cryptographic hash function and a key.

[9] Although all votes takes place at the same servers each voting card number is associated with the polling station number of the voter.

the new encrypted value in the database of the ballot box. The voting card number is also marked as voted with a time-stamp from the beginning of the process. Storing of the electronic ballot and updating the electoral register is one transaction which will either be executed as a whole or not at all. After this procedure, it is possible to look if and when a voting card number has been used by typing it in the Java-applet.

2.4 Tallying process

One day before the electoral day the e-voting server is closed and disconnected from the Internet. The same people who are involved in the set up procedure, come together in an official session on the electoral day to count the votes. The components entrusted to the members of the group have to be present for this process. Additionally, the administrator provides a quantum random generator for mixing the ballots before decrypting them.The administrator connects the admin-PC to the electoral network, downloads a copy of the data in the ballot box, starts the mixing procedure and compares the integrity meter with the two other counters. The USB stick or the CD is connected to the PC and the two groups of the CEC have to input their passwords to decrypt the private key. If one group has forgotten it, the notary can open the corresponding envelope to recover it. With the private key all electronic ballots and the corresponding polling station location are decrypted, the test votes are separated and the real votes are transmitted to another PC where they are mixed with the postal votes. Then all votes are retransmitted to the admin-PC which produces the final result (e-mail correspondence). Before the votes are mixed with the postal votes on the other PC, the test votes are compared with the documents and the result is presented to the CEC. Statistical tests are also done with the voting result in order to uncover systematic manipulations. The handling of these results and information on which concrete actions will be performed if abnormalities are discovered, is not publicly documented. Two copies of the electronic ballot box exist on backup hardware which can be used for recounting on another PC. A recount can be ordered by the CEC or a judge. This is the reason why the data on the ballot box and the backup hardware are kept for 50 days after the last counting / recounting.

3 Security requirements

This paper analyzes the security of the Geneva e-voting system based on the security requirements that are postulated in the Article 27d of the Ordinance on political rights. In the state Council's report these requirements are quoted [Gen07, page 15]:

a) "only the electorate is able to take part in the ballot (after verification of voting capacity);"

b) "a voter will only have one vote and will only vote once (one man, one vote);"

c) “it is impossible for third parties to capture, modify or systematically deviate electronic votes and decisively influence the main result of the vote or election (i.e. the guarantee that the citizens’ wishes are expressed);”

d) “it is impossible for third parties to know the content of votes (i.e. the guarantee of voting secrecy);”

e) “all votes cast will be taken into consideration during the count (i.e. the guarantee that the citizens’ wishes are being faithfully expressed);”

f) “the possibility of any systematic fraud is ruled out (i.e. a ballot compliant with the rules).”

The state Council’s report also describes that the e-voting system should not be 100 % secure, but it should be as secure as postal voting or voting at the polling station. We analyze which of the requirements are broken and whether the other voting methods also have a similar vulnerable point. The description of the system can be deprecated or falsified if new information about the system is published or something in the system is changed. Also the identified security vulnerabilities could be repaired or, if the given information is wrong, even not exist.

4 Security analysis

In this section, the security of most of the components described in Section 2 is analyzed based on the requirements formulated in Section 3. The firewall, the register of inhabitants and the quantum random number generator are not analyzed because not enough information can be found on them. Information about the Java-applet is poor, but it is possible to serve a manipulated one to the client-PC. This possibility is discussed in Section 4.5.

4.1 Printing office

The printing office has access to the printing data and the voting card. An attacker can try to copy the data, to manipulate it or to steal the voting card. These attempts are very difficult, because the printing office is specialized in secure printing activities and secures the printing data (see [Gen07, page 21]). Stealing the voting card or a manipulation of the printing data would hinder the voter from voting, but this attempt is detected if the voter misses her voting card or can not vote because some data on the card is wrong. If at least one voter recognizes these manipulations the referendum has to be repeated. The security requirements are not broken and the only benefit for an attacker would be a loss of confidence in the system. The traditional voting methods could only manipulated this way by stealing the voting card which also is not practical. Copying the printing data can breach the voting secret if the attacker can get access to the votes and the corresponding VCNs (for instance from e-voting server). If an attacker is able to combine the printing

data with the date of birth and the municipality of origin of the voters, she could also vote for them. This attempt is certainly also recognized by the users. An improvement of this approach is to vote only for voters who have not voted for many years. This data is only stored in the electoral register for a short time. Another problem is that the date of birth and the municipality of origin are the only data that is constant for all referenda. This makes it very hard for an attacker to estimate who has not voted in previous years. For postal voting or voting at the polling station a voting card is needed to vote. Even if the attacker can print voting cards, she has the same problem to find voters who have not voted for many years.

4.2 Postal service

An attacker at the postal service can note the data on the voting card or try to steal the voting card. The possibility of stealing the voting card is discussed in Section 4.1. Collecting the data printed on the voting card needs a lot of resources and the password which is covered can only be determined by scratching the cover off, which would be recognized by the voter. So the collected data can not be used to vote. The attacker can try to use the VCN, the name and the address in combination with other sources to breach the voting secret. This possibility is not very probable because the effort to collect this information is high. It is easier to collect this data at the printing office.
Postal voting offers the possibility to open the envelope of the letter the voter sends back to the polling station. This would break the voting secret and the attacker could exchange the ballot. Both attacks are inefficient because to open these letters a lot of personnel and resources are necessary.

4.3 Voter

There are two possibilities to manipulate the referendum at this entity. The first possibility is to pay the voter for her vote. The second possibility is that a person who is familiar to the voter votes for him. This approach is called *family voting* (see [Sta13, page 25]). Postal voting also inhered this problem and the Geneva State Chancellery calls 2 % of voters who voted over the e-voting system to ensure that they have voted and nobody has influenced them (see [Sta13, page 28]). Both attacks violates the security requirement *one man, one vote* and the principle that only the electorate is able to vote, but it can not be used to systematically manipulate the result of the election. Further to these two requirements, buying of votes enables an attacker to influence the main result of the referendum. But to reach this aim, a lot of people have to be paid which is very expensive and increases the possibility that the manipulation will be found out.

4.4 Client-PC

Postal voting and voting at the polling station do not need a client-PC, an internet connection or an e-voting server. So all identified security holes at the client-PC , the e-voting server and the connection between them can not be compared with traditional voting methods. The client-PC has access to all information concerned in the voting protocol. Additionally the PC also stores personal information of the voter. If malware infects the client-PC, an attacker has access to all the data and is able to manipulate them. Stuxnet and other viruses have demonstrated that a specialized virus can not be detected for some years if it does not infect each PC (see [MMDC13]). For the Swiss system it would be practical to locate the IP-address of the PC on which the malware runs. If the IP-address is not located in the Swiss the malware could remove itself from the PC. The effort to develop such a system is very high, but if it succeeds, there exists several possibilities for the malware to influence the referenda:

- Store the data transmitted during the voting process.
- Store the data, simulate the voting process and vote later.
- Vote at the same time the voter votes.

All three possibilities enable the attacker to calculate an intermediate voting result. Since the malware has access to the VCN, it is also possible that the attacker can gain the voters identity from data which connects her name with the VCN (e.g. data from the printing office). The data stored on the PC or the websites the voter visits (e.g. Facebook) are an easier way to determine the voters identity. If the malware only stores the data of the voting process and the security software on the PC does not detect it, there is no measure of the e-voting system which protects the voter against it.
The second and the third attacks can violate the principle of ”one man, one vote” and allow the capture, modification or systematical deviation of electronic votes. The malware which simulates the voting process and tries to vote later could be identified if the voter compares the control-code on her voting card with the control-code the client-PC displays to her. A malware which votes at the same time has the possibility to estimate the control-code. The control-code can be compared with CAPTCHAS and for CAPTCHAS there are known several attacks. One efficient possibility is that the malware could try to use optical character recognition (OCR) software to extract the control-code from the image (see [MM03]). Crowdsourcing is another way to extract the control-code (see [Kot04]).
As shown above the success of the first and the third approach depends on the security software of the client-PC. To solve this problem, additional hardware has to be added. One example for this additional hardware could be a Smartcard reader with a pin pad and a Smartcard. The Smartcard can secure the connection with the server and the choice for the vote could take place on the Smartcard reader (e.g. type 1 for “Yes” and 2 for “No”). Because Smartcard readers are developed to be as secure as possible, it would be more difficult to find a security hole in this system in order to manipulate the referenda.

4.5 Connection between client and server

A simple phishing mail or the manipulation of the DNS in a public WLAN can route a voter to a manipulated e-voting website. If this website persuades the voter and she does not check the fingerprint of the delivered website, a manipulated Java-applet could be delivered. As described in Section 2.3 the Java-applet has to be signed with a code signing certificate of an official certification authority (CA). This does not hinder an attacker from signing a manipulated applet with an arbitrary code signing certificate from a CA, because information about the certificate which signs the original applet is not made public. Now the attacker has the same possibilities as in Section 4.4. The only difference in the security analysis is that the fingerprint does not help to detect malware installed on the PC. While malware could manipulate the Java-Plugin in the web browser or the fingeprint the browser displays, a server which serves a manipulated website can not manipulate the fingerprint the web browser shows. This means the success of all three approaches depends on the attention and the skills of the voter.
If an attacker tries to route the connections to the e-voting server over her own servers, the administrators who monitor the system could notice that many voters use the same IP-address. To circumvent this problem the manipulated Java-applet could establish a direct connection to the e-voting server in order to cast the manipulated vote. The symmetrical encryption which is established in the SSL tunnel and the mutual SSL connection do not secure the e-voting system against this attacks, because all data including the data needed for the mutual SSL connection are transmitted to the attacker. A Smartcard reader and a Smartcard would also solve this problem because a Smartcard would decrypt and encrypt all messages. If the received data can not be decrypted properly, the Smartcard can refuse the connection.

4.6 E-voting server

The e-voting server handles the whole communication with the voter and encrypts the ballot. So it has access to all the ballots and can manipulate them. With the access to this server it is possible to calculate the result of the referendum and manipulate the electronic ballots. In combination with data from the printing office or other sources it is possible to determine the identity of the voter. If an attacker has full access to this server, no security requirement could be satisfied. In Section 2 it is described that the e-voting server is placed behind a firewall and that the whole system is continuously monitored by administrators. But details about the firewall and the monitoring system are kept secret. The test votes would not protect against a manipulation on the server because it is possible to determine the polling station locations that belong to these votes.
A simple measure to minimize this problem would be an encryption of the electronic ballot on the client-PC. Because the e-voting server has no access to the private key which decrypts the ballot paper and the encrypted data which consist of the ballot and a random salt does not allow one to infer the ballot content, the voting secret cannot be broken. This measure would not hinder the e-voting server from exchanging the electronic ballots

before they are stored in the electronic ballot box. This shows that security of this entity completely depends on the installed software, the administrators and the people that observe the system (CEC members or experts commissioned by the CEC).

4.7 Servers for electronic ballot box and electoral register

The electronic ballot box has access to all encrypted electronic ballots and the integrity meter. The ballot box neither has access to the symmetric key which encrypts the integrity meter nor to the public-private key pair which encrypts and decrypts the electronic ballot. If an attacker would have access to the public key stored on the e-voting server, she could exchange the ballots in order to "influence the main result" of the referendum. But because a salt is appended to each electronic ballot before it is encrypted, it is infeasible to differ the ciphertext of the ballots from each other. So she has to exchange all electronic ballots including the test votes which should result in a difference between decrypted test votes and the documents of these votes. The traditional ballot box at the polling station can not be manipulated this way. It is opened at a public procedure and a single person has no possibility to exchange the ballot paper before.

If an attacker has access to the electoral register she can try to manipulate entries in order to allow a voter to vote more than once. This attempt would be difficult because integrity meter, the counter in the ballot box and the number of voters from the electoral register are compared at the tallying process. It would be easier if the electoral register sends the data of the voters who have not yet voted to the attacker a short time before the e-voting server closes. With this information the attacker or a computer program can vote. The monitoring of the system and the fact that the electoral register is not directly connected to the Internet reduces the chances for success. If they are successful, both attacks would infringe the principle of "one man, one vote" and influences the main result of the referendum.
Although it seems that the electronic ballot box and the electoral register are secure and an intrusion is detected, it is important to inform the voters about the measures which protect the system. Without this information the voter cannot form her own opinion about the security of the servers.

4.8 CEC and participants at set up and tallying process

Neither the two groups of the CEC nor the other participants - except the administrator with the admin-PC - can manipulate the result without the help of the other people. During maintenance of the admin-PC, the administrator can try to manipulate it but this is not possible while the processes are running because the participants could follow her operations on a second screen (see e-mail correspondence). If all participants would collaborate the result could be changed. The feasibility of this approach should be as high as the attempt to compromise the personnel at the polling station. Buying all the personnel and the observers at one polling station is nearly impossible, so it should also be infeasible to

buy all the participants at the set up and tallying procedure. Only if this would succeed it would be possible to ”decisively influence the main result” of the referendum.

4.9 Admin-PC and administrator

The admin-PC has access to the printing data, to the data that are stored in the electoral register and the electronic ballots. The final result of the Internet votes is also calculated on this PC. As described in Section 2.4 the votes are only recounted if it is ordered. Although the admin-PC is not connected to the Internet and is always stored in a secure location, an administrator could manipulate it. Another possibility to manipulate this PC would be hardware like a simple mouse which is able to infect it with a virus (see [Net]). But a virus which infects the admin-PC could only manipulate the system if the attacker knows details about the software installed on this PC. So for all attacks the help of an insider is needed. No details are made public about the administrator who is operating the admin-PC at the set up and tallying process. If this administrator is randomly chosen, it is hard for an attacker to compromise her. It is impossible to estimate the security of the admin-PC because many factors are kept secret .

5 Conclusion

With the Geneva e-voting system the state chancellery tries to find a compromise between security and usability. Each voter who is able to use a web browser, has access to a PC with Internet connection and received her voting card, is able to use the e-voting system. This is a problem, because a computer could be infected with malware, the voter could not have the knowledge to examine the fingerprint or is too lazy to do it. So especially phishing mails and malware installed on the client-PC are security problems in the Geneva e-voting system. Although a lot of effort has been expended to secure the system, these problems are not solved. The only possibility to solve it is that the voter secures his PC and always controls the fingerprint. The mutual SSL connection and the additional symmetrical encryption with KCryptDH to repair some weakness in the protocol are examples of that effort. As shown in Section 4.5 the mutual SSL tunnel does not offer more security than the normal SSL tunnel if the private key is transmitted over the connection which should be secured. The additional symmetric encryption helps to repair some weakness in SSL connection, but also it does not help against the shown attacks.
A further problem is that a lot of data about the e-voting system is kept secret. The construction of the e-voting system necessitates that the voter has to have confidence in some person such as the notary, the VED representative or the administrator. A sealed envelope or a sealed bag does not hinder somebody from breaking the seal and counterfeiting a new one later. To create this confidence it would be important that the voters know how the electronic ballot box and the voting register work, how the servers are monitored and what happens if a break-in is detected.

Acknowledgements

The author would like to thank Professor Melanie Volkamer for her guidance , Michel Chevallier for the information about the e-voting system and Maina Olembo for proof-reading.

References

[DMSTW12] Ardita Driza-Maurer, Oliver Spycher, Geo Taglioni, and Anina Weber. E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons. In *Electronic Voting*, volume 205 of *LNI*, pages 173–187. GI, 2012. 1617-5468.

[Gen07] Geneva State Government. State Council's Report to the Grand Council on the Geneva electronic voting project. Retrieved 02.12.2012 from `http://www.geneve.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf`, July 2007.

[Kot04] M. Kotadia. Porn gets spammers past Hotmail, Yahoo barriers. Retrieved 07.12.2012 from `http://news.cnet.com/2100-1023-5207290.html`, 2004.

[MM03] J. Malik and G. Mori. Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. In *CVPR'03 Proceedings of the 2003 IEEE computer society conference on Computer vision and pattern recognition*, pages 134 – 141, 2003.

[MMDC13] G. McDonald, L. Murchu, S. Doherty, and E. Chien. Stuxnet 0.5: The Missing Link. Retrieved 05.03.2013 from `http://www.symantec.com/connect/blogs/stuxnet-05-missing-link`, 02 2013.

[Net] Netragard. Netragard's Hacker Interface Device (HID). Retrieved 19.12.2012 from `http://pentest.snosoft.com/2011/06/24/netragards-hacker-interface-device-hid`.

[Sch06] Schweizer Bundesrat. Bericht über die Pilotprojekte zum Vote électronique (german), May 2006.

[Sta] State Chancellery of Geneva , Information Technology Centre of the State of Geneva. Uncovering the veil on Geneva's internet voting solution. Retrieved 12.11.2012 from `http://www.ge.ch/evoting/english/Uncovering_the_veil_a.asp`.

[Sta13] Staatskanzlei Genf. DAS GENFER VOTE ELECTRONIQUE PROJEKT (german). Retrieved 03.04.2013 from `http://www.geneve.ch/evoting/deutsch/doc/e-voting_all_web.pdf`, Mar 2013.

[Swi] Swiss Federal Department of Foreign Affairs. Information about Switzerland - Politics. Retrieved 06.12.2012 from `http://www.eda.admin.ch/eda/en/home/doc/infoch.html`.

[TMK03] A. Trechsel, F. Mendez, and R. Kies. REMOTE VOTING VIA THE INTERNET The Canton of Geneva pilot project. In *Secure Electronic Voting*, 2003.