Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting

Robert Krimmer

Melanie Volkamer

Working Paper Series on Electronic Voting and Participation
Nr. 01/2006

Editor:
E-Voting.CC: Competence Center for Electronic Voting and Participation

www.e-voting.cc/topics/wp/

e-voting.cc

Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting

Robert Krimmer

E-Voting.CC
Competence Center for Electronic Voting and Participation
Liechtensteinstrasse 143/3
A-1090 Vienna, Austria
r.krimmer@e-voting.cc

Melanie Volkamer

DFKI GmbH
Research in Artifical Intelligence
Stuhlsatzenhausweg 3
D-66123 Saarbrücken, Germany
volkamer@dfki.de

Abstract

Electronic Voting as one of the main applications of Electronic Democracy has come to the attention of many governments in their movement to modernize elections. Although very popular with many visionaries and politicians, there is a lot of controversy for the use of electronic means in elections. Especially in young democracies, so-called democracies in transition have to invite international election observer to raise the level of transparency and to calm discussions. There exists a lot of documentation and guidelines on the topic of election observation of paper based voting. As the observation of electronic voting processes is very new, there exists little to no experience with it. In this paper, the authors present a model how to detect threats to the voter's anonymity using common criteria methodology. The work is based on experience in the 2005 parliamentary elections in Venezuela as e-voting experts to audit the parliamentarian elections where e-voting machines with a voter verifiable audit trail were used. To do so, first give a background on electronic voting in Venezuela is given then the Common Criteria methodology is described and applied it to the e-voting process. Finally, they come up with the summarized model of how to observe elections with electronic voting machines.

Keywords

Electronic Voting, Observation, Anonymity, Common Criteria

This paper is the extended version of the paper accepted for the EGOV06 Conference in Krakow, Poland held from 4th to 7th September 2006 by the same authors.

1. Introduction

In the past few years, many governments have started to adopt computer-supported applications for their administrative processes; applications range from the simple download of forms to Internet-based submission of applications. Amongst these the most controversial application is electronic voting, which stands for the use of electronic means in elections.

Around the world, many experiments and reports on the use of electronic voting have been conducted. The several approaches can be categorized in: (1) countries conducting voting in small binding field trials (France, Switzerland, the United Kingdom); (2) countries conducting non-binding remote electronic voting tests (Austria, Denmark, Spain); (3) countries that have implemented voting machines (India, Ireland, Germany, the United States, Germany, Brazil, Venezuela); and (4) only Estonia implemented remote electronic voting in their 2005 local elections as a legally binding voting channel available to any voter to date [for an overview see 1].

Although worldwide approaches might be different in detail, all efforts still share criticism by the public concerning the lack of transparency of the machines or applications. Recent studies by Oostveen and van den Besselaar have shown that trust in the e-voting process is not dependent on the actual level of security but on the user's belief of how secure the system is [2]. This belief is largely dependent on the transparency of a system and here the "main challenge for electronic voting [lies in] the lack of transparency" [3].

Traditionally, countries that are considered to be young, or so-called transition democracies, are expected to invite international election observers to guarantee elections in accordance with international standards. There is a great deal of documentation and guidelines on this topic for how to observe traditional paper-based voting. As the observation of electronic voting processes is very new, there exists little experience with it.

The authors therefore develop a model for how to detect threats to the voter's anonymity based on experiences in the 2005 parliamentary elections in Venezuela, which used e-voting machines with a voter verifiable audit trail.

To do so, we first give a background on electronic voting in Venezuela, then describe the common criteria methodology and apply it to the e-voting process. Finally, we present the summarized model of how to observe elections with electronic voting machines.

2. Electronic Voting in Venezuela

The reasons for the high tensions when talking about e-voting projects are manifold. Amongst the most important reasons are in accordance to [4]: enabling mobility of the voters, facilitating the participation in elections from abroad, reducing costs, raising voter turnout by offering additional channels, widening access for citizens with disabilities, and delivering voting results reliably and more quickly..

In transition democracies the last two reasons are especially important as they promise to solve, on the one hand, problems with illiteracy of the population and, on the other hand, problems with infrastructure in regards to delivering the results in time. Technology alone cannot solve problems in education and infrastructure.

It is especially important to know which voting processes are intended to be supported by e-voting. The first voting machines date back to the end of the 19th century, and only served as an aid in counting the votes. By now, machines can support all three main voting processes: (1) the Pre-Election Phase: identification of the voter and checking eligibility; (2) the Election Phase: casting the vote; and (3) the Post-Election Phase: counting the votes.

The main challenge for any voting is to solve the problem of unequivocally identifying the voter's eligibility while at the same time guaranteeing their anonymity and still delivering an accurate and verifiable result.

This is especially challenging using an electronic medium. Both paper and electronic media share common problems in either controlled or uncontrolled environments. In the latter there is the shared problem of vote buying and vote coercion [5]. Due to these shared problems it is advisable to begin with a structured overview on the different forms of voting.

Environment / Medium	Controlled	Uncontrolled	
Paper	Polling Place	Postal Voting	Counting Machine
Electronic	Stand-Alone Electronic Voting Machine	Remote Electronic Voting (PC, Cell Phone)	Counting Machine
	Networked Electronic Voting Machine		
	Networked Kiosk Electronic Voting Machine		

Table 1: Forms of voting [6]

In the 2005 Venezuela parliamentary elections, networked electronic voting machines were used that consisted of two parts:

1. The Captahuella, which is a notebook with an attached fingerprint reader. The notebook has a database with a list of eligible voters and, if available, their fingerprints. The computers were used to identify the voter using their ID-card and to check the authenticity by comparing the fingerprint to the stored image. In case it was not available, it was captured for future comparisons. After the election was finished the machines were connected to the central server to upload the data on who voted and who did not. These machines were used only in part and for testing purposes.
2. The electronic voting machines, which were manufactured by Smartmatic, cast the votes of the voters. Each of the 27,000 polling stations were equipped with one such machine. After the end of the election each machine was connected to the central counting server using cell phones, landlines, or satellite connections to submit the votes to the server.

Figure 1: The Venezuelan networked E-Voting Machine

Although the machines were strictly separated, during the audits a flaw was found in the voting machines that would have allowed for reconstruction of the sequence the voters cast their votes. This led to the removal of the Captahuellas, as without them there was no automated way to register the sequence [7].

The problem with the feared secrecy of the vote was not the only problem in Venezuela, but one major outcome of the observation mission. In order to come to such results in a structured way this paper proposes a model on e-voting observation. We use common criteria methodology to develop possible threats to the voter's anonymity and then to deduct the tasks for the observers to detect them. Although in this paper the authors concentrate on networked electronic voting machines with connected identification and vote casting, as intended to be used in Venezuela, appropriate references for the situation for remote electronic voting are given.

3. Developing the Methodology on how to Observe E-Voting

For analyzing electronic voting threats, we use the methodology of the internationally accepted framework of the Common Criteria (CC) [8]. They are an international standard (ISO 15408) for computer security. The official name is "The Common Criteria for Information Technology Security Evaluation". Its purpose is to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims. The Common Criteria are improved continually. Now, the official Common Criteria is on version V2.3. Today many

nations (e.g., Germany, France, and the UK) have introduced the Common Criteria to define and certify IT security products and procedures. There is a growing list of nations that at least accept the CC-certificates (e.g., Austria, Spain, Greece, and Italy).
For our purpose, we work following the CC-structure similarly to a vulnerability and security analysis to:

1. define the security objective (i.e., what is to be protected),
2. analyse the possible threats (attacks) to these objectives,
3. approach these threats using functional or operation security functions,
4. and finally check what the observer can do to ensure that threats are handled properly.

The clear differentiation between the threats that have to be dealt with and the environment in which the system is run is a clear benefit from the common criteria formalization. This also helps formulate instructions to the observers.

3.1. Security Objectives

Electronic Voting and elections respectively have to meet the international election standards. Consequently, the security objectives for voting systems - either electronic or paper-based – have to be deduced from these standards. Here the main ones are the election principles that demand an election to ensure a free, secret, universal, and equal election. In this paper, we want to concentrate on election secrecy and election freedom, respectively. Only a voter who can cast an anonymous (secret) vote can cast their ballot without any coercion. The secrecy objective as such is a very general objective that can be split up in more precise objectives:

1. The E-Voting system must ensure that the link between the content of a vote and the voter be irreversible.
   More precisely, the secrecy of the vote has to be guaranteed during the casting, transfer, reception, collection, and tabulation of votes. Very important in this point is that the secrecy must also be ensured at any time in the future [9], at least when talking about parliamentary elections.
   None of the actors involved in the voting process (organizers, election officials, trusted third parties, voters, and attackers from inside and/or outside) is able to link the content of a vote to an identifiable voter.
2. No voter should be able to prove that he/she voted in a particular way, in order to prevent voter coercion and ballot buying.

For the following discussion, we will concentrate on the secrecy objectives, which are implicitly deduced from the important operational policy of the international election standards.
The central question an observer has during the whole voting process is whether or not an attacker has the possibility to link the voter to their vote and if so, how.

3.2. General Threats

The following description of threats includes all threats to the election secrecy against which specific protection within an E-Voting system or within its environment is required. The attacker needs points in the voting process at which he gets information about the voter and his ballot as well. Thus, there are several points at which the attacker can try to interact with the E-Voting System:

- The Act of Ballot Casting: the attacker could physically observe the voter casting their ballot at the voting terminal.
- The Electronic Ballot Casting Device: a 'Trojan horse' on the voting terminal.
- The Voting Protocol: sniffing on the network.
- The Electoral Server: depending on the applied voting protocol, the election servers are another attacking point.
- Other Anonymity Threats: the Voter Audit Trail could also be used to link a voter to their vote.

In general, there are four different possibilities to link the electronic voter ID to her electronic ballot. The simplest one would be messages consisting of both the voter ID and the ballot. Other possibilities are the protocol sequence and the time when the voter was identified and cast their vote, the IP addresses used to first send the voter ID and later the voter's ballot.

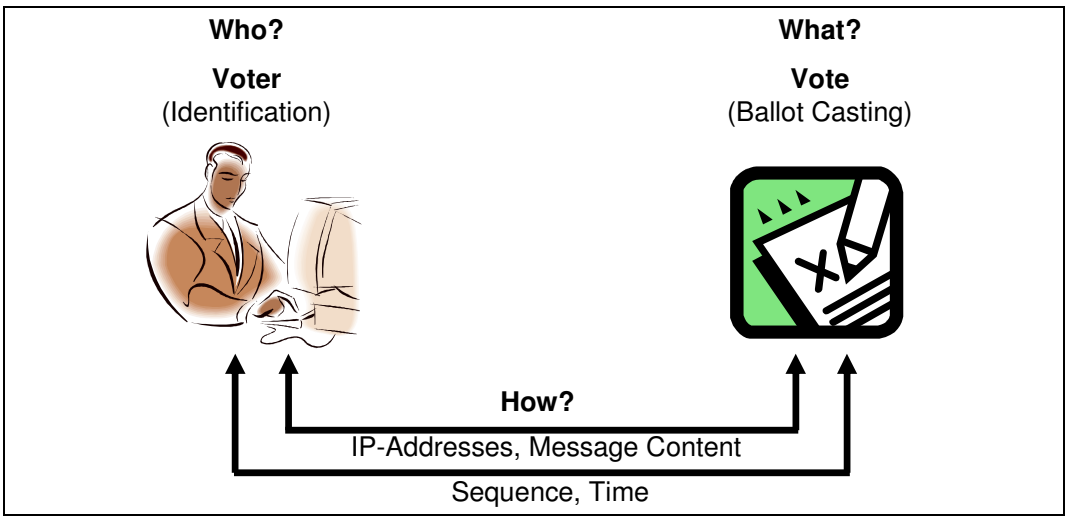

Figure 2: Ways the voter can be linked to their vote

3.3. Security Requirements

Thus, an E-Voting system has to meet several security requirements to overcome all these threats. There exist several catalogues of security requirements that have been deduced from all election principles. A good summery of relevant and common requirements can be found in [4]. In the following we will only take those into account that belong to the defined secrecy objectives. Here the generic requirement is defined as follows: "E-Voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote." [4, No. 16 in IV Secret suffrage] We will have a more detailed look as it is also done in the catalogues and divide the requirements in *functional (F)* and *the environment (E)*. The observer has to verify both; the first one with respect to the E-Voting system itself and the second group of requirements with respect to the environment in which the system is applied.

3.4. Observer's Tasks

The fourth and final step in our analysis is the definition of the observer's tasks to be done during their observation mission. These concrete measures provide a basic checklist for the observer to check if their observations are complete or if there is a situation or check that has not been thought of; thus completes our model to e-voting observation.

4. Analysis of the Threats to Voter's Anonymity

In the following we will discuss the threats and the attacks in more detail. Each threat is described in terms of an identified threat agent and the attack. Aspects such as expertise and available resources are addressed, as well as attack methods and any vulnerability exploited. We deduce the functional and environmental requirements to list what the observer shall verify with respect to either the technical system or the operational and organisational environment, and come up with recommendations for what to observe. Therefore, we will discuss each of the five general threats separately.

4.1. The Act of Ballot Casting and Anonymity

Threats. The most obvious threat to the voter's anonymity is given in the polling station. The attacker could observe the voter casting their ballot at the voting terminal. There are two possibilities to do so. First, the attacker can be physically present at the polling station and look over the voter's shoulder. This would be quite obvious. However, an attacker could observe the voter casting their ballot from distance, e.g., through the window (T1). Second, the attacker could have installed a camera that films the voter casting their vote in the polling booth. In particular, the monitor of the voting terminal is filmed (T2). Even if both

threats are not specific for Online-Voting - both are also applicable within traditional ballot casting - an observer has to take these into account.

Security Requirements. From threat (T1) and (T2), which are very similar from their ideas, we can deduce one requirement to the environment (E1): the terminal has to be applied in a secure environment with respect to personal and technical (e.g., camera) observation. Voters must not be able to observe each other and the electoral staff must not be able to observe the voter applying the election terminal (E2). There are special requirements for the position: e.g., the polling booth must not be situated next to a window in order to prevent observations from outside, or next to steps where everyone who goes up or down can see how the voter votes.

Observer Tasks. The election observer has to control whether or not there is a polling booth (C1). In addition, they must check whether or not the polling booth is shaped in a way that the voter can cast their ballot unobserved (C2). Moreover, the observer has to look for camera objectives (C3).

Remote. In the case of a remote E-Voting System, the election observer cannot avoid voters being observed when casting their ballot. In this case, the problem is comparable to the one with postal voting and should be treated in the same way [2] (e.g., as in Germany where postal voting is only allowed as an exception because the voter is ill or away on the Election Day).

4.2. The Electronic Ballot Casting Device and Anonymity

Threats. In general, the voting terminal/device in an E-Voting System for polling stations is some kind of computer (hardware and software components as well as an operating system). This computer must be connected to the Internet to check the voter's right to vote and to transmit the ballot. The main problem is that terminals know the voter's ID and the voter's decision in plaintext. Thus, the attacker could try to manipulate the terminal in order to either forward to himself the voter's ballot unencrypted together with the voter's ID or to store the information at the terminal. In the latter case, the attacker needs access to the terminal to get the stored data, e.g., after the election or during the election with the help of a memory device (simply burned on a CD at the terminal). The data (ballot and voter ID) can also be transmitted by other interfaces: e.g., Bluetooth or Infrared. Both forms of manipulation can be done by wrong voting software (T3) or by Trojan horses or other viruses (T4) on the voting device/ computer. The Trojan horse could sniff the data from the input devices (keyboard and/or mouse) to get the voter's ID and voting decision in order to transmit it to the attacker. Thus, available sniffing Trojan horses have "only" to be modified a little bit. In the first case, the attacker installs the wrong voting software – software whose user interface is similar to the correct one but with the additional function to transmit the ballot unencrypted, together with the voter's ID, to the attacker. The attacker has three possibilities to get the wrong software installed: first he could try to fake the delivered terminals by installing the wrong software. Second, in case he is an eligible voter he could try to change the software when he is (unobserved) in the polling booth. Last, he could try to substitute the correct software with the fake software by remote access via the Internet. Trojan horse or other malware could also either be installed at the delivered voting terminal, by an attacker who is an eligible voter and has access to the polling booth, or by unauthorized remote access. Thereby it is easier to get a Trojan horse installed on the terminal which just listens but not influence the process, than it is to substitute the whole or part of the voting software.

Security Requirements. The terminal's deployment and delivery to the polling booth must be organized in a way that manipulation is excluded (E3). There must be a possibility to check if the terminal is authorized (E4). In addition, the system must provide a function to verify if the right voting software is installed (F1).

Observer Tasks. Before the election itself the observer has to ask for the delivery procedure and verify it (C4). An observer has to check whether or not the terminal is correct and not modified. This has to be done before the election but also during the Election Day (C5). An analogous check for the correctness of the installed software has to be done before the election and several times during the Election Day (C6). First, the observer has to verify if the voting software ensures that the ballots and/or voter ID information is only sent encrypted and only addressed to the election servers. In addition, the respective information must be encrypted in a way that only the corresponding electoral server is able to decrypt the message. Moreover, it must be checked that the software does not store the

voter's ID and ballot on the terminal. In addition, the information deleted from these needs to be irreversible. This is so that an attacker who has access to the terminals after the election does not get any information by analyzing its databases, memory, and so on. Next, the election observer must have the possibility to verify if the software on the terminal is the one they checked and verified before. This could be done by a checksum generator. The observer must either check this value several times on the Election Day – in best case before each voter casts their ballot - or have the system offer a mechanism that automatically verifies if the correct software is installed. This software should also check if the whole terminal configuration is still satisfactory. In addition, the observer has to verify whether or not the terminal prevents unauthorized Internet access (C7) so that changing the software and the installation of malware can be excluded. To do so, they have to check:

- Are the applied Firewall and Virus Scanners state of the art? Are they correctly configured?
- Are only the needed communication ports open and all others blocked?
- Is the only software installed that which is needed?
- What kind of operating system is installed? The best case would be an operating system that separates the software in a way that different software does not influence each other.

Moreover, the election observer has to check whether or not an attacker has the possibility to modify the terminal by access in the polling booth (C8). So the terminal must only offer the voter/the attacker the possibility to authenticate and to cast a ballot. But it must not be made up of a whole keyboard and the voter cannot have the possibility to reboot the system. In addition, the voter/attacker must not have access to the hardware or any external interfaces like a drive. Additionally, the election observer must verify that the terminal does not have any external transmission interfaces like Bluetooth and infrared. All the named checks could be simplified and reduced by the application of Trusted Computing. The observer also has to check if all locally stored data is deleted after the election, using safe data disposal methods (C9).

Remote. Within remote E-Voting this is even more of a problem, because, in general, we cannot make any statements about the trustworthiness of arbitrary voter PCs; also, the voter's will not, in general, be able to verify or improve the trustworthiness self-dependently. In addition, the application of Trusted Computing is impossible because of the cost and usability point of views, at least at present.

4.3. The Voting Protocol and Anonymity

Threats. Another point to violate the voter's anonymity is sniffing on the Internet. The problem here is that the voter's ID, as well as their (encrypted) ballot, is sent over the Internet. The attack scenario is the following: the observer sniffs all voting protocol messages transmitted to the electoral server, stores this data in a database, and analyses it after the election (T5). He can sort the messages by their timestamp. Thus, though this they could know the whole protocol for each voter. But, the attacker does not know which message block can be assigned to which voter, because these messages are encrypted - encrypted with state-of-the-art encryption algorithms. The problem with respect to the anonymity requirement is that the chosen algorithms are classified to be secure for the present, but no statements for the future can be made. On the one hand, single protocol messages can always be decrypted by using adequate computational power; e.g., by Brute Force trials. On the other hand, all messages can be encrypted at an arbitrary time when someone finds a fast algorithm to decrypt messages without the knowledge of the secret key. Thus, depending on the attacker's computational power, they will be in a position to decrypt all or at least single encrypted ballot messages after the election. When this future date will be depends on the strength of the encryption function. At some point in the future the networking observer is able to link a decrypted ballot to a voter. Thus, temporal unlimited election secrecy is not ensured against such a network attacker. The chosen attack potential is quite high, but the attack is in general not impossible. At least within political elections we keep this in mind.

Security Requirements. The communication between the E-Voting clients and the servers should be done in a network that limits possibilities of external sniffing (E5).

Observer Tasks. So, the question to be answered by the election observer for the individual voting protocols is whether the sniffing attacker is able to link the decrypted vote to an identified voter or if he only gets decrypted ballot messages but cannot link these to single voters. Therefore, the time-

stamp must become useless. The election observer has to verify if the applied protocol and system setup prevents the violation of the voter's anonymity in an adequate way (C10). This could be done by a special secure network or the application of mixed networks. So, all protocol messages pass a mix or a mix cascade, which forwards several messages at the same time to the electoral server. Here the sniffing nodes are limited and the observer has to sniff on nodes before the first mix because the messages are made anonymous by mixing the messages. So it gets more difficult for the sniffing attacker because he cannot sniff at an arbitrary node. Time constraints are a problem with this approach. The mix will only start working when they receive several protocol messages. Thus, the voter in the polling booth can only continue when some other voters vote at the same point of time. Another possibility is to meet the anonymity problem on the protocol layer at the local storage of the ballots. The stored ballots are either transmitted at the end of the Election Day or they are transmitted in blocks of ballots as introduced in [10]. Within the latter solutions the election observer has to ensure that the software randomly mixes the ballots before storing them locally or sending them to the electoral server (C11) [4, 11].

Remote. The protocol analysis in [12] shows that the voting protocols for remote E-Voting do not ensure temporal unlimited election secrecy because of the bindings to the voter's IP-address. Here the observer has to check if an adequate solution is offered: e.g., multi-ballot casting with the option to cast the vote in the polling booth even if the voter has already cast an electronic vote (this improvement produces legal problems with respect to the equal election), the application of mix-networks to complicate sniffing, and separation between the voter verification phase and the ballot casting phase. Here the general idea is that the voter's IP-address is different for both phases. If the observer collects messages with the same IP-addresses, he does not know if both messages are from the same voter or not.

4.4. The Electoral Server and Anonymity

Threats. The election servers are yet another attacking point. The attacker could either attack both the election register as well as the ballot box. From the first server he might get the allocation [voter ID, terminal-number, time] and from the ballot box the allocation [terminal, time, ballot] or at least [terminal, time, encrypted-ballot]. With this knowledge the attacker can either directly allocate a voter ID to a ballot or be able to do so when they are able to decrypt the corresponding ballot (T6). Another possibility is that the attacker only gets access to the ballot box, but in addition they can observe who cast their vote at what time in a particular polling booth (this is possible because the polling station is a public place) (T7). Here the attacker allocates his observing knowledge [voter, terminal-number, time] with the allocation from the ballot box. In both cases the attacker is able to break the anonymity. Just like with the terminal security, the attacker could try to get physical access to the server or through the Internet. The attacker can try to transmit the information or get it through physical access (T8).

Security Requirements. The administration of both the E-Voting machines and the servers has to make sure no person is able to access the data (E6). In addition, the system must provide for a safe data disposal procedure at a reasonable time after the election (F2)

Observer Tasks. Researchers and system developers come up against this threat with organizational measures, e.g., access control based on the four-eyes-principle [13]. The election observer has to check if such concepts are implemented (C12). Additionally, he has to verify that the ballot box deletes information about time and the terminal in an irrevocable way (C13). So, only the ballot (or the encrypted data) is stored. To prevent access to the servers the server has to provide the same security measures as the terminal (C14). This has to be checked by the election observer. Furthermore, the observer has to check that all data on the respective systems are safely disposed ay a reasonable time after the election because the data stored in separate locations (registration and ballot box servers, clients) could be used to link the voter to the vote (C15).

4.5. Other Anonymity Threats: Voter Audit Trails

Threats. Some voting systems offer a voter audit trail [14] to increase the voter's confidence to the new election system. Hereby the voters get some information either on paper or through digital information. The voters check if the information on the paper is the same as on the E-Voting Machine and later put in a separate ballot box so a recount is possible. The problem is that the audit trail could be used by the voter to prove against their decision (T9). So the system could give the voter a possibility to break their own anonymity. Moreover, such an audit trail could be used for ballot buying. The voter could prove to the purchaser how they voted and then get money for it.

Security Requirements. The voting process in the polling station should be organized in a way that no voter can leave the station without putting the voter audit trail paper in a separate ballot box (E7). The system must provide a way that the voter audit paper proves the decision (F3).

Observer Tasks. In any voting system that provides a voter audit trail, the election observer has to check if the received recipe can be used to prove the decision (C16). This could be done either by cryptographic functions or by paper audit trail, which the voter has to put in the turn box before leaving the polling station. In the first case, the voter's decision can only be verified with the help of an electoral device, but otherwise not because the information is decrypted or it is stored on a device that can only be read by the electoral device. In the later case the paper ballots can be counted if there are problems with the E-Voting system or if someone mistrusts the electronic result. Further, the observers have to check the layout of the polling stations so no voter is able to take the audit paper with them (C17).

Remote. Here it is only possible to apply cryptographic alternatives in order to provide audit trails. A paper audit trail is not possible because of ballot buying and voter coercion with respect to the paper the voter would get at home. Here the chosen algorithm has to be verified with respect to anonymity leakage.

4.6. Overview of Threats, Security Requirements, and Observer Tasks

In the previous subchapters we analysed the possible places (act of ballot casting, electronic ballot casting device, the voting protocol, the electoral servers, and other anonymity threats like VVAT) where an attacker could try to deface the voter's secrecy. Now we try to contrast the threats and environmental and functional requirements to the observer's tasks in the table on the next page.

Place	Threats	Security Requirements	Observer tasks
Ballot Casting	**T1:** Observation from distance **T2:** Filming the casting	**E1:** Place E-Voting Machine in secure environment **E2:** Polling staff must not observe	**C1:** Is there a polling booth? **C2:** Is the booth unobservable? **C3:** Are there cameras?
Casting Device	**T3:** Wrong software **T4:** Trojan horses/viruses	**E3:** Secure deployment **E4:** Right terminal **F1:** Right software	**C4:** Check delivery procedure? **C5:** Right terminal? **C6:** Right software? **C7:** Unauthorized internet access? **C8:** Unauthorized access in polling station? **C9:** Safe disposal of local data?
Voting Protocol	**T5:** Sniffing and collecting data	**E5:** Secure communication	**C10:** Violation of anonymity protocol and system setup? **C11:** Random mixing of ballots?
Electoral Servers	**T6:** Breaking encryption **T7:** Allocating observation with data **T8:** Physical access	**E6:** No access to machines and servers possible **F2:** Safe data disposal	**C12:** Check for four-eye principle? **C13:** Deletion irrevocable? **C14:** Unauthorized access to server? **C15:** Safe data disposal?
Other Measures	**T9:** Use VVAT to prove decision to third parties	**E7:** Voter taking VVAT out of PS **F3:** VVAT must prove decision to voting machine	**C16:** Check if VVAT is proving a ballot right of the voting machine? **C17:** No voter taking VVAT along?

Table 2: Overview of observer tasks to check for anonymity

5. Conclusion

The method we presented here is based on the experience made in the Venezuelan election. The method presents a way to verify whether or not threats to voter's anonymity in an election using Electronic Voting Machines have been addressed adequately. Still, the described checks are difficult to perform as not all data might be available or not everything can be observed due to local traditions (as was the case in the above election).

It would help if the Electronic Voting Machines were certified and developed using common criteria. In this case the observers would only have to check the CC inspection report and security target of the machines to ensure that all necessary measures have been taken. Then the observer could concentrate on the polling stations and would not have to stick to software evaluations.

One point that is open for discussion is whether the observers should only check concepts or if they should also check the source code for the right implementation of the concepts. Further, the observer also has to define the attacker potential because this allows for elimination of some threats, as the attacker is not able to conduct the described attacks.

We are sure that this model of observing e-voting helps raise the transparency in elections using electronic devices and leads, in the end, hopefully to higher confidence of the voters in the democratic system.

References

1 **Buchsbaum, T. M. (2004): E-Voting: International Developments and Lessons Learnt, Proceedings of the ESF TED Workshop on Electronic Voting in Europe, Schloss Hofen/Bregenz, pp. 31-42.**

2 **Oostveen, A., van den Besselaar, P. (2005): Trust, Identity, and the Effects of Voting Technologies on Voting Behavior, Social Science Computer Review (23) 3, pp. 304-311.**

3 **Vollan, K. (2005): Observing Electronic Voting. NORDEM Report 15/2005.**

4 **Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Straßburg, 2004. www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf [retrieved on 9.2.2006]**

5 **Krimmer, R., Volkamer, M. (2005): Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In EGOV (Workshops and Posters), pp. 225-232.**

6 **Volkamer, M., Krimmer, R.: Die Online-Wahl auf dem Weg zum Durchbruch. Informatik Spektrum (2) 2006 (in print).**

7 **European Commission (2005): Final Report of the December 4th Election in Venezuela, Caracas, http://www.eueomvenezuela.org/final_statement_en.pdf [retrieved on 15.3.2006].**

8 **CC/ISO (1999): Common Criteria, Security Evaluation. Version 2.1, August 1999. ISO/IEC 15408:1999. And Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999. www.bsi.bund.de/cc/. See also www.commoncriteriaportal.org [retrieved on 9.2.2006]**

9 **Markus Ullmann and Frank Koob and Harald Kelter: Anonyme Online-Wahlen - Lösungsansätze für die Realisierung von Online-Wahlen .DUD * Datenschutz und Datensicherheit 22, 2001**

10 **Volkamer, M.; and Hutter, D. (2004): From Legal Principles to an Internet Voting System. In: Prosser, Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society. Workshop of the ESF TED Programme, 7-9 July 2004, Bregenz. Lecture Notes in Informatics, P-47, GI, Bonn 2004. 111-120.**

11 **Volkamer, M., Krimmer, R.: Secrecy forever? Analysis of Anonymity in Internet-based Voting Protocols, accepted for ARES2006, Vienna.**

12 **Physikalisch-Technische Bundesanstalt (PTB, 2004): Online Voting Systems for Nonparliamentary Elections – Catalogue of Requirements. Technical Paper PTB-8.5-2004-1, Berlin, April 2004. http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf [retrieved on 27.2.2006]**

13 **LDS Brandenburg (2000): Pflichtenheft und ergänzende Regelungen zur Durchführung der Simulation einer Personalratswahl im Internet, Potsdam, 5 pages.**

14 **Mercuri, R. (2001): Electronic Vote Tabulation: Checks & Balances, Dissertation, University of Pennsylvania, Philadelphia.**