Stockholm University

Security and Privacy in e-Government: Systems, IT, Laws and Ethics (SECGOV) VT2020

Course assignment II

E-voting in Venezuela: Threats and Countermeasures

Author:
Giorgio Ottolina - giot6166[at]student.su.se

Contents

1 Introduction and E-Voting in Venezuela

As far as e-voting in concerned, Venezuela, along with Germany, Ireland, India, the USA and Brazil, has successfully adopted voting machines. Nowadays these systems are able to support all three main voting processes:

1. **Pre-Election Phase**: the voter is identified and his/her eligibility is checked;
2. **Election Phase**: the vote is cast;
3. **Post-Election Phase**: the votes are finally counted

Electors' anonymity can be subjected to several threats; the 2005 parliamentary elections' experience in Venezuela is a perfect starting point to develop a model to detect them and to understand how to react. This essay will provide a background on e-voting in Venezuela, and then describe and apply common criteria methodology to it. The main reasons behind complexity of e-voting and the tensions it can cause tensions are [1]: electors' mobility; voters' participation in elections from abroad; costs' reduction; opportunities for people with disabilities; reliable and fast delivery of votes. Van Den Besselaar and Oostveen have recently shown in their studies that the most important factor as far as trust in the e-voting process is concerned, is users' confidence in the system's security, rather than its actual security level [2]. This confidence heavily depends on the system's transparency, so it is accurate to say that the "main challenge for electronic voting [lies in] the lack of transparency" [3]. E-voting needs to effectively address the issue of unequivocally identifying whether electors are eligible, while simultaneously assuring their anonymity and delivering a reliable and accurate result. Vote buying and coercion are also two problems that must be taken into consideration [4]. The aforementioned Common Criteria (CC) [5] methodology is the internationally recognized framework for dealing with e-voting threats and the international ISO 15408 standard for computer security. The Common Criteria structure can be followed in a similar way to a vulnerability analysis, in order to:

1. **Declare the security goals**;
2. **Identify and analyze all possible threats to these goals**;
3. **Counter attack the threats using operational or functional measures**;
4. **Address the actions that can be implemented by an observer to deal with the threats**

Instructions as to how the observers should behave are decided based on the threats to defeat and the kind of environment where the e-voting system runs.

2 Methods of Attacks, Threats and Countermeasures

There are several ways for hackers to compromise an electronic voting process. Since the following ones lead to unathorized system modifications, data tampering, thefts of information regarding voters and their ballots, and eventually new vulnerabilities that didn't even exist before, they are amongst the most serious that can be encountered:

1. **Spoofing and man in the middle attacks**: the hacker interferes between the legitimate communicating parties and simulates each one to the other;
2. **Denial of Service (DOS) attacks**: one or more devices are used to interrupt communication between a client and a server by flooding the target with more requests than it can handle;
3. **Trojan software and Distributed Denial of Service (DDOS) attacks**: software programs (daemons) are installed on terminals to perpetrate an attack;
4. **Packet Sniffing and Brute Force Attacks**: an attacker can view the confidential data from the database and take advantage of it to break through the server;
5. **Anonymity threats perpetrated exploiting the voter verified audit trails**

Let's now have a detailed look at some of the most important e-voting steps, the aforementioned threats and where the latter can possibly take place. Using Figure 1 from Module 2 Article 1 as a reference, and depending on who or what would be affected by the threats, each element of the list has been associated to the corresponding security architecture layer, where the security problems could happen and countermeasures should be implemented:

1. **The Act of Ballot Casting (Access and E-Government Layer - Citizens and channels)**:
    - **Threats**: The attacker could be physically present or observing the voter from distance.
    - **Countermeasures**: The voting terminal needs to run 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 can't observe the voter.
2. **The Electronic Ballot Casting Device (Access Layer - Voting terminals / Infrastructure Layer - Network and Servers)** - Trojan software on the voting terminal, DOS/ DDOS attacks, man in the middle, spoofing :
    - **Threats**: Since the terminals must be connected to the Internet, they know the voter's ID and his/her voting decision in plain text. Thus, the attacker could try to manipulate the terminal in order to either forward to himself the unencrypted voter's ballot and his/her ID or to store the information at the terminal itself, using wrong voting software or Trojan horses and being able to shut out the vote server and spoof the entire interaction with the voter acting as man in the middle.
    - **Countermeasures**: It must be possible to check whether the terminal is authorized. The system must also provide a function to verify whether the right voting software is installed.
3. **The Voting Protocol (E-business Layer - Databases / Infrastructure Layer - Network Infrastructure)** - sniffing on the network, brute force attacks:
    - **Threats**: The observer sniffs all voting protocol messages, stores them in a database and sorts them by their timestamp after the election. The attacker does not know which message block can be assigned to which voter, because the messages are encrypted with state-of-the-art encryption algorithms, but strong enough Brute Force trials can work anyway.
    - **Countermeasures**: Sniffing can be limited by a special secure network or by using mixed networks. All protocol messages pass a mix or a mix cascade, which forwards several of them to the server at the same time. The observer is then forced to sniff on nodes before the first mix, since messages are made anonymous because of it.
4. **The Electoral Server (Infrastructure Layer - Servers)** - depending on the voting protocol in use, the election servers could be another attacking point:
    - **Threats**: The attacker might get the allocation (voter ID, terminal number, time) from the first server and the allocation (terminal, time, ballot or at least encrypted ballot) from the ballot box, directly allocating a voter ID to a ballot.
    - **Countermeasures**: No one can have access to the data. Organizational measures, e.g., access control based on the four-eyes-principle [6] can be implemented though and they can be very effective.
5. **Other Anonymity Threats (Access and E-Government Layer - Citizens and channels)**: the Voter Audit Trail could be used to link a voter to their vote.
    - **Threats**: Some voting systems offer a voter audit trail [7] to increase the voter's confidence regarding their safety. Hereby the electors get some information either on paper or through digital information. They check whether the information on the paper is the same as on the E-Voting Machine and later they put it in a separate ballot box so that a recount is possible. The problem

is that the audit trail could be used to prove against the voters' decisions or for ballot buying.

- **Countermeasures**: The election observer has to check the accuracy of the received recipe and see if it can be used to prove the decision, either by applying cryptographic functions or by paper audit trail (which the voter has to put in the turn box before leaving the polling station).

3 Conclusion

The observations presented in this essay are based on the experience of the 2005 Venezuelan election: possible threats to voters' anonymity inside an e-voting process carried on using Electronic Voting Machines have been addressed adequately. Still, sometimes not all data might be available or legally observable due to local traditions or regulations. Below, a table illustration and recap of where the threats and countermeasures can occur is inserted.

Place	Threats	Security Requirements	Observer Tasks
Ballot Casting	• Observation from distance • Filming the casting	• Place E-Voting Machine in secure environment • Polling staff must not observe	• Is there a polling booth? • Is the booth unobservable? • Are there cameras?
Casting Device	• Wrong software • Trojan horses/viruses	• Secure deployment • Right terminal • Right software	• Check delivery procedure? • Right terminal? • Right software? • Unauthorized internet access? • Unauthorized access in polling station? • Safe disposal of local data?
Voting Protocol	• Sniffing and collecting data	• Secure communication	• Violation of anonymity protocol and system setup? • Random mixing of ballots?
Electoral Servers	• Breaking encryption • Allocating observation with data • Physical access	• No access to machines and servers is possible • Safe data disposal	• Check for four-eye principle? • Deletion irrevocable? • Unauthorized access to server? • Safe data disposal?
Other Measures	• Use VVAT (Voter Verified Audit Trail) to prove decision to third parties	• Voter taking VVAT out of PS • VVAT must prove decision to voting machine	• Check if VVAT is proving a ballot right of the voting machine? • No voter taking VVAT along?

I declare that I have followed the DSV Code of Honour.

References

[1] **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

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

[5] **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.* retrieved on 9.2.2006 from: www.bsi.bund.de/cc/. See also www.commoncriteriaportal.org

[6] **LDS Brandenburg** (2000). *Pflichtenheft under gänzende Regelungen zur Durchführung der Simulation einer Personal ratswahl im Internet, Potsdam, 5 pages.*

[7] **Mercuri, R** (20001). *Electronic Vote Tabulation: Checks Balances, Dissertation, University of Pennsylvania, Philadelphia.*