E-Voting System Security Optimization

Barbara Ondrisek
Vienna University of Technology
barbara.ondrisek@gmx.net

Abstract

Security of e-voting systems does not only depend on the voting protocol[1] *or the software used but concerns the whole system with all its components. To guarantee security a holistic approach, which considers all parts of such a complex system, has to be chosen. The security of an election system cannot be ensured unless every single element and its security-related characteristics, interfaces to other elements, and their impact on the whole system are examined.*

This paper presents the E-Voting System Security Optimization *method, which is based on such an approach and was developed to evaluate the security of e-voting systems. This method points out security flaws, shows security optimization potential, and can be used to compare different election systems. The methodology differs from other approaches insofar as it uses a holistic approach, visualizes the security situation of an e-voting system in a clear way, and shows its potential for improvement.*

1. Introduction

E-voting has been a very controversial topic ever since the presidential elections in the U.S. in 2000. Many security flaws were found [9, 7], the standards for the implementation of e-voting systems were shown to be too weak [1] and many (scientific) experts expressed their negative opinions on e-voting [18, 19, 20]. Nevertheless, efforts are still made to introduce e-voting in countries that use traditional paper ballots.

E-voting is an election method in which the votes are cast or collected electronically [21, p. 6]. A computer system whose main element is an software component that maps the voting procedure electronically is called an e-voting system. A *direct recording electronic* (DRE) machine is a special case of such a system as it implements all steps in the voting process, from registration and ballot casting to counting.

There are two different forms of voting: distance and presence voting [2, pp. 714]. In presence voting, a voter can cast his or her vote in a polling station under the supervision of the election's administration. Examples for presence voting are conventional elections in polling stations or voting with e-voting machines. In distance voting, the voter acts without the supervision of the electoral commission and casts his or her vote from a place other than a polling booth, such as casting absentee ballots via mail or internet voting.

1.1. Fundamental Election Rules, Suffrage, and Law

For e-voting systems the following legal principles are fundamental [22]:

universal suffrage: every person (restricted by age) may vote;

equality of votes: every vote counts the same;

free suffrage: voter’s autonomy of decision must be granted;

secrecy of votes: anonymity must be granted;

direct voting (vs. indirect voting): voting without intermediaries or electors must be granted;

personal right to vote: personal voting without representatives must be granted.

One rule outside of the canon of conventional election rules is essential for traditional voting procedures as well as for e-voting systems:

publicity and transparency: election observation and audit processes must be implemented.

If these rules are not followed strictly, the integrity of the election process is at risk and this can constitute a single point of failure for the democratic process. The e-voting system can be classified as unusable as soon as one of these election rules is disregarded.

2. E-Voting Systems

An e-voting system is a system consisting of mechanical, electromechanical, and electrical parts. It

[1] A voting protocol (also called “voting scheme” or “voting algorithm”) is defined as the general architecture of the software system (e.g. separation of issuance- and urn server) on the one hand and as the steps to complete a vote (e.g. first step authentication) on the other hand.

978-0-7695-3450-3/09 $25.00 © 2009 IEEE

contains software to control the devices, to define the ballots, to cast and count the votes, and to calculate and display the results.

The main tasks of e-voting systems are [25]:

registration: registration of the voters in a list or registry;

legitimation: identification, authentication, and authorization of users;

casting of votes: the electronic ballot is displayed and may be cast anonymously by a citizen;

collecting of votes: votes cast are collected by an urn server;

processing of votes: votes are processed and an election result is calculated and presented.

2.1. Elements of an E-Voting System

Similar to the separation into physical, syntactic, and semantic attacks [16], or into system hardware, system software, and the human operator of the system [17, p. 73], an e-voting system can be divided into three main categories: hardware, software, and human factors.

Therefore, the security-relevant elements are the following:

hardware: mechanical, electromechanical, and electrical parts;

software: operating system, drivers, compilers, programs, databases, rules used in the program, procedures and sequences (order of voting events, voting protocol, encryption techniques);

human factors: this category comprises usability, rules, strategies (e.g. information flow, security management), politics, and other diverse aspects such as transparency, acceptance, and trust.

All parts of the system have to be considered as equally important in terms of security risks.

3. Security of E-Voting Systems

Security is a fundamental criterion for the selection and use of electronically supported election systems. To assure security in e-voting systems, an integral approach that covers all parts of this complex system should be chosen. This method is also called *holistic security* [11]. In this approach, all elements of a system and all aspects of security, such as system stability, secrecy, integrity, availability, reliability, safety, and maintainability, also have to be considered.

3.1. Related Work

The Common Criteria standard is widely used for certification of the security of IT systems, but no protection profile for e-voting systems has been published so far. The Common Criteria is restricted to security and does not handle safety and other aspects of reliability. Guidelines such as the standards of the Council of Europe [4] or of the US Federal Election Commission [5] are steps in the right direction, but these regulations are not obligatory.

Studies published so far compared a selection of e-voting schemes on the grounds of different aspects of security [6, 15]. These papers dealt with the theoretical fundamentals of the electronic election process, but did not focus on the practical application in complex e-voting systems.

The *Test Process Improvement* (TPI®) model [23], a model for the improvement of the software test process, and the *Capability Maturity Model*© (CMM) [24] use methodologies for the assessment of systems that are similar to the EVSSO method, but they too have very different focuses.

3.2. A Method for Evaluation and Optimization of the Security of E-Voting Systems

The *E-Voting System Security Optimization* method was developed, taking into account detailed analyses of many e-voting systems and their problems and security flaws. This method is a tool for the optimization of the security of e-voting systems. It may be used to visually determine the level of maturity of security in an objective and detailed manner. Through its checklist-styled structure, the model enables the formulation of specific and practically realizable suggestions to optimize the safeguards of the tested e-voting systems.

EVSSO offers a generic measurement scheme and is therefore applicable to many different e-voting systems, especially DRE voting machines. It cannot be applied to internet election systems because they are inherently insecure (no secret or free suffrage, coercion and vote buying, denial of service attacks, no possibility for reasonable and authentic audit-mechanisms, and other risks) [3, 8, 12, 13].

3.3. Core Areas of the EVSSO Method

EVSSO evaluates various aspects of security. Through their assessment, strengths, and weaknesses of security measures can be pinpointed. These aspects are also called core areas and are associated with the three main categories of an e-voting system: hardware, software, and human factors.

Hardware:

- compliance with election principles
- safety
- physical security
- cryptography

Software:

- compliance with election principles
- data integrity
- cryptography
- transparency
- software engineering
- protection of software

Human factors:

- compliance with election principles
- security management
- user interface
- transparency
- organization of election
- validation of independent testing authorities

The EVSSO method is based on the fundamental legal principles of elections in European democracies but can be applied to most e-voting systems in democratic republics as most democracies have the same legal basis regarding elections.

3.4. Levels of the EVSSO Method

The EVSSO method describes 16 core areas, each of which is categorized into one of three levels. These levels are defined in a way that moving up from one level to a higher one constitutes a significant improvement of the quality of security.

The three levels are labeled A, B, and C. In some of the core areas only level A, or A and B, are defined, in other areas all three levels are applied. The criteria to meet a specific level are clearly defined for every core area. Some of the criteria for a certain level are detailed and contain many requirements which must be met in order to attain this level. Others are more compact. A detailed list of the criteria for meeting a certain level can be found in the appendix, chapter 6.

The core areas and levels are displayed in the EVSSO matrix (see figure 1) which visualizes priorities and dependencies of the levels.

By using this level system, the current situation of security can be clearly defined for every core area. This procedure also shows incremental improvements in the security of the assessed system by looking at the criteria of the higher level that was not reached.

Maturity level ***Core area***	0	1	2	3	4	5	6	7	8	9	10
1 Hardware - Compliance with Election Principles		A			B			C			
2 Hardware - Safety			A			B			C		
3 Hardware - Physical Security			A			B				C	
4 Hardware - Cryptography			A			B					
5 Software - Compliance with Election Principles		A			B						
6 Software - Data Integrity			A			B					
7 Software - Cryptography			A				B			C	
8 Software - Transparency				A				B			
9 Software - Software Engineering			A			B					C
10 Software - Protection of Software				A					B		C
11 Human Factors - Compliance with Election Principles		A			B						
12 Human Factors - Security Management				A				B			
13 Human Factors - User Interface			A		B						C
14 Human Factors - Transparency			A			B				C	
15 Human Factors - Organization of Election					A			B			
16 Human Factors - Validation of Independent Testing Authority							A				

Fig. 1: The EVSSO Matrix

For the evaluation of an e-voting system, a detailed checklist with criteria and qualifications for achieving a certain level is used. A level can only be reached if all of its requirements are met. If only some of the points of a higher level are accomplished but all conditions of a lower level are met, the core area has to be set to the latter one.

3.5. The EVSSO Matrix

The vertical axis of the matrix lists the core areas, the horizontal axis shows the maturity level the e-voting system was classified into. The maturity levels from 0 to 10 in the matrix are not numeric values for the security of an e-voting system but are merely used to position the different levels. The empty boxes mark the gap between the levels that have to be passed in order to achieve a higher level. A classification into more than one level (A, B, or C) at a time is not possible, i.e. it is not sufficient to meet only some criteria of the next higher level (e.g. B); as long as the voting system does not satisfy all criteria of B, it is classified as level A.

The positions of the levels present priorities and dependencies. The different levels are not equally important from the point of view of security; for example: level A of core area 5 is more important than level A of core area 15. These priorities are displayed through the EVSSO matrix. The levels of the core areas with higher priorities are placed to the right of the levels of core areas that are not as important.

The EVSSO matrix not only shows priorities but also dependencies among certain levels of various core areas. The levels of the core areas on the left hand side have a higher priority than the levels on the right hand side and the higher the priority, the greater the influence on the maturity of the security of the e-voting system is.

Dependencies between the levels are also expressed by the positions of the levels: some levels can only be reached after all conditions of another level are met. Such levels whose requirements have to be met first are positioned on the left hand side of the levels that depend on them.

In the EVSSO matrix, the different levels are mapped to a certain maturity level of security, of which there are ten. The categorization of the core areas shows the maturity level with respect to the quality of the e-voting system's security. Level C is always on the right hand side of level B and therefore higher than B, level B is higher than A. The security increases with the level. The higher (and more secure) the level, the more to the right it is placed. Integrity checks (a criterion in level B of core area 10) for instance only make sense after a certain standard of quality has been reached (level A of core area 9).

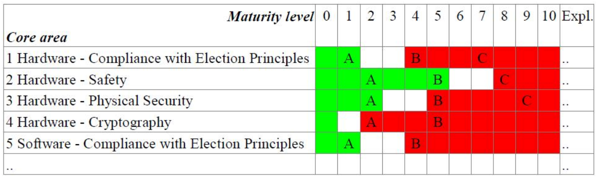
4. Evaluation of an E-Voting System with the EVSSO Method

An individual EVSSO matrix is filled out for every e-voting system by critically analyzing the system and determining the level of every single core area. The levels which have been reached are marked green in the matrix. The levels that have not been reached are marked red. The boxes between the levels are also colored. If a core area has not even reached level A, level 0 is marked green. The boxes between an achieved level and the next higher level are left blank (white) in order to show the gap between those levels.

For every core area, a short explanation should be given for why a certain level was reached. This enables others to understand the evaluation method and its conclusions.

A fictitious example for a filled-out EVSSO matrix is shown in figure 2.

The coloration of the matrix offers a clear description of the security situation of an e-voting system. Areas colored in red show optimization potential for the security of the assessed e-voting system, green areas show the accomplished maturity level of security.



Maturity level *Core area*	0	1	2	3	4	5	6	7	8	9	10	Expl.
1 Hardware - Compliance with Election Principles	🟩	🟩 A			🟥 B	🟥	🟥	🟥 C	🟥	🟥	🟥	..
2 Hardware - Safety	🟩	🟩	🟩 A	🟩	🟩	🟩 B			🟥 C	🟥	🟥	..
3 Hardware - Physical Security	🟩	🟩	🟩 A			🟥 B	🟥	🟥	🟥	🟥 C	🟥	..
4 Hardware - Cryptography	🟩		🟥 A	🟥	🟥	🟥 B	🟥	🟥	🟥	🟥	🟥	..
5 Software - Compliance with Election Principles	🟩	🟩 A			🟥 B	🟥	🟥	🟥	🟥	🟥	🟥	..
..												..

Fig. 2: Example of a filled-out EVSSO matrix after the assessment of an e-voting system

The maturity level can be read in the matrix by looking at the levels accomplished. A particular maturity level is reached when the column of this level contains only green or white boxes. In the example above, the maturity level is 1 because maturity level 1 is the right-most column not containing any red squares. The maturity level is just a means and not a numeric value for the system.

The necessary order for optimization measures can also be derived from the maturity level of the matrix. The vertical column containing the red squares is a checklist of requirements to be fulfilled in order to ascend to the next higher level. The matrix also shows the priority of the measures to be taken: by working from left to right in the diagram crucial measures are handled before less important ones.

In the example above, level A of core area 4 should be prioritized, because if this level is reached the maturity level of the e-voting system will take a leap and jump from 1 to 3. The objective of the optimization is to reach maturity level 10.

5. Conclusion

Security is a value that is difficult to evaluate as it is not easy to quantify. The method introduced offers a qualitative evaluation scheme that suggests specific steps for optimization and an increase in security of an e-voting system.

Besides a descriptive and simple visualization of the quality of security and a clear evaluation of an e-voting system, the matrix of the EVSSO method offers step-by-step optimization suggestions. The main purpose of the EVSSO matrix is to show the strengths and weaknesses of security measures of an e-voting system and to give a clear view of the security situation and possible optimizations. The requirements to meet a certain level provide general recommendations for improvements, from which specific measures can be derived.

Applying this method does not guarantee an improvement of security but it offers an approach to structure the necessary steps in a better way. The EVSSO method identifies security holes and vulnerabilities and offers suggestions to achieve a higher security level.

As of now, this method is a theoretical approach and has not yet been applied in a case study. It can be used as a basis for governmental certifications or a future Common Criteria protection profile.

One of the problems this method shows is the difficulty of defining security in specific terms. Security in elections supported electronically cannot be measured in absolute numbers. A system can never be considered 100 % secure because such a system can simply not be developed. In an environment as complex as this one, too many things have to be factored in, and in software development finding all bugs in any non-trivial application is virtually not achievable as it is [10].

6. Appendix

The appendix shows a short version of the EVSSO checklist. The long version of the list is available in [14, pp. 145-154].

1 Hardware - Compliance with Election Principles
Level A:

- secrecy of votes: no linear traceability or traceability by time
- secrecy of votes: use of polling booths

Level B:

- publicity and transparency: access to devices, storage media (cards), and their documentation granted before election
- limit access to devices and storage media during build-up or use

Level C:

- storage, locking, and sealing of devices and storage media, periodic controls and documentation of safety precautions
- secrecy of votes: protection from Tempest attacks and minimization of noise level

2 Hardware - Safety
Level A:

- correctness of construction
- homogeneous architecture
- safety of construction and installation
- availability

Level B:

- capacitance
- durability, reliability
- protection during transport and storage
- power supply

Level C:

- emergency plan
- absence of reaction

3 Hardware - Physical Security
Level A:

- protection from physical attacks
- no (possibility for an) internet connection
- removal of unused devices and interfaces
- access control for machines

Level B:

- protection of storage media: physical attacks, ability to remove modules, methods to identify copies

Level C:

- protection from (internal) Denial of Service Attacks, redundant systems
- setting of BIOS passwords

4 Hardware - Cryptography
Level A:

- use of secure anonymous connections for confidentiality
- telecommunications security for confidentiality and data integrity

Level B:

- hardware encryption of hard disks

5 Software - Compliance with Election Principles
Level A:

- general right to vote: correct collection of the voters' data in the voters' register
- equality of votes: one ballot per voter, every vote counts the same

- secrecy of votes: anonymous channels, encrypted connections, anonymous ballot casting to urn server

Level B:

- publicity and transparency: analysis of source code with peer reviews, plausibility of casting of votes
- public list of additional software used

Level C:

- publicity and transparency: analysis of source code of firmware, device drivers and used Commercial Off-the-Shelf (COTS) products used through peer reviews

6 Software - Data Integrity

Level A:

- correct implementation of vote storage, vote counting, and result display
- management and audit functions of application

Level B:

- protection of data and reliability: loss of data after crash of machine (backup systems)
- use of synchronized internal clocks of machines

7 Software - Cryptography

Level A:

- trusted paths / channels
- protection of user data and ballots
- use of asymmetric keys for identification, authentication, and authorization

Level B:

- use of strong up-to-date algorithms
- key management
- methods to recognize duplicates or manipulations of storage media

Level C:

- encryption of configuration files and databases

8 Software - Transparency

Level A:

- open source code for inspection by third parties, peer reviews
- repeated test elections prior to legally valid elections

Level B:

- test of COTS products and operating system
- internal error analysis system

9 Software - Software Engineering

Level A:

- quality management: reviews in every phase of development process
- risk management in planning phase
- traceability of anonymous votes
- user input checks
- interoperability with existing systems

Level B:

- quality management: automatic and manual testability
- implementation guidelines
- security tests and auditing after implementation: black box tests

Level C:

- team split-up: dual development
- security tests and auditing after implementation: review of security characteristics of application, white box tests, penetration tests
- code analyses (metrics)
- grant future interoperability by using open, not proprietary standards

10 Software - Protection of Software

Level A:

- homogeneous operation systems with up-to-date security updates
- no default passwords or PINs, strong passwords

Level B:

- version checks and checks of integrity of source code, of external (standard) libraries used, and of configuration files
- secure update mechanism
- uninstallation of unused pre-installed software
- scalability

Level C:

- authenticity checks of compiler
- protection from diverse software security risks
- protection from man-in-the-middle attacks

11 Human Factors - Compliance with Election Principles

Level A:

- free right to vote: neutral design of ballot and voting machine. The voter is able to cast an invalid vote (for no party / candidate).
- personal right to vote: vote personally without representative
- general right to vote: clarification and introductory training for voters in e-voting system

Level B:

- publicity and transparency: inspection of source code by electoral commission, access to voting machines, and verifiability with paper receipts

12 Human Factors - Security Management

Level A:

- introductory training for employees and creation of security plans
- security measure: dual control
- documentation of handling of software, hardware, and storage media for a permanent comprehensible control of all processes

Level B:

- background checks of employees
- security awareness trainings for all (external) employees

13 Human Factors - User Interface

Level A:

- representation of ballot on one screen page without scrolling
- order of parties / candidates has to correspond to order on paper ballot
- adequate representation of course of casting of votes
- no illegal interference with process of election
- privacy during voting
- correct representation of ballot
- feedback during and after casting of votes
- online help pages for every single step (context sensitive)
- acceptable response times of application

Level B:

- multilingualism
- magnification of screen (magnifying glass function) for visually impaired voters
- audio support for blind voters

Level C:

- usability checks with a representative test group

14 Human Factors - Transparency

Level A:

- provision of information on all topics of elections
- public announcement of district results
- possibility for independent election observation prior to, during, and after elections
- checks if number of ballots cast corresponds to number of voters who requested a ballot
- anonymous paper ballots

Level B:

- audit phase after election with lessons learned for next election
- comparison of exit polls of current and previous years
- definition of thresholds for manual recounts

Level C:

- voting protocol which can be discussed in public and that is publicly available, strong cryptographic algorithms

15 Human Factors - Organization of Election

Level A:

- registration for electronic voting should not be a stumbling block for citizens
- begin and end of electronic elections at the same time as for conventional elections
- prevention of delays of casting of votes
- parallel service: alternative voting with paper ballot is possible
- possibility of a test vote

Level B:

- acceptance and distribution (expense factor): absorption of costs by state / county

16 Human Factors - Validation of Independent Testing Authority

Level A:

- examination, certification or test of correctness and security by independent testing authorities (ITA)

7. References

[1] E. Barr, M. Bishop, and M. Gondree, “Fixing Federal E-Voting Standards”, Communications of the ACM, Volume 50, Issue 3 (March 2007). Emergency response information systems: emerging trends and technologies. COLUMN: Viewpoint. ACM, 2007, pp. 19-24.

[2] G. Brands, “IT-Sicherheitsmanagement - Protokolle, Netzwerksicherheit, Prozessorganisation” (German), Springer, 2005.

[3] S. Bruck, D. Jefferson, and R. Rivest, “A Modular Voting Architecture ("Frogs")”, Workshop on Trustworthy Elections WOTE '01, August 26-29, 2001, Marconi Conference Center, 2001.

[4] Council of Europe, “Legal, Operational And Technical Standards For E-voting”, Recommendation Rec(2004)11 30th of September 2004, Council of Europe Publishing, 2004.

[5] Federal Election Commission, “Voting System Standards. Volume I: Performance Standards”, U.S. Federal Election Commission, 2002.

[6] D. Gritzalis, “Secure Electronic Voting - New trends, new threats....”, 7th Computer Security Incidents Response Teams Workshop Syros, Greece, September 2002.

[7] B. Harris, “Black Box Voting: Ballot-Tampering in the 21st Century”, Talion Publishing, 2004.

[8] D. Jefferson, A. Rubin, B. Simons, and D. Wagner, “Analyzing internet voting security: An extensive assessment of a proposed internet-based voting system”, Communications of the ACM, Volume 47, Issue 10 (October 2004), pp. 59-64.

[9] T. Kohno, A. Stubblefield, and A. Rubin, “Analysis of an Electronic Voting System”, Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on 9-12 May 2004. IEEE, 2004, pp. 27-40.

[10] G. McGraw, “Software Security: Building Security in”, Addison-Wesley Professional, 2006, pp. 108.

[11] L. McLaughlin, “Interview: Holistic Security”, Security & Privacy Magazine, IEEE. Volume 3, Issue 3, IEEE, 2005, pp. 6-8.

[12] R. Mercuri, “A better ballot box?”, Spectrum, IEEE, Volume 39, Issue 10. 2002. pp. 46-50.

[13] Y. Mu, and V. Varadharajan, “Anonymous secure e-voting over a network”, Computer Security Applications Conference, 1998, 14th Annual Proceedings, pp. 293-299.

[14] B. Ondrisek, “Sicherheit elektronischer Wahlen“, (German) Publisher Dr. Müller, 2008.

[15] K. Sampigethaya, and R. Poovendran, “A framework and taxonomy for comparison of electronic voting schemes”, Computers & Security, Vol. 25, No. 2, Elsevier 2006, pp. 137-153.

[16] B. Schneier, “Inside risks: semantic network attacks”, Communications of the ACM, Volume 43, Issue 12 (December 2000), ACM, 2000, p. 168.

[17] I. Sommerville, “Software Engineering”, (German) 8. ed., Pearson Studium, 2007.

[18] M. Bishop, and D. Wagner, “Risks of e-voting“, Communications of the ACM, Volume 50, Issue 11. COLUMN: Inside risks. ACM, 2007, p. 120.

[19] D. Dill, B. Schneier, and B. Simons, “Voting and Technology: Who Gets to Count Your Vote?“, Communications of the ACM August 2003/Vol. 46, No. 8. ACM, 2003, pp. 29-31.

[20] Open Rights Group, “May 2007 Election Report - Findings of the Open Rights Group Election Observation Mission in Scotland and England“, 20 Juni 2007.

[21] Communications-Electronics Security Group, “E-Voting Security Study“, X/8833/4600/6/21, (Copyright The Crown) Issue 1.2 31 United Kingdom, 2002.

[22] European Commission for Democracy Through Law, “Code of Good Practice in Electoral Matters”, CDL-AD(2002)023rev, 18-19 October 2002.

[23] T. Koomen, and M. Pol, “Test Process Improvement. A Step-by-step Guide to Structured Testing”, Addison-Wesley Longman, 1999.

[24] W. Humphrey, “Managing the Software Process“. Addison-Wesley, 1989.

[25] L. Cranor, and R. Cytron, “Sensus: A security-conscious electronic polling system for the internet”, Proceedings of the Hawaii International Conference on System Sciences. Wailea, Hawaii, IEEE Computer Society Press (1997), pp. 561-570 vol.3.