UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

FB 4
Informatik

Security Requirements for Non-political Internet Voting

Rüdiger Grimm
Robert Krimmer
Nils Meißner
Kai Reinhard
Melanie Volkamer
Marcel Weinand
Jörg Helbach

Nr. 06/2007

Arbeitsberichte aus dem Fachbereich Informatik

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Paulus

Kontaktdaten der Verfasser

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: grimm@uni-koblenz.de

Security Requirements for Non-political Internet Voting

Authors: Grimm, Rüdiger (1); Krimmer, Robert (2); Meißner, Nils (3); Reinhard, Kai (4); Volkamer, Melanie (5); Weinand, Marcel (6); Helbach, Jörg (7)

Affiliations: (1) Universität Koblenz-Landau, (2) Wirtschaftsuniversität Wien, (3) PTB Berlin, (4) Micromata Kassel, (5) DFKI Saarbrücken, (6) BSI Bonn, (7) GI Bonn

A 10-pages extract of this report is published in: Krimmer, Robert (Ed): Electronic Voting 2006. Proceedings of the 2nd International Workshop on Electronic Voting, 2-4 Aug 2006, Bregenz. Lecture Notes on Informatics 86, 2006, pp.203-212.

Abstract

This paper describes the development of security requirements for non-political Internet voting. The practical background is our experience with the Internet voting within the *Gesellschaft für Informatik* (GI – Informatics Society) 2004 and 2005. The theoretical background is the international state-of-the-art of requirements about electronic voting, especially in the US and in Europe. A focus of this paper is on the user community driven standardization of security requirements by means of a Protection Profile of the international Common Criteria standard.

1 Starting with legal voting principles

At first sight, online-voting seems to be yet another security sensible Internet application like online-banking, online-shopping or online-auctions. But there is an important difference. Elections are a constitutional part of democracy. Therefore, the election process (paper or electronic) has to satisfy a specific set of technical requirements and especially of security requirements very strictly. In order to specify technical requirements for Internet voting, we proceed as follows. We start with the constitutional and legal aspects of elections in general, we refer to their origin and background, and from these legal aspects we deduce the requirements for online-voting.

While election laws are country specific, their principles and values are similar in all democracies. In Germany the constitution („Grundgesetz") and electoral laws demand elections to satisfy these five basic voting principles: elections have to be *universal*, *equal*, *free*, *secret* and *direct*. But what is the meaning of these five important terms? There are several interpretations with respect to online-voting, for example by Mitrou et al. (2003) and Volkamer/Hutter (2004). The meaning of the principles is as follows.

The principle of *universal* elections guarantees that every eligible voter can participate in the election. Moreover, no eligible voter can– directly or

indirectly – be excluded from the election. Thus, the technology must ensure access to the election for every eligible voter.

The principle of *equality* requires that all voters have equal voting rights. All cast ballots must have the same influence on the result, according to the principle „one voter, one vote". Moreover, all voters are able to vote in the same formal way. In particular, voters must have equal access to the election technology. Votes must be protected against loss and against unauthorized change or submission. On the side of the candidates, the principle of equality guarantees equal chances for all candidates. The registration, authentication, submission and counting mechanisms have to support this equality principle.

The principle of *free* elections requires that every voter casts his or her ballot free of duress and without unlawful and undue influence. This can be controlled only by casting the ballots in a polling booth. Nevertheless, in some countries postal voting is allowed (e.g. in Switzerland and in Germany) in order to ensure the universal election principle. Thereby the constitution accepts that voters may be observed or even forced (see Krimmer/Volkamer (2005) for a deeper discussion of this issue). Moreover, the election freedom requires that a voter is not influenced by leaking intermediate results of an ongoing election.

The principle of *secret* elections demands that only the voter is aware of his voting decision, which may never revealed to anybody else. Thus, nobody involved in the voting process will ever be able to link an identified voter to his ballot. Thereby the principle of secret elections is an essential precondition for free voting. In addition, to prevent external forces like blackmail, it must be ensured that a voter cannot prove his voting decision.

The principle of *direct* elections prevents someone from voting on behalf of other eligible voters and it forbids the use of an electoral college. This principle is not constitutional for every election system, e.g. the presidential elections in the USA are indirect.

The next step is to deduce technical requirements for an Internet voting system from these five legal principles, in order to comply with electoral laws. These requirements can be divided into functional and organizational requirements. A special subset of these requirements addresses security issues. Security requirements are particularly important for electronic voting and are thus in the focus of this paper.

Functional requirements for the services and tasks of an online-voting system are designed to support specific forms of elections and may change for each election. In general, functional requirements refer to the following issues: the form and appearance of the electronic ballots, the voting period, the

calculation and evaluation of the result, the supported voting clients, and the form of the electoral register.

Organizational requirements do not aim at the software or hardware technology but at the whole online-voting process. They contain the process instructions for the initiation and operation of the voting servers, the information policy for the voters, and the preparation of the electoral register. The orderly progress as well as the formal end of an election is also supported by organizational means.

Security requirements are related to the system structure and architecture. They are partly organizational and partly functional. Security requirements have two aims: they specify the undisturbed functioning of the voting process and they support the legal rights of all participants of an election. In some cases, security requirements have to take a balance between different (if not incompatible) rights such as the anonymity of voters versus the identification (and refusal) of unauthorised voters. Security requirements with respect to the undisturbed functioning are often invisible for the voters (but not for the administrators). Security requirements which support user rights, on the other hand, are not always invisible to voters, for example in that voters have to understand and explicitly use authentication mechanisms. Security requirements are, in general, common for all online-voting systems, in that they are determined by the democratic election principles.

Four security requirements can be deduced from the principles of an *equal* and *universal* election:

- First of all the voter must be identified and authenticated unambiguously to ensure that only eligible voters have the possibility to cast a vote. Moreover, the system must ensure that every voter can only cast one vote.
- The second requirement covers the integrity and authentication of the ballot. The online-voting system must ensure that any manipulation of an election such as the deletion and creation of ballots is detected. This requirement includes the casting, the transport and the storage of the ballots.
- Thirdly, ballots must not disappear in case of a server or client breakdown or in case of communication problems.
- The fourth requirement, which is mainly derived from the equality principle, refers to the correctness of the result calculation. In particular, it must be ensured that all cast ballots are counted.

Another class of requirements complies with the principles of a *secret* and *free* election:

- The secrecy must hold for the casting and transfer of ballots, as well as for the collection and tabulation of votes (ideally forever). It must also hold if a voting system offers receipts to voters.
- Neither the organizers, nor the election officials, nor any trusted third party, nor any voter should be able to link the content of a vote to an identifiable voter.
- Even with respect to the voter himself, the system must not give the voter any information which he can use to prove his vote.
- The voting system should not calculate or even reveal intermediary results.
- All secrecy requirements must be unconditionally ensured regardless of ongoing technological improvements.

The fifth principle of *direct* elections does not require any technical support by online voting systems. Indirect elections may be performed by an online system, as well. As a matter of course, however, any form of direct or indirect elections must be supported by organizational means.

The rest of the paper is organized as follows. Chapter 2 describes an early requirements work in Germany by the national metrology institute PTB. Chapter 3 is the main part of this paper and discusses the development of the requirements catalogue of the *Gesellschaft für Informatik* (GI – Informatics Society) during the real experience of Internet elections 2004 and 2005. In Chapter 4 we look at international initiatives on electronic voting. In chapter 5 we argue in favour of an international standard in order to formulate security requirements. We find the method of a protection profile according to the Common Criteria appropriate, which is described in chapter 6. In the last chapter 7 we draw conclusions from the work done so far and sketch our future work.

2 A first experience: the German PTB catalogue

In 1998 the German Ministry of Economics (BMWi) started the funding of the project „Wählen via Internet“ (Internet voting). The goals of the project were to tackle technical and legal problems and to develop a prototype of an Internet voting system called „i-vote“, in analogy to postal voting. During the project some test elections with i-vote were carried out, as well as the first legally binding election over the Internet at the University of Osnabrück in February 2000.

After the „i-vote“-project the BMWi funded the follow-up project „W.I.E.N. (2002-04) – Wählen in elektronischen Netzen“ (voting in electronic networks) starting in 2002. Main aspects of „W.I.E.N.“ were organisational

configuration, legal questions and acceptance research, as well as the further development of the technology. It was the aim to provide tested voting systems which allow safe and simple voting over open communication networks, networked polling places and portable devices. During the W.I.E.N. project further test elections with i-vote were executed, for example at a provincial state agency (Landesamt für Datenverarbeitung und Statistik, Brandenburg, LDS 2000) and at the Telecom branch T-Systems CSM.

To explore possibilities of quality enforcement for online voting systems in 2003 a project called „Development of concepts for testing and certification of online voting systems" was started at the national metrology institute (*Physikalisch-Technische Bundesanstalt*, PTB) also funded by the Federal Ministry of Economics. This project was to accompany the „W.I.E.N." project and had the explicit task to examine the i-vote system thoroughly. One of the first steps in the project was to develop a catalogue of requirements for online voting systems. During the project the requirements were discussed in two expert groups, namely „Testing and certification of online voting systems" and „Legal framework conditions for online voting" established by the funding Ministry of Economics.

In April 2004 the „Catalogue of Requirements of Online Voting Systems for Non-parliamentary Elections" was published (Hartmann/Meißner/Richter, PTB 2004).

The scope of the requirements catalogue covers legally prescribed, non-parliamentary elections such as, e.g., staff and workers council elections and shareholder elections. As a first step, the requirements assume that elections take place exclusively at networked polling stations under the organisational control of the elections administration. Applications allowing voting from home or any other private place are not included in the definition. In the catalogue the entire voting procedure has been divided into election phases: preparation of an election, the casting of ballots, the counting of votes. The requirements are defined independently of any system concepts. The requirements list includes the aspects IT quality and ergonomics, as well. However, these aspects are not visible as special categories.

The PTB catalogue was a first step to a requirements catalogue for e-voting. It didn't address the submission of votes across the Internet from home PCs. As this was the project aim of the GI, the PTB catalogue had to be extended. In the following chapter 3, the GI project for Internet voting will be described.

3 Practical experience with the GI (Informatics Society)

3.1 General Information about the GI and its elections

The *Gesellschaft für Informatik* (GI) is a society for computer science with presently about 24.000 members mainly from Germany. There are also associated memberships in Austria and Switzerland. It was set up in 1969 in Bonn. The rules for elections of the bodies of the GI are formally specified by the GI (GI 2003/2004). Since July 2003, the article 3.5.4 of the constitution of the GI allows the application of Internet voting. Here the precondition is that the Internet voting system provides the same security level as postal voting. In all cases where postal voting is admitted the election committee can decide to give members also the possibility to use an Internet voting system – as long as it is comparably secure. In summer 2004, the chairmanship (Präsidium) decided unanimously to offer both, postal voting and Internet voting for the chairmanship elections in December 2004. In order to generate a legally binding election, the GI adapted the election regulations (GI 2003/2004, 21-09-2004). The election was successful. As a consequence the persons in charge decided to apply Internet voting again in 2005 for the election of the chairmanship and of the executive board of the GI. Until now the GI has voted online twice and plans to do so again in 2006.

3.2 Election 2004

After a market survey the GI chairpersons decided to use the POLYAS system (Micromata 2005) for Internet voting. The POLYAS system provides two authorization schemes, one based on authentication with digital signatures, the other employs PINs instead. For better usability and simplicity, election PINs and personal user-ids were chosen for the GI election. Every GI member received a paper letter with the information material how to use the Internet voting system. In particular, the letter informed the member, that the user-id is the GI membership number. The PIN was printed on the letter and concealed by an opaque (not transparent) sticker on the letter. The user-id and election PIN was used for registration. Finally, the letter specified the URL for the Internet voting system. Every voter who did not want to cast her vote electronically could alternatively participate by using postal voting.

The GI established a group of security experts to accompany the pilot election and the future process of online voting in the GI. The group consists of German experts in IT-security and electronic voting from universities, the national metrology institute (PTB), and the executive board of the GI. This group examined the specification and the documentation of the system, in

particular with regard to data protection and manipulations. A main task of the expert group was to develop and enforce ad-hoc security requirements in cooperation with Micromata.

Micromata has done some minor changes on POLYAS to comply with the security requirements. Most security requirements could be met by organisational means. On a technical level, the following features were implemented

- audit proof archiving of the ballots preventing later manipulation of votes;
- separation of the electoral register from the ballot box; in particular, any shared marks were removed;
- SHA-signatures of software packages and result files.

The first election was a success. Over 5000 members used the online voting system. The participation was significantly better than in several years before.

3.3 Election 2005 – Restructuring the security requirements

In December 2004, the Internet voting expert group of the GI decided to develop a requirements catalogue for „Internet-based elections in societies". They agreed on two preconditions. Firstly, the security requirements must ensure a security level not less than that of postal voting. Secondly, the catalogue should be short and crisp and should not exceed six printed pages. Four requirements catalogues were already available and could be used as a basis for further development: Council of Europe 2004, SCC 38 2004, PTB 2004. After several iterations, a last version was published in (GI 2005).

The catalogue starts off with some preliminary notes and explicates assumptions under which any applied Internet voting system must ensure the security requirements. For example, it is assumed that the voter casts her ballot from an arbitrary Internet device connected to the Internet. Other assumptions are these: A non-secret name or a membership number (user-id) is applied for the voter identification. A secret alphanumeric password (one-time election PIN) is used for the voter authentication. The electronic ballot box and the electronic election register are installed on different servers. The two servers are located in different organisations. Postal voting is possible for every voter who does not want to cast an electronic ballot. The preliminary notes also define issues which are out-of-scope of the security requirements catalogue. For example, the candidate nomination and the maintenance of the list of eligible voters are not considered in the catalogue. Rules for a long-time storage of the election results are not addressed, either.

The catalogue of 2005 separates the *requirements on the system development* and on the *election execution* from those requirements on the Internet voting system itself. The requirements on the voting system itself are divided in requirements on the *election servers* and on the *election software.*

The *general requirements on the system development* contain requirements on the type and level of details of the system description, the security analysis and the manuals. There are especially strong requirements on the anonymity concepts. This category includes requirements on the development process, the system tests and the key management. The requirements on the *election execution* contain the distribution of the election PIN, the election register management and the installation as well as the de-installation of the voting system. The catalogue requires for the *election servers* to run a secure operating system, and to isolate the election software from all other applications. Only authorized persons may have access to the servers.

For the requirements on the *election software* the following categories were used.

- General requirements to an Internet voting system and its security
- Specific functional requirements to the Internet voting system
- Requirements with respect to the anonymity of votes
- Specific requirements to ensure a universal and equal election
- Ergonomic and usability requirements

The *general functional requirements* include the systems reliability and logging as well as the guarantee of consistent system states in case of any interruption. *Specific functional requirements* refer to the electronic register and to the electronic ballot box. *Requirements with respect to the anonymity* specify a *secret, equal and universal election*. The last category of requirements on the election software addresses *ergonomics and usability*.

3.4 Election 2005 – Meeting the requirements

On the basis of this agreed catalogue of requirements, Micromata was requested to explain how the POLYAS system ensures each of the requirements. Micromata has developed a new major release called POLYAS 2005 complying with the new catalogue of requirements. The main issues were:

- separation of the two servers, the ballot box and the election register;
- creation of a third server instance called the validator: the validator signs every entry of the electoral register before the elections starts; during the

voting process the validator checks this signature of every voter from the register before it enables the voter to cast his ballot;

- system recovery, e. g. after system errors or client aborts during the election;
- detection of manipulations without violating the confidentiality of the ballots;
- several mechanisms to minimize possible system attacks by both, external Internet users and internal corrupted administrators: e.g. a check sum of each vote, the storage of votes as readable text and not as a database reference, splitting up the keys in a passphrase and a secret key to support the four-eyes-principle, firewalls and a „secure" operating system.
- documentation of all technical and organisational solutions to accomplish the security requirements;
- anonymous creation of the voters' PINs for the print service provider.

The technical solutions concerning error handling, recovery mechanisms, manipulation and threat scenarios were documented in detail. Organisational security solutions are mostly based on the four-eyes–principle. At least two different persons must cooperate for administration of the systems, for starting the election application etc. The roles and responsibilities of the actors (management, administrators, voters, service providers etc.) are clearly specified in the documentation.

By applying the POLYAS system to the requirements catalogues we found out that several terms were used inconsistently. Thus, we developed a glossary including the terms election voting system, election voting software, ballot box, ballot box server, and authentication token.

The group of experts was extended due to growing challenges. Workshops in Kassel (home of Micromata) and Munich (home of one of the GI board members) revealed four new challenges:

1. *Source code inspection*: In order to increase trust in the decency of the software, and especially in order to identify undetected errors, Micromata and the GI expert group invited external experts to inspect the code of the POLYAS system. The inspection was not formal. Different experts of the GI community and of the PTB inspected parts of the code on their own choice and on the background of their personal engineering experience. The code proved to be well structured. However, a set of improvements were initiated.

2. *A simplified voters' guide* (GI/F-Secure 2005): The GI expert group specified a set of guidelines for online voters, which contains one page of general hints and thirteen easy-to-follow one-sentence rules for voters. The

guidelines do not provide the illusion of a 100 percent secure client (which does not exist), but helps users to better assess their security level and to improve it on their own responsibility.

3. *CC standardization of the requirements catalogue*: In order to standardize the findings on security requirements the Common Criteria (CC) is the suitable framework. The GI expert group founded a sub-group to specify a CC protection profile for the security requirements of online voting for private societies and other non-governmental organisations. The GI would be one application field of the protection profile. This issue is discussed in chapters 5 and 6 of this paper in more detail.

4. *A suitable comparison of online voting with postal voting*: Despite the regulation of the GI elections that the security of online voting must be at least on the level of postal voting, these two voting methods cannot be compared in every respect. There are pros and cons with both systems, and in some respect, online voting is even much more secure than postal voting. For example an Internet voting system has the possibility to send an acknowledgement to the voter which informs the voter that her ballot has been stored. With postal voting the voter cannot know exactly if or if not her ballot arrives at the electoral office in time or if it arrives at all. The enforcement of anonymity is another advantage of Internet voting. Electronic ballots can be encrypted safely. Within postal voting, in contrast, it is much easier to open the well marked election letters. For a deeper discussion of this issue see (Krimmer/Volkamer 2005).

3.5 The future of GI elections

The GI elections 2005 were a success, too. The participation was kept on the same improved level as 2004. There were no serious security attacks.

One problem was that the stickers on the paper letters were not as opaque as they should have been: very strong light was able to make the covered PINs visible. This is not a problem of the electronic system, but of the organizational implementation of the system. Another general problem is that a voting system must be able to handle differences between the number of voters that are registered as having voted and the number of votes in the ballot box. This may happen when messages between the servers get lost. The Polyas system offers protocol security mechanisms to detect such inconsistencies and fix them dynamically.

Plans for the next major release 2006 are:

- further improvement of the Internet voting protocol for a better system recovery after system failures;

- as an extension of the four-eyes-principle: implementation of an m-n threshold scheme for key distribution;
- support of EML (election markup language) for an easier configuration management;
- modified modules will help local chairs of GI subsections to administer their own elections.

Long term plans include the implementation of a rich voting client using bulletin board systems technologies. Rich voting clients allow for the implementation of security anchors in the hand of the voters.

As a consequence from this encouraging experience, the GI will continue to offer online voting to its members. Especially for the departments and working groups of the GI, online voting will be cheap, safe, and easy, and it will include much more members to execute their democratic right to elect their chairpersons.

4 International and European standards for e-voting

Discussions about the security of e-voting systems have often been led in a very emotional way. Following the falsification principle of Karl Popper the security of an e-voting system can never be proved but only perceived secure until proven otherwise. This, and the fact that anonymity in electronic processes is not an easy task, has led to numerous reports about erroneous and fraudulent e-voting systems. In order to reach confidence of the voters, developers and election operators have soon started to develop requirement documents which have often emerged to real standards. Note that electronic voting comprises the usage of voting machines and remote e-voting systems.

Germany was one of the first to have legal regulations concerning the use and testing of mechanical *voting machines*. The „Regulation of voting machines" (Germany 1975/1999) was set into place as a law on voting machines in 1975 and was changed in 1999 to allow for electronic voting machines. Currently only e-voting machines built by Nedap have passed the official tests by the German test authority PTB. These machines had been in discussion in Ireland for the national elections 2004. They are in use in several locations all over Germany. In the United States the use of voting machines is decided on a district level which makes national standards on those machines hard to push. Still the IEEE made an effort with the „Project 1583" (IEEE 2005) to develop such a standard in the aftermath of the 2000 Florida experiences. After a controversial debate about the draft standard, it finally was turned down and the working group is still trying to deliberate on the controversial issues.

For *remote electronic voting* one of the first discussions around requirements was the working group set up by US President Clinton in 2000 (Internet Policy Institute 2001). It took place during the Arizona Primaries which was the first political election to feature e-voting for participation by the general public. The report of this working group defined a number of quality criteria for remote e-voting software to be met for a successful usage. In the succession of the Arizona experiment another project evolved: the election mark-up language standard. This has been developed by companies engaged in e-voting under the umbrella of the standardization organisation OASIS (2005). In Germany the national metrology institute PTB developed a criteria catalogue for networked polling stations in order to support the W.I.E.N. project. (PTB 2004). It uses a similar methodology like the one used for voting machines. This catalogue may serve as a basis for evaluation of Internet voting systems in Germany.

The largest effort to come to a common understanding by a set of criteria for both, remote electronic voting and voting machines, has been conducted by the Council of Europe (2004). With the help of delegates from all 48 member states it has developed a set of legal, operational and technical standards on electronic voting. It is the most comprehensive and universal standard to date.

There are even many more collections of requirements with different foci. Nevertheless hardly any of the e-voting systems have ever been tested with reference to an international standard. The perceived security of the systems is most often based on some kind of an independent audit by experts. This lack of transparency can only be improved by proper documentation in the framework of an internationally accepted standard.

Without independent certification and appropriate documentation it is hard to observe the correct use of electronic voting systems. For example, elections in Venezuela had been under high observation, in 2004 by the US Carter Mission, and in 2005 by the European Commission. In both missions the lack of preparation and documentation of the e-voting system had been criticized (Venezuela 2004/2005). Finally an independent audit using a standard like the Common Criteria (CC/ISO 1999) is necessary. So far no electronic voting system is known to have been certified in this way.

5 The importance of standardized security requirements

Requirements establish a link between technology and its application in the reality. The link is two-fold: firstly, requirements express guidelines for developers of a technology how to implement it. Secondly, requirements

express guidelines for users and evaluators of an implemented system in order to examine if the implemented system does the right things.

Practically the evaluation phase is important for later updates. Mentally the evaluation phase is important to establish trust of the technology users. This is particularly important with respect to security requirements. Transparent evaluation of the security of a system is a basic means of trust.

During evaluation the requirements catalogue must be read and interpreted. Any inconsistency must be corrected. Hence, the language of a requirements catalogue must be understood by many different parties. If the party that orders a piece of technology is a huge customer, such as a bank or a car manufacturer, it might be sufficient to develop its own in-house structure of a requirements catalogue. However, if the application is not proprietary, but public, and if it is security-sensitive, then the need for a standardized requirements structure and language is inevitable. This is – no doubt – the case for Internet voting.

Internet voting may be restricted to non-public environments in a first approach. However, democratic decisions are based on the same principles in every environment, private or public. In the long run, Internet voting must be implemented on the basis of common rules and it must meet a common set of security requirements. The first requirements catalogues of e-voting were not standardized, but proprietary, such as (PTB 2004) and (GI 2005). In parallel semi-standardized requirements were specified, e.g. the European recommendations (Council of Europe 2004), and the rules of the IEEE community (IEEE 2005). But none of them is yet an accepted international standard across all voting environments.

Security requirements for Internet voting systems are not a static list of statements, but they must serve an iterative process of implementation and evaluation. It is both inefficient for the authors, and confusing for the readers to develop ad-hoc requirement formats, depending on the voting environment and on the system in use. In contrast, we need a standardized approach which is independent of concrete applications and systems. This would allow concrete Internet voting systems to be evaluated with respect to concrete Internet voting environments on a common set of criteria. This would allow applications to select appropriate systems for their specific environment. And it would convince users that the system they use are secure on a state-of-the-art level.

The common criteria (CC/ISO 1999) provide an internationally accepted framework which allow security requirements to be specified in the format of a so-called protection profile. Protection profiles are adapted to a specific technology independently of concrete applications, systems or products. A

protection profile can be used as a guideline to developers to learn which aspects must necessarily be implemented in their product. It can be used particularly well by evaluators to check and certify the security of a product. Security certificates of concrete products against a given protection profile make the security levels of the products comparable with one another and with the state-of-the-art.

The CC formalization provides additional advantages. There is a clear distinction between the threats which have to be countered by the voting system itself and the assumptions about the environment which is upheld by the technical and organisational infrastructure. This includes the definition of attack scenarios describing the attacker model (technical expertise, resources and motivation), the attack procedures (opportunity, methods and vulnerabilities), and the value of the attacked targets.

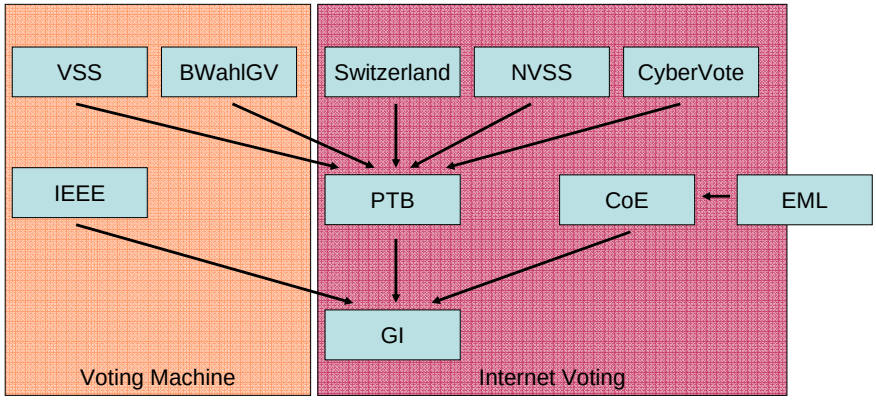

Figure 1: Influences of earlier requirements catalogues on later catalogues.[1]

[1] [VSS] Voting System Standards (USA), www.fec.gov, [BWahlGV] Bundeswahlgeräteverordnung 20. April 1999, Bonn 23.4.1999, S. 753 ff., [IEEE SCC 38 2005], [Switzerland] Verordnung über die politischen Rechte vom 24.5.1978/ 28.1.2003, www.admin.ch/ch/d/sr/161_11/, [NVSS] Network Voting System Standards (USA, 12.4.2002), www.fec.gov, [CYBERVOTE] IST-1999-20338, www.eucybervote.org/reports.html, [PTB 2004], [CoE] Council of Europe 2004, [EML] E-Vote Markup Language (OASIS 2005), [GI 2005].

Therefore we have decided to write a protection profile according to the common criteria in order to specify the security requirements of Internet voting. In a first approach, however, we will restrict the protection profile to non-public elections within private organisations. We expect that that the value of political elections is higher to attract potential attackers and, therefore, that the legal framework is stricter. The principles, however, remain the same for political and for non-political elections.

History shows that older requirements catalogues for electronic voting have influenced later catalogues, as is shown in figure 1.

6 The CC approach of protection profiles

6.1 History and world-wide acceptance of the common criteria

The Common Criteria (CC) is 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 users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims. Thus, the CC distinguishes three groups: the customer, the developer and the evaluator. Independent of these three groups a certification authority certifies the related statements.

The Common Criteria results from a standardization of national security criteria from different sources, starting with the „Orange Book" of the US DoD 1985. The criteria are improved continually. At the moment the official Common Criteria version is the version V2.3. Today many nations (e.g. Germany, France, UK) have introduced the Common Criteria to define and certify IT security products and procedures. There is a growing list of nations which at least accept the CC-certificates (e.g. Spain, Greece, Italy).

6.2 Common Criteria and Protection Profiles

The CC contains three parts: the Introduction and Common Model (part 1), the Security Functional Requirements (part 2), and the Security Assurance Requirements (part 3): There is also a related document, the „Common Evaluation Methodology" (CEM). The CEM guides an evaluator in applying the CC. They convert the assurance requirements of the CC to concret verification tasks. The CC defines two most important document types: the Protection Profile document (PP), and the Security Target document (ST).

A PP is a set of security requirements for a category of possible products, so-called Targets of Evaluation (TOE) that meet specific consumer needs. The requirements are independent of technical solutions, that is, PPs leave the technical implementation open. A PP distinguishes between *security functional* requirements and *security assuranc*e requirements, described in a very specific (semiformal) way defined by the CC. In addition there is a description part which describes the security concepts and the threats. In particular the description part maps requirements to the threats.

An ST document is to be created by a system developer, who identifies the security capabilities of his/her particular product. An ST may claim to implement zero or more PPs.

Both PPs and STs can go through a formal evaluation. The evaluation is done by an accredited laboratory. An evaluation of a Protection Profile is a pure document check. It simply ensures that the PP meets various syntactical and documentation rules as well as sanity checks. Therefore the evaluator has to check whether the set of requirements is exhaustive and self-contained. Successfully evaluated PPs are accredited by the German Federal Office of Information Security (BSI). Certificates for protection profiles are recognized and published internationally on the Common Criteria Portal.

A Security Target, in contrast, compares a concrete product with an ST document. The purpose of an ST evaluation is to ensure that the actual product (the TOE) meets the security functional requirements described in the Security Target. An ST can be based on one or more Protection Profiles if all included PPs are evaluated and if they have received a certificate of compliance. The evaluation insensitivity of the related TOE depends on the Evaluation Assurance Level (EAL), fixed as a minimum level in the ST or PP. The CCs predefine seven test depths (EALs) whereby Level 1 is the lowest and Level 7 the highest level. Level 4 is the highest level for typical commercial products and includes the source code evaluation. From level 5 and higher we need more and more formal specification documents.

6.3 The structure of Protection Profiles

A Protection Profile contains seven main parts: the Introduction, the TOE Description, the Security Environment, the Security Objectives, the Security Requirements, the Application Notes and the Rationales. A PP starts with the introduction part which contains document management and overview information. This part should help a potential user of the PP to determine whether the PP is of interest or not. The TOE description provides context for the evaluation to improve the understanding of the security requirements. The statement of TOE security environment shall describe the security aspects of the environment in which the TOE is intended to be used and the manner in which it

is expected to be employed, i.e. assumptions about the environment, threats, and organisational security policies OSP (the OSP cover all regulations or laws which have to be supported by the TOE) . The statement of security objectives are deduced from the security environment. The security requirements part of the PP defines the detailed IT security requirements to be satisfied by the TOE or its environment. The security requirements are the text blocks predefined in the CC-catalogue. The application notes are optional. They may contain additional supporting information about the construction, evaluation, or use of the TOE. The rationales part of the PP presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. This is a self check chapter for the PP editor.

6.4 Expected effect and limits

The CC are a tool to build documents like PPs in a very high quality way as „standard documents". The description language of Common Criteria is internationally harmonized. As a consequence, any CC conformant description of the security is unique and may therefore be better understood. International standards like the CC allow the *product providers* to sell their products on the international market. There are advantages for *customers* as well: The normalized products are easier to compare. This is particularly true for the Protection Profile concept. The evaluated and certificated Protection Profiles are registered, available and accepted on an international level. Thus, by developing a PP the author can influence or even set up international standards. The PP concept offers the customers the possibility to define their security requirements and standards for products. Product *developers* enjoy the advantage to read the customers' requirements in a unique way. Thus, they are able to implement products that meet the customers' needs. Finally, the security *evaluation of a product* is much *cheaper* if it is based on a certified PP.

On the other hand, there are also limits of the Common Criteria. The quality of basic security mechanisms such as single cryptographic mechanisms cannot be certified by the CC. Usability and ergonomic requirements are other important aspects of security which are not covered by the Common Criteria. Electromagnetic radiation and physical requirements are no themes in the CC.

7 Summary and Conclusion

Internet voting has to guarantee the anonymity of voters and the authenticity of their votes. These two security requirements seem to be contradictory, but in fact they are not. Early solutions by homomorphic cryptographic functions or

blind signatures have fascinated the academic community. However, related solutions were not accepted by a broad user community. Therefore, the German „Gesellschaft für Informatik" (GI) has decided to learn from earlier experiences and to try out a simpler version of Internet voting. Voter authentication was based on PINs and TANs, and the integrity of the polling administration was enforced by an organizational separation-of-duty concept. It was completely clear from the very beginning of the project 2004 that the system must satisfy a high level of usability and transparency. In order to make this project serious, the GI – together with a professional system provider – developed an existing solution further and performed two elections electronically with the system while it was developed.

Besides other measures to improve security and transparency like source code inspection and usage guidelines, a set of security requirements was formulated and refined by public and expert discussion. A simple iterative process of formulating requirements on the basis of growing experiences will soon develop its own language and thus understanding will be limited to the regional community of project participants. But voting is not a local application. Voting principles are basically the same in all democratic societies of the world. Therefore, it makes sense to formulate the security requirements in a way that the international community can share the experience and take influence. A standardized way of security requirements created by a user community is given by the instrument of a Protection Profile of the Common Criteria (CC/ISO 1999).

We have initiated a working group to work on such a Protection Profile. As a first step we restrict ourselves to non-political elections. Realistic applications are groups which have a need for decisions but do not often meet physically. Examples in the academic community are IFIP technical committees and working groups, IETF and W3C committees, and distributed project teams. In the economic life staff and workers councils and shareholder groups could profit from Internet voting. We expect a first published version of a Protection Profile for non-political Internet voting by late summer 2006.

References

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 [6.4.2006]

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. http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-

voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf [6.4.2006]

Department of Defence Standard: Trusted Computer System Evaluation Criteria (DoD 1985): Orange Book. DoD 5200.28-STD of December 1985. Departement of Defence, Washington D.C. 1985.

Germany (1975/1999): Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland („Regulation of voting machines for elections of the German and European parliament"), 03-09-1975, last update 20. 4.1999, http://bundesrecht.juris.de/bundesrecht/bwahlgv/ [6.4.2006]

Gesellschaft für Informatik (GI, 2003/2004): Satzung der GI („Constitution of GI"), Bonn, 2003-07-21. http://www.gi-ev.de/wir-ueber-uns/unsere-grundsaetze/satzung/ [download 06 Jan 2006]. And Wahlordnung der GI („Regulation of Voting for GI"), 2004-09-21, Bonn, http://www.gi-ev.de/wir-ueber-uns/leitung/wahlen-und-ordnungen/ [6.4.2006].

Gesellschaft für Informatik (GI, 2005): GI-Anforderungen an Internetbasierte Vereinswahlen („GI requirements for Internet based elections in non-governmental organisations"). 4. August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf [6.4.2006]

Gesellschaft für Informatik und F-Secure Deutschland (GI/F-Secure 2005): Information für GI-Mitglieder zu möglichen Sicherheitsproblemen auf Clientseite bei Vorstands- und Präsidiumswahlen mit dem Online-Wahlverfahren. („Information about possible security problems for clients of online-voting").

IEEE Standards Coordinating Committee 38 (SCC 38, 2005): Voting Standards. Project 1583 – Voting Equipment Standard; and Project 1622 – Electronic Data Interchange. http://grouper.ieee.org/groups/scc38/index.htm [6.4.2006]

Internet Policy Institute (2001): Report on the National Workshop on Internet Voting, Issues and Research Agenda. March 2001. http://news.findlaw.com/hdocs/docs/election2000/nsfe-voterprt.pdf [6.4.2006]

i-vote (2002): i-vote Report. Chancen, Möglichkeiten und Gefahren der Internet-Wahl („Opportunities and risks of Internet voting"). Online Report of the Universität Osnabrück, UOS 2004. www.wahlkreis300.net/fgiw/uploader/data/Kurzfassung.pdf [6.4.2006]. See also Homepage of Research Group Internet Voting: www.internetwahlen.de/ [6.4.2006].

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

Landesamt für Datenverarbeitung und Statistik, Brandenburg (LDS, 2000): Bericht zur Personalratswahlsimulation via Internet („simulation of the elections of the employees' representatives"). 2000. www.brandenburg.de/evoting/dokumente/evoting_int.pdf [6.4.2006]

Micromata (2005): Polyas Online Voting Solutions – Online-Wahlen für Verbände und Vereine. Kassel. http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf [6.4.2006]

Mitrou, L.; Critzalis, D.; Katsikas, S.; and Quirchmayr, G. (2003): Electronic voting: Constitutional and legal requirements, and their technical implications. In D. Gritzalis (Ed.), Secure electronic voting. The Netherlands. Kluwer Academic, 2003. 43-62.

OASIS (2005), Election Markup Language v.4. Last modified: January 24, 2005. http://xml.coverpages.org/eml.html [6.4.2006]

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 [6.4.2006]

Venezuela (2004/2005): Carter Mission in Venezuela (2004), Carter Center, Washington D.C., http://www.cartercenter.org/doc2020.htm. And European Commission (2005): Preliminary Report of the December 4th Election in Venezuela, Caracas, 2005, http://www.eueomvenezuela.org/pre_statement_en.pdf [6.4.2006]

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.

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik
(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 06/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß: „grUML – Eine UML-basierte Medellierungssprache für T-Graphen“, Arbeitsberichte aus dem Fachbereich Informatik, 05/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 04/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik,03/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik,02/2007

Anastasia Meletiadou, J.Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 01/2007

„Gelbe Reihe“
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005