GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of "Seminars", "Proceedings", "Monographs" and "Dissertation Award", current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: http://www.gi-ev.de/service/publikationen/lni/

Robert Krimmer (Ed.): Electronic Voting 2006

GI-Edition

Lecture Notes in Informatics

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2nd to 4th of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.

P-86

Proceedings

Security Requirements for Non-political Internet Voting

Grimm, Rüdiger[1]; Krimmer, Robert[2]; Meißner, Nils[3]; Reinhard, Kai[4];
Volkamer, Melanie[5]; Weinand, Marcel[6]; Helbach, Jörg[7]

[1]Universität Koblenz-Landau; [2]Wirtschaftsuniversität Wien; [3]PTB Berlin;
[4]Micromata Kassel; [5]DFKI Saarbrücken; [6]BSI Bonn; [7]GI Bonn
for further questions: grimm@uni-koblenz.de

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 Europe and in the US. 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. An extended version of this article (20 pages) is published as technical report by the University in Koblenz (see reference list).

1 The GI and its election 2004

The Gesellschaft für Informatik (GI) is a society for computer science with presently about 24.000 members mainly from Germany. The rules for elections of the bodies of the GI are formally specified by the GI [GI03; GI04]. 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. 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.

After a market survey the GI chairpersons decided to use the POLYAS system [MM05] for Internet voting. The POLYAS system provides two authorization schemes, one based on authentication with digital signatures, the other employs PINs and user-ids 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 election and the future process of Internet voting in 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.

Over 5000 members used the Internet voting system. The participation was significantly better than in several years before.

2 GI 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: [CoE04; SCC04; PTB04]. After several iterations, a last version was published in [GI05].

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 GI 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 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.

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 Physikalisch-Technische

Bundesanstalt (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 [GIFS05]: 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 Internet 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 Internet voting with postal voting: Despite the regulation of the GI elections that the security of Internet 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, Internet 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 [KrVo05].

4 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 Internet voting to its members. Especially for the departments and working groups of the GI, Internet voting will be cheap, safe, and easy, and it will include much more members to execute their democratic right to elect their chairpersons.

5 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" [DE75; DE99] 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" [IEEE05] 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 [IPI01]. 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 [EML05]. 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 04]. 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 [CoE04]. 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 checked 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.

6 The CC approach of protection profiles

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).

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 assurance 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.

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.

The CC is a tool to build standard documents. The evaluated and certificated Protection Profiles are registered, available and accepted on an international level. The PP concept offers the customers the possibility to define their security requirements and standards for products. Thus, product developers are able to implement products that meet the customers' needs.

7 Summary and Conclusions

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. 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. 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 [ISO99].

We have initiated a working group to work on such a Protection Profile. 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

[CC99] 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]

[CoE04] 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]

[DE75] 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

[DE99] Update 1999 of Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, Last update 20. 4.1999, http://bundesrecht.juris.de/bundesrecht/bwahlgv/ [6.4.2006]

[EML05] OASIS: Election Markup Language v.4. Last modified: January 24, 2005. http://xml.coverpages.org/eml.html [6.4.2006]

[GI03] 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].

[GI04] 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].

[GI05] 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]

[GIFS05] Gesellschaft für Informatik and F-Secure Deutschland: 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“), 2005.

[Grim06] Grimm et al. (2006): Security Requirements for Non-political Internet Voting. An extended version (20 pages) of this article is published as technical report by the Institute for Information Systems Research of the University in Koblenz. 2006. http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGGrimm/Downloads [21.4.2006]

[IPI01] 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]

[KrVo05] Krimmer, R.; and Volkamer, M.: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In EGOV (Workshops and Posters), 2005. 225-232.

[MM05] Polyas Online Voting Solutions – Online-Wahlen für Verbände und Vereine. Kassel. http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf [6.4.2006]

[PTB04] 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]

[SCC05] 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]