Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria

Andreas Ehringfeld[1], Larissa Naber[1], Thomas Grechenig[1],
Robert Krimmer[2], Markus Traxl[3], Gerald Fischer[1]

[1]Vienna University of Technology
Industrial Software (INSO)
1040 Vienna, Austria
{firstname.lastname}@inso.tuwien.ac.at

[2]E-Voting.CC gGmbH
Competence Center for Electronic Voting and Participation
1190 Vienna, Austria
r.krimmer@e-voting.cc

[3]Institut für Verwaltungsmanagement
6020 Innsbruck, Austria
markus.traxl@verwaltungsmanagment.at

Abstract: This paper discusses the recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting in light of the various attacks against the 2009 Austrian federation of students election. This election was the first instance of e-voting being implemented in a legally binding election in Austria. The question is if the recommendation published in 2004 is sufficient to handle real-world attacks against elections using e-voting. Based on the experience gained, several amendments to the recommendation are described.

1 Introduction

According to [BSSL01] and [SZKK88] regular re-evaluation and re-assessment are fundamental security principles. The recommendation Rec(2004)11 on legal, operational and technical standards for e-voting [Rec04] of the Committee of Ministers to member states was developed by [CEIP04] between 2002 and 2004 and remained unchanged so far.

The effectiveness of Rec(2004)11 is analyzed based on the experience of a recent e-voting election, which suffered from various different attacks such as the first Denial of Service attack (DoS) against a legally binding electronic election worldwide.

1.1 Case Study: 2009 Austrian Federation of Students Elections

The Austrian federation of students elections (*Hochschülerinnen- und Hochschülerschaftswahlen*) takes place every two years. Of the 240,000 eligible voters only about 30% participate in the voting (average for the past thirty-six years). The voting period is three days long during which students at all universities in Austria can cast their votes. Prior to the 2009 election, paper-based voting was the only channel.

The idea using electronic voting for the federation of students election was first introduced in May 2000 by the national federation of students. As a consequence of [OeH00], the federation of students law was adapted to allow for the possibility of remote voting like e-voting or postal voting. This amendment led to an evaluation project [EV07] with the heads of the national federation of students and members of the Austrian ministry for science, focusing on e-voting at the University of Economics in Vienna.

In May 2007, the minister for science and research announced that e-voting would be an additional voting channel in the 2009 federation of students election. The project's goal was to enable students (such as students currently abroad) to cast their votes from home.

Four months later, the national federation of students published a statement in [OeH07] summarizing their objections to e-voting and concluding that the technology conflicts with the idea of a free and secret ballot. Despite the fact that the threats concerning e-voting are similar to those in almost all other modes of voting, especially all modes of remote voting (e.g., [AH04] and [AH08]), e-voting (and the risks involved) became a very controversial topic and thus one of the major topics of most election campaigns [OHER10].

Other than federation of students' resistance, the federation of students election made for a very good field study because it has a very high organizational complexity, despite the small number of potential voters (260,000), with more than 400 individual voting options across the twenty-one participating universities. The required technical skill and in-depth knowledge of the election process can rival any other Austrian election.

1.2 Methodology

The Edwards Deming Plan-Do-Check-Act Cycle (PDCA Cycle) [ED50] can be employed to improve upon Rec(2004)11.

Plan (Hypothesis): The question is whether the recommendations in Rec(2004)11 are sufficient to handle state-of-the-art real world attacks.

Do (Experiment): The 2009 Austrian federation of students election was chosen for this analysis because it is a recent example of a legally binding e-voting election, which used the Rec(2004)11 as a benchmark in the certification process and caused much controversy, which guarantees a high number of skilled attacks. The voter base - students - are skilled, creative, personally motivated, and equipped with both technical resources and enough time to plan and execute attacks. This makes them a force to reckon with.

Check (Evaluation): The various attacks during the electronic voting period are described; countermeasures are explained and related to the recommendations in Rec(2004)11. Identified gaps are analyzed and conclusions drawn. Potential amendments for further improvement of Rec(2004)11 are presented.

Act: The final step in the Deming Cycle lies within the biennial review cycle of Rec(2004)11 where additional recommendations and updates are discussed in detail.

1.3 Related Work

Related work deals with security relevant aspects of e-voting from different views. The legal bearings of e-voting at the Austrian federation of students election are discussed in [KLSV09; LC10]. Papers like [SLBV09] show technical requirements while [XAMA05] deals with the procedural security and social acceptance in e-voting.

2 Recommendation Rec(2004)11 for E-Voting

As part of the project [CoED04] the Committee of Ministers established an expert committee to prepare recommendations on legal, operational, and technical standards for e-voting in the years 2002–2004. The standards were adopted as Rec(2004)11 on 30 September 2004.

The measures included in the Recommendation are grouped into legal standards (thirty-five measures), operational standards (twenty-five measures), and technical requirements (fifty-three measures).

A continuous improvement process over a biennial cycle forms an integral part of the Recommendation. Currently additional recommendations derived from the experiences gained in recent projects are in discussion (see [CoEO10]). These amendments pertain to election observation and the certification processes of e-voting systems.

3 Certification of the E-Voting System of the 2009 Federation of Students Election Based on the Recommendation Rec(2004)11

The timeline, activities, and responsibilities of the federation of students election are defined in the federation of students law [HSG98] and the election regulations [HSWO05]. Concerning e-voting this means that although the specifications are technology neutral and non-discriminatory, they shape how e-voting is implemented. The legal framework stipulates - among other aspects - that the e-voting system has to be approved by the Austrian data protection commission. Furthermore a certification process based on Common Criteria and the recommendation Rec(2004)11 has to be passed.

The technical components to be used—especially those related to the vote casting and the voters' authentication—have to be certified sixty days before the election by a certification authority according to the laws [Sig10], [HSG98] and election regulation [HSWO05].

The e-voting software (documentation, development process descriptions, architecture, security descriptions, threat analysis, technical descriptions, and source code) was audited between December 2008 and March 2009. On 27 March, the certification process ended successfully with the publishing of a certification [ASC09]. The published certificate stipulated key types and length, the compliance of processes for compilation, installation, configuration and operation of the software as well as operating conditions and security information to be released to the voters.

4 Technical Attacks during the E-Voting Period

E-voting, as a new voting channel in the 2009 Austrian federation of students election, was scheduled to be completed before the traditional on-site paper-based vote. Thus voters were able to cast their vote electronically between 18 May at 8:00 AM and 22 May at 6:00 PM. Students could choose whether they wanted to cast their votes electronically or vote in the traditional paper-based election between 26–28 May.

During the e-voting period, different attacks against the e-voting system, voters' acceptance, and the elections were discovered. Several of those attacks are described in the following sections.

4.1 Distributed Denial of Service Attack

Three days before the electronic election started preparations of a distributed Denial of Service (dDoS) attack were detected by the e-voting provider's security staff. An Austrian organization, registered as an organization working toward the use of information technology and telecommunication in a humane, socially responsible and private way, published a web tool which was touted as a harmless server availability checking tool. It was stated that everyone has the right to stress test (check the availability of) the e-voting system, and therefore it was absolutely legal, and practically mandatory, for as many people on as many PCs as possible, to do so, preferably day and night.

Fig. 1: GUI of the dDoS attack tool

The tool was written in javascript and opened a certain URL in invisible iframes as specified within a form textbox on the webpage (per default prefilled with the e-voting website). To avoid browser caching, random characters were added at the end of the URLs opened by the iframes. The other parameters defined how many iframes were opened/refreshed at the same time and at which interval. As the Austrian Computer Emergency Response Team (CERT.at) analyzed the potential danger of the script, even a brief analysis showed that a single PC using commonplace ADSL connectivity produced a permanent load of 10 Mbit/s on the web server.

The most interesting aspect of this attack is that although it was managed centrally, the attackers were distributed using their local resources and their local IP, which made the detection of attackers and possible blocking harder. Unlike most dDoS, this attack did not require a bot-net to be in place; the attackers participated willingly, even if sometimes unwittingly, to the potential problems caused.

An effective technical countermeasure to stop the attack was to include code written in javascript on every webpage of the e-voting system, which checked if the site was opened within a frame and reopened the site within the parent window, thus effectively stopping the tool.

This attack highlighted several of the practical problems stemming from denial of service attacks on e-voting systems. Even though dDoS attacks are not limited to e-voting systems, the ramifications of dealing with them in an e-voting setup are different. Blocking all incoming traffic from the source IP is a common measure. In an e-voting situation, this might deprive an unknown number of other voters of their legal voting rights. Configuration changes and parameter, or even software, adaptations are other popular counter measures. Again in the case of an e-voting system, it has to be considered whether these measures invalidate the existing certification and thus disqualify the whole election. The problem might be compounded by several adaptations

on the attackers' side forcing even more adaptations on the e-voting systems. These questions mostly belong in the realm of law and likely will keep legal practitioners occupied for years.

In case of the Austrian federation of students election, configuration changes were not necessary as the javascript code was already part of the e-voting system and certified months before. The original intention of the existing codes was to keep political parties and others from directly including the voting system via frames as part of their webpages. The same code was added to the gateway pages to also protect those pages from being attacked. As these pages were not part of the certified voting system, no conflicts resulted.

The most important countermeasure however was that e-voting was an additional voting channel scheduled before the paper-based election. According to the law, the election commission can—in the case of specific problems—decide to annul the e-vote, and the students who already voted electronically would be advised to vote again during the paper-based voting period. Consequently not even a successful dDoS attack can effectively harm the election. We suggest to amend the existing paragraph within Rec(2004)11 (art. 45) to not only state that "*remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations…*" but also to include a statement that ending the remote election period before the opening of the polling stations and establishing a process for informing all remote voters in case of annulment due to technical problems may be a way to countermeasure the effect of a dDoS attack.

4.2 Phishing Attack with Mock E-Voting System

To successfully cast a vote students using their own personal computer had to use an Austrian citizen card [BK10], a card reader, and an internet browser with java support. To access the voting system the students had to visit the official federation of students election website, http://www.oeh-wahl.gv.at [OeW10], where they received all relevant information concerning the election. The e-voting system was only linked to the official federation of students election website during the actual e-voting period. The link to the voting system was not published in advance. By clicking a link marked "to the electronic voting," the students were transferred to the voting system.

During the voting period, a political party published a website similar to the official website to mislead the voters. Even a voting process was simulated. The URL used was easily mistaken for the official URL:

Official URL:	www.oeh-wahl.gv.at
Attacker's URL:	www.oeh-wahlen.at
Differences:	election vs. elections (translated) and missing government (gv) subdomain.

This attack could be considered as a phishing attack to gain sensitive information or, at the least, to irritate and mislead the voters. Phishing attacks are not e-voting specific so there are many anti-phishing approaches like [MP08] in banking or [QRYM07] in e-mail systems.

From the technical point of view, this attack could be counteracted by a combination of several measures. First of all, an official website of the election has to be established. It should be the single point of official information concerning everything related to the election. This especially includes the time the election takes place, the description of the voting process, the locations of the polling stations, the names of the candidates and political parties, results of previous elections, and the final results of this election. Furthermore this official website should be the portal to the e-voting system during the e-voting period. The website should be announced through multiple channels such as posters, links from other trustful websites, and much more which reflects Rec(2004)11 Art. 46 which states, "*For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.*"

Evaluation of the referrer HTTP header in the portal server logs showed that about 42 percent of the visitors directly navigated the website by entering the official URL manually into the browser. Most other visitors searched for the name of the election using their favorite search engine (keywords: "federation of students election, information, e-voting" before the election, "federation of students election, e-voting" during the election period, "federation of students election, results" after the election). Consequently active monitoring of search engine results on typical queries and decisive action against phishers are essential countermeasures against such phishing attacks. Buying domains easily mistaken for the real URL and therefore likely targets for phishers is another appropriate countermeasure.

As described in [QSM07], proofing the integrity of the website is very important which concludes to the recommendation to use extended validation certificates (EV) which add verified identity to SSL as described in [CF11]. Furthermore, official websites and internet voting systems related to legally binding elections should be hosted within the government domain space (in Austria e-voting.oeh-wahl.gv.at).

From the organizational point of view, the political party's fake website conflicts with the principles of honest e-voting based on the experience of internet voting in the Estonian parliamentary elections [TSBA07]. In the Austrian federation of students election all election commissions and political parties were made aware of the principles, which were recommended by the Council of Europe, however, never accepted.

Different studies have shown that server-side security indicators and client-side mechanisms like browser warnings do not guarantee prevention of phishing attacks [DHC06] [DTH06] [SDOF07] [WIFE05] [WMG06]. This is due to the fact that if phishers can convincingly imitate the appearance of legitimate web sites, users tend to ignore security warning or do not interpret security cues appropriately [YWAP08]. As an

additional technical countermeasure, the security layer of the Austrian citizen card used for authentication per default only allows access to the personal data stored on the card if the connection is based on HTTPS and the requested data is either sent to a .gv.at domain or a domain identified by a special certificate denoting the URL as a government related resource. Naturally neither .gv.at domains nor a government OID certificate are freely obtainable. For further details on the security architecture of the Austrian citizen card, please refer to [LHP02].

From the operational point of view, before and during the election period the registration and use of domain names similar to the official domain name have to be strictly monitored. Any suspicious activity should be brought to the attention of the election commission as soon as possible to allow for enough time to instigate counter measures.

Even though this advice is not explicitly included within Rec(2004)11, it is addressed by article 103: "*The audit system shall record times, events and actions, including: [...] any attacks on the operation of the e-voting system and its communications infrastructure [...] malfunctions and other threats to the system.*" Nevertheless, considering the danger of such an attack, a paragraph denoting the importance of preventing and handling phishing attacks in remote elections would lead to further improvement.

4.3 Vote Flipping Video

E-voting systems are susceptible to a class of attacks that usually does not feature in other web-based attacks: campaigns to discredit, or smear campaigns. The aim of these attacks is not to disturb or subvert the voting process as such, but to foster the rejection of e-voting as a viable voting channel by alluding that the e-voting process was either not secure or even subverted. Most of the arguments brought against e-voting can be used against any form of remote voting. However, there is one class of arguments that only pertains to e-voting systems and that is the inherent lack of transparency in computerized systems. The technology involved is usually beyond the grasp of the average citizen, and the fact that the same technology powers everything from banking to telecommunications, does not stop people from believing, that this technology will be subverted to nefarious purposes once applied to e-voting.

A vote flipping video was used in a campaign to discredit the federation of students election. This video tried to prove that a voter could select one candidate while on the electronic ballot sheet a different candidate would be marked. The video was released to the media during the election phase.

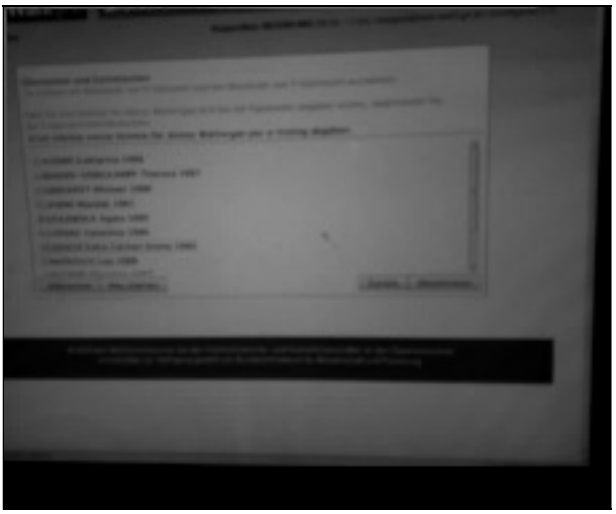

Fig. 2: Fake vote flipping video

Although the video was quite blurry and of bad quality, it was identified as a fake by experts after some investigation. Nevertheless, this experience of the 2009 Austrian federation of students election demonstrates several important aspects. First of all, an incident response team has to be established to react to such events and support the election commission with the analysis as stated in Rec(2004)11 (art. 76): "*Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.*"

Furthermore to allow the timely reaction to attacks, a public communication channel has to be established and announced beforehand. The communication channel should also serve as a contact point for the press in the case of suspicious materials offered to the media. It should be made clear that proof of failure or other reproaches addressed to the media should be handed in for validation before publishing.

Based on this experience it is advisable to declare an official communication channel for announcing possible security relevant incidents. This can be reflected in the appropriate manner in the recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting.

4.4 Vote Buying Campaign

The federation of students election suffered from a second campaign to discredit it, this one a case of alleged vote buying. On the first e-voting day, flyers were found in several lecture rooms at a university asking students to cast their votes using the e-voting system in front of a specific political party's election observers to receive a payment of fifteen euros.

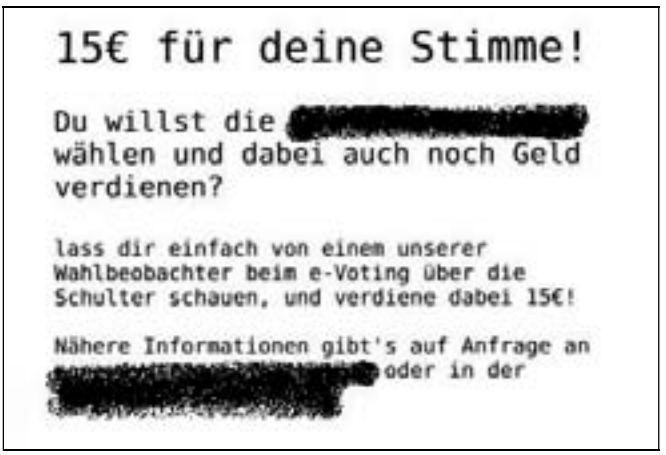

Fig. 3: Flyer for vote buying

Translation:

> 15 € for your vote!
> Do you want to vote for [XXXXXXXX] and at the same time earn money for it?
> Let one of our election observers watch you vote electronically and earn 15€ at the same time.
> Per request, more information is available at [XXXXXXXX]
> or at [XXXXXXXX].

Please note that the names of political parties have been removed.

Although not absolutely proven, it seems relatively certain that the flyers were a fake. The intention of the vote buying flyers could have been not only to discredit the political party named on the flyers, but also to irritate and discourage students eligible to vote from using the e-voting system. However, the e-voting system might not have been the primary target in that case.

Vote buying is the most regular form of violation according to [CAPA07]. If votes are cast in secret, there is no way for candidates and party organizers to be certain that the vote was cast according to the agreement between the voter and the briber. Vote buying is possible for all forms of remote elections and thus not unique to the e-voting process. Rec(2004)11 includes this requirement by several recommendations that have to be

combined to be effective. (art. 80) "*The e-voting system shall restrict access to its services, depending on the user identity. User authentication shall be effective before any action can be carried out."* And (art. 51) *"A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.*" In the 2009 Austrian federation of students election, the voter had to confirm with the digital signature of her/his citizen card that she/he votes free and in secret. This confirmation was an integral part of the authentication process in which the voter's identity was proven by verifying the digital signature. As with any security related system, it is necessary to balance security with usability. The benefit of enforcing such a confirmation at the beginning of the voting process is that the voter's awareness is improved and confirmed before filling out the ballot sheets.

In general Rec(2004)11 should include the recommendation of establishing the voter's awareness that votes should be freely cast and in secret in remote elections.

4.5 Unknown Social Engineering Attacks

During the e-voting period, user-support was handled by the Federal Computing Centre of Austria (BRZ). Voters could contact user-support by e-mail, phone or by an online contact form. A self diagnosis tool, which was integrated within the website, turned out to be very helpful in debugging problems on the user/client side.

As stated in Rec(2004)11 (art. 79), "*The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.*" A technical monitoring system was established to ensure that during the polling period, the voting equipment and its use satisfied the requirements. A traffic light display showed the operations team the functional status of the system without having physical or virtual access to the sealed system. The user-support team was well-trained, especially against social engineering attacks. Processes had been established to identify and counter such malicious attempts.

5 Conclusion

The recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting was published in 2004. Since then there have been periodic iterations by means of biennial review meetings to revisit the impact of the recommendations and to identify necessary amendments.

The focus of this paper was the question of whether the described recommendations are sufficient to handle these state-of-the-art attacks. The basis of this analyze was a discussion of the various attacks that occurred during the 2009 Austrian federation of students election with conclusions regarding suggested improvements for Rec(2004)11.

Based on the distributed denial of service attack, it is a possibility that if e-voting is an additional voting channel, mechanisms could be put in place to recast the vote on election day on paper.

The danger of phishing attacks turned out to be very critical. Therefore Rec(2004)11 could be further improved by explicitly pointing out the necessity of implementing adequate countermeasures.
The acceptance of e-voting as a new voting channel is a key success factor in every project. Various attacks don't target the election directly, but rather target the voters' acceptance by publishing, for example, fake videos of vote flipping as happened during the 2009 Austrian federation of students election. Dealing with such attacks is very difficult and demands the development of a special security strategy, which should be recommended in Rec(2004)11.

Counteracting attack attempts against the e-voting system by social engineering methods demands awareness programs, trained staff, and well-designed processes as requirements that could be included in the recommendation.

The recommendation Rec(2004)11 has been reviewed in 2006, 2008 and will undergo a third review in fall of 2010. The experiences of the Austrian federation of students election can provide interesting insights for this continuous improvement process.

Bibliography

[AH04] Alvarez, R., and T. Hall. 2004. Point, click, and vote. The future of internet voting. Washington, DC.: Brookings Press.

[AH08] Alvarez, R., and T. Hall. 2008. Electronic elections. The perils and promise of digital democracy. Princeton NJ, USA: Princeton University Press.

[ASC09] Certificate according to §34 (6) HSG 1998 for the federation of students election 2009. http://www.a-sit.at/.

[BK10] Austrian Citizen Card and Specification of the Austrian Citizen Card Technology. http://www.buergerkarte.at/en/.

[BSSL01] Schneier, Bruce. 2001. Secret and Lies. IT-Sicherheit in der vernetzten Welt. dpunkt.verlag/Wiley.

[CAPA07] Parliamentary Assembly Council of Europe. 2007. Secret ballot. European code of conduct on secret balloting, including guidelines for politicians, observers and voters.

[CEIP04] Integrated Project "Making Democratic Institutions work" (2002 – 2004), Conference on The future of democracy in Europe 17-19 November 2004, Barcelona (Spain)

[CF11] Extended Validation Certificates Add Verified Identity to SSL. http://www.cabforum.org/.

[CoED04] Council of Europe. 2002-2004. Integrated Project "Making Democratic Institutions work." http://www.coe.int/t/dgap/democracy/activities/Previous%20Projects/.

[CoEO10] Council of Europe. 2010. Workshop on the "Observation of e-enabled elections", Oslo, 18-19 March. http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Evoting_Oslo_Seminar/.

[DHC06] Downs, J.S., M. B. Holbrook, and L. F. Cranor. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the SOUPS*, 79–90.

[DTH06] Dhamija, Rachna, J.D. Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the CHI*, 581–590.

[ED50] Deming, W. Edwards. Deming Circle PDCA, Presented during lectures in Japan during World War II

[EV07] Krimmer, R. 2007. *Machbarkeitsstudie. Durchführung der Hochschülerinnen- und Hochschülerschaftswahlen mittels elektronischer Abstimmungsverfahren*.

[HSG98] Federation of students law. 1998. Hochschülerinnen- und Hochschülerschaftsgesetz 1998 (HSG 1998).

[HSWO05] Election regulations. 2005. Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 (HSWO 2005).

[KLSV09] Krimmer, R., C. Lehner, S. Stangl, B. Varga, R. Stein, G. Wenda, J. Kozlik 2009. E-Voting im Rahmen der Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft 2009, in Hauser, W., M. Kostal: *Hochschulrecht 09,* Wien, NWV, 539-551.

[LC10] Lehner, C. 2010. Die Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft, Doctoral Dissertation at the University of Vienna.

[LHP02] Leitold, H., A. Hollosi, and R. Posch. 2002. Security architecture of the Austrian citizen card concept. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, 391–400.

[MP08] San Martino, Antonio, and Xavier Perramon. 2008. Defending e-banking services. Antiphishing approach. Universitat Pompeu Fabra, The Second International Conference on Emerging Security Information, Systems and Technologies.

[OeH00] Head of Federation of students 2000. Statement concerning federation of students law.

[OeH07] Head of federation of students 2007. Bedenken der ÖH Bundesvertretung zu e-voting bei Hochschülerinnen- und Hochschülerschaftswahlen, September 2007

[OeW10] Informational website of the federation of students election by the election commissions. http://www.oeh-wahl.gv.at/.

[OHER10] E-Voting Evaluation Report. 2010. E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009 – Evaluierungsbericht.

[PKK04] Prosser A., R. Krimmer, and R. Kofler. 2004. Implementing an internet-vased voting system for public elections. Project experience. In *Enterprise information systems V*, ed. O. Camp, J.B.L. Filipe, S. Hammoudi, and M. Piattini, 294–299. Boston, USA/Dordrecht, Netherlands: Kluwer Academic Publishing.

[QRYM07] Qiong Ren Yi Mu Susilo, W. 2007. SEFAP. An email system for anti-phishing. In *Univ. of Wollongong, Wollongong, Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference*, 782–787.

[QSM04] Quasthoff, Matthias, Harald Sack, and Christoph Meinel. 2007. Why HTTPS is not enough. A signature-based architecture for trusted content on the social web. Hasso Plattner Institute, University of Potsdam, IEEE/WIC/ACM International Conference on Web Intelligence.

[Rec04] Council of Europe. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. https://wcd.coe.int/ViewDoc.jsp?id=778189/.

[SDOF07] Schechter S. E., R. Dhamija, A. Ozment, and I. Fischer. 2007. The emperor's new security indicators. An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the IEEE symposium on security and privacy*, 51–65.

[SLBV09] Schmidt, A., L. Langer, J. Buchmann, M. Volkamer 2009. Specification of a Voting Service Provider. In: *Requirements Engineering for E-Voting Systems (RE-VOTE).*

[Sig10] Austrian Government. Electronic signature law. Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG).

[SZKK88] Sunzu. 1988. *Die Kunst des Krieges*. Droemersche Verlagsanstalt.

[TSBA07] Trechsel, A., G. Schwerdt, F. Breuer, and M. Alvarez. 2007. *Internet voting in the March 2007 parliamentary elections in Estonia*. European University Institute. http://www.vvk.ee/public/dok/Coe_and_NEC_Report_E-voting_2007.pdf/.

[WIFE05] Whalen, T., and K. M. Inkpen. 2005. Gathering evidence. Use of visual security cues in web browsers. In *Proceedings of the conference on graphics interface*, 137–144.

[WMG06] Wu, M., R. C. Miller, and S. L. Garfinkel. 2006. Do security toolbars actually prevent phishing attacks? In *Proceedings of the CHI*, 601–610.

[XAMA05] Xenakis A., A. Macintosh 2005. Procedural Security and Social Acceptance in E-Voting. In: *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*.

[YWAP08] Yue, Chuan, and Haining Wang. 2008. Anti-phishing in offense and defense. In The College of William and Mary, annual computer security applications conference, 345–354.