Recent Developments in the Context of Online Elections and Digital Polls in Germany

Bernhard Beckert[1], Jurlind Budurushi[2], Armin Grunwald[3], Robert Krimmer[4], Oksana Kulyk[5], Ralf Küsters[6], Andreas Mayer[7], Jörn Müller-Quade[8], Stephan Neumann[9], Melanie Volkamer[10]

Abstract: The paper summarizes the technical report [Be21] which was published in 2021. The aim of the paper is to summarize and critically discuss the situation in Germany concerning electronic voting.

1 Introduction and Motivation

During the COVID-19 pandemic many organizations (including unions, companies and public institutions) have been faced with the issue of conducting their elections and secret polls without jeopardizing the health of their voters and poll workers. Several election organizers have decided for conducting online voting elections. At the same time, there were hardly any experiences with online voting in Germany before the pandemic, as the topic was barely discussed due to the Federal Constitutional Court Decision on voting machines in 2009[11]. After a year of the pandemic, however, the situation has changed: in the meanwhile, several of elections and polls took place online. However, the systems used often do not correspond to the state of the art in research. Therefore, for the future usage of online elections and digital polls (especially after the pandemic) it is important that election organizers, candidates and voters understand the risks that the currently used systems may imply and how they can be addressed in the context of online elections. Only in this way

[1] Karlsruhe Institute of Technology, https://formal.iti.kit.edu/beckert/index.phtml
[2] Cloudical Deutschland GmbH, https://jurlindbudurushi.com
[3] Karlsruhe Institute of Technology, https://www.itas.kit.edu/kollegium_grunwald_armin.php
[4] University of Tartu, https://www.etis.ee/CV/Robert_Krimmer/est?lang=ENG
[5] IT University of Copenhagen, https://okskulyk.github.io/
[6] University of Stuttgart, https://sec.uni-stuttgart.de
[7] Hochschule Heilbronn, https://www.hs-heilbronn.de/andreas.mayer
[8] Karlsruhe Institute of Technology, https://crypto.iti.kit.edu/head_of_institute.php
[9] https://www.stephanneumann.it
[10] Karlsruhe Institute of Technology, https://secuso.aifb.kit.edu/Team_Volkamer.php
[11] Decision: Order of March 3, 2009 - 2 BvC 3/07, 2009. http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html

doi:10.18420/sicherheit2022_16

informed decisions can be made regarding whether the risks are appropriate and manageable for a particular system to be used in a specific use case.

A number of legal and technical requirements have been proposed regarding the security of online voting[12]. A significant part of these requirements are related to vote privacy, as well as public nature of elections, transparency and verifiability for the individual cast votes as well as for the tallied results.

In our work, we therefore set the goal to support election organizers to make an informed decision regarding choosing the approach and the implemented system for conducting online elections. We aim to draw attention to which aspects are important for the general risk assessment as well as to the potential threats and misconceptions related to already conducted online elections. More specifically, we have looked at several real-world elections and studied the security and the risks of the underlying election systems. This document also contains information and discussions about technical guidelines of the Federal Office for Information Security (BSI) on online elections. Here, we briefly discuss three such elections. We kindly refer the reader to the full version of our paper [Be21] for all details.

2 Christian Democratic Union (CDU) Party Conference

Due to the COVID-19 pandemic, the annual party conference of the CDU took place online in 2021. One particular novelty of this party conference was that a total of 1001 delegates have cast their vote online for the first time to elect the future leader of CDU. In conducting this vote, the party relied on Polyas, a company that specializes in providing services for online elections[13].

In order to ensure that the vote will be cast and stored in the digital ballot box as intended by the voter, the delegates receive a so-called verification code after casting their vote. The verification code is meant to serve as the anonymous proof that one's voting choice has been correctly recorded, in that after the party conference the CDU made all the anonymous verification codes together with the corresponding vote available. The use of such codes has been already discussed in academic publications. In particular, previous research warned about the possibility of so-called "clash-attacks" (see e.g. [KTV]): simply expressed, the adversary would issue the same verification code to several delegates who voted for the same candidate, and assign the remaining votes to other candidates. The information about such an attack has been published and is known to the developers of the voting system. However, this case shows that the users of online voting systems need to be made aware about possible risks and vulnerabilities of a system, so that informed decisions can be made. Furthermore, in case of the CDU party conference, postal voting was offered as an alternative voting channel, thus requiring a clear and transparent process in case of possible discrepancies.

[12] See e.g. the requirements on the European level: https://rm.coe.int/0900001680726f6f

[13] https://www.polyas.de/blog/de/allgemein-de/der-cdu-bundesparteitag-und-polyas (Last visited: 23.08.2021)

3 Online election at the German Informatics (GI) Society

Since 2004, the GI has been conducting their annual elections (Präsidiums- and Vorstandswahlen) online. The members can also cast their vote via postal voting upon request. The access credentials for the online voting system consist of the GI member number and a password which gets sent to the voters via post. For the election, different online voting systems, provided by the company Polyas, have been used. For many years a so-called black box system by Polyas was in use, and it was decided to switch to an end-to-end verifiable system in 2018 [Be19]. The new system has step-by-step been developed towards being end-to-end verifiable. The development is currently still in progress. The voting systems used by the GI so far hence contain a number of risks, such as (1) manipulations by Polyas as system provider cannot fully be detected by the GI, the voters or the candidates, (2) detection of manipulations by administrators of the computing centers or by cyber criminals is in place but still a bit limited, and (3) malware on the end devices of the voters can change the vote without being detected. The responsible persons at the GI are aware of these risks and consider them to be acceptable. The main reason is that the GI members are trusted to keep their devices appropriately secured. Moreover, it is assumed that neither the candidates nor external entities are interested in manipulating the election, since the elected people are already engaged in the organization and the position is offered on a honorary basis. Finally, it was decided that Polyas can be trusted not to engage in any manipulations.

The GI is aware that many of the election organizers are looking at them as an example of which systems to use. The risk of the deployed systems, however, does not only depend on the security background knowledge among the voters. Therefore, it is important for every election organizer to decide themselves whether the risks and attack possibilities that may exist in specific online voting scenarios are acceptable for their election or not.

4 Shareholder elections

The shareholders' meetings in companies have also been conducted mostly online in 2020 due to the pandemic, including the needed voting. The basis for conducting virtual shareholders' meetings is the Legislation for Mitigation of Consequences of COVID-19 Pandemic in Civic, Bancrupcy and Criminal Law (Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht)[14] that was adopted under the emergency procedure by the Federal Assembly. According to the Justice Ministers in the Federal States, the virtual shareholders' meetings should be adopted as an equal alternative to meetings in person in the long term[15].

[14] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Corona-Pandemie.pdf (Last visited: 23.08.2021)

[15] https://www.zeit.de/news/2021-06/17/justizminister-wollen-dauerhaft-virtuelle-hauptversammlung (Last visited: 23.08.2021)

A study published at the 17. German IT-Security Congress of the Federal Office for Information Security in February 2021 analyzed the security of eight shareholders' meetings web platforms [Ma21]. These web platforms were used in the time period from 28. April 2020 to 31. December 2020 to conduct 584 virtual shareholders' meetings in German companies. The results show that almost 72% of the investigated virtual shareholders' meetings contained critical vulnerabilities that could in particular lead to undetected manipulation of the vote, complete takeover of a shareholder's account by the adversary, targeted prevention of conducting the meeting or leaking personal data of shareholders.

It is worth noting, that the analysis only included well-known web-based attacks from the OWASP Top 10 list[16]. Some of the possible attack vectors were thus not investigated, in particular, attacks by other actors such as malicious server administrators, election organizers or service providers. Additionally, the study showed that further methods for ensuring the principles of public nature of elections, transparency and verifiability of individual votes as well as the tallied results are not being offered by any of the platforms. Especially, it is unclear how a notary can ensure the integrity of the voting system and how they can check the results of the voting at the end of the meeting against errors and manipulations.

5 Summary

The choice of an online voting system is not trivial for a variety of reasons. The security of such systems is often determined by small details. There is no single approach or implemented system that is optimal for all kinds of elections, and the service providers of such systems understandably advertise the advantages and security of their own product. Therefore, the following questions should be answered before conducting online elections: (a) Under which adversary model and under which assumptions does the system fulfill the fundamental election principles? Are these assumptions realistic? (b) Can manipulations via cyber-attacks, malicious administrators and election organizers be detected, or does one have to trust that all the involved entities are honest and the possibility of cyber-attacks is excluded? (c) On which information and assumptions about the system do security properties and attacker model rely on? Finally, we want to mention that extensive research has been done on the topic of security in online voting. This research covers in particular numerous cryptographic protocols for different forms of voting as well as studies on the usability of the verifiability techniques. On top of that, other countries such as Switzerland and Estonia already offer – other than the elections being conducted in Germany – verifiability.

Acknowledgement. This work was supported by funding of the Helmholtz Association (HGF) through the POF subtopic 46.23.01 called 'Methods for Engineering Secure Systems'.

[16] https://owasp.org/www-project-top-ten/

Bibliography

[Be19] Beckert, B; Brelle, A; Grimm, R; Huber, N; Kirsten, M; Küsters, R; Müller-Quade, J; Noppel, M; Reinhard, K; Schwab, J; Schwerdt, R; Truderung, T; Volkamer, M; Winter, C: GI Elections with POLYAS: a Road to End-to-End Verifiable Elections. In: E-Vote-ID. Gesellschaft für Informatik (GI), p. 293–294, 2019.

[Be21] Beckert, B; Budurushi, J; Grunwald, A; Krimmer, R; Kulyk, O; Küsters, R; Mayer, A; Müller-Quade, J; Neumann, S; Volkamer, M: Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen. Technical report, 2021. 46.23.01; LK 01.

[KTV] Küsters, Ralf; Truderung, Tomasz; Vogt, Andreas: Clash Attacks on the Verifiability of E-Voting Systems. In: 2012 IEEE Symposium on Security and Privacy. pp. 395–409.

[Ma21] Mayer, Andreas: Virtuelle Hauptversammlungen: Ein sicherer Ersatz für Präsenzveranstaltungen? Tagungsband zum 17. Deutschen IT-Sicherheitskongress, 2021.