– DRAFT –

"Verifiability: a New Concept Challenging or Contributing to Existing Election Paradigms?

Robert Krimmer
Tallinn University of Technology
Ragnar Nurkse School of Innovation and Governance
Akadeemia tee 3, SOC-439
12618 Tallinn, Estonia
E-mail: robert.krimmer@ttu.ee

for Presentation at the 13th Electoral Management Bodies Conference
Bucharest, 14-15 April 2016

Abstract

In this presentation a short motivation is given why it is important to look into the latest development around improving the security and transparency of electronic elections: Verifiability. After this a short overview of the roots and the main applications in the area of Internet voting is given. Finally some preliminary research questions are developed that should guide our future research on this topic.

Keywords: Verifiability, E-Voting, New Voting Technologies, Internet Voting

1. Introduction

In the municipal elections on 7 May 1989 the former German Democratic Republic (GDR) organized for the last time. While the electoral system in use didn't follow full democratic principles, but much rather were an administrative process where the goal of a polling stations election administration was to have the highest possible voter turnout and the highest approval rating for the unified party list. Actually, the voters also had no real choice, they could take the ballot paper and put it into the ballot box. But there was one way to make a real choice, by invalidating all candidates on the ballot paper. This was making the rounds and the civil society wanted to show that they are not satisfied with the ruling party by invalidating as many ballot papers as possible. Also, the voters were allowed to stay in the polling station to conduct a domestic election observation activity. So they stayed and counted the number of invalidated votes. The election authorities, however, didn't report the correct number of invalidated votes (rather ameliorated numbers), and the voters in turn went on the streets a month later in what was known as the election fraud demonstrations. These demonstrations that proved how corrupt the system was.

Picture 1: Domestic Election Observation Effort During 7 May 1989 Municipal Elections in the German Democratic Republic

Picture 2: Demonstrations Against Electoral Fraud in June 1989 in the German Democratic Republic

This experience was a leading motive when the German Constitutional Court had to assess the appeal of a citizen against the 2005 *Bundstag* elections finally in March of 2009. Its ruling came a bit surprising, but was of revolutionary nature: it ruled that voting machines - without the possibility for the voters to count the votes without prior knowledge ("laymen") – were to be considered unconstitutional (and thereby demanded that voter-verifiable paper audit trails would have to be introduced) and that ended the story of e-voting in Germany (Federal Constitutional Court, 2009).

2. Verifiability

Elections are generally considered to be one of the essential elements of modern-day democracy in order to establish "the rule by the people." The procedures by which elections are held have evolved considerably over time and differ depending largely on the context in which they take place and the available technology. Over time, many different methods have been used, including casting votes by shouting, a show of hands, swords, stones, wax tablets, etc. Today, the predominant form of casting votes worldwide in order to participate in elections is to fill out a paper ballot (see, also Krimmer, 2012). Internationally accepted norms depicting the voting process such as the Int. Covenant on Civil and Political Rights (United Nations, 1966)

or the Copenhagen Document (OSCE, 1990) are used to establish what constitutes a democratic election. While these do not mention a preference for a particular form of casting a vote, it is clear that they have been developed and written with the paper-based voting process in mind.

The evolution of more-sophisticated voting technology than the paper ballot has its roots in the mid-19th century. This period saw the discussion of mechanical vote-casting devices, which was followed by proposals for electrified voting machines for parliaments. The US can be considered the forerunner in adopting various forms of mechanical and electr(on)ic vote-casting and counting devices, including pull-lever machines, punch-card systems, direct-recording e-voting machines or ballot scanners (Jones and Simons, 2012). Their adoption flourished due to the decentralised nature of US election administration and their decision-making processes (Harris, 1934).

All of these voting technologies have one inherent problem in common: The process from casting votes to counting votes is pretty much unobservable, due to the need to keep the voters' choices secret as well as the problem that one cannot touch bits and bytes (Lenarčič, 2010). Despite some critical voices (Saltman, 1975, 1988), these technologies were nevertheless considered safe for a long time.

The US presidential elections of 2000, particularly in the state of Florida, changed this picture considerably. In the close presidential race between George W. Bush and Al Gore, the high failure rate of punch-card systems combined with the lack of a robust legal framework led to problems in trying to determine the "original voter intent" and a delayed determination of the election's outcome. Not only did this lead to a decline in the public's confidence in voting technology but also in the validity of calling the US the "greatest democracy on Earth." Contrary to expectations, the US invested even more heavily in voting technology, believing that the source of the problem was the choice of the wrong voting technology instead of a complete overhaul of the way the election administration, legal framework, and voting technology interact. (Saltman, 2006)

This debacle, however, gave impetus to cryptographic researchers who since the early 1980s had been trying to realize fully e-voting processes (Chaum, 1981, 1982). With computer systems, sharing of power is hard to realise. Early on, proposals included functionalities to

allow for the public to check whether the election administration reported the results honestly and did not manipulate the elections. In paper-based elections, this can be verified by recounting the ballots. In e-elections, recounting the ballots does not necessarily result in greater confidence in the results, as long as the system being utilized for the count does not use a programming system different from the original tool. Hence, there was a need for a different method for checking the election administrators and of verifying their honest reporting of election results. The concept of verifiability by individual voters and the general public was born (Benaloh, 1987, Schoenmakers, 1998, 1999).

As one of the first, the Office for Democratic Institutions and Human Rights (OSCE/ODIHR) took up this development and defined "verifiability on an individual basis [… where] voters are provided with possibilities to verify that their vote was cast as intended, stored as cast, and (ideally) counted as recorded." On a universal (public) level, a voting technology with verifiability "provide[s] means for an independent third party to establish that the result of an election was reported honestly and without manipulation through either manual or mathematical checks" (OSCE/ODIHR, 2013).

With the transformation of transactions in the private and public sector through the general availability of the Internet in the 1990s, it seemed only a matter of time until elections too would be held via the Internet. A real race had begun to see which country would be the first to offer Internet voting (I-voting) to all its voters (Kubicek et al., 2002). Despite promising initial efforts in the US (Gibson, 2001) and Germany (Otten, 2001), it was Estonia that succeeded with a rather simple system in 2005 (Drechsler and Madise, 2004, Madise and Martens, 2006). However, only a small number of countries followed suit to offer I-voting for first-order elections, including the Netherlands, France, Switzerland, and Norway (Krimmer and Kripp, 2009). Furthermore, most of the algorithms used were rather simplistic in their design and did not offer any possibility for voters to verify their votes (Krimmer et al., 2007).

The 2009 verdict of the German Constitutional Court changed the public view on e-voting machines when the court decided that it must be possible for voters to ascertain for themselves without "prior knowledge" that election results had been reported honestly and that their votes had been entered in the results (Federal Constitutional Court, 2009). This led the project managers of the Norwegian I-voting project to look for solutions to this problem, and during

their procurement process, a verifiable I-voting protocol was proposed by researchers from Estonia (Ansper et al., 2009). The Norwegian elections in 2011 can be considered the first use of verifiability in Europe.

In the same year as the first use of verifiability, an Estonian student managed to program a Trojan horse that would cast a different vote than the one intended by the voter in the 2011 Riigikogu elections. He consequently filed a complaint, which was eventually turned down by the Estonian Constitutional Court (OSCE/ODIHR, 2011). This incident led to an electoral reform process where it was decided to introduce individual verifiability for upcoming elections where I-voting is offered (Vinkel, 2012). It was first used in the 20 October 2013 municipal elections in Estonia. Further, Switzerland has also announced making the introduction of verifiability a requirement for elections with full I-voting (Schweizer Bundesrat, 2013).

3. Some Questions to Put Forward in Regards to Verifiability

Thinking along the lines of the outline above regarding verifiability some questions come into mind that can guide our future investigations on the topic:

1) What are the aims provided in the academic (mainly technical) literature for introducing the concept of 'verifiability' to existing election processes, including I-voting, and what purported use do the decision makers in practice plan to gain from introducing this concept;

2) How does verifiability actually work in practice, and what would a generic process model for individual and universal verifiability look like;

3) Does verifiability as a concept also have applicability for paper-based elections, i.e. without Internet voting?

On the basis of the existing academic literature, one can put forth the following working hypotheses which we will have to investigate further:

1) Verifiability is a new concept that enables voters on an individual level to verify whether their votes were cast as they intended, recorded as cast, and counted as recorded, as well as on a universal level that no manipulations occurred, and the results were reported honestly.

2) Verifiability adds a new paradigm to the world of elections. It has the potential to add a considerable level of control for the general public over the conduct of elections.

3) Verifiability has been invented and defined by cryptographic researchers and hence needs to be translated into the reality of elections, i.e., define a legal framework for its use, make it usable and understandable by voters so that it actually makes a difference, etc.

4) In line with the general trend to provide more accountability to the public, future elections will have to offer voters the potential to control the election administration. Therefore, in the future verifiability will play an important part not only for election administration of I-voting but also of paper-based elections.

4. Summary

The concept of verifiability is currently our only answer towards trying to solve the dilemma of enabling only eligible voters to cast votes via the Internet and still keeping their votes secret. In a world with ever increasing capabilities to capture and process information this becomes increasingly difficult. It is therefore important to learn more about the applicability of this new technical method and the possibility to apply it for both Internet voting and existing paper-based voting methods.

5. References

ANSPER, A., HEIBERG, S., LIPMAA, H., ØVERLAND, T. A. & VAN LAENEN, F. 2009. Security and Trust for the Norwegian E-Voting Pilot Project E-valg 2011. Identity and Privacy in the Internet Age. Berlin: Springer.

BENALOH, J. 1987. Verifiable secret-ballot elections. PhD thesis, Yale University.
CHAUM, D. 1981. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM, 24, 84-88.

CHAUM, D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceedings of CRYPTO '82, 1982 Santa Barbara, California, USA. 199-203.

DRECHSLER, W. & MADISE, Ü. 2004. Electronic Voting in Estonia. In: KERSTING, N. & BALDERSHEIM, H. (eds.) Electronic Voting and Democracy: A Comparative Analysis. London: Palgrave.

FEDERAL CONSTITUTIONAL COURT. 2009. Use of voting computers in 2005 Bundestag election unconstitutional [Online]. Available: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html.

GIBSON, R. K. 2001. Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary. Political Science Quarterly, 116, 561–583.

HARRIS, J. P. 1934. Election Administration in the United States, Washington, Brookings Institution Press.

JONES, D. & SIMONS, B. 2012. Broken Ballots: Will Your Vote Count in the Electronic Age?, Stanford, CSLI Publications.

KRIMMER, R. 2012. The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy. Ph.D. Dissertation, Tallinn University of Technology.

KRIMMER, R. & KRIPP, M. 2009. Generic Tools and Policies for an Electronic Democracy. In: E-VOTING.CC (ed.) Working Papers on Electronic Voting and Participation. Vienna.

KRIMMER, R., TRIESSNIG, S. & VOLKAMER, M. 2007. The development of remote e-voting around the world: A review of roads and directions. In: ALKASSAR, A. & VOLKAMER, M. (eds.) E-Voting and Identity. Springer.

KUBICEK, H., KARGER, P. & WIND, M. 2002. Stilles Wettrennen. Kommune21, 12-13.

LENARČIČ, J. 2010. Address by Ambassador Janez Lenarčič, Director of the OSCE Office for Democratic Institutions and Human Rights (ODIHR), at the OSCE Chairmanship Expert Seminar on the 'Present State and Prospects of Application of Electronic Voting in the OSCE Participating States', in Vienna, Austria on 16 September 2010. [Online]. Vienna. Available: http://www.osce.org/odihr/71361.

MADISE, Ü. & MARTENS, T. 2006. E-Voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In: KRIMMER, R. (ed.) Electronic Voting 2006. Bonn: Gesellschaft für Informatik.

OSCE. 1990. Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE [Online]. Available: http://www.osce.org/odihr/elections/14304.

OSCE/ODIHR. 2011. Election Assessment Mission Report on the 6 March 2011 Parliamentary Elections in Estonia [Online]. Available: http://www.osce.org/odihr/77557.

OSCE/ODIHR 2013. Handbook for the Observation of New Voting Technologies, Warsaw, OSCE/ODIHR.

OTTEN, D. 2001. Wählen wie im Schlaraffenland? Erfahrungen der Forschungsgruppe Internetwahlen mit dem Internet als Wahlmedium. In: HOLZNAGEL, B., GRÜNWALD, A. & HANSSMA, A. (eds.) Elektronische Demokratie: Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis. Munich: Verlag C.H. Beck.

SALTMAN, R. G. 1975. Effective Use of Computing Technology in Vote-Tallying. Washington D.C.: National Bureau of Standards.

SALTMAN, R. G. 1988. Accuracy, Integrity, and Security in Computerized Vote-Tallying. Washington D.C.: National Bureau of Standards.

SALTMAN, R. G. 2006. The History and Politics of Voting Technology. In the Quest of Integrity and Public Confidence, New York, Palgrave Macmillan.

SCHOENMAKERS, B. 1998. 5 May 1998: An announcement for the Dutch voting experiment [Online]. Available: http://groups.yahoo.com/group/e-lection/message/17.

SCHOENMAKERS, B. 1999. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. Advances in Cryptology - Crypto99. Springer-Verlag.

SCHWEIZER BUNDESRAT 2013. Bericht des Bundesrates zu Vote électronique. Auswertung der Einführung von Vote électronique (2006–2012) und Grundlagen zur Weiterentwicklung. Bundesblatt 2013. Bern.

UNITED NATIONS. 1966. International Covenant on Civil and Political Rights [Online]. Available: http://www2.ohchr.org/english/law/ccpr.htm [Accessed 08-10 2011].

VINKEL, P. 2012. Presentation to the OSCE Human Dimension Committee on 27 March 2012 by the Estonian Delegation on Follow-up to the Recommendations contained in the 2011 OSCE/ODIHR Election Assessment Mission Report. Vienna.

6. About the Author

Prof. Dr. Robert Krimmer is Full Professor of e-Governance within Ragnar Nurkse School of Innovation and Governance at the Faculty of Social Science, in Tallinn University of Technology, Estonia. He is focusing on electronic participation and democracy, as well as e-voting, the transformation of the public sector, and all issues further developing a digital society. Associate Editor of the international scientific journal Government Information Quarterly (GIQ) where he is in charge of participation issues. He has been one of the lead experts for the Council of Europe Ad-Hoc Committee on Electronic Democracy and drafted Annex 1 of the CoE Recommendation (2009)1 on e-Democracy. Teaching on e-Governance, e-Democracy, incl. e-Participation and e-Voting as well as End-User Management Information Systems at Tallinn University of Technology, University of Applied Sciences Hagenberg, Danube University Krems, and WU Vienna University of Economics and Business. Mentor of more than twenty graduation theses. Author and/or editor of ten books/special issues of scientific journals. Author of some 80 international scientific articles. He has been cited some 640 times with an Hirsch index of 13 according to Google Scholar.