**Noname manuscript No.**
(will be inserted by the editor)

# A Review of E-voting: the past, present and future

**J Paul Gibson · Robert Krimmer · Vanessa Teague · Julia Pomares**

Received: date / Accepted: date

**Abstract** Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades. Despite lack of agreement on whether this has been a 'success', there has been - in the last few years - enormous investment in remote electronic voting (primarily as a means of exploiting the internet as the underlying communication technology).

This paper reviews the past, present and future of on-line voting. It reports on the role of technology transfer, from research to practice; and the range of divergent views concerning the adoption of on-line voting for *critical* elections.

**Keywords** Remote electronic voting · Internet · Review · State-of-the-art

J Paul Gibson
SAMOVAR, Télécom Sud Paris, CNRS, Université Paris Saclay, 9 rue Charles Fourier, 91011 Evry Cedex
E-mail: paul.gibson@telecom-sudparis.eu

Robert Krimmer
Tallinn University of Technology, Estonia,
E-mail: robert.krimmer@ttu.ee

Vanessa Teague
University of Melbourne, Australia,
E-mail: vjteague@unimelb.edu.au

Julia Pomares
CIPPEC, Argentina,
E-mail: jpomares@cippec.org

## 1 Introduction: from post via phone to space and the cloud

Postal voting is the earliest example of remote voting — traced back as far as the Roman Empire[51] — that depends on an underlying communication network to function properly. More reliable records date back to the 17th century where postal voting was allowed for merchants in Switzerland[7]. Postal voting is still in use in many elections around the world, and is the standard against which remote electronic voting (**REV**) is most often compared[35]. The next major communications infrastructure that facilitated remote voting was the telephone network, which has provided an alternative voting procedure for a specific subset of the electorate — usually those with disabilities — in a small, but significant, number of democratic elections. The telephone network is also used to support convenience voting[22], including voting by FAX. In contrast to the primitive technology used in postal voting, some American astronauts have been able to vote from space since 1997: the first American to do so was David Wolf, who was living on Russia's Mir Space Station and was granted special disposition to vote remotely by his home state of Texas[1].

Since then, as we shall see in the remainder of this paper, there has been much research into remote voting using the internet. As the internet evolves, then so also do the remote voting systems built upon it. As we progress towards cloud services and virtual networks[16] then the future of remote voting may be as just another trustworthy e-government service[11] on the cloud[53]. Configuring and running elections on a virtual machine is certainly appealing, but we must address the problems associated with internet voting, in general, before we can examine the additional complexities introduce by virtualisation.

In the remainder of this article, we provide an overview of the historical foundations of REV and a short analysis of the main issues within this problem domain. We then review the current state-of-the-art in remote e-voting from a geographic perspective. To conclude our analysis, we consider the future of electronic voting and make some recommendations. The final section in this article reviews the papers that were accepted for this special issue, and place their innovative contribution, and potential impact, within the context of the previous sections.

## 2 E-voting on-line: the past

### 2.1 Historical foundations

The foundations of internet voting are found in the democratization movement and the general availability of mass electronic media, like the television, after the second world war. At the same time as the internet was in its infancy — as a network of distributed computers, communicating using packets of information[15] — the idea of enhancing democracy through the use of electronic means was supported by several great thinkers in order

[1] `http://www.nasa.gov/mission_pages/station/expeditions/expedition18/vote.html`

for democracy to finally come true[17]. Initially, private networks were used for computer-mediated communciation and decision making within private organisations[26]; but secrecy was not considered as a central issue — it was either not considered to be a fundamental requirement, or it was guaranteed by organisational processes rather than properties of the network communication mechanisms.

The next step was the transfer of responsibility for secrecy away from the organizational processes and towards the network through the use of asynchronous cryptography. During this period, there were a significant number of research results concerned with the development of secure multi-party communications, for which elections turned out to be an interesting application field (for an overview of early proposals and protocols see [28]).

After the initial theoretical work, some researchers applied the results in order to implement REV prototypes/systems; for example, the Sensus system by Cranor and Cytron[13] or the EU Cybervote system[2]. In addition, several new technology start-up companies, such as *Election.com*, *Safevote.net*, or *Votehere.net*, focused on REV products.

With this increasing interest, a 'political race' began in the mid 1990s to see which country would be the first to allow for Internet voting in their general elections. It seemed — at that moment — only a matter of time rather than a question of technical feasibility; particularly after Bill Clinton ordered further investigation of the issues at the end of 1999. The resulting report was published at the beginning of 2001[45], but the events in the November presidential elections (Bush vs Gore) focused American attention on the integrity and auditability of election results. Most Internet voting trials have been outside the USA.

But with the adoption of different types of REV around the world came the realization that it is not purely a technical issue. Many political, social and legal matters arise when deploying Internet voting. Further, the research community demonstrated that there were outstanding technical challenges which none of the deployed systems had addressed in an adequate manner. We review these issues in the following subsection.

### 2.2 Main outstanding technical issues with remote e-voting

E-voting that is physically supervised by some authority — such as the use of direct recording electronic (DRE) machines at polling stations — initially, and quite rightly, drew much criticism[41]. However, the vast majority of experts would now acknowledge that — even though there are many reported and ongoing problems with systems that are currently in use, see for example [33] — such systems can be built and operated in a satisfactory manner provided they support some form of voter verified printed audit trail (VVPAT)[52], with a risk-limiting audit or manual recount[36]. There are no outstanding

[2] The EU Cybervote Project. Retrieved from `http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=4850479`

fundamental theoretical or technical challenges that should prohibit the development and use of such systems. This is not the case for REV, which is the subject of this special issue of the journal.

REV permits the voter to record a vote without having to be physically present in a supervised environment. In order to facilitate this, the voter must trust unsupervised mechanisms for recording and transmitting their vote. In the modern world, this will most likely be an electronic computer/device that is connected to the internet. There is such a complex interaction between the different requirements that such systems may be required to meet [21], in general, that it is not yet clear whether a universally acceptable solution exists. Much of the current research in this area is concerned with better understanding these interactions, designing and implementing systems that meet certain combinations of requirements, and evaluating the use of such systems during elections.

Why is remote electronic banking widely accepted as being safe and secure whilst the same cannot be said for remote electronic voting? First observe that electronic banking is not perfectly secure: most electronic banking and e-commerce systems suffer a significant rate of fraud, despite the opportunity to verify the process. Furthermore, voting is harder. The key issue that is unique to electronic voting is the interaction between those requirements concerned with authentication, anonymity/privacy and verifiability/auditability. A single voter may be required to authenticate themselves in order to record a vote and at the same time they may require that no-one can see if/how they have voted; later the same voter may require that they can check if their vote has been correctly recorded and counted, and if that is not the case then they can demonstrate this (without revealing how they have voted). This is feasible in a traditional polling station, where voters can observe the paper ballots (that have been completed in private in a voting booth) being deposited in the urns, the transfer of the ballots after the urns are closed, the opening of the urns when the count starts, the counting process and the announcement of the results. With DRE voting machines, the observation of the electronic processes is quite different in nature, but mechanisms—such as VVPATs—exist to provide each voter with guarantees that are equivalent to what they can observe in the traditional system. With REV, it remains an open topic of research as to whether it is possible to build a system that can provide such guarantees without compromising the other requirements that are typically expressed.

It it posslbe that REV may bring benefits [43, 42], though these are hard to support with empirical evidence. Such systems could reduce the costs of running elections, but there is no consensus regarding the economics of building, using and maintaining REVs. Permitting voters to vote remotely may increase turnout/participation: asking voters to physically attend a voting station in order to vote can be considered a hurdle/barrier to their participation; but there are many other—perhaps more significant—reasons for low turnout. Remote voting using the postal service is, in general, problematic[35]; and it might be possible that replacing postal vote services with internet-based ser-

vices could address some of these problems. In constituencies where voters do not trust the election system (or administrators) then requiring voters to vote in a physically controlled environment may be seen as a threat to the democratic process, and REV may be one way of avoiding such a threat. E-voting may even make some forms of fraud easier to detect [2]. However, it should be emphasised that there is no clear evidence that REV would necessarily solve any of these problems, nor that it would be the best solution even if it could be designed to be secure.

Voter coercion is a major potential problem with REV—if the voter records their vote in an uncontrolled environment then it is reasonable to ask what is to stop a coercer from being present and obliging the voter to follow their wishes? Research has led to the development of Helios coecion-resistant REV systems[4,12,30], but it is a challenge to create such a scheme which can be understood by voters and which does not require an unacceptable use of resources (human and/or machine). We should not forget that other forms of convenience voting (by post, FAX or procuration, eg) help, rather than hinder, potential coercers.

REV which is based on end-to-end-verifiable (E2E-V) systems offers guarantees that many other REV systems do not, by ensuring that:

- voters have an opportunity to verify that their vote is cast as they intended and correctly recorded (individual verifiability), and
- anyone can verify that all recorded votes were properly included in the tally (universal verifiability).

This provides a high degree of evidence that the outcome is correct, assuming that the voters correctly performed the verifications. End-to-end verifiable systems also typically use sophisticated cryptographic techniques for providing privacy (though this is not part of the definition of end-to-end verifiability). Such protocols should guarantee that voters do not need to blindly trust any component of the system; all components can be scrutinised so that their computation can be verified if their trustworthiness is in doubt.

However, even requiring the use of E2E-V REV systems does not guarantee that the system will meet all the requirements of secure government elections. With all REV systems, including those with E2E-V, voter authentication is a major issue: a strong universally deployed electronic-ID system would overcome many of the problems associated with the weak authentification mechanisms that are currently in use, but this does does not yet exist in the context of most elections. Privacy still depends on trusting the device on which you will make your vote; without centralised control over such devices, malware and spyware are significant issues. Individual verifiability gives voters the opportunity in principle to verify that their vote is cast as they intended, even on an untrustworthy device, but there are significant challenges in practice. For example, verification generally requires another device that does not collude with the malware on the primary device. Most individual verifications steps require significant care and attention from the voter, who may be receiving their instructions from the very device that is trying to cheat.

REV also requires trusting the network over which your vote is transmitted; using a public network such as the internet makes it very difficult to protect the system against denial of service attacks. Voters should understand the process that is used to record, transmit and count their votes; E2E-V introduces complexity to the process and significantly compromises understandability. The mechanisms/interfaces with which voters interact with the system should be easy to use; yet the cryptographic protocols used in assuring privacy/anonymity/secrecy in REV systems often compromise their 'usabillity'. End-to-end verifiable systems have been used successfully in polling-place electronic voting systems [10,6,14], and over the Internet for professional society elections such as the IACR's [1], but significant challenges remain before they can be seen as a complete solution to secure REV for government elections.

Clearly, there is a significant challenge in the development of REV systems that meet their requirements. In the next section we report on how various countries around the world have tried to (or are preparing to) address this challenge.

## 3 E-voting on-line: the present status around the world

It is not possible to provide a comprehensive review of REV in every country around the world[3]. Instead, we categorize different stages that countries have followed in the adoption of REV and provide an illustrative example of a single country in each category (where published scientific papers exist to provide more detailed information), and — were appropriate — list some of the other countries in a similar stage. (It should be noted that we have not included the United States in our analysis, as each state acts autonomously in its procedures for administrating elections.)

**Promoting Adoption**

In many countries (typically in the developing world), there has been a call for the adoption of REV as a means of improving the democractic process. In Ghana there have been reports of wide-spread electoral fraud, and a subsequent call for the introduction of REV[5]. It is unlikely that such calls will have a significant impact on the government bodies who currenty control the democratic process. Other countries in a similar phase of promotion are: New Zealand, Greece, Jordan, Nigeria, and Turkey.

**Considering**

Many countries are considering internet voting and their governments have commissioned reports regarding its implementation. The use of voting technology has been discussed in Switzerland for quite some time[8,49]. It was as early as 1975 when the Swiss authorities considered the use of punch card systems for counting votes electronically, however it was deemed too early to implement this into the law. Nearly 20 years later, when Switzerland introduced postal voting as a voting channel available in any kind of election country-wide, it

[3] A comprehensive view of the state of electronic voting in all the countries in the world can be found at `https://www.e-voting.cc/en/it-elections/world-map/`.

again considered the use of electronic means but still considered that the time was not right for adoption. The topic did not leave the political debates, and returned in 1998 when the government included Internet voting in its information society strategy. It foresaw the need to assess the feasibility of using the Internet for involvement of the citizens in the democratic decision making process. In 2000, the Swiss parliament with its agenda setting committee came forward with two motions essentially tasking the federal chancellery to further develop the topic of direct democracy via the Internet. The federal chancellery in turn installed a working group assess the feasibility of introducing Internet voting as a general method of voting by the year 2010. There is currently no clear decision arising out of these studies. Other countries in a similar phase of consideration are: the United Kingdom, Iceland, Finland, Lithuania

**Small-scale trials**

Some countries are trialing the use of internet voting in a small subset of elections/constituencies (relative to a national election), where only a small percentage of electors vote by internet. France has mainly focused on expatriate voting[48], and there is some discussion as to whether REV would be suitable in a country, like France, which values the tradition of going to the polling station in order to participate in the democratic process[44]. Other countries in a similar phase of small-scale trials are: Spain and the United Arab Emirates

**Large-scale trials**

A few countries are trialing the use of internet voting in a significant subset of elections/constituencies (relative to a national election), where a significant percentage of electors vote by internet. Australia has held one of the most significant on-line elections — in terms of the number of participants (280,000 approx.) — during the 2015 New South Wales state elections. The voters had to declare that they met eligibility criteria which covered ease of access to a polling station and disability. They could vote using a web browser or by phone, but the vast majority chose to use the web. An independent security assessment[24] conducted during the election period found significant "security failures and verification flaws" in the iVote system. The security vulnerabilities were due to the introduction of an analytics script from a third-party server vulnerable to the FREAK and logjam attacks. Although iVote did include a telephone-based method of allowing voters to query what vote had been recorded on their behalf, only limited data from this system are now available. The most important statistic, the rate of failues among those voters who attempted to verify, remains unavailable. Other countries in a similar phase of large-scale trials are: India and Switzerland.

**Evaluating**

A small number of countries have already carried out a significant number of large-scale trials and are in the process of deciding whether to adopt internet voting on a national scale. Canada is a good example of a country which has

carried out numerous experiments[4]: with internet voting, but has yet to make a concrete decision as to whether to adopt or reject the use of such elections[47, 20]. It is unlikely that this decision will be made in the near future.

**Adopted**

Only a few countries have run a significant number of internet elections on a national scale; and of these, only Estonia has continued with plans for universal adoption. The small Baltic republic of Estonia was the first country in the world to introduce remote electronic voting for all elections in 2005[38, 39]. Since then it has held five nation-wide elections with an electronic remote channel. The Estonian government relies heavily on Internet services, and their electronic national ID system; and they are notorious for having suffered the first major distributed Denial of Service Attack in 2007. Security analysis of the I-voting (cleint server system) has identified many potential weaknesses for exploitation[50]. More recently, detailed analysis of the log files from national elections has identified software bugs and audit deficiencies[25]. In 2013 they started publishing source code and introducing individual verifiability, planning to adopt universal verifiability in 2017.

**Rejected**

Some countries have rejected the use of internet voting (after having passed through one of the previous phases). The Netherlands was one of the earliest adopters of e-voting. KOA was trialled in the European 2004 elections (replacing postal vote by remote voting via Internet or phone). The original system was designed by Logica CMG and a fully open-source version was later developed[31,32]. Analysis of the main feeback from this experiment was that risk and trust were significant concerns for the public[27] The RIES (Rijnland Internet Election System) system replaced KOA in a follow-up experiment, but many security issues were identified[29]. Subsequently, after an NGO — *We Dont Trust Voting Computers* — demonstrated that the machine's software could be replaced with a manipulated version within one minute[19]), the Netherlands stopped the development of their Internet voting project RIES as well as the use of their electronic voting machines. Other countries in a similar phase of rejection are: Austria, Germany, , Kazakhstan, and Norway.

## 4 E-voting on-line: the future - some recommendations/opinions from the guest editors

There are a large number of divergent views concerning the future of remote electronic voting, and it is a subject for which every expert has their own opinion. Rather than trying to provide an objective analysis of all the different attitudes and beliefs, the following subsection illustrates the divergent nature of the issue by including a short position statement from each of the four guest editors of this special issue:

[4] An excellent report - *City of Toronto RFP #3405-13-3197* - can be found at `https://assets.documentcloud.org/documents/1310860/toronto-internet-voting-security-report.pdf`

**Gibson, J Paul** — Electronic voting, within the context of democratic government elections, should be considered as a safety-critical system[40]: it must be both trustworthy for, and trusted by, its users (the voters, candidates, election administrators and independent observers). Unfortunately, the history of electronic voting has included a significant number of voting systems that were neither trustworthy not trusted. Remote electronic voting (using the internet) raises the even more significant problem of untrustworthy systems being naivly trusted by users just because they use technology with which they seem to be familiar. A central issue is the need for REV system developers, vendors and procurers to be more honest and open about the requirements that their systems do (or do not) meet. As this special issue has shown, the REV research community does not (yet) fully understand the interactions between all the different requirements. Furthermore, rapid advances in ICTs may give rise to novel solutions to some of the outstanding issues; but these advances may also render the problem more complex. The future for REV is sure to hold many surprises, for academics and industrialists alike.

**Krimmer, Robert** — Using ICT in elections has been a topic of intense debates around the world. In an effort to contribute to this debate objectively we have selected scientific papers where different scientists examine aspects of the issue from different perspectives and where data is gathered and analysed carefully employing scientific methodology. Next to academic discourse this issue shall also contribute to the debate amongst practitioners and policy makers so that decisions can be made on the basis of the best evidence and reason available.

**Pomares, Julia** — Unlike in social processes where digital technologies have been embraced unquestioningly, ICT use in elections has been slow and erratic. The envisaged surge in the role of technology in voting has not come to pass  at least not yet and to the extent expected  and instead of REV superseding attendance-based polling, there has been the sort of toing and froing over the issue of ICT in elections that few would have forecast a couple of decades back. Also, geographically the trend has been surprising. Developing countries were predicted to shift slowly to electronic voting with established democracies taking the lead. However, Brazil, Venezuela and India were the first in a line of nations defying this, and with no apparent plans to phase in remote systems. Several established democracies, meanwhile, have chosen to experiment with REV prior to even testing attendance e-voting. This pattern calls for a more nuanced understanding of technological change and adaptation in election processes. That is the ultimate aim of this volume.

**Teague, Vanessa** — Secure Internet voting is not an objective in itself — the real objectives are to understand and improve the quality of elections, including their integrity, accessibility, and levels of participation. There are numerous interesting ways to use technology to improve elections, without necessarily trusting The Internet for the return of voted ballots. End-to-end verifiable attendance voting systems have seen practical deployments in government elections, at a state and local government level. Risk limiting audits of voter-verified paper records have been deployed successfully in Europe and

the USA. Remote end-to-end verifiable Internet systems such as Helios are used in professional society elections such as those of the International Association for Cryptologic Research[23]. Much recent research focuses on trying to design secure enough software to run government elections over The Internet, but significant open problems remain. We hope this volume contributes an accurate understanding of the security properties of e-voting systems, and inspires creativity in using technology to solve important open problems in election conduct.

## 5 The special issue: the contribution of the accepted papers

For this special issue, five papers were selected, each of which makes a significant contribution to the debate on electronic voting. Significantly, two of the papers consider the use of technology to improve electoral integrity through the use of ICT, but not by REV over the Internet.

The work by Aranha, Ribeiro and Paraense, reported in *Crowdsourced integrity verification of election results: an experience from Brazilian elections*[3] describes an experiment for evaluating the integrity of election results from attendance-based polling. They show how to crowdsource the verification of election data, and get more citizens involved in post-election tallying process, by combining two common mobile applications — photography and crowdsourcing.

The paper *An Experiment on the Security of the Norwegian Electronic Voting protocol*[18], authored by Gjsteen and Anders Smedstuen, reports on a statistical method for assessing the outcome of a verification process, assuming that the REV verification protocol itself is sound. Given that, it aims to provide convincing evidence that a voting protocol was not attacked during the election process. It is based on the assumption that a significant number of voters are willing and able to use the voting protocol as required. The use of such statistical methods is an on-going area of research with promising results.

In the third accepted paper — *An Investigation into the Usability of Electronic Voting Systems for Complex Elections*[9] — Budurushi *et al.* address the issue of how voting machine interfaces can be better designed in order to facilitiate the tasks of voters and election administrators, with emphasis on the use of such interfaces for complex elections. The issue of trusting a remote voting device is shown to be tightly linked to the quality of the interface it provides, which influences voters on whether or not they then proceed to verify their ballots. As voter verification is a key issue in electronic voting, this paper raises the important issue of the relationship between usability, verifiability and trust.

Much of the ongoing research in remote electronic voting is concerned with the design and verification of cryptographic voting protocols which guarantee desirable properties. Everlasting privacy is a privacy property that withstands the explosion of computational resources over time, allowing votes to remain private even after the cryptographic parameters of their time can be easily

brute-forced. In *Receipt-Free Remote Electronic Elections with Everlasting Privacy*, Locher and Haenni report on such an innovative protocol[37].

The final paper that was accepted for this special issue, co-authored by Neumann *et al.*, is concerned with a *Quantitative Security Evaluation Framework for Internet Voting Schemes*[46]. The paper proposes a model for comparing voting schemes within the context of any given election setting; and the model is applied to the specific context of Estonian internet voting in order to make concrete proposals concerning the type of voting system that is most appropriate to that particular context. This type of contextual reasoning/analysis is very important in the future development and procurement of 'generic' voting systems that are re-usable in different environments.

To conclude, each of the five accepted papers examines the issue of electronic voting from a different persepective. Some focus on addressing challenges in remote electronic voting; others focus on using technology to improve polling-place voting. They should provide the readers of this special issue with an overview of the range of complex challenges in the domain of electronic voting.

**Acknowledgements** Dr Gibson acknowledges the funding he received from the French ANR project IMPEX (13-INSE-0001).

## References

1. Adida, B.: Helios: Web-based open-audit voting. In: USENIX Security Symposium, vol. 17, pp. 335–348 (2008)
2. Alvarez, R.M., Hall, T.E., Hyde, S.D.: Election fraud: detecting and deterring electoral manipulation. Brookings Institution Press (2009)
3. Aranha, D.F., Ribeiro, H., Paraense, A.L.O.: Crowdsourced integrity verification of election results. Annals of Telecommunications pp. 1–11 (2016). DOI 10.1007/s12243-016-0511-1
4. Araújo, R., Rajeb, N.B., Robbana, R., Traoré, J., Youssfi, S.: Towards practical and secure coercion-resistant electronic elections. In: Cryptology and Network Security, pp. 278–297. Springer (2010)
5. Arthur, J.K., Adu-Manu, K.S.: A trustworthy architectural framework for the administration of e-voting: The case of Ghana. International Journal of Computer Science Issues (IJCSI) **11**(3), 97 (2014)
6. Bell, S., Benaloh, J., Byrne, M.D., DeBeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S., et al.: Star-vote: a secure, transparent, auditable, and reliable voting system. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) (2013)
7. Braun, N.: Stimmgeheimnis: Eine rechtsvergleichende und rechtshistorische Untersuchung unter Einbezug des geltenden Rechts. Stampfli Verlag (2005)
8. Braun, N., Brändli, D.: Swiss e-voting pilot projects: Evaluation, situation analysis and how to proceed. In: Krimmer [34], pp. 27–36
9. Budurushi, J., Renaud, K., Volkamer, M., Woide, M.: An investigation into the usability of electronic voting systems for complex elections. Annals of Telecommunications pp. 1–14 (2016). DOI 10.1007/s12243-016-0510-2
10. Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., et al.: Scantegrity ii municipal election at takoma park: The first e2e binding governmental election with ballot privacy (2010). `http://static.usenix.org/legacy/events/sec10/tech/full_papers/Carback.pdf`

11. Carter, L., Bélanger, F.: The utilization of e-government services: citizen trust, innovation and acceptance factors*. Information systems journal **15**(1), 5–25 (2005)
12. Clarkson, M.E., Chong, S., Myers, A.C.: Civitas: A secure remote voting system. In: D. Chaum, M. Kutylowski, R.L. Rivest, P.Y.A. Ryan (eds.) Frontiers of Electronic Voting, *Dagstuhl Seminar Proceedings*, vol. 07311. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany (2007)
13. Cranor, L.F., Cytron, R.K.: Sensus: A security-conscious electronic polling system for the internet. In: System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on, vol. 3, pp. 561–570. IEEE (1997)
14. Culnane, C., Ryan, P.Y., Schneider, S., Teague, V.: vvote: a verifiable voting system. ACM Transactions on Information and System Security (TISSEC) **18**(1), 3 (2015)
15. Davies, D.W., Bartlett, K.A., Scantlebury, R.A., Wilkinson, P.T.: A digital communication network for computers giving rapid response at remote terminals. In: Proceedings of the First ACM Symposium on Operating System Principles, SOSP '67, pp. "2.1–2.17". ACM, New York, NY, USA (1967). DOI 10.1145/800001.811669
16. Fernandes, N.C., Moreira, M.D., Moraes, I.g.M., Ferraz, L.H.G., Couto, R.S., Carvalho, H.E., Campista, M.E.M., Costa, L.H.M., Duarte, O.C.M.: Virtual networks: Isolation, performance, and trends. Annals of telecommunications-annales des télécommunications **66**(5-6), 339–355 (2011)
17. Fuller, R.B.: No More Secondhand God: And Other Writings. Southern Illinois University Press (1967)
18. Gjøsteen, K., Lund, A.S.: An experiment on the security of the norwegian electronic voting protocol. Annals of Telecommunications pp. 1–9 (2016). DOI 10.1007/s12243-016-0509-8
19. Gonggrijp, R., Hengeveld, W.J.: Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective. In: EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2007 on Electronic Voting Technology Workshop. USENIX Association, Berkeley, CA, USA (2007)
20. Goodman, N.J.: Internet voting in a local election in canada. In: The Internet and Democracy in Global Perspective, pp. 7–24. Springer (2014)
21. Gritzalis, D.: Principles and requirements for a secure e-voting system. Computers & Security **21**(6), 539–556 (2002)
22. Gronke, P., Galanes-Rosenbaum, E., Miller, P.A., Toffey, D.: Convenience voting. Annu. Rev. Polit. Sci. **11**, 437–455 (2008)
23. Haber, S., Benaloh, J., Halevi, S.: The helios e-voting demo for the international association for cryptologic research (IACR). IACR, May (2010)
24. Halderman, J.A., Teague, V.: The new south wales ivote systevem: Security failures and verification flaws in a live online election. In: E-Voting and Identity, pp. 35–53. Springer (2015)
25. Heiberg, S., Parsovs, A., Willemson, J.: Log analysis of estonian internet voting 2013–2014. In: E-Voting and Identity, pp. 19–34. Springer (2015)
26. Hiltz, S.R., Turoff, M.: The network nation: Human communication via computer. Mit Press (1993)
27. Horst, M., Kuttschreuter, M., Gutteling, J.M.: Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. Comput. Hum. Behav. **23**(4), 1838–1852 (2007). DOI http://dx.doi.org/10.1016/j.chb.2005.11.003
28. Horster, P., Michels, M.: Der vertrauensaspekt in elektronischen wahlen. In: Trust Center, pp. 180–189. Springer (1995)
29. Jacobs, B., Pieters, W.: Electronic voting in the netherlands: from early adoption to early abolishment. In: Foundations of security analysis and design V, pp. 121–144. Springer (2009)
30. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: V. Atluri, S.D.C. di Vimercati, R. Dingledine (eds.) WPES, pp. 61–70. ACM (2005). DOI 10.1145/1102199.1102213
31. Kiniry, J.R., Morkan, A.E., Cochran, D., Fairmichael, F., Chalin, P., Oostdijk, M., Hubbers, E.: The koa remote voting system: A summary of work to date. In: U. Montanari, D. Sannella, R. Bruni (eds.) TGC, *Lecture Notes in Computer Science*, vol. 4661, pp. 244–262. Springer (2006)

32. Kiniry, J.R., Morkan, A.E., Cochran, D., Oostdijk, M., Hubbers, E.: Formal techniques in a remote voting system. SIGSOFT Softw. Eng. Notes **31**(6), 1–2 (2006). DOI http://doi.acm.org/10.1145/1218776.1218793
33. Kohno, T., Stubblefield, A., Rubin, A.D., Wallach, D.S.: Analysis of an electronic voting system. In: IEEE Symposium on Security and Privacy (S&P04), pp. 27–40. IEEE (2004)
34. Krimmer, R. (ed.): Electronic Voting 2006: 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC, August, 2nd - 4th, 2006 in Castle Hofen, Bregenz, Austria, *LNI*, vol. 86. GI (2006)
35. Krimmer, R., Volkamer, M.: Bits or paper? comparing remote electronic voting to postal voting. In: K.V. Andersen, Å. Grönlund, R. Traunmüller, M. Wimmer (eds.) EGOV (Workshops and Posters), *Schriftenreihe Informatik*, vol. 13, pp. 225–232. Universitätsverlag Rudolf Trauner, Linz, Austria (2005)
36. Lindeman, M., Stark, P.B.: A gentle introduction to risk-limiting audits. IEEE Security & Privacy (5), 42–49 (2012)
37. Locher, P., Haenni, R.: Receipt-free remote electronic elections with everlasting privacy. Annals of Telecommunications pp. 1–14 (2016). DOI 10.1007/s12243-016-0519-6
38. Maaten, E.: Towards remote e-voting: Estonian case. In: A. Prosser, R. Krimmer (eds.) Electronic Voting in Europe, *LNI*, vol. 47, pp. 83–100. GI (2004)
39. Madise, Ü., Martens, T.: E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. In: Krimmer [34], pp. 15–26
40. McGaley, M., Gibson, J.P.: E-Voting: A Safety Critical System. Tech. Rep. NUIM-CS-TR-2003-02, NUI Maynooth, Computer Science Department (2003)
41. Mercuri, R.: A better ballot box? IEEE Spectr. **39**(10), 46–50 (2002). DOI http://dx.doi.org/10.1109/MSPEC.2002.1038569
42. Mercurio, B.: Democracy in decline: can internet voting save the electoral process. J. Marshall J. Computer & Info. L. **22**, 409 (2003)
43. Mohen, J., Glidden, J.: The case for internet voting. Commun. ACM **44**, 72–85 (2001). DOI http://doi.acm.org/10.1145/357489.357511
44. Monnoyer-Smith, L.: How e-voting technology challenges traditional concepts of citizenship: an analysis of french voting rituals. In: Krimmer [34], pp. 61–68
45. Mote Jr, C.: Report of the national workshop on internet voting: issues and research agenda. In: Proceedings of the 2000 annual national conference on Digital government research, pp. 1–59. Digital Government Society of North America (2000)
46. Neumann, S., Volkamer, M., Jurlind, B., Prandrini, M.: Secivo: A quantitative security assessment model for internet voting schemes. Annals of Telecommunications pp. 1–14 (2016)
47. Pammett, J.H., Goodman, N.: Consultation and evaluation practices in the implementation of internet voting in canada and europe (2013). Ottawa: Elections Canada, research report
48. Pinault, T., Courtade, P.: E-voting at expatriates' mps elections in france. In: Electronic Voting, pp. 189–195 (2012)
49. Serdult, U., Germann, M., Mendez, F., Portenier, A., Wellig, C.: Fifteen years of internet voting in switzerland [history, governance and use]. In: 2015 Second International Conference on eDemocracy & eGovernment (ICEDEG), pp. 126–132. IEEE (2015)
50. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J.A.: Security analysis of the estonian internet voting system. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 703–715. ACM (2014)
51. Staveley, E.S.: Greek and Roman Voting and Elections. [London]Thames & Hudson (1972)
52. Villafiorita, A., Weldemariam, K., Tiella, R.: Development, formal verification, and evaluation of an e-voting system with vvpat. Trans. Info. For. Sec. **4**(4), 651–661 (2009). DOI http://dx.doi.org/10.1109/TIFS.2009.2034903
53. Zissis, D., Lekkas, D.: Securing e-government and e-voting with an open cloud computing architecture. Government Information Quarterly **28**(2), 239–251 (2011)

Author/s:
Gibson, JP;Krimmer, R;Teague, V;Pomares, J

Title:
A review of E-voting: the past, present and future

Date:
2016-08-01

Citation:
Gibson, J. P., Krimmer, R., Teague, V. & Pomares, J. (2016). A review of E-voting: the past, present and future. Annales des Telecommunications/Annals of Telecommunications, 71 (7-8), pp.279-286. https://doi.org/10.1007/s12243-016-0525-8.

Persistent Link:
http://hdl.handle.net/11343/283292