To be published in proceedings of the International Conference on Human Aspects of Information Security, Privacy and Trust (HAS) at HCII-2017

An Assessment of the Security and Transparency Procedural Components of the Estonian Internet Voting System

Jason R.C. Nurse[†1], Ioannis Agrafiotis[1], Arnau Erola[1], Maria Bada[1,2], Taylor Roberts[1,2], Meredydd Williams[1], Michael Goldsmith[1,2], and Sadie Creese[1,2]

[1]Department of Computer Science, University of Oxford, Oxford, UK
[2]Global Cyber Security Capacity Centre, University of Oxford, UK
[†]jason.nurse@cs.ox.ac.uk

Abstract. The I-Voting system designed and implemented in Estonia is one of the first nationwide Internet voting systems. Since its creation, it has been met with praise but also with close scrutiny. Concerns regarding security breaches have focused on in-person election observations, code reviews and adversarial testing on system components. These concerns have led many to conclude that there are various ways in which insider threats and sophisticated external attacks may compromise the integrity of the system and thus the voting process. In this paper, we examine the procedural components of the I-Voting system, with an emphasis on the controls related to procedural security mechanisms, and on system-transparency measures. Through an approach grounded in primary and secondary data sources, including interviews with key Estonian election personnel, we conduct an initial investigation into the extent to which the present controls mitigate the real security risks faced by the system. The experience and insight we present in this paper will be useful both in the context of the I-Voting system, and potentially more broadly in other voting systems.

Key words: E-Voting; Cybersecurity; Transparency; Procedural controls; Human Factors; Practical experiences

1 Introduction

Electronic voting (or e-voting) is widely understood as the use of electronic means to record, process or tally votes. As the use of the Internet has become a central part of modern society, several countries have looked to apply Internet technologies to support the e-voting process. Nations that have utilised some form of Internet voting include the US, Canada, Estonia, and India [1]. The first state to allow online voting nationwide was Estonia, in 2005, via their I-Voting system. This platform is aimed specifically at taking advantage of the numerous benefits of online voting such as increased efficiency and accessibility, but also at providing a secure and reliable voting platform and process.

While some observers hail Estonia's success in Internet voting, their I-Voting system has also come under close scrutiny [2, 3, 4]. Security concerns have drawn on in-person election observations, code reviews, adversarial testing on system components, and topics such as the impact of infected voter computers and the lack of end-to-end verification. Some articles have sought to demonstrate these potential problems using simulated examples of attack payloads and patterns to compromise the electoral process [3]. Others point to the fact that integrity should be supported by technological means rather than a complex set of manual checks and procedures [4]. The sum of these assessments has led to some parties concluding that there are multiple ways in which insider threats, sophisticated criminals or nation-state attackers could successfully compromise the I-Voting system.

In this article, we reflect on the Estonian I-Voting system in light of such concerns in order to evaluate how vulnerable it may be to cyber-attacks, intentional or accidental. We limit our scope to *procedural* security components, and thus do not address purely technical issues, such as those pertaining to software engineering or encryption details. Our aim is to consider: firstly, the extent to which procedural controls employed may be adequate to protect against attacks; and secondly the extent to which the existing transparency measures are able to provide confidence in the security of the I-Voting system. This focus on procedural components is guided by the fact that the principles underpinning a secure and democratic online voting system often create conflicting requirements [5]. These conflicts have been deemed impossible to be resolved by software engineering alone [6], hence the need for and importance of broader procedural controls. Such controls are particularly crucial in the Estonian I-Voting system and its processes.

The structure of this paper is as follows: Section 2 presents an overview of the I-Voting system, including where key procedures feature and the properties that they seek to guarantee. Next, in Section 3, we present the methodology that we adopt. This is heavily based on interviews with key individuals involved in Estonian elections; this is also where our work is particularly insightful as it engages with, and triangulates data from, various officials so as to gain detailed insights into previous elections. Section 4 then presents, reflects on, and discusses our findings regarding the security offered by the procedural components of the I-Voting system, as well as highlighting areas for further improvement. Finally, in Section 5, we conclude our report.

2 The Estonian I-Voting system

Estonia is one of the most experienced countries in the world in practising electronic democracy. While there was a slow start in the local elections of 2005 with only 1.9% of votes cast using the I-Voting system, in the 2015 parliamentary elections 30.5% of votes were cast online [7]. The I-Voting system that is used for elections consists of four main components: the I-Voting Client Application (IVCA), the Vote Forwarding Server (VFS), the Vote Storage Server (VSS)

and the Vote Counting Application (VCA) [6]. The IVCA is an application released for each election that allows voters to cast their votes using a personal computing device; to vote, citizens must be connected to the Internet and have either their national ID card or a mobile ID. The VFS is the only public-facing server of the system; it is responsible for authenticating voters as they vote via the IVCA, and forwarding the votes to the VSS. The VSS stores all votes which have been cast, including repeated ones. After the close of advance polls, it checks and removes the cancelled votes, and separates the outer encryption envelopes (which hold the voter identity) from inner envelopes (which contain the vote cast).

Finally, the VCA, an offline and air-gapped server, is loaded with the valid votes. This loading is achieved via a DVD which allows votes to be securely passed from the VSS to the VCA. Next, votes are decrypted with the private key possessed by members of the National Electoral Committee (NEC), and the VCA then tabulates the votes and outputs the results. To assist the NEC in the organisation and running of the Internet voting process, in 2011 the Electronic Voting Committee was established.

Security has been a core consideration in the I-Voting system since its inception in 2005. There are a number of reports discussing the security features of the system, but one of the most comprehensive is that of the Estonian NEC [8]. Their report provides descriptions of detailed security measures on: how they ensure that the architectural components of the system will not be compromised; information on audit, monitoring, incident-handling and recovery practices; and operational measures (such as the distribution of tasks and formal procedures on managing risks) that complement technical security tools to ensure that a breach of policies is deterred. There are several key procedures to achieve these measures, including: independent auditors to verify that security procedures are followed by election officials; documented procedures for the generation and management of election keys; procedures for submitting and handling voting-related complaints and disputes; and strategies for responding to incidents or suspicious occurrences detected during online voting [6, 8].

While these procedures may go some way to address the security and privacy concerns of the system, as mentioned in Section 1 there are still many criticisms of the level of security of the I-Voting's system. To address these concerns, Estonian officials and software developers have made several modifications to the system over its lifetime. For instance, a method to verify that a vote has been cast-as-intended and recorded-as-cast has been implemented [9]. Moreover, facilities for in-depth monitoring of the voting platform have been established to allow detection of attacks on a server and system malfunctions. In addition, this monitoring enables the retrospective study of voter behaviour and issues that may have been encountered in using the system [10].

One of the most notable features of I-Voting is that large parts of the system source code, as well as full documentation on protocols and procedures, have been made publicly available [11]. The various features mentioned here and those above seek to bring I-Voting closer to fundamental constitutional require-

ments of the voting process, i.e., generality, freedom, equality, secrecy, directness and democracy [5], with security added to ensure that these principles are safeguarded.

3 Methodology for research study

Our method to assess the procedures for maintaining security and transparency in the I-Voting system consists of three main stages. The first stage involves a reflection on the I-Voting system and related electronic-voting literature. This includes reviewing all publicly available documentation (e.g., on procedures) on the system, and its challenges and weaknesses, both self-reported and those identified through independent assessments. This review allows us to gain insight into the system and also to contextualise the procedural and transparency mechanisms in order to scope our assessment.

The next stage of our methodology involves the planning and conducting of semi-structured interviews with key individuals involved in Estonian elections. Our line of questioning is designed specifically to examine many of the issues identified in our prior review. Questions cover reported voting concerns, unresolved challenges, and areas where we believe there might be security or transparency weaknesses. For the interviews themselves, we have recruited seven individuals from Estonia with detailed knowledge of, and insight into, the I-Voting system, including its design, administration, process aspects, security functions, and operations in situ; this is the criterion for participation. The majority of participants possess at least twelve years of experience with Internet voting and elections in general. This experience and expertise, including each individual's seniority in their respective organisation, is crucial to ensuring our assessment is well-informed. While we appreciate that publishing the names and roles of participants would support the credence and authority of our study, we opt for anonymous reporting of interview commentaries and findings. The main reason for this is to encourage honest and open responses, which would lead to more insightful conclusions.

After conducting interviews with these experts (each lasting approximately one hour), our final stage involves analysing the data using content analysis and, more specifically, a mixture of deductive and inductive reasoning [12]. This analysis leads to the identification of several core response themes related to the main research areas. We then reflect critically on these themes, triangulate the responses of individuals, and use these findings to guide the final assessment.

We believe that the pragmatic methodology we adopt – which is based on primary and secondary data sources – and our emphasis on engaging with those involved in Estonian elections is where our work has the most value. While we accept that first-hand (i.e., our own) observation of security during actual elections would also be ideal, our current method allows us to examine the state of security via reports from people actually present during elections and those with knowledge as to why certain security and transparency efforts may not be in place. Moreover, we are able to uncover nuances in the election system which

can help to better understand its apparent success, while also highlighting areas for future improvement. This could help inform future studies, for instance, in exploring the security of the next upcoming election.

4 Assessing I-Voting: Results and discussion

In what follows, we present and discuss the findings from our analysis and the interviews. As the section progresses, we highlight areas where procedures of the I-Voting system are performing well (i.e., functioning as expected and addressing the targeted risk), and areas which could be improved. This assessment is structured according to the two topics identified in Section 1, i.e., procedural components for security and transparency respectively.

4.1 Procedural security components

Procedural security controls are core components of the I-Voting system. These controls define the main manual activities and practices that election officials engage in to protect the system from risks. Throughout the course of the interviews, procedural controls were discussed in a variety of contexts, but the following topics were the most salient in our findings: the key role of auditors in the election process; maintaining the security of the devices and equipment used during elections; processes pertaining to handling disputes and incidents; how election knowledge and know-how is maintained and transferred; and procedures to address the risk regarding voters and their context.

The role of the auditor: Procedural security controls were referred to directly and indirectly by several interviewees. The primary report documenting these controls is the election manual, and amongst other things, its aims are to ensure: (a) that data integrity between online and offline systems is maintained; (b) that access to election systems is regulated; and (c) that there are mechanisms for dispute resolution and system continuity. These aims would work in conjunction with the variety of technical mechanisms implemented.

Auditors play a key role in ensuring that those various security processes are followed, especially in relation to maintaining data integrity in elections. For instance, there are procedures set within I-Voting to ensure that two professionals serve as auditors to observe core processes. These include when the encryption keys for the election servers are being generated, or when election data is transferred from the online server (where votes are collected) to the offline server (where they are tallied). In these instances, auditors use the election manual to ensure that all tasks relating to the secure treatment of keys and data are followed as prescribed. As one interviewee stated, "... you had to trust... that this private key of the server is not somehow leaked... and making sure that this doesn't happen actually relies quite heavily on organisational measures".

From our analysis of such measures, we found the auditing procedures in place to be well considered, and thus might reduce the potential for malicious

attacks (given that such attacks could be detected) and identify instances of human error in the conducting of procedures. This is especially helped by the fact that auditors are required to produce written reports – interim, and at the end of elections – regarding the compliance with procedures, which can be passed to the National Electoral Committee (NEC) for review or further investigation as necessary.

Devices and equipment used in the electoral process: Devices and equipment used in the electoral process are also governed by a number of procedures to mitigate potential attacks. For example, there are procedures to verify that the hardware is fit-for-purpose and malware-free, since as one interviewee stated, "[it may be] delivered to us deliberately modified to falsify our elections". From our assessment, we found existing procedural controls (such as drawing on an independent pre-voting expert analysis of system security) to be well thought out, but with a few caveats. For instance, while it is important that the experts employed have significant skills and experience in the system and security, a reality is that experts may miss severe problems [13].

An additional suggestion that we would make is for the analysis of the system to be conducted on a regular basis to account for any changes in the software and the changing threat landscape. Firmware-level malware checks are also becoming more important to mitigate the possibility of a sophisticated, and deeply-embedded attack. The concept of Advanced Persistent Threats, i.e., slow-moving and deliberate attacks applied to quietly compromise systems without revealing themselves [14], could be particularly relevant here. We highlight this given that there are increasing concerns about the ability of external parties to influence a country's elections [15].

In order to avoid physical attacks on the system (i.e., servers) and to generally maintain system resilience, we found that several security requirements have been identified for election facilities. For instance, when selecting facilities to host systems, one interviewee mentioned that there are strict "security measures of what this room must [have]" (i.e., security criteria that chosen facilities must fulfil). Given the importance of the server room, access to it is controlled, and in it, all server ports are covered with security seals (to prevent unauthorised server access) and regularly checked for tampering. Here, the tension of balancing transparency (in terms of allowing people to witness from close proximity the electoral process) and security is particularly evident, highlighting the importance of procedural controls, such as sealing the machines, to alleviate the conflict. We must note that while the use of security seals is encouraging, seals themselves are not a panacea and need to be carefully checked and of high quality to stand any chance of being effective [16].

To focus briefly on the individuals who have access to servers and the server room, interviewees mentioned that, "there are very specific people who can go [in] there". This highlights the requirement that only those adequately authorised can enter the server room. In our opinion, this was expected given the room's importance, but we were unable to verify whether any other checks are conducted to ensure that individuals cannot bring potentially malicious devices

(e.g., infected pen drives) into the room. While attacks using such devices — whether purposeful or inadvertent — may be unlikely given the relationships and professional trust described by interviewees, the risk should be considered and addressed. For instance, there could be mandatory checks for unauthorised devices prior to entering secure areas and temporary confiscation of devices as required.

A good example of the issue regarding the presence of additional devices in secure areas has already been witnessed in prior elections (e.g., see [3]). In that case, system glitches reportedly prevented the use of DVDs to transfer voting data (votes for tallying) to the VCA, and as a fall-back, officials used a removable device. This behaviour was strictly against documented procedures and protocol, and could easily have resulted in system infection had the device been compromised. Preventing additional devices from entering these areas could act to reduce the likelihood of such attacks, and potentially deter less determined attackers. Moreover, there should be well-vetted (e.g., by the Electronic Voting Committee) and agreed procedures to handle instances where glitches prohibit the usual operations of the system. These procedures should also appreciate the perspective and intentions of observers as they witness deviations from documented protocol.

Handling disputes and incidents during the electoral period: Two related areas where we found procedures to be crucial were in the handling of disputes and incidents. To comment on dispute-resolution procedures first, we were pleased that there are very clear mechanisms to contest the validity of a vote or to make a complaint about some aspect of the election. According to one interview, in order to reach a speedy resolution of the dispute, the legal time-frames are as follows: three days to file a complaint, five days to resolve the issue, and another three days to contest the decision in the Supreme Court. These procedures have helped to minimise the risk posed by questionable actions, and have provided a formal mechanism for resolving disputes.

While these mechanisms are valuable, a challenge we discovered was that it can be difficult to submit a formal complaint, as the person submitting it would need to have knowledge of legislation regarding the I-Voting. This is due to the fact that complaints that do not follow a very strict structure and do not raise an argument regarding legislative discrepancies in the voting process are not considered. Upon querying this point, interviewees stated that the Electronic Voting Committee also has instituted an informal "notice" procedure that would enable a complaint to be submitted without knowledge of the I-Voting legislation. We view this as a significant addition and one that could increase accessibility and voter confidence in the system. The only other potential improvement that could be made is to encourage increased awareness and education of the legislation regarding I-Voting; but this may not be suitable (or of interest) for a majority of individuals.

With regards to the handling of incidents, we found that a core component of the Estonian voting system is its Incident Report Centre. This centre has two purposes: to address technical glitches reported to the client support centre, and

to actively scan for anomalous behaviours in cooperation with the Computer Emergency Response Team (CERT) environment. Given the potential risk from significant threat actors, it is evident that Estonia relies on an effective CERT actively monitoring for attacks on the voting platform. From our interviews, we were especially encouraged to hear that once anomalies are registered, there are specific processes in place to address the issues appropriately, which may result in technicians being dispatched to the area of concern.

For instance, interviewees mentioned a case where a team was dispatched to a house suspected of spreading malware targeting voting applications. Although it transpired to be an elderly lady who knowingly voted more than 500 times, this case clearly demonstrates the capabilities of the incident response team to be deployed rapidly. Once incidents are identified, they are reported based on significance and severity to the NEC. The NEC may then decide to take further action and could ultimately request that affected citizens cast their vote using other means (e.g., paper ballots). This control is somewhat aggressive (i.e., it blocks further I-Voting votes for that election) but ensures that people who are facing problems voting electronically can still participate in a given election. The only other issue this raises is for people that are not within physical reach such as those outside of the country.

Procedural controls and knowledge transfer: While procedural controls can arguably improve security, it is essential that they are properly managed and communicated. This relates to one of our main concerns, i.e., the sustainability of existing security procedures, particularly knowledge definition and transfer. When asked about incorporating lessons-learned from dispute resolution measures for example, one interviewee said, "if you're asking if we have some sort of formalised process for that then, no". Our interactions with interviewees made it clear that such information is generally incorporated in post-election reflections, however, there are few formal mechanisms to guide or ensure that incorporation. This may work well for a close-knit society such as that of Estonia; lack of procedural formality on the other hand does risk some aspects being inadvertently overlooked or forgotten. More broadly, this might also raise concerns about insider attacks, given that if procedures are not formalised and accessible to observers and auditors, that reduces the ability to monitor that they are being followed and that associated risks are being addressed. We would, therefore, strongly recommend that more formal procedures be put in place to facilitate the definition, assessment, transfer and persistence of election knowledge and know-how.

Staffing is another point worth considering in this general context. Given that most of the electoral staff have remained the same over time, in our interviews we noticed a general feeling that everyone already knows what to do. Indeed, one interviewee stated, "they already know what to do, so we don't go on details over it," i.e., some aspects of the system or processes. While it is advantageous to have a core set of professionals to rely upon, in our judgement the extent to which there are formalised procedures for staff training and knowledge sharing was unclear. This could be very important for knowledge-transfer generally and

especially if future vote collection is outsourced, as one interviewee suggested it might be. Moving forward therefore, emphasis should be placed on ensuring that all procedures and security knowledge regarding the I-Voting process are fully documented and disseminated to ensure system sustainability.

Voter technology and the risks: Human voters and the technology they use to vote (e.g., PC, mobile) have been recognised as the most vulnerable link in the I-Voting system [8]. Interviewees generally agreed with this point, even stating, "e-voting [has been introduced] by accepting the risk that the voter is the weakest link [...] we cannot deny that many things can happen in the voter's computer". This highlights the fact that there is little chance to fully control the voter environment, albeit acknowledging that the system will "still depend on [it] being virus free". Herein lies the challenge therefore.

To avoid potentially malicious code-insertion attempts to compromise the voting system, input from public interfaces (e.g., voters) is thoroughly verified to ensure that "the elements of the digital signature are there, that the zip container is well formed". Moreover, the decrypted ballot is checked for compliance against rules that have been set to define valid ballots. These are commendable practices, as it is of crucial importance that malformed votes are removed before reaching the main systems (e.g., the VSS). In the past, technically-skilled voters have actually engineered the official application code "[to] change the [candidate] number to reflect a non-existent candidate or to write some completely garbled code and then they have encrypted this"; these may be regarded as protest votes. This ability to customise the content sent to the system is why checks on incoming votes are helpful, as they can assist in blocking attacks such as malware injection attempts, and thereby protect the security of the system.

Although a fundamental risk emanates from the voter's device, a large-scale attack affecting voter machines is considered highly unlikely by the NEC [8]. The risk is accepted because of the perceived low likelihood of undetected malware affecting a significant proportion of votes. Looking forward, however, we believe the probability of a large-scale attack to be higher. This is due to the increasing prevalence of malware infections impacting home users [17, 18] and the shifting threat landscape towards attacking election systems [15].

Moreover, in the past, citizens in Estonia have used pirated, and thus potentially insecure [19], operating systems. We refer to an incident a few years ago where a significant number of Internet voters had issues voting. It transpired that the reason for this was that they were using the pirated version of Windows. This issue is especially worrying because as one interviewee recounted, "people who did not have official ... Windows XP were not able to build up a secure channel between the application and the server. So some layers of security had to be changed on the first day. [...] we didn't expect that so many people would have [problems]". This therefore demonstrates the impact on system security.

If we extend this particular example, one can imagine an attacker exploiting a widespread use of pirated software in two ways. In one way, an attacker may insert malware into a pirated version of Windows (or another popular application), and promote this to Estonian citizens via bit-torrent applications or

illegitimate third-party app stores. Or, a simpler way is to disguise malware as a legitimate files (e.g., software, games, apps, etc.) — a common practice as highlighted in [20] — and again, promote it to Estonian citizens. These are, of course, only thought experiments; however, determined attackers may find novel ways to exploit such situations, if only to cause havoc.

Also, while there are warnings on both the voter application and election websites advising voters to install anti-virus software (as seen in [21]), we believe that efforts should focus as well on larger issues including educating users about the perils of pirated or unsupported software. The Windows XP case may not be an isolated incident, and it would be prudent to plan for such potential issues, especially given Estonia's strides towards a digital society.

4.2 Transparency measures

Transparency measures seek to provide insight into the I-Voting system and the way it functions, with the aim of building public trust and confidence. Our analysis of these measures explores three key areas: the auditing, observation and monitoring of the election process; the broad topic of public awareness of e-voting and secure practices; and the ability for voters to verify their votes.

Auditing, observation, and monitoring of the election process: The monitoring of the I-Voting process by auditors was one of the main transparency measures cited by interviewees. As discussed in Section 4.1, several independent auditors are contracted by the voting committee during an election period to provide feedback on the extent to which critical processes are followed. After elections, they provide a report with their findings, which is then published. Reflecting on this process, it is our opinion that the use of auditors and the publication of subsequent audit reports can act to increase trust in the I-Voting process. The only question that we would raise here is with regards to the extent to which these reports are publicly available and comprehensible to lay readers; the more accessible and easier to understand, the better. Although some reports suggest that they are accessible [3], others speak to the contrary [2].

In addition to auditors, observers drawn from the public are allowed to witness the election process. A press release before the elections invites the public and all political parties to observe the I-Voting process in situ. Anyone can serve as an observer; no formal vetting is undertaken, and the process is such that they can view elections in real-time and comment with suggestions and feedback. In our judgement, and considering earlier findings regarding procedural controls, we were especially interested in how such feedback was used by election officials. We were pleased to discover that there is a method to capture and reflect on this feedback, both during and after elections. One example of this is the change from the use of only formal complaints to less formal 'notice' procedures when issues are identified by observers or voters.

One challenge that we noted, which was also expressed by interviewees, was that observers often do not fully understand the voting system. The electoral

committee is obliged to offer a two-day course for observers to learn the technical details, but attendance is low. Moreover, the majority of attendees do not complete the course, due to an overload of (often complex) information. This is an interesting conundrum yet to be addressed, since the manner in which the committee can communicate details to the public is rather restricted, due to political and party complexities. Certain parties believe that the I-Voting system is favoured by the government and influences the outcome of elections, therefore rendering any intervention as a political problem. As pointed out by interviewees, concerns regarding misleading the public may be raised if the technical details are simplified. An outstanding challenge, therefore, is to balance voter interest and political considerations. This is particularly important because some voters may not be interested in technical aspects, but still wish to understand how the system maintains standard voting requirements (as mentioned in [5]).

Publication of the system documentation is one of the most crucial transparency measures [6]. These documents cover topics from preparing the system, to conducting e-voting and final operational procedures. The filming of critical processes (e.g., server software installation) is also conducted for purposes of transparency. Speaking with reference to the server details, one interviewee mentioned, "... the screen of a computer is filmed as key procedures are performed ... and 97% of the code used is also made public". Some of these videos have also been released post-election on YouTube for public consumption.

We view the publication of documents, code (particularly for community review) and videos as encouraging transparency measures that should be continued. However, as highlighted by other articles [3], better care must be taken to ensure security despite the pursuit of transparency. A perfect example of this issue is inadvertently exposing sensitive information (e.g., passwords) in published videos, or observers being able to take photos or film passwords themselves. Balancing security and transparency in such cases is not trivial, but careful planning and procedures (e.g., being aware of when sensitive data is being entered and protecting that data-entry) may allow for an adequate balance to be struck. Here, we need to note our finding that further procedural measures have been implemented to prohibit such issues and that videos are now uploaded online only after the elections have concluded.

With regard to the 3% of the code that is not published, we discovered that this is focused on malware detection and avoidance at the voter's machine, and therefore, publication would effectively defeat its purpose. We found two transparency procedures implemented to protect voters here. Firstly, the code is checked and audited by independent and trusted third parties, and secondly, the voting protocol is fully documented online and hence any individual (given the appropriate skills) could create their own compliant voting software. It is our view that these efforts by election officials are well-considered for the assessed risk, and they also demonstrate a notable impetus towards a transparent system. As the threat landscape shifts and adversaries become more determined, however, current practice around unpublished code will need to be revisited as security through obscurity is known to be ineffective [22].

E-voting security and awareness: Awareness is another important factor in supporting transparency. At its initial launch, the I-Voting system was heavily promoted to enable the public to understand the online voting process and the core aspects of security. As mentioned above, there is also a significant amount of detail on the system available online (e.g., NEC documents) [8, 11]. In this way, trust might be built based on information and understanding. More recently, when the phone-based vote-verification application was released, there were media campaigns and articles explaining to the public how to engage with the new technology.

We noticed, however, that there does not appear to be a comprehensive, ongoing (that is, before and during elections) official campaign to promote secure online voting. Such a campaign should be grounded in best practice [23, 24] and focused on raising public awareness of the range of risks as well as how they might be mitigated. For instance, mitigation via secure practices such as updating anti-virus solutions (though the current value of anti-virus might be debatable, it is a still a first line of defence [25]). We note the formal acceptance of the risk present with voter PCs (NEC) [8] and the mention of anti-virus software on the voting page, but still felt that more effort is required.

When we mentioned these points to interviewees, they reported that such campaigns were run in the past and are considered for the future, but there were political challenges with bespoke online voting campaigns. That is, such efforts were seen by some political parties to prefer or give more attention to one form of voting over another. This is a difficult predicament, but we would recommend two potential solutions that are worth exploring. These are: running smaller security-focused campaigns for all voting methods (on and offline); and/or incorporating such information into e-governance campaigns more broadly.

The next municipal elections (scheduled for October 2017) might be an ideal opportunity to explore the suggestions mentioned above. This is because Estonia has lower the local-election voting age to sixteen [26]. This new development will create around 24,000 potential new voters, so a special awareness campaign is expected for them. Having online safety as part of the school curriculum would also build awareness and provide a better understanding of how I-Voting procedures are established, thus benefiting online-voting transparency. We have already witnessed awareness campaigns in Estonia, but these have been promoted via other, non-governmental means [27].

Verification of votes: Allowing citizens to verify their votes via a smartphone application is another measure used within the I-Voting system to enhance transparency. Procedurally, the verification application performs as expected and appears simple to use. According to one interviewee, "the verification application allows for actual proof of the process and enhances trust". This has also been witnessed through a user study of the system where officials found that even though only around 3% of the voters verified their votes, the availability of the application increased their confidence in the system generally.

In our judgement it was encouraging to witness the separation in devices used for casting and verifying votes. Amongst other aspects, this meant that

successful vote-hijacking, particularly on a large-scale, would be challenging, as malicious parties would need to control both users' PCs and smartphones. We do stress, however, that the application will only be truly helpful to the I-Voting process and related security concerns, if it is widely used. There are approaches towards this goal (e.g., the availability of the application on Android, iOS and Windows platforms), and future efforts in information dissemination (e.g., via official government websites) and wider educational campaigns should continue to encourage its use. Another area worth further consideration is whether usability issues, which are common with vote-verification systems [28], might have influenced the uptake of the application. We are yet to find any publications or usability studies of the application, so would recommend this as an imperative area of future research. If it is the case that usability is an issue, designers will need to reconsider the application, as vote-verification is a critical part of transparency in I-Voting.

4.3 Summarising the state-of-security of the I-Voting system

Reflecting generally on our analysis and interview findings as discussed above, there were many positives, but also some challenges and areas for improvement. We found that procedural security controls are fundamental to the system as designed, and overall they go a long way towards mitigating certain attacks. Procedures that are particularly well considered include: the use of independent auditors to ensure system compliance and monitor for any issues; and the processes by which disputes and incidents are handled by election officials. These procedures enable the prevention and detection of various attacks (intentional and accidental) that may seek to compromise the voting process.

As highlighted in our assessment, there are areas where procedures may be improved. For instance, while crucial procedures are clearly documented, some situations appear to be addressed in more informal ways which rely heavily on staff knowledge. These processes still work well given the close professional relationships between officials, and their vast experience, but this could change if key individuals leave their roles or are unexpectedly unable to participate. Furthermore, if procedures are not always formally defined, observers and auditors have little against which to judge whether actions by election officials are valid or are actually part of an insider attack, whether accidental or intentional.

Another area of potential improvement pertains to procedures on the assessment of devices and equipment. We believe that the security of the system could be enhanced by: conducting a more thorough initial assessment of election servers (e.g., for firmware level malware); engaging in mandatory checks for unauthorised devices prior to allowing persons' entry to secure areas; and having suitable system continuity plans to avoid unauthorised deviations from procedures. It may also be appropriate to revisit the risks originating from the voter's environment given that there are an increasing number of large-scale, sophisticated attacks which make such risks more salient today.

Focusing on the topic of transparency, we found that the measures adopted appear to have had a noteworthy impact on building confidence and trust in the

I-Voting system both locally and internationally. The publishing of system documentation, source code and election videos, in addition to the open-door policy on election observers, are crucial initiatives in maintaining such transparency. As such, we would strongly recommend that these continue. With respect to procedural improvements, there are a few areas we identified in our assessment. These particularly relate to the difficulty in educating observers, running voting awareness campaigns and in increasing voter usage of transparency measures (e.g., verification). We have suggested small security-focused campaigns for all voting methods – thus not preferring one over the other – and this may also be used to highlight the benefits of verifying votes as well as generally being secure. It is important that politics does not leave voters at a disadvantage, and that they have the support they need in understanding voting processes to the extent that they feel appropriate and comfortable.

Lastly, we must state that even though the research methodology that we adopted is sound, our research relies heavily on interview reports on voting systems from individuals in Estonia; this is as opposed to direct observation of the I-Voting process in situ. We attempted to counteract this limitation by engaging in a critical reflection on the documented system and existing literature, and also by interviewing a range of experts from across Estonia. In the future, we hope to expand on this study, and further address these issues in two ways. The first way is in terms of participants, and aiming to have named officials engage with us via several rounds of interviews. This would help us delve into greater detail and conduct more critical analyses. Secondly, we would seek to participate in actual election observations (the October 2017 local government elections would be an ideal opportunity).

4.4 The new I-Voting system

With the core topic areas of this article now examined, we briefly expand on our work to discuss the upcoming version of the I-Voting system. Whilst we were aware that there were plans for a new system iteration before our study commenced, it was only during the interview process that we recognised how different it would be. This future system is the result of more than ten years of experience in e-democracy — from laws and regulations to technical and socio-technical aspects. This was a point that interviewees emphasised, i.e., the system was not being overhauled due to concerns about its integrity, but rather it was felt to be the appropriate time to update the full system (including enriching server-side code, as opposed to incremental improvements, as has been done for many years).

One of the most significant changes in the new system will be its structure and focus on returning complete authority to the NEC. In line with this goal, there are a few key modifications worth noting. First, as was mentioned in Section 4.1, the vote collection system (i.e., the system that interacts with voters directly) is likely to be outsourced. The benefit of this change is that in order to run an election, the NEC only needs to provide directives, the list of candidates, the cryptography to be used and the key and e-signature methods. Second,

given the shift in power, the Electronic Voting Committee is to be dissolved. To accommodate for the technical understanding required to fulfil the new charter of the NEC, an IT auditor will assume a role on the NEC.

To comment on these changes generally, we view the decision to return the power to the NEC as a commendable move for democracy. This is especially the case given that an IT auditor will now be a core part of the election oversight and process. Our main concern with this new approach relates to the selection of companies to implement the vote collection system, and the level of checks on code and processes that will be conducted. It is crucial that any tendering process for the selection of companies to build election systems is monitored for fairness. Furthermore, it is essential that the good practices highlighted in our analyses above (e.g., independent assessments, code reviews, and audits), are continued to avoid placing democracy at risk.

Another finding of interest from interviewees was that the next iteration of the voting system will shift, in part, from procedures to incorporate more technology. This is likely to mean that monitoring will be reduced, and only processes related to encryption of results will be subject to observation. By reducing the amount of monitoring, public trust in the system may be affected. One interviewee noted that, "It is trust in mathematics rather than people," where the shift would occur. We agree that the move to an end-to-end verifiable and formally-proven system is ideal in many ways. The difficulty will come in communicating these details to the general public, when current engagement in courses for the mainly procedural system is low. The very nature of voting and its link to democratic rights means that attempts must be made for more accessible outlets for information about the national e-voting system.

A point related to our reflection above is the goal of the new system to allow for more formal verifiability. This particularly refers to making server-side operations more mathematically transparent and comprehensive as compared to previous years. This is clearly important as any changes in the votes, such as deletion or modification, will be more-easily detected. It is premature to report specifics of the new system, but as one interviewee stated, "[the] tender description suggests that it will include mix-nets, homomorphic encryption and provable decryption, and that the existing double envelop method will remain"; also, the server code will be openly published. These modifications will enable officials to prove that the decryption and tabulation of votes is performed correctly, and give additional assurance to external parties that want to verify election results.

Lastly, there is also the fact that for this new system, there will be a more substantial reliance on voter and client support. If voters notice that the system is not performing as expected, they will require various options for assistance. In the current system, there are several excellent support options and we would hope that this would continue in the future. Moreover, an interviewee pointed out that, "the new system could be used also outside Estonia in the future", as there is the possibility of removing its linkages to the Estonian ID card. This highlights a broader scope, but only time will tell whether such a system would be adopted outside of Estonia.

5 Conclusion

Estonia has been one of the main countries pioneering the adoption of a national Internet voting system. Our aim in this article was to assess the procedures relating to security and transparency in the system, and the extent to which they fulfilled their aims. While we found areas where these procedures performed well, there were also areas that could be improved. Some of these improvements are straightforward, but others (e.g., instituting awareness campaigns) require more delicate handling to avoid political controversy. Overall, we view the I-Voting system as one with many successes, but these arguably rely heavily on the expertise, knowledge and professional relationships between the individuals involved. This works for a close-knit society such as Estonia, but may be problematic in other, larger contexts.

We deem our article to be well-timed since the Estonian system will be changed significantly for the next elections in 2017. It is of paramount importance that the decision on which controls will be discarded will follow a certain procedure and that citizens' feedback will be taken into account. The I-Voting system has established a trust relationship with its citizens, and though mathematical proofs are scientifically justifiable as more secure, they may not necessarily provide the same assurance to citizens. This is especially true considering that citizens currently show little interest in technical system details. Still, with major changes on the horizon, it is essential that procedures are continuously critically reflected on and improved.

Acknowledgements

This research has been funded by the European Social Fund and the Estonian Government. It has been conducted on behalf of the Cyber Studies Programme at the Department of Politics and International Relations, University of Oxford. A much earlier version of this paper is available on the Cyber Studies Programme working paper series website.

References

1. i Esteve, J.B., Goldsmith, B., Turner, J.: International experience with e-voting. International Foundation for Electoral Systems (2012)
2. Organisation for Security and Co-operation in Europe (OSCE): Estonia Parliamentary Elections, OSCE/ODIHR Election Expert Team Final Report (2015) http://www.osce.org/odihr/elections/estonia/160131.
3. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J.A.: Security analysis of the Estonian Internet voting system. In: ACM SIGSAC Conference on Computer and Communications Security, ACM (2014) 703–715
4. Halderman, J.A.: Practical attacks on real-world e-voting. In Hao, F., Ryan, P.Y., eds.: Real-World Electronic Voting: Design, Analysis and Deployment. (2016)

5. Gritzalis, D.A.: Principles and requirements for a secure e-voting system. Computers & Security **21**(6) (2002) 539–556
6. Estonian National Electoral Committee: Internet Voting in Estonia (n.d.) http://www.vvk.ee/voting-methods-in-estonia/engindex/#Brief_description_of_the_I-voting_system.
7. Estonian National Electoral Committee (NEC): Statistics about Internet Voting in Estonia (2005) http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.
8. Ansper, A., Buldas, A., Jrgenson, A., Oruaas, M., Priisalu, J., Raiend, K., Veldre, A., Willemson, J., Virunurm, K.: E-voting concept security: Analysis and measures. Technical Report EH-02-02, Estonian National Electoral Commitee (2010)
9. Heiberg, S., Parsovs, A., Willemson, J.: Log analysis of Estonian Internet voting 2013–2014. In: Conference on E-Voting and Identity, Springer (2015) 19–34
10. Heiberg, S., Willemson, J.: Verifiable Internet voting in Estonia. In: 6th International Conference on Electronic Voting (EVOTE), IEEE (2014) 1–8
11. Estonian National Electoral Committee: E-voting system: A general overview (2010) http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf.
12. Berg, B.: Qualitative research methods for the social sciences. Pearson, MA (2004)
13. Yee, K.P.: Extending prerendered-interface voting software to support accessibility and other ballot features. EVT **7** (2007)
14. Friedberg, I., Skopik, F., Settanni, G., Fiedler, R.: Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security **48** (2015) 35–57
15. Schneier, B.: By November, Russian hackers could target voting machines (2016) https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/.
16. Appel, A.W.: Security seals on voting machines: A case study. ACM Transactions on Information and System Security (TISSEC) **14**(2) (2011)
17. PCWorld: Malicious, large-scale Google ad campaign slams users with malware (2015) http://www.pcworld.com/article/2907492/largescale-google-malvertising-campaign-hits-users-with-exploits.html.
18. ZDNet: Mirai botnet attack hits thousands of home routers, throwing users offline (2016) http://www.zdnet.com/article/mirai-botnet-attack-hits-thousands-of-home-routers-throwing-users-offline/.
19. TechRepublic: Pirated copies of Windows OS in China prone to security issues (2013) http://www.techrepublic.com/blog/asian-technology/pirated-copies-of-windows-os-in-china-prone-to-security-issues/.
20. Cuevas, R., Kryczka, M., González, R., Cuevas, A., Azcorra, A.: Torrentguard: Stopping scam and malware distribution in the bittorrent ecosystem. Computer Networks **59** (2014) 77–90
21. Estonian National Electoral Committee (NEC): Elections and Internet voting (n.d.) https://www.valimised.ee/eng/juhis.
22. Hoepman, J.H., Jacobs, B.: Increased security through open source. Communications of the ACM **50**(1) (2007) 79–83
23. Bada, M., Sasse, A., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society. (2015) 118–131
24. Kritzinger, E., von Solms, S.H.: Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security **29**(8) (2010) 840–847
25. Sukwong, O., Kim, H., Hoe, J.: An empirical study of commercial antivirus software effectiveness. Computer **44**(3) (2010) 63–70

26. Parliament of Estonia: The Riigikogu gave 16 and 17 year olds the right to vote at local elections (2015) https://www.riigikogu.ee/en/press-releases/the-riigikogu-gave-16-and-17-year-olds-the-right-to-vote-at-local-elections/.
27. UNITE-IT: Get Online Week (2016) http://www.unite-it.eu/profiles/blogs/get-online-week-2016-in-estonia-raising-awareness-and-contest.
28. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: From error to error: Why voters could not cast a ballot and verify their vote with helios, prêt à voter, and scantegrity ii. USENIX Journal of Election Technology and Systems (JETS) (2015) 1–25