Cyber Studies PROGRAMME

UNIVERSITY OF OXFORD

www.politics.ox.ac.uk/centre/cyber-studies-programme.html

Working Paper Series – No. 6 September 2016

An Independent Assessment of the Procedural Components of the Estonian Internet Voting System

Jason R.C. Nurse
Research Fellow, Department of Computer Science, University of Oxford
jason.nurse@cs.ox.ac.uk

Ioannis Agrafiotis
Research Fellow, Department of Computer Science, University of Oxford
ioannis.agrafiotis@cs.ox.ac.uk

Arnau Erola
Postdoctoral Researcher, Department of Computer Science, University of Oxford
arnau.erola@cs.ox.ac.uk

Maria Bada
James Martin Fellow, Global Cyber Security Capacity Centre, University of Oxford
maria.bada@cs.ox.ac.uk

Taylor Roberts
James Martin Fellow, Global Cyber Security Capacity Centre, University of Oxford
taylor.roberts@cs.ox.ac.uk

Meredydd Williams
Doctoral Candidate in Cyber Security, Department of Computer Science, University of Oxford
meredydd.williams@cs.ox.ac.uk

Michael Goldsmith
Senior Research Fellow, Department of Computer Science, University of Oxford
michael.goldsmith@cs.ox.ac.uk

Sadie Creese
Professor of Cybersecurity, Department of Computer Science, University of Oxford
sadie.creese@cs.ox.ac.uk

European Union
European Social Fund

Investing
in your future

This publication is funded by the European Social Fund and the Estonian Government

ABSTRACT

The I-Voting system that was designed and implemented in Estonia in 2005 is the first Internet voting system to have been adopted anywhere in the world. Since its inception, it has been met with both praise and scrutiny. Concerns include in-person election observations, code reviews, and adversarial testing on system components. As a result of these concerns, some parties have concluded that there are various ways in which insider threats and sophisticated external attacks could compromise the system's integrity and thus the voting process.

This paper examines the procedural components of the I-Voting system, with an emphasis on the controls related to procedural security mechanisms, high-level operational security aspects, and system transparency measures. The methodological approach is based on both primary and secondary data sources, including interviews with key Estonian election personnel, in order to determine the extent to which the present controls mitigate the security risks faced by the system.

This study makes three main arguments. First, we found procedural controls to be fundamentally important to the design of the I-Voting system. While these mechanisms go a long way toward preventing cyberattacks, problems in the system still exist. For instance, some security situations appear to be addressed in informal ways which rely heavily on the knowledge, experience, and professional relationships between officials. Second, in terms of operational controls, we were generally impressed by the state of the controls adopted, particularly the incident-handling processes during elections, as well as checks and investigations during and after elections. Our main concern regarding resilience is the increasing potential for more highly sophisticated attacks. As time progresses, attackers will naturally become stronger, and systems will have to adapt in order to accommodate this evolution. Third, the system's transparency measures have had a noteworthy impact on building confidence and trust in the I-Voting system, both locally and internationally. Challenges still exist, however, especially pertaining to the difficulty in running voter awareness campaigns, as well as increasing voter usage of transparency measures.

INTRODUCTION

Electronic voting (or e-voting) is widely understood as the use of electronic means to record, process, or tally votes. Almost all election systems today have some electronic components. In general, therefore, voting systems either possess some electronic components or are procedurally dependent on electronic systems. As use of the Internet becomes more and more central to modern society, several countries—including the United States, Canada, India, and Estonia—have used Internet technologies to support e-voting.[1] Estonia, via their Internet voting (I-Voting) system in 2005, was the first state to allow online voting nationwide. This system aimed to take advantage of the numerous benefits of online voting (e.g., increased efficiency and accessibility), but also to provide a secure and reliable voting process and platform.

While many observers hail Estonia's success in e-voting, their I-Voting system has also come under great scrutiny.[2] Concerns have been based on in-person election observations, code reviews, and adversarial testing on system components. As a result, some parties have concluded that there are multiple ways in which insider threats, sophisticated online criminals, or nation-state attackers could successfully compromise the I-Voting system. Clearly these are serious concerns, given the potential impact of system compromise on democracy and the rights of Estonian citizens.

In this paper, we examine the Estonian I-Voting system in light of such concerns in order to understand how vulnerable the system may be to cyberattacks or accidental disruption. We review the general procedural security components of the system, particularly procedural security controls, high-level operational security aspects, and transparency measures. We therefore do not focus

1 Jordi Barrat i Esteve, Ben Goldsmith, and John Turner, "International experience with e-voting," International Foundation for Electoral Systems (2012).

2 Barbara Simons, "Verified Voting Blog: Report on the Estonian Internet Voting System," September 2011, https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/, accessed 1 June 2016; Sven Heiberg, Peeter Laud, and Jan Willemson, "The Application of I-voting for Estonian Parliamentary Elections of 2011," in E-Voting and Identity, (September 2012) pp. 208-223. Springer Berlin Heidelberg; Organisation for Security and Co-operation in Europe (OSCE), "Estonia Parliamentary Elections OSCE/ODIHR Election Expert Team Final Report," May 2015, http://www.osce.org/odihr/elections/estonia/160131, accessed 12 April 2016; Drew Springall et al., "Security analysis of the Estonian internet voting system," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Arizona, USA, 3-7 November 2014, pp. 703-715.

on software engineering or encryption related issues in the computer systems. Our scope is guided by the fact that the fundamental principles underpinning a secure and democratic online voting system create conflicting requirements.[3] These conflicts cannot be resolved by software engineering alone,[4] hence the need for, and importance of, broader procedural controls. Such controls are particularly crucial in the Estonian I-Voting system and process.

The specific research questions we aim to explore are as follows:

RQ1:
To what extent are the procedural controls employed in the Estonian I-Voting system adequate protection against attacks?

RQ2:
What operational security measures are employed in the Estonian I-Voting system, and how resilient is this part of the system to attacks?

RQ3:
How transparent are key procedures in the Estonian I-Voting system for the electorate and observers, and to what extent is such transparency able to generate confidence in the security of the system?

To address the research questions outlined above, we followed a three-step methodology. First, we identified and contextualised the security aspects of the I-Voting system. Second, we interviewed key personnel involved in various stages of the election process in order to gain detailed insights into the procedural security mechanisms and how they function. Third, we conducted a thematic analysis in order to determine the extent to which present controls mitigate the security risks facing the Estonian I-Voting system. Where appropriate, we also suggest enhancements.

We found that Estonia has significant expertise and experience in conducting successful electronic elections that value security and transparency. While we noted many positive attributes of the I-Voting system, there are also some key areas in which opportunities for improvement exist. For RQ1, we found that procedural controls are fundamental to the system and go a long way in preventing attacks. Crucial procedures are clearly documented, but some situations appear to be addressed in somewhat informal ways that rely heavily on the knowledge of particular officials. Given the close professional relationships between existing officials and their vast experience with the I-Voting system, these processes work well at present. But this could change if a few of these key individuals left their roles or were unexpectedly unable to participate.

In terms of the operational controls in RQ2, we were generally impressed by the state of the controls adopted, particularly the computer incident-handling processes during elections, as well as the analyses, checks, and investigations during and after elections (e.g., on incoming ballots, server logs, etc.). Our main concern regarding resilience is the increasing potential of highly sophisticated attacks (either via large-scale compromise of voter machines or attacks on hardware before reaching the system). As time progresses, attackers will become stronger and systems must be updated constantly in order to accommodate this concern.

With regard to RQ3, we found that transparency measures (e.g., the use of observers and the vote verification app) have had a noteworthy impact on building confidence and trust in the I-Voting system. A small set of key challenges still exists, however, particularly pertaining to the difficulties in running voter awareness campaigns and in increasing voter usage of transparency measures (e.g., the verification app). As these issues are known to election officials and committees, we hope to see measures taken to improve the system in the future, which would go further in building voter confidence.

Finally, we must state that there is one main limitation to our work. This relates to the fact that our research relies on interview reports on voting processes and systems from individuals in Estonia, as opposed to direct observation of the I-Voting system in process. We attempted to counteract this potential weakness by engaging in a critical reflection on the documented system and existing literature, as well as by interviewing a range of experts from across Estonia.

3 Dimitris A. Gritzalis, "Principles and Requirements for a Secure e-Voting System," Computers and Security, Vol. 21, No. 6 (October 2002), pp. 539-556.

4 Estonian National Electoral Committee (NEC), "Internet Voting in Estonia," http://www.vvk.ee/voting-methods-in-estonia/engindex/#Brief_description_of_the_I-voting_system, accessed 5 June 2016.

BACKGROUND: E-VOTING FOR NATIONAL ELECTIONS AND THE I-VOTING SYSTEM

Two main types of e-voting mechanisms exist: on-site systems and remote systems.[5] On-site systems were the first to be adopted. These require electronic polling stations in which voters can cast their ballots. By contrast, remote electronic voting or I-Voting allows users to vote online from their designated devices. The latter approach is favoured by countries and governmental authorities embracing e-voting for reasons of accessibility, participation and cost reduction.[6]

Improving representative democracy and fortifying procedures that focus on empowering citizens are fundamental principles of any e-voting system. Thus, it is imperative to ensure equality and equity with respect to ease and opportunity of access, as well as transparency and public scrutiny for the electoral process. Major requirements elicited from these principles can be grouped into six categories: generality, freedom, equality, secrecy, directness, and democracy.[3] Security, which ensures that some of these qualities are maintained, is also essential to the process.

Countries that have been involved in testing e-voting systems in electoral processes include Estonia, the Netherlands, Canada, and Australia. The systems used for elections in these countries have been analysed from various perspectives, ranging from how they comply with security needs to how they address verifiability and transparency requirements. As a result of these evaluations, some systems have been discontinued (e.g., in the Netherlands), while others (e.g., in Estonia) have stood the test of time.[7]

Estonia is one of the most experienced countries in the world in practising electronic democracy. This comes as little surprise, since the nation has always been at the forefront of adopting innovative technologies to enhance the lives of its citizens. The I-Voting system, which is intended to further enhance democratic procedures and increase the turnout in electoral processes, is one of Estonia's many technical achievements.

The I-Voting system has 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).[8] The IVCA is used by the voters to cast their votes, typically through a personal computing device. The VFS is the only public-facing server of the system; it is responsible for authenticating voters 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. These votes are decrypted with the private key possessed by members of the National Election Committee (NEC), and the VCA then tabulates the votes and outputs the results of the I-Voting process.

Security has been a core consideration in the I-Voting system since its inception in 2005. In 2010, the Estonian National Electoral Committee (NEC) produced a security analysis and measures report.[9] This report provides detailed security measures on how to ensure that the architectural components of the system will not be compromised; information on the audit, monitoring, incident handling and recovery practices; and operational measures (such as the division of tasks and formal procedures on managing risks), complementing technical requirements to ensure that a breach of policies is deterred. The report concludes with the opinion that the security of the I-Voting system exceeds the security of conventional voting with ballot papers.

Regardless of its apparent success in implementation and achieving increased electoral participation,[10] some observers have raised concerns about procedural and technical predicaments. These include the possibility of infecting the PC of a voter and changing their vote, and the lack of end-to-end verification and forensic audit trials of

5 Peter Haynes and Jason Healey, "Online Voting, Rewards and Risks," 2014, http://www.atlanticcouncil.org/images/publications/Online_Voting_Rewards_and_Risks.pdf, accessed 11 April 2016.

6 Jordi Barrat i Esteve, Ben Goldsmith, and John Turner, "International Experience with e-Voting," International Foundation for Electoral Systems (2012).

7 J. Paul Gibson, Robert Krimmer, Vanessa Teague, and Julia Pomares. "A Review of E-Voting: The Past, Present and Future." *Annals of Telecommunications*, Vol. 71, No. 7 (2016); pp. 279-286.

8 NEC, "Internet Voting in Estonia."

9 Arne Ansper et al., "E-voting Concept Security: Analysis and Measures," Estonian National Electoral Committee. 2010. EH-02-02.

10 Estonian National Electoral Committee (NEC), "Statistics about Internet Voting in Estonia," 2015, http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics, accessed 12 May 2016.

the system.[11] In a similar vein, Marco Prandini and Marco Ramilli conclude that no e-voting system is ready to be implemented on a large scale yet, and that the adoption of such a system remains affected by fundamental issues, such as trust, that technology cannot completely address.[12] They further highlight the costs of implementing the I-Voting system—good Internet access and offline support for the system.

As the I-Voting system has evolved, Estonia has made several modifications to the system with additional procedural controls being implemented. For instance, a novel method to verify that a vote has been cast as intended and recorded as cast has now been provided.[13] In addition, in-depth monitoring of the voting system has been established to detect server attacks and system malfunctions, as well as studying voter behaviour.[14] Large parts of the source code underpinning the system and documentation regarding the procedural details have also been made publicly available.[15] These actions seek not only to bolster security of the system and enforce key requirements,[16] but also to build trust and confidence in the system from both voters and independent assessors.

Despite these enhancements, recent studies suggest that problems still exist. Some articles have sought to demonstrate these issues using simulated examples of attack-payloads and patterns to compromise the electoral process.[10] Others point to the fact that the reliance on a complicated set of procedures rather than technical means to achieve integrity may not be ideal.[17] Further concerns have also been identified in the operational and transparency measures proposed in the system. As a result of these ongoing concerns, we examine and reflect on these specific features of the I-Voting system: procedural security, operational security, and transparency measures.

ASSESSMENT OF THE I-VOTING SYSTEM

OVERVIEW

In this section, we assess the procedural security controls, operational security measures and transparency measures of the I-Voting system, as well as the extent to which they mitigate security and trust risks. First, we analysed the literature pertaining to these three main components, and then developed a set of interview questions to explore those areas in more detail. These queries focused on reported voting concerns, outstanding security challenges, and general system functionality.

Second, we recruited seven individuals with detailed knowledge of, and insight into, the I-Voting system (including its administration, process aspects, and security functions). The majority of the participants had at least twelve years of experience with Internet voting and elections in general. Moreover, in order to encourage honest and open responses, we opted for anonymous reporting of interview commentaries and findings. We analysed the resulting data using content analysis, as well as a mixture of deductive and inductive reasoning.[18] In this way, we identified several core response themes, which we discuss below.

PROCEDURAL CONTROLS

Procedural security controls are a core component of the I-Voting system. These controls define the main manual activities and practices that election officials engage in to protect the voting system. Throughout the course of the interviews, procedural controls were discussed in a variety of contexts. Two main areas were highlighted by our thematic analysis: the importance of procedural controls and knowledge transfer.

Reflecting on the importance of procedures

Procedural controls were referred to both directly and indirectly by several interviewees. The primary report documenting these controls is the election manual. Among

11 Drew Springall et al., "Security Analysis of the Estonian Internet Voting System," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Arizona, USA, 3-7 November 2014, pp. 703-715.

12 Marco Prandini and Marco Ramilli, "Internet Voting: Fatally Torn between Conflicting Goals?," in Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance, NY, USA, October 22-25, 2012, pp. 58-61.

13 Sven Heiberg, and Jan Willemson, "Verifiable Internet Voting in Estonia," in Proceedings of the 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), Lochau, Austria, 29–31 October 2014, pp. 1-8.

14 Sven Heiberg, Arnis Parsovs, and Jan Willemson, "Log Analysis of Estonian Internet Voting 2013–2014," *E-Voting and Identity*, 2015, pp. 19-34.

15 Estonian National Electoral Committee (NEC), "E-Voting System: A General Overview," 2010, http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf, accessed 12 February 2016.

16 Gritzalis, "Principles and Requirements for a Security e-Voting System."

17 J. Alex Halderman, "Practical Attacks on Real-World E-Voting in Real-World Electronic Voting: Design, Analysis and Deployment", in Feng Hao and Peter Y.A. Ryan, eds., Real-World Electronic Voting: Design, Analysis and Deployment (Oxford: Taylor and Francis, 2016).

18 Bruce L. Berg, Qualitative Research Methods for the Social Sciences (Oxford: Pearson, 2004).

other things, its aims are to ensure: (a) that data integrity between online and offline systems is maintained; (b) that access control is regulated; and (c) that there are mechanisms for dispute resolution and system continuity. Most interviewees felt that the procedural controls mentioned in the election manual were very important. Server operations were deemed particularly crucial to protect. One interviewee even stated that "procedural controls are relied upon because of the trust required to operate under the assumption that the key to the server was not somehow leaked or that the privacy of the system is not interrupted."[19] Moreover, because of the architectural design and technical setup of the I-Voting system, Estonia relies quite heavily on such procedures.

Another example can be found in the context of maintaining data integrity. There is a procedure to ensure that two individuals serve as auditors who observe key processes, such as when the server key is being generated, or when election data is transferred from the online server to the offline server. The auditors use the election manual to ensure that all tasks relating to the secure treatment of keys are being followed. 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."[20] These processes are regarded as valuable in reducing the potential for malicious attacks or human error.

Taking procedural mechanisms for secure server access during elections as another example, interviewees mentioned that "there are very specific people who can go there."[21] This indicates that only those with proper authority can enter the server room. This was a positive and noteworthy finding. We were unable to verify whether any other checks were conducted to ensure that officials were not able to bring potentially malicious devices (e.g., infected pen drives) into the room, however. 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 dealt with appropriately.

Finally, to comment on dispute resolution procedures, we were pleased to see that there are very clear mechanisms for contesting the validity of a vote or making a complaint. According to one interviewee, in order to reach a speedy dispute resolution, 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 unregulated actions, and have provided a formal mechanism for resolving disputes. It can, however, be difficult to submit such a complaint, as the person submitting needs to have knowledge of the law relevant to the complaint. While increased awareness and education may help address this issue, the Electronic Voting Committee also has instituted an informal "notice" procedure that would enable a complaint to be submitted without knowledge of the legal context. This is definitely a positive and welcome measure.

Procedural controls and knowledge transfer

While procedural controls improve security, we had concerns about the sustainability of existing security procedures, particularly with reference to knowledge definition and transfer. For example, when asked about incorporating lessons learned from dispute measures in particular, an interviewee said: "if you're asking if we have some sort of formalised process for that, then no."[22] Our interactions with interviewees made it clear that such information is generally incorporated, but that there appear to be few formal mechanisms to guide or ensure that incorporation. This may work well for a close-knit society such as that of Estonia. A lack of procedural formality does, however, risk some aspects being inadvertently overlooked or forgotten.

Staffing is another point worth considering in this general context. Given that most of the electoral staff has 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 into detail over it,"[23] referring to some aspects of the system or processes. While it is advantageous to have a core set of professionals to rely upon, from our perspective, the extent to which there are formalised procedures for staff training and planning for future knowledge sharing was unclear. This could be very important for knowledge transfer, especially if in future vote collection is outsourced, as one interviewee suggested. While this could help build a thriving market around I-Voting consulting, there would need to be a programme for knowledge transfer in order to maintain adequate levels of security. Moving forward, it will be interesting to track the usage of procedural controls as the system evolves.

19 Author interview.
20 Author interview.
21 Author interview.
22 Author interview.
23 Author interview.

OPERATIONAL CONTROLS

The fundamental principles underpinning a secure and democratic I-Voting system create conflicting requirements.[24] These conflicts are deemed impossible to resolve by software engineering,[25] rendering the design and implementation of operational security controls the cornerstone of a successful system. Regarding I-Voting, we concentrate on three operational security control concerns: incident handling during the electoral period, voter context and risks, and devices and equipment used in the electoral process.

Incident handling during the electoral period

The Incident Report Centre is a core component of the Estonian voting system. This centre has two purposes: to address technical glitches reported to the client support centre and to actively scan for anomalous behaviours in the Computer Emergency Response Team (CERT) environment. Given the potential threat from significant actors, it is evident that Estonia relies on an effective CERT in order to actively monitor potential attacks on the voting platform. From our interviews, we found it more than encouraging to hear that once anomalies are spotted, there are specific processes in place to appropriately address the issues, which may even result in technicians being dispatched to an area of concern.

For instance, interviewees mentioned a case in which a team was dispatched to a house suspected of spreading malware targeting voting applications (which turned out to be that of an elderly lady who had voted more than 500 times, assuming each vote would be counted separately). But this case clearly demonstrates the capability of the incident response team to be deployed rapidly. Once incidents are identified, they are reported based on their severity to the NEC. The NEC may then decide to take further action, which could, under extreme circumstances, lead to turning off the I-Voting system for a particular election and request that citizens cast their votes by traditional means. This control would be somewhat aggressive, but would ensure that people who are facing problems voting electronically would still be able to participate in a given election.

Voter context and risks

The human voter has previously been recognised as the most vulnerable link in the I-Voting system.[26] Our analysis concurs with this observation. Interviewees agreed that "[they] have introduced e-voting by accepting the risk that the voter is the weakest link, so we cannot deny that many things can happen in the voter's computer."[27] Therefore, they acknowledge that there is little potential for them to control the voter environment, though the system "still depend[s] on [it] being virus free."[28]

To avoid potentially malicious code being spread by users' devices or malicious attempts to control the voting system, input from public interfaces is thoroughly checked to ensure that "the elements of the digital signature are there, that the zip container is well formed."[29] 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 irregular votes are removed before reaching the main system. 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."[30] Thus, such checks on incoming votes are helpful at blocking any malware injection attempts, if such an attack occurs.

Although a fundamental risk emanates from the voters' devices, a large-scale attack affecting voters' machines is considered highly unlikely by the NEC.[31] The risk that is involved is acceptable because of the perceived low likelihood of undetected malware affecting a significant proportion of votes. We believe the possibilities of a large-scale attack to be higher, especially since there have been situations where citizens used unlicensed versions of the Windows operating system. The number of complaints from voters regarding that operating system were so significant that they forced the e-voting committee to adapt the verification requirements of voter's software in order to allow them to vote. An interviewee recounted that "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

24 Gritzalis, "Principles and Requirements for a Security e-Voting System."
25 NEC, "Internet Voting in Estonia."
26 Estonian National Electoral Committee (NEC), "E-Voting System: A General Overview," 2010. http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf, accessed 12 February 2016.
27 Author interview.
28 Author interview.
29 Author interview.
30 Author interview.
31 Arne Ansper et al., "E-voting Concept Security: Analysis and Measures," Estonian National Electoral Committee. 2010. EH-02-02.

on the first day…. We didn't expect that so many people would have [problems]."[32] Therefore, one can imagine an attacker exploiting this vulnerability by inserting a virus into a pirated version of Windows and promoting this to Estonian citizens via torrent applications (i.e., where people can download a variety of digital materials).

There are some notices, within the voter application and online, that advise voters to install anti-virus systems. We believe that this information should also focus on larger issues, such as educating users about not obtaining illegal or unsupported software. The Windows XP case, albeit a serious breach of security, is unlikely to occur in the future because most operating systems now allow users to upgrade to new versions for free. In addition, the verification of votes procedure, when fully used by the voters, enables them to detect that their vote has been manipulated.

Devices and equipment used in the electoral process

The hardware used during elections is another potential source of attacks. There are strict procedures to verify that the hardware is malware-free, since it may be "delivered to us deliberately modified to falsify our elections."[33] We believe that existing checks appear sufficient, but that there should be additional checks for firmware malware in order to eliminate the possibility of a sophisticated attack. It is possible that the concept of Advanced Persistent Threats, i.e., slow-moving and deliberate attacks applied to quietly compromise information systems without revealing themselves,[34] may also be relevant here. We highlight this because there are increasing concerns about the ability of external parties to influence a country's elections.[35]

In order to avoid physical attacks on the system (i.e., servers), and to generally maintain system resilience, there are also several security requirements in place regarding the facilities. For instance, one interviewee stated that there are strict "security measures of what this room must [have]" when selecting facilities to host systems.[36] The server room is deemed of critical importance, and access to the room is controlled. Every possible input port to the server is covered with red tape and regularly checked for tampering. Here, the conundrum of balancing transparency (in terms of allowing people to witness from close proximity the electoral process) and security is more evident than ever, highlighting the importance of the red-tape operational control to alleviate the conflict.

Finally, in order to maintain anonymity in the voting process, once the votes are stripped of the first level of encryption, these are transferred to the Vote Counting Application for the counting process. Standard procedures require the use of DVDs for transferring the data, but there have been occurrences in which glitches in the system have led to officials using removable devices instead. Though a serious violation of the operational security controls as defined by existing Estonian procedures, all the components are backed up and every action is logged to reduce undetected attempts at vote manipulation; monitoring practices would also enable the detection of malware. We must emphasise, however, that better procedures are needed to handle such issues in the future. These procedures should be designed with consideration of observers and the perceptions they will have if there are variations from documented protocol.

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; public awareness of e-voting and secure practices; and vote verification.

Auditing, observation, and monitoring of the election process

The monitoring of the I-Voting process by auditors was one of the main transparency measures mentioned by interviewees. Several independent auditors are employed during an election period; they provide feedback on the extent to which critical processes are followed. After elections, auditors issue a report with their findings. The use of auditors not only enhances transparency, but also provides an opportunity for the election committee to consider and reflect on the lessons learned once the election period is over.

In addition to auditors, public observers are allowed to witness the election process. A press release before the elections addresses the public and all parties to the election, providing them with the opportunity of observing

32 Author interview.
33 Author interview.
34 Ivo Friedberg, Florian Skopik, Giuseppe Settanni, and Roman Fiedler, "Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection," Computers and Security Vol. 48 (Oct 2015) pp. 35-57.
35 Bruce Schneier, "By November, Russian Hackers Could Target Voting Machines," The Washington Post, 27 July 2016, https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/?utm_term=.d4779b79e22b, accessed 1 August 2016.
36 Author interview.

the I-Voting process. Anyone can serve as an observer; no vetting is necessary, and the process is such that they can view elections in real time and provide suggestions and feedback. From our perspective, and considering earlier findings regarding procedural controls, we were especially interested in how such feedback was utilised by election officials. We were pleased to discover the use of a method which accommodates and reflects on this feedback, both during and after elections. As one interviewee mentioned, "the suggestions provided by observers have already been implemented quite a lot."[37] Though we were unable to explore this matter further due to time constraints of the study, it is an unequivocally positive sign of transparency and democracy.

One challenge 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 on the technical details for observers, but attendance is low. Moreover, the majority of attendees do not complete the course due to an overload of information. There is an interesting conundrum to be addressed, since the manner in which the committee can engage with the public to communicate the I-Voting system's details is rather restricted. As pointed out by interviewees, questions regarding misleading the public may be raised if the technological details are simplified. An outstanding challenge, therefore, is to balance the level of voter interest with the amount of information provided. This is especially important because some voters may not be interested in highly technical aspects, but still desire some engagement to understand how the system works and maintains standard voting requirements (as in the article by Dimitris Gritzalis).[38]

Publication of the I-Voting system's documentation is one of the most crucial transparency measures.[14] 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. As one interviewee points out with respect to the server details, "the screen of a computer is filmed…and 97 percent of the code used is also made public."[39] After the elections, some of these videos have also been released on YouTube for public consumption. We view the publication of these documents, code (particularly for community review), and videos as encouraging transparency measures.
With regard to the 3 percent of the code not published, we discovered that this code is focused on malware detection and avoidance at the voter's machine, and that publishing it would therefore effectively defeat its purpose. Two transparency options for this issue have been made available. First the code is checked and audited by independent and trusted third parties; second, the voting protocol is fully documented online, and hence any individual (given the appropriate skills) could create his or her own compliant voting software. These efforts by election officials are noteworthy and demonstrate some real impetus toward operating a transparent system.

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 voting process and the key aspects of security. As mentioned above, there is also a significant amount of detail on the system online (e.g., the NEC).[40] In this way, a platform of trust could be built based on information and understanding. More recently, when the vote-verification application was released, there were media campaigns and newspaper 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 (at least leading up to and during elections) official campaign to promote secure e-voting. This campaign would inform the public of best practices for secure electronic voting, such as having updated malware and antivirus software installed, as well as being aware of the range of risks and how to mitigate them. We note the formal acceptance of the risk of voter PCs,[41] but still felt that more could be attempted in this area. When we mentioned this to interviewees, they stressed that such campaigns had been run in the past and were being considered for the future, but that there were political challenges with bespoke e-voting campaigns, namely that such efforts were seen by some parties to provide more attention to one form of voting over another. This is a difficult predicament, but there are two potential solutions: running smaller, security-focused campaigns for all voting methods; or incorporating such information into e-governance campaigns more broadly.

37 Author interview.
38 Gritzalis, "Principles and Requirements for a Security e-Voting System."
39 Author interview.
40 Arne Ansper et al., "E-Voting Concept Security: Analysis and Measures," Estonian National Electoral Committee. 2010. EH-02-02; and Estonian National Electoral Committee (NEC), "E-Voting System: A General Overview," 2010, http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf, accessed 12 February 2016.
41 Arne Ansper et al., "E-Voting Concept Security: Analysis and Measures," Estonian National Electoral Committee. 2010. EH-02-02.

The next municipal elections (scheduled for 2017) might be an ideal opportunity to explore the suggestions mentioned above. This is because Estonia plans to lower the voting age to 16- and 17-year-olds (for local elections only). This new development will create 25,000 new voters, and it is expected that a special campaign will be run 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 e-voting transparency. We have already witnessed some awareness efforts in Estonia but they are promoted via other means.[42]

Verification

Allowing users to verify their votes via a smartphone application is another mechanism for enhancing transparency. Procedurally, the verification application performs as expected and is simple to use. According to one interviewee, "the verification application allows for actual proof of the process and enhances trust."[43] This has also been witnessed through a system study in which officials found that while only around 3 percent of voters verified their votes, the availability of the application increased confidence in the system generally. From our perspective it was ideal to see the separation in devices used for casting and verifying votes. This meant that successful vote hijacking, particularly on a large scale, would be more difficult, as a malicious party would need to take control of both a PC and a smartphone. We do stress, however, that the application will only be truly helpful to the I-Voting process (and security concerns) if it is more widely used. We note that there are approaches in Estonia toward this goal (e.g., the verification application is available on Android, iOS and Windows platforms). Future efforts should continue to encourage their adoption and usage.

THE NEW I-VOTING SYSTEM

With the core topic areas of this report now examined, we briefly expand upon our initial findings to discuss the new version of the I-Voting system. While we were aware that there would be 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 over ten years' experience of e-democracy—from laws and regulations to technical and socio-technical aspects. This was a point highlighted by interviewees: the system was not being overhauled due to concerns about the integrity of the previous system, but rather because it was felt to be the appropriate time to update the full system, including enriching server-side code (as opposed to simply improving it, as had been done for many years).

One of the most significant changes in the new system is its structure, with a focus on returning power to the NEC. In line with this goal, there are a few key modifications worth noting. First, as we briefly mentioned earlier, the vote collection system (i.e., the system that interacts with voters directly) will be outsourced to a third party, to be chosen through a tender. The benefit here 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 this shift in power, the Internet 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 in the NEC.

To comment on these changes more generally, we view the decision to return the power to the NEC as a commendable move for democracy. This is especially true because a technically experienced individual will now be a core part of the election oversight and process. The only concern that may arise with this approach relates to the selection of companies to implement the vote collection system, and the level of checks on code and processes conducted. Independent assessments must continue to ensure that democracy is not placed at risk.

Our interviews suggested that, as the future voting system shifts from procedures to technology and mathematics, monitoring may 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 this shift represents "trust in mathematics rather than people."[44] We agree that the move to a formally verified and technically proven system is ideal in many ways. The difficulty will come in communicating these details to the general public, when current engagement in courses on the system is low. The very nature of voting and its link to democratic rights means that an attempt must be made for more accessible outlets for information about the national e-voting system.

42 UNITE-IT, "Get Online Week 2016," 2016, http://www.unite-it.eu/profiles/blogs/get-online-week-2016-in-estonia-raising-awareness-and-contest?xg_source=activity, accessed 27 May 2016.

43 Author interview.

44 Author interview.

A related point to our reflection above is the emphasis on the new system allowing for verifiability. This also makes server-side operations more mathematically transparent and comprehensive in order to verify elections. This is clearly important, as any changes in votes (such as deletions or modifications) will be more easily detected. It is premature to report on the specifics of the new system, but one interviewee stated that the "tender description suggests that it will include mix-nets, homomorphic encryption and provable decryption, and that the existing double envelop method will remain";[45] the server code will also be openly published in its majority. These modifications will enable officials to prove that the decryption and tabulation of votes is performed correctly, and will give additional assurance to external parties who may wish to verify the election results.

Finally, in this new system there will be a more substantial reliance on voter and client support as a key service in the election process. If voters notice that the system is not performing as expected, they will need various options for client support. In the current system, there are several excellent support options; we hope that this continues in the future. Moreover, as an interviewee pointed out, "the new system could also be used outside Estonia in the future"[46] (i.e., adapting the system to other countries), as there is the possibility of removing its linkages to the Estonian ID card. This highlights broader applicability, though time will tell whether such a system would arouse interest outside of the Estonian context.

CONCLUSION: STATE OF SECURITY OF THE I-VOTING SYSTEM

Estonia has been pioneering the adoption of an I-Voting system as an alternative to traditional voting. With the experience of successfully conducting electronic elections for the last eleven years and gaining the trust of more than 30 percent of Estonian citizens,[47] it is evident that the I-Voting system has by far surpassed other systems in terms of success. Electronic voting presents a huge challenge because many principal requirements are conflicting in nature, which means that designing effective operational and procedural controls is fundamental for the success of the system. Transparency and anonymity differ from security and verifiability, and the legislative efforts which typically follow technological developments are fundamental for the adoption and implementation of the e-voting process.

These challenges are evident in the Estonian I-Voting system. Due to the small size of the country, officials have relied since the system's inception on building trust through interpersonal relations. Technological advancements and lessons learned were converted to legislation, not always via formalised and clearly defined procedures, but also through the expertise of the electoral committee and their close proximity to the Estonian Parliament. Throughout its existence, the I-Voting system has adapted technological developments slowly due to the time-consuming legislative processes which have to be approved by the majority of the Estonian parliament. For instance, although homomorphic encryption (i.e., an encryption scheme where computations can be performed without access to original data) was technically feasible years ago, only recently were political circumstances in Estonia mature enough to legislate accordingly and allow the voting system to incorporate this.

Certain controls could be enhanced with simple measures (e.g., instituting awareness campaigns). Some of these, however, are prohibited due to political controversy. The conundrum is evident in the two-day course, which is deemed highly technical and arduous for citizens, but which may give rise to political confrontation if changed. In a similar vein, awareness campaigns are prohibited due to the principal of equal treatment of all forms of voting – this may expose the I-Voting system to a potentially large attack surface via the voter, even though the impact per user would be rather in favour of. Political parties claim that awareness campaigns for the I-voting, although they are for the benefit of the voters, may motivate more people voting through I-voting, thus the rational for this view is that influencing the result of the elections. The assumption behind this concern is that a certain demographic with a clear political preference only votes via I-voting.

Our interviews demonstrate that Estonia has the experience and expertise for running successful electronic elections, but this success depends on the skills and expertise of key people who are involved in the process. While important procedures are codified, in some cases incidents and feedback reports appear to be addressed in a somewhat informal way. This may currently be effective, due to the professional relationships between the individuals in the committee. In the event of numerous persons leaving key roles, however, this could raise a problem. We believe, therefore, that these informal processes (including

45 Author interview.
46 Author interview.
47 Estonian National Electoral Committee (NEC), "Statistics about Internet Voting in Estonia," 2015, http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics, accessed 12 May 2016.

lessons learned) should be further clarified and formally documented, especially for the preservation of knowledge and expertise across generations of election officials.

The Estonian system will change significantly before the next elections in 2017. With respect to discarding current controls, it is of paramount importance that such a decision follow an established procedure, and that citizen feedback be taken into account. The I-Voting system has established a trust relationship with Estonian citizens. Though mathematical proofs are scientifically justifiable as more secure, they may not necessarily provide the same assurance to citizens, especially as the majority of citizens tend to show little interest in highly technical details of the system. With major changes on the horizon, it is essential that the system's procedures continue to be critically reflected upon and improved.

About the Cyber Studies Programme

The Cyber Studies Programme seeks to create a new body of knowledge that clarifies the consequences of information technology for the structures and processes of political systems.

Our research mission is (a) to produce scholarly works that contribute to major academic debates and opinions; and (b) to apply these new understandings in the analysis of major policy problems affecting the security and welfare of states and citizens.

Our teaching mission is (a) to support, guide, and train students and researchers in Oxford and beyond in the work and methods of cyber studies within the subdisciplines of political science; and (b) to foster understanding across technical and non-technical communities to promote the development of this new field of study more broadly.

The Cyber Studies Programme is sponsored by the Centre for International Studies in the Department of Politics and International Relations, University of Oxford.

European Union
European Social Fund

Investing
in your future

This publication is funded by the European Social Fund and the Estonian Government