Security Analysis of the Estonian Internet Voting System

Drew Springall[†] Travis Finkenauer[†] Zakir Durumeric[†]
Jason Kitcat[‡] Harri Hursti Margaret MacAlpine J. Alex Halderman[†]

[†]University of Michigan, Ann Arbor, MI, U.S.A.
[‡]Open Rights Group, U.K.

For additional materials and contact information, visit estoniaevoting.org.

ABSTRACT

Estonia was the first country in the world to use Internet voting nationally, and today more than 30% of its ballots are cast online. In this paper, we analyze the security of the Estonian I-voting system based on a combination of in-person election observation, code review, and adversarial testing. Adopting a threat model that considers the advanced threats faced by a national election system — including dishonest insiders and state-sponsored attacks — we find that the I-voting system has serious architectural limitations and procedural gaps that potentially jeopardize the integrity of elections. In experimental attacks on a reproduction of the system, we demonstrate how such attackers could target the election servers or voters' clients to alter election results or undermine the legitimacy of the system. Our findings illustrate the practical obstacles to Internet voting in the modern world, and they carry lessons for Estonia, for other countries considering adopting such systems, and for the security research community.

1. INTRODUCTION

Several countries have experimented with casting votes over the Internet, but today, no nation uses Internet voting for binding political elections to a larger degree than Estonia [42]. When Estonia introduced its online voting system in 2005, it became the first country to offer Internet voting nationally. Since then, it has used the system in local or national elections seven times, and, in the most recent election, over 30% of participating voters cast their ballots online [19]. People around the world look to Estonia's example, and some wonder why they can't vote online too [54].

Nevertheless, the system remains controversial. Many Estonians view Internet voting as a source of national pride, but one major political party has repeatedly called for it to be abandoned [31]. Although Estonia's Internet Voting Committee maintains that the system "is as reliable and secure as voting in [the] traditional way" [20], its security has been questioned by a variety of critics, including voices within the country (e.g. [47, 51]) and abroad (e.g. [61]). Despite these concerns, the system has not previously been subjected to a detailed independent security analysis.

For these reasons, the Estonian Internet voting (I-voting) system represents a unique and important case study in election security. Its strengths and weaknesses can inform other countries considering the adoption of online voting, as well as the design of future systems in research and practice.

In this study, we evaluate the system's security using a combination of observational and experimental techniques. We observed operations during the October 2013 local elections, conducted interviews with the system developers and election officials, assessed the software through source code inspection and reverse engineering, and performed tests on a reproduction of the complete system in our laboratory. Our findings suggest the system has serious procedural and architectural weaknesses that expose Estonia to the risk that attackers could undetectably alter the outcome of an election.

Most Internet voting schemes proposed in the research literature (e.g. [1, 9]) use cryptographic techniques to achieve a property called end-to-end (E2E) verifiability [8]. This means that anyone can confirm that the ballots have been counted accurately *without* having to trust that the computers or officials are behaving honestly. In contrast, Estonia's system is not E2E verifiable. It uses a conceptually simpler design at the cost of having to implicitly trust the integrity of voters' computers, server components, and the election staff.

Rather than proving integrity through technical means, Estonia relies on a complicated set of procedural controls, but these procedures are inadequate to achieve security or transparency. During our in-person observations and in reviewing official videos of the 2013 process, we noted deviations from procedure and serious lapses in operational security, which leave the system open to the possibility of attacks, fraud, and errors. Transparency measures, such as video recordings and published source code, were incomplete and insufficient to allow outside observers to establish the integrity of results.

The threats facing national elections have shifted significantly since the Estonian system was designed more than a decade ago. Cyberwarfare, once a largely hypothetical threat, has become a well documented reality [49, 60, 64, 65], and attacks by foreign states are now a credible threat to a national online voting system. As recently as May 2014, attackers linked to Russia targeted election infrastructure in Ukraine and briefly delayed vote counting [10]. Given that Estonia is an EU and NATO member that borders Russia, its threat model should not discount the possibility that a foreign power would interfere in its elections.

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
ACM 978-1-4503-2957-6/14/11.
http://dx.doi.org/10.1145/2660267.2660315.

Figure 1: **I-voting client** — Estonians use special client software and national ID smartcards to cast votes online.

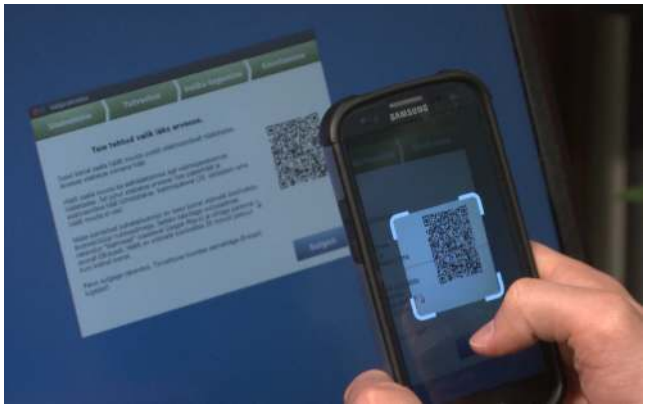


Figure 2: **Verification app** — A smartphone app allows voters to confirm that their votes were correctly recorded. We present two strategies an attacker can use to bypass it.

To test the feasibility of such attacks, we reproduced the I-voting system in a lab environment and played the role of a sophisticated attacker during a mock election. We were able to develop client-side attacks that silently steal votes on voters' own computers, bypassing safeguards such as the national ID smartcard system and smartphone verification app. We also demonstrate server-side attacks that target the implicitly trusted vote counting server. By introducing malware into this server, a foreign power or dishonest insider could alter votes between decryption and tabulation, shifting results in favor of the attacker's preferred candidate.

We conclude that there are multiple ways that state-level attackers, sophisticated online criminals, or dishonest insiders could successfully attack the Estonian I-voting system. Such an attacker could plausibly change votes, compromise the secret ballot, disrupt elections, or cast doubt on the integrity of results. These problems are difficult to mitigate, because they stem from basic architectural choices and fundamental limitations on the security and transparency that can be provided by procedural controls. For these reasons, we recommend that Estonia discontinue the I-voting system.

We returned to Estonia in May 2014 and shared these findings with election officials and the public. Unfortunately, government responses ranged from dismissive to absurd. The National Electoral Committee stated that the threat vectors we consider have already been adequately accounted for in the design, and that the attacks we describe are infeasible [26]. We disagree on both counts, but readers can review the evidence and reach their own conclusions. Prime Minister Taavi Rõivas and President Toomas Hendrik Ilves insinuated to the media that we had been bought off by a rival political party seeking to disparage the system. This we vehemently deny, but it illustrates how the Estonian public discourse concerning election technology has become dominated by partisanship. We hope that the country can separate technical reality from political rhetoric in time to avert a major attack.

2. BACKGROUND

Our analysis focuses on the Estonian I-voting system as it was used for the 2013 municipal elections [22]. In these elections, Internet voting was available for seven days, from October 10–16, and the main in-person poll took place on October 20. Results were declared that evening. According to official statistics [19], 133,808 votes were cast online, corresponding to 21.2% of participating voters.[1]

In this section, we review the design and operation of the I-voting system. Figure 4 gives an overview of the interactions between the main system components.

2.1 National ID Cards

An essential building block of the I-voting system is Estonia's national ID infrastructure [13], which plays a central role in the country's high-tech and e-government strategy [37]. Estonian national ID cards are smartcards with the ability to perform cryptographic functions. With the use of card readers and client software, Estonians can authenticate to websites (via TLS client authentication [53]) and make legally binding signatures on documents [15]. The cards are popularly used for online banking and accessing e-government services [21]. In the I-voting system, voters use their ID cards to authenticate to the server and to sign their ballots.

Each card contains two RSA key pairs, one for authentication and one for making digital signatures. Certificates binding the public keys to the cardholder's identity are stored on the card and in a public LDAP database [16]. The card does not allow exporting private keys, so all cryptographic operations are performed internally. As an added safeguard, each key is associated with a PIN code, which must be provided to authorize every operation.

Estonians can also use mobile phones with special SIM cards for authentication and signing, through a system called Mobile-ID [14]. In the 2013 election, 9% of online votes were cast using this method [19]. We exclude Mobile-ID from our analysis because we did not have access to the external infrastructure that would be needed to test it.

2.2 I-Voting Server Infrastructure

The majority of the I-voting server source code is published to a GitHub repository 2–3 weeks prior to the election [30]. The server infrastructure is configured in a public ceremony one week before the election and consists of four machines:

[1]Estonia used the system again, shortly after we made our findings public, for May 2014 European Parliament elections. There were only minor changes to the software and procedures. The fraction of votes cast online increased to 31%.

Vote forwarding server (VFS/HES) The VFS (or HES in Estonian) is the only publicly accessible server. It accepts HTTPS connections from the client software, verifies voter eligibility, and acts as an intermediary to the backend vote storage server, which is not accessible from the Internet.

Vote storage server (VSS/HTS) The VSS is a backend server that stores signed, encrypted votes during the online voting period. Upon receiving a vote from the VFS, it confirms that the vote is formatted correctly and verifies the voter's digital signature using an external OCSP server.

Log server This server is an internal logging and monitoring platform that collects events and statistics from the VFS and VSS. The source code and design have not been published. While this server is not publicly accessible, it can be accessed remotely by election staff.

Vote counting server (VCS/HLR) The VCS is never connected to a network and is only used during the final stage of the election. Officials use a DVD to copy encrypted votes (with their signatures removed) from the VSS. The VCS is attached to a hardware security module (HSM) that contains the election private key. It uses the HSM to decrypt the votes, counts them, and outputs the official results.

2.3 Voting Processes

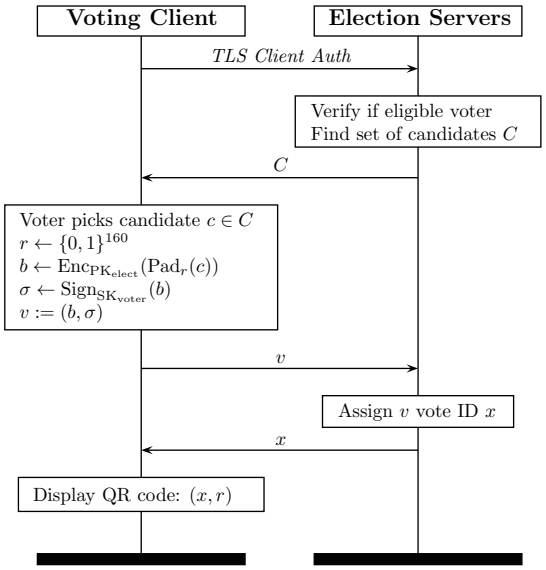
The I-voting system uses public key cryptography to provide a digital analog of the "double envelope" ballots often used for absentee voting [24]. Conceptually, an outer envelope (a digital signature) establishes the voter's identity, while an inner envelope (public key encryption) protects the secrecy of the ballot. Once each voter's eligibility has been established, the signature is stripped off, leaving a set of anonymous encrypted ballots. These are moved to a physically separate machine, which decrypts and counts them.

Casting At the start of each election, the election authority publishes a set of voting client applications for Windows, Linux, and Mac OS, which can be downloaded from https://valimised.ee. The client is customized for each election and includes an election-specific public key for encrypting the voted ballot and a TLS certificate for the server.

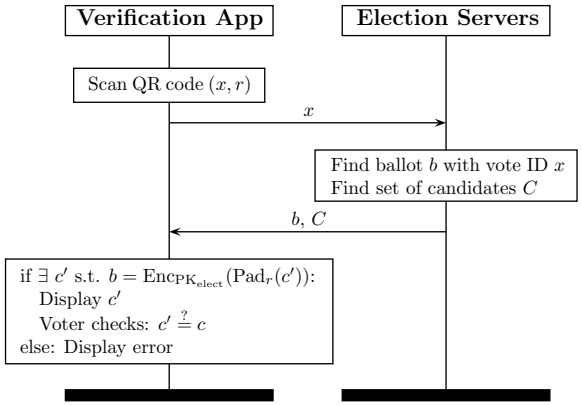
Figure 3a shows the protocol for casting a vote. The voter begins by launching the client application and inserting her ID card. She enters the PIN associated with her authentication key, which is used to establish a client-authenticated TLS connection to the VFS. The client verifies the server's identity using a hard-coded certificate. The server confirms the voter's eligibility based on her public key and returns the list of candidates for her district [11].

The voter selects her choice c and enters her signing key PIN. The client pads c using RSA-OAEP and randomness r, encrypts it with using the 2048-bit election public key, and signs the encrypted vote with the voter's private key. The signed and encrypted vote is sent to the server, which associates it with an unguessable unique token x and returns x to the client. The client displays a QR code containing r and x.

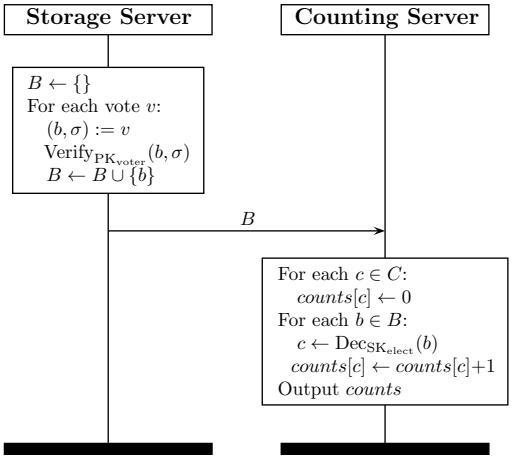
As a defense against coercion, voters are allowed to vote multiple times during the online election period, with only the last vote counted. All earlier votes are revoked but retained on the storage server for logging purposes. While the client indicates whether the user has previously voted, it does not display the number of times. The voter can also override her electronic vote by voting in person on election day.



(a) **Vote casting process**



(b) **Vote verification process**



(c) **Vote tabulation process**

Figure 3: **I-voting system protocols**

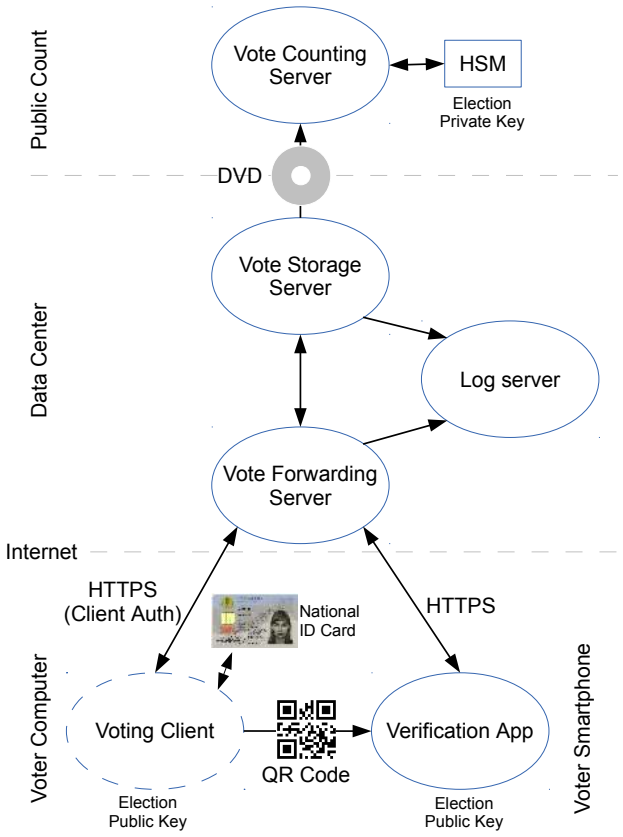


Figure 4: **I-voting system overview** — Major components of the system, and how information flows among them.

Verification The voter can confirm that her vote was correctly recorded using a smartphone app provided by the election authority [25, 27, 28], as seen in Figure 2. This protocol is shown in Figure 3b. The app scans the QR code displayed by the voting client to obtain r and x. It sends x to the election server, which returns the encrypted vote b (but not the signature) as well as a list of possible candidates. The app uses r to encrypt a simulated vote for each possible candidate and compares the result to the encrypted vote received from the server. If there is a match, the app displays the corresponding candidate, which the voter can check against her intended choice. The server allows verification to be performed up to three times per vote and up to 30 minutes after casting.

Tabulation Figure 3c shows the sequence that occurs at the conclusion of an election. After online voting has ended, the storage server processes the encrypted votes to reverify the signatures and remove any revoked or invalid votes. During a public counting session, officials export the set of valid votes after stripping off the signatures, leaving only anonymous encrypted votes. These are burned to a DVD to transfer them to the counting server.

The counting server is attached to an HSM that contains the election private key. The server uses the HSM to decrypt each vote and tallies the votes for each candidate. Officials export the totals by burning them to a DVD. These results are combined with the totals from in-person polling stations and published as the overall results of the election.

3. OBSERVATIONS

The first part of our analysis follows an observational methodology. Four of the authors (Halderman, Hursti, Kitcat, and MacAlpine) visited Estonia as officially accredited election observers during the October 2013 municipal elections and witnessed the operation of the I-voting servers. During that time, they also met with election officials and the I-voting software developers in Tallinn and Tartu. Later, we closely reviewed published artifacts from the election: the server source code [30], written procedures [17], and nearly 20 hours of official videos that recorded the I-voting configuration, administration, and counting processes [18]. Ultimately, we identified a range of problems related to poor procedural controls, lapses in operational security, and insufficient transparency measures.

3.1 Inadequate Procedural Controls

While the Internet Voting Committee (the administrative body that runs the system) has published extensive written procedures covering many steps in the election process [17], we observed that some procedures were not consistently followed and others were dangerously incomplete.

Procedures for handling anomalous conditions that could imply an attack appear to be inadequately specified or do not exist. For example, tamper-evident seals are used on the server racks in the data center.[2] When asked what would happen if the seals were found to be compromised, election staff responded that they were unsure.

Anomalous situations that occurred during the 2013 election were handled in an ad hoc manner, sometimes at the discretion of a single individual. On multiple occasions, we observed as data center staff restarted server processes to resolve technical glitches, and repeated failed commands rather than troubleshooting the root cause. Similar issues were observed during tabulation when the election officials attempted to boot the vote storage server to export the encrypted votes. The machine reported errors stating that the drive configuration had changed—a possible indication of tampering. Instead of investigating the cause of the alert, staff bypassed the message.

Some procedures appeared to change several times over the observation period. For example, observers were initially allowed to film and photograph inside the server room, but were prohibited the next day because of the unsubstantiated claim of "possible electronic interference." In a similarly abrupt change in procedure, observers were required to leave their mobile phones outside the data center after multiple days where this was not the policy. Rewriting the rules on the fly suggests that the procedures had not been adequately thought out or were insufficiently defined for staff to implement them consistently.

Even when procedural safeguards were clear, they were not always followed. For example, procedure dictates that two operators should be present when performing updates and backups [11]. Yet, on October 14, we observed that a lone staff member performed these tasks. Without a second operator present, the security of the system relies on the integrity of a single staff member.

[2]We note that tamper-evident seals like those used in Estonia are known to be easy to defeat using widely available tools [38–41]. Their usefulness for election security has been questioned in other countries [3, 66].

3.2 Lax Operational Security

Since the I-voting system treats parts of the server infrastructure as implicitly trusted, the processes used to install and configure those servers are crucial for the security of the election. We witnessed numerous serious lapses in operational security both during our on-site observations and in the official videos released by the Internet Voting Committee.

Pre-election setup Several problems can be seen in the official videos of the pre-election setup process, which takes place in the National Electoral Committee's offices in Tallinn.

The videos show election workers downloading software for use in the setup process from a public website over an unsecured HTTP connection (Figure 6). A network-based man-in-the-middle attacker could compromise these applications and introduce malware into the configuration process.

In other instances. workers unintentionally typed passwords and national ID card PINs in view of the camera (Figures 7 and 8). These included the root passwords for the election servers. Similar problems occurred during daily maintenance operations in the data center. Physical keys to the server room and rack were revealed to observers; these keys could potentially be duplicated using known techniques [45].

The most alarming operational security weakness during pre-election setup was workers using an "unclean" personal computer to prepare election client software for distribution to the public. As seen in Figure 5, the desktop has shortcuts for an online gambling site and a BitTorrent client, suggesting that this was not a specially secured official machine. If the computer used to prepare the client was infected with malware, malicious code could have spread to voters' PCs.

Daily maintenance We observed further operational security weaknesses during daily maintenance procedures that took place during the voting period. The I-voting servers are hosted at a government data center in Tallinn, and workers go there to perform operations at the server consoles. While there were security video cameras at the data center, there appeared to be no 24/7 security personnel nor any definitive information on who monitored the cameras.

Standard practice during daily maintenance is for workers to log in to the election servers under the `root` account and perform operations at the shell. Logging in as `root` is contrary to security best practice, as it simplifies many attacks, disables user-based privilege separation for operator functions, and increases the risk of human error.

Unencrypted daily backups were casually transported in workers' personal backpacks. DVDs holding updated voter lists from the population register were handled in a similarly casual way after having been created, we were told, by a member of staff at their own computer. We did not observe any audit trail or checks on the provenance of these DVDs, which were used daily at the heart of the I-voting system.

Tabulation The tabulation process at the end of the election was also concerning. After the votes were decrypted on the counting server, an unknown technical glitch prevented workers from writing the official counts and log files to DVD. Instead, officials decided to use a worker's personal USB stick to transfer the files to an Internet-connected Windows laptop, where the results were officially signed. This USB stick had been previously used and contained other files, as shown in Figure 10. This occurred despite protest from an audience member and deviated significantly from the written procedure, adding multiple potential attack vectors. Malware present on the laptop or USB stick could have altered the unsigned results, or malware on the USB stick could have been transferred to the trusted counting server.

These instances illustrate a pattern of operational security lapses on the part of the workers who operated the I-voting system. This is particularly alarming given the high degree of trust the I-voting system design requires of the election servers, client software, and the election workers themselves.

3.3 Insufficient Transparency

The election officials have implemented a number of transparency measures, including allowing in-person public observation, publishing videos of operator tasks, and releasing large parts of the server source code. While these measures appear to be well intended, they are incomplete and insufficient to fully establish the integrity of election results.

One limitation is that these measures cannot show whether malicious actions were performed on the servers or hard disks before recording and observation commenced. In practice, they also do not capture everything going on in the facilities. On many occasions, there were multiple machines or screens in use simultaneously but only a single camera.

Although we attempted to follow these simultaneous operations during our in-person observations, on occasion the operators appeared to be deliberately evading us. For instance, on Monday, October 14, we were physically present in the server room when one of the servers produced abnormal output, which appeared to be a failure of the update operation. The official video recording was following the other display, and the operator, upon seeing the error message, quickly flushed it from the screen. In another instance when an error appeared on the server console, an election worker quickly cleared the display and then asked us to rotate out of the room and let other observers in, allowing him a block of observation-free time.

An auditor from a major international consulting firm had been hired by the Internet Voting Committee, and his report also documents procedural and operational shortcomings [56]. However, the auditor's role was chiefly to observe, and he was not provided with the access needed to confirm secure operation of the system.

Election officials have made large parts of the server software open source [30]. This is a positive measure as it allows independent review and assessment — indeed, our study made extensive use of the code. However, security-critical pieces of code are missing from the published sources, including the entire client application and code that is executed on every server machine (see Section 4.1).

Officials told us that the client source is not released (and furthermore, the client binary is obfuscated) because they are concerned that attackers might modify it and distribute a trojan lookalike. Creating client-side malware is feasible without the source, as we show in Section 5.1. At the same time, keeping source code secret prevents the public from understanding what they are being asked to run on their computers, and it increases the risk that any centrally introduced malicious changes to the client will go undetected.

As these transparency measures are practiced today, the videos, public observation, and open-source components risk providing a false sense of security. It is possible for the systems to be corrupted prior to videotaping, for media used to update servers to be maliciously modified, or for unpublished

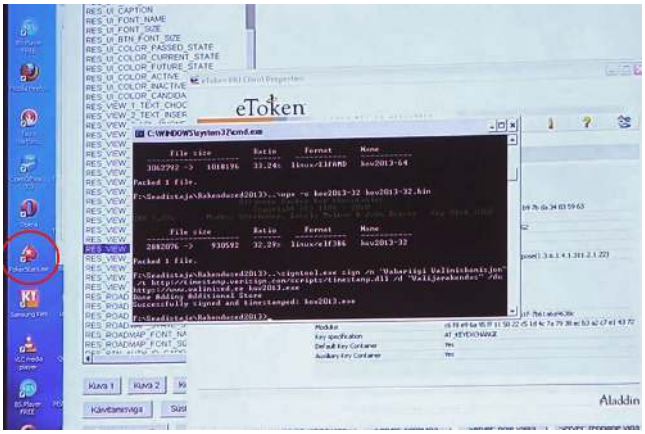


Figure 5: **Unsecured build system** — Operators used a PC containing other software, including PokerStars.ee, to sign the official voting client for public distribution. This risks infecting the client with malware spread from the PC.

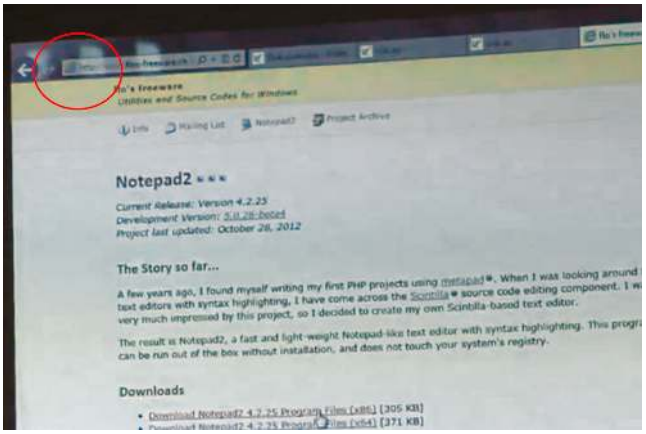


Figure 6: **Insecure software downloads** — Operators downloaded software over insecure connections for use in pre-election setup. An attacker who injected malware into these downloads might be able to compromise the process.

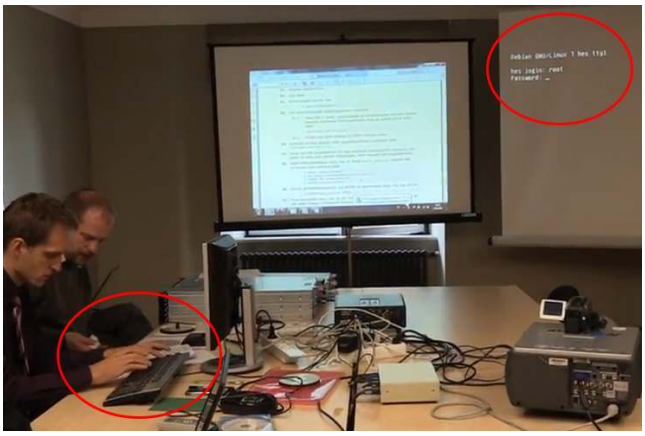


Figure 7: **Keystrokes reveal root passwords** — Videos posted by officials during the election show operators typing, inadvertently revealing root passwords for election servers.

Figure 8: **Video shows national ID PINs** — During pre-election setup, someone types the secret PINs for their national ID card in full view of the official video camera.

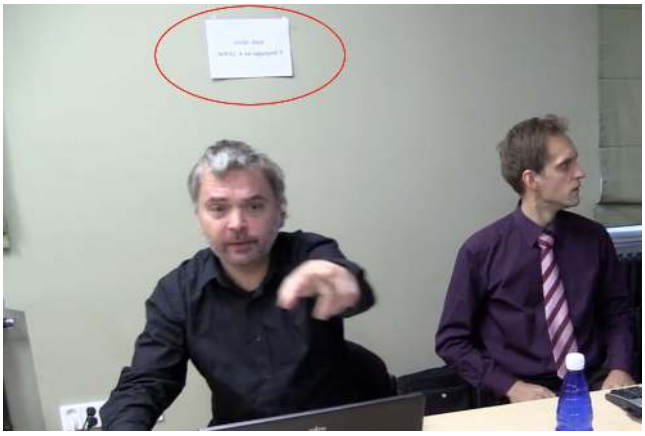


Figure 9: **Posted Wi-Fi credentials** — The official video of the pre-election process reveals credentials for the election officials' Wi-Fi network, which are posted on the wall.

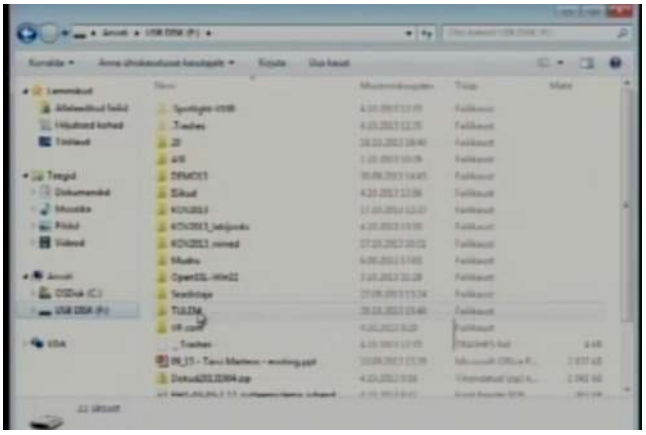


Figure 10: **Personal USB stick** — Against procedures, an official used a USB stick, containing personal files, when moving the official election results off of the counting server.

pieces of software to contain errors or malicious code — all invisible to the public under current transparency measures.

To illustrate these limitations, we conducted an experimental server-side attack on a reproduction of the system, as detailed in Section 5.2. We have published a series of videos (see https://estoniaevoting.org/videos/) matching the procedures in the official videos step-by-step, but where the result of the election is dishonest because of malware surreptitiously introduced before the start of pre-election setup.

3.4 Vulnerabilities in Published Code

The published portions of the I-voting server software [30] contain 17,000 lines of code, with 61% in Python, 37% in C++, and the remainder in shell scripts. The codebase is quite complex, with a large number of external dependencies, and exhaustively searching it for vulnerabilities would be a challenging task well beyond the scope of this project. We understand that volunteers from the Estonian security community have already audited it — a testament to the virtues of publishing code. Nonetheless, we discovered some minor bugs and vulnerabilities while examining the code in order to conduct our other experiments. We disclosed these issues to the Internet Voting Committee in May 2014.

One of the problems we found allows a denial-of-service attack against the voting process. If a client sends an HTTP request containing unexpected header fields, the server logs the field names to disk. By sending many specially crafted requests containing fields with very long names, an attacker can exhaust the server's log storage, after which it will fail to accept any new votes. In the 2013 election, the size of the log partition was 20 GB. We estimate that an attacker could fill it and disable further voting in about 75 minutes. Curiously, the vulnerable code is only a few lines from the comment, "Don't write to disk; we don't know how large the value is." This indicates that the developers were aware of similar attacks but failed to account for all variants.

A second problem we discovered is a shell-injection vulnerability in a server-side user interface that is intended to allow operators to perform pre-determined administrative tasks. The vulnerability would allow such an operator to execute arbitrary shell commands on the election servers with root privileges. Under current procedures, this is moot, since the same workers perform other administrative tasks at the command line as root. However, shell injection vulnerabilities can be exceedingly dangerous [67], and the fact that the issue was not detected in advance of the election is a reminder that open source cannot guarantee the absence of vulnerabilities [44].

4. EXPERIMENTAL METHODOLOGY

In order to further investigate the security of the I-voting system, we set up a copy of the system in our lab, reproducing the software and configuration used for the 2013 election. While pen testing during a real election would have involved numerous legal and ethical problems [57], our laboratory setup allowed us to play the role of attacker in our own mock election without any risk of interfering with real votes.

4.1 Mock Election Setup

To reproduce the I-voting servers, we used the source code published on GitHub by the election authority [30]. We set up the servers by following published configuration documents [17] and matching step-for-step the actions performed by election workers in the official videos [18]. As part of this process, we generated our own key pairs for the web server TLS certificate and for the election key.

Some components were missing from the published server code, but we attempted to recreate them as faithfully as possible. First, the software for the log server, the `ivote-monitor` package, was not made available; we operated a standard `rsyslog` [58] server instead. Additionally, there was no source provided for the `evote_post.sh` script, which runs on every server during installation of the packages. We attempted to reproduce its functionality based on output shown during server configuration in the official videos.

In real elections, Estonia uses a hardware security module (HSM) in order to handle the election private key and decrypt votes. Since we did not have compatible hardware available, we emulated the HSM in software using OpenSSL and Python. Since this deviates from the fielded setup, we ensured that none of our attacks depend on vulnerabilities in the HSM.

We set up our own certificate authority and OCSP responder as stand-ins for the national ID card PKI. This allowed us to generate identities for mock voters. Since we did not have access to actual Estonian ID cards, we had to emulate them. We replaced the ID card on the client with a software-based emulator that speaks the protocol expected by the voting client application. Once again, we ensured that the success of our attacks does not rely on the changes we made. We assume for purposes of this study that the ID cards and associated infrastructure are secure.

For the client software, we started with the official voting client from the 2013 election, which we downloaded from the election website [23] in October 2013. For convenience, we focused on the Linux version of the client. Since the election public key and server certificate are hard-coded into the client, we needed to patch it in order to replace these with the keys of our mock election and server. Similarly, we used the official source code for the Android-based verification app [29] and modified it to communicate with our server.

Virtual machines we used to reproduce the election, together with source code for our demonstration attacks, are available online at https://www.estoniaevoting.org.

4.2 Threat Model

After setting up the mock election, we attempted to compromise it, allowing ourselves the resources and capabilities of a sophisticated but realistic attacker. This attacker could be a foreign state, a well-funded criminal organization, or a dishonest election insider. These kinds of attackers are difficult to defend against, but they represent a serious and realistic threat to modern elections given the enormous political and financial consequences at stake.

Since the time the Estonian system was introduced, cyberwarfare has become a well documented reality. Chinese espionage against U.S. companies [49], U.S. sabotage of Iran's nuclear enrichment program [60], and attacks by the U.K. against European telecommunications firms [65] are just a few examples. An increasing number of nations possess offensive computer security capabilities [52], and investment in these capabilities is reported to be growing at a significant rate [32]. Estonia itself suffered widespread denial-of-service attacks in 2007 that have been linked to Russia [64]. More recently, in May 2014, attackers linked to Russia targeted election infrastructure in Ukraine, which uses a computerized system to aggregate results from around the country. The

attackers reportedly attempted to discredit the election process by disrupting tallying and causing the system to report incorrect results [10].

A state-sponsored attacker would have powerful capabilities. We assume that they could obtain a detailed knowledge of the I-voting system's operation, which can be gleaned from published sources and reverse engineering (as we did), from insider knowledge, or by compromising systems used by the software developers and election officials. We also assume that if reverse engineering is required, the attacker would have sufficient human and technical resources to accomplish this on a short timescale. For client-side attacks, we assume that the attacker has the ability to deliver malware to voters' home computers. This could be done externally to the voting system, either by purchasing pre-existing criminal resources, such as a botnet, or by buying or discovering zero-day vulnerabilities in popular software. Another route would be to compromise the voting client before its delivery to voters, either by a dishonest insider who can alter the software or by other attackers who can compromise the computers used to build or distribute it.

5. ATTACKS

We used our reproduction of the I-voting system to experiment with a range of attacks. The I-voting system places significant trust in client and server components, making these highly attractive targets for an attacker.

While certain server operations are protected by cryptography (e.g., cast votes cannot be decrypted on the front-end web server, since it lacks the requisite private key), in other instances the servers are completely trusted to perform honestly and correctly when handling votes. Similarly, while the smartphone verification app gives voters some ability to check that the client software is behaving honestly, there are major limitations to this safeguard that can be exploited to hide malicious client behavior.

We experimentally verified that these trusted components are vulnerable by conducting two sets of demonstration attacks against them in our mock election setting. The first type are attacks on the client that are within reach of a financially capable attacker, in which an attacker can change votes in a retail manner for large numbers of individual voters. The second kind are server-side attacks within the reach of a well-resourced state-level attacker or dishonest insider, in which an attacker could change the wholesale results of the entire election by compromising the vote counting server.

5.1 Client-side Attacks

The voter's client machine is a trusted component of the I-voting system, and there are several ways that an attacker might try to infect a sufficient number of Estonian clients to alter election results in a close race. One is to rent bots from pre-existing botnets. Botnet operators frequently offer them for rent on the black market, and these can be targeted to a specific country or region [12]. A second way would be to discover or purchase a zero-day exploit against popular software used in Estonia. While this would be expensive, it would not be out of reach for a state-level attacker—several companies specialize in selling zero-day exploits to governments [33]. A third strategy would be to infect the official I-voting client before it is delivered to voters. The operational security problems documented in Section 3.2 suggest that this is a practical mode of attack.

Figure 11: **Malware records secret PINs** — Estonians use their national ID smartcards to sign and cast ballots. We developed demonstration client-side malware that captures the smartcard PINs and silently replaces the user's vote.

If the attacker's goal is merely to disrupt the election, far fewer infected system would be required. Estonian law allows election officials to cancel online balloting if a problem is detected [35]. In that case, Internet voters would have their electronic votes canceled and be required to go to the polls on election day. This is a useful emergency measure, but it requires election officials to both detect the attack and make a snap decision about its severity. Suppose an attacker infected a small number of clients with vote-stealing malware, allowed some of them to be detected, and designed the attack such that it was difficult to quickly determine the size of the infected population. Under these circumstances, officials might be compelled to cancel the online portion of the election, yet the attacker would need relatively few resources.

In order to investigate how an attacker could modify votes through the client application, we implemented two experimental client-side attacks. Both assume that the attacker has used one of the techniques noted above to initially infect the client machine. Each attack uses a different mechanism to defeat the smartphone verification app (see Section 2.3), the only tool available to voters to detect whether their ballot choices have been manipulated by client-side malware.

Both attacks involve hidden malicious processes that run alongside the I-voting client application and tamper with its execution. In order to develop them, we first needed to reverse engineer parts of the client software used in 2013. The client is closed source, and the developers took measures to complicate reverse engineering. The executable is obfuscated using the UPX packing tool. Strings, public keys, and other resources are hidden by XORing them with the output of a linear congruential generator. These measures did not significantly complicate the construction of our attacks. We used the UPX application with the `-d` switch to unpack the binary and used the IDA Pro disassembler and Hex-Rays decompiler to reverse the portions necessary for our attacks.

Ghost Click Attack In the first attack, we use malware on the client machine to silently replace the user's vote with a vote in favor of an attacker-selected candidate. At a high level, the malware silently sniffs the victim's PIN during the original voting session. The real vote is cast, and everything

appears normal, including the verification smartphone app if the voter uses it. Then, the malware waits until it is too late to verify again — either until the 30 minute time limit has passed or until after the user closes the client software and the QR code can no longer be scanned.

At that point, the malware checks whether the voter's ID card is still present in the computer. If so, it opens a copy of the I-voting client in a hidden session and, through keystroke simulation, submits a replacement vote. If the ID card has already been removed, the malware remains dormant until the card is inserted again. Since Estonian ID cards are used for a variety of applications, many voters are likely to use their cards again within the week-long online voting period.

In our implementation, the malware attaches to the voting client process and captures PINs by setting breakpoints using `ptrace` [55]. Upon reaching a breakpoint, it reads the PIN from the client's memory and stores it for future use. Although our implementation runs in userspace, a kernel-level rootkit could be used to make the attack even more difficult to detect [36]. The malware could be extended to sniff PINs opportunistically any time voters use their ID cards, such as when logging into a bank.

Bad Verify Attack The Ghost Click attack defeats the verification app, but applying it on a large scale would lead to a suspiciously high number of replacement votes. We also experimented with a stealthier but more complicated style of attack that targets the verification app directly.

The verification app is premised on the notion that the smartphone is an independent device that is unlikely to be compromised at the same time as the client PC. However, modern smartphones are not well isolated from users' PCs, as there is typically regular communication between the two devices. Users frequently plug their phones into their PCs to charge them or to transfer files. User content is regularly synchronized between devices through Google Drive, Dropbox, and other cloud services. Android even allows users to remotely install applications on their phones from their PCs through the Google Play Store web interface, and other platforms have similar mechanisms [50]. As a result of this convergence, there are abundant means by which PC malware can attempt to infect the user's phone. This would allow the attacker to deploy a dishonest verification app that colludes with malware on the PC to fool the voter.

To experiment with such an attack, we implemented tandem PC and smartphone malware. Malware on the PC detects which candidate the voter selects and modifies the QR code shown by the I-voting client so that it encodes the voter's chosen candidate. A malicious verification app on the voter's phone behaves just like the real verification app, except that it displays whatever candidate is embedded in the QR code, rather than the candidate for whom the vote was actually cast. This allows the PC malware to arbitrarily change the submitted vote without being detected by verification or causing a suspicious number of replacement votes.

This form of attack adds complexity, due to the need to compromise both devices simultaneously. It also carries an elevated possibility of detection if used on a large scale, since some voters may attempt verification with devices owned by others. However, it illustrates that as the PC and smartphone platforms continue to converge, it will become increasingly unsafe to treat them as independent devices.

5.2 Server-side Attacks

The integrity of the count depends on the correct operation of the counting server and its HSM, which are the only components with the ability to decrypt votes. Similarly, ballot secrecy depends on the counting server to not leak information about the correspondence between encrypted and decrypted votes. An attacker who infects the counting server with malicious software can violate these critical security properties.

Although the counting server is not connected to a network, there are a number of other means by which it might be attacked. State-level attackers are known to employ firmware-based malware [4], for instance, which could be used to infect the BIOS or hard disk before delivery to election officials. Sophisticated attackers can also target component supply chains and distribution infrastructure [43]. We were informed during our observation mission that the Internet Voting Committee has a bid process prior to every election to rent the servers that they use, and attackers could try to introduce subverted hardware through this process.

Another infection strategy would be to compromise the server software before it is installed at the beginning of the election. We pursued this route in our experiments.

Injecting malware Despite procedural safeguards [17], an attacker who strikes early enough can introduce malicious code into the counting server by using a chain of infections that parallels the configuration process. During pre-election setup, workers use a development machine, which is configured before setup begins, to burn Debian Linux installation ISOs to DVDs. These DVDs are later used to configure all election servers. If the machine used to burn them is compromised — say, by a dishonest insider, an APT-style attack on the development facility, or a supply-chain attack — the attacker can leverage this access to compromise election results.

We experimented with a form of this attack to successfully change results in our mock election setup. We first created a modified Debian ISO containing vote-stealing malware intended to execute on the counting server. The tainted ISO is repackaged with padding to ensure that it is identical in size to the original. In a real attack, this malicious ISO could be delivered by malware running on the DVD burning computer, by poisoning the mirror it is retrieved from, or by a network-based man-in-the-middle.

Defeating integrity checking During the setup process, election workers check the SHA-256 hash of the ISO file against the `SHA256SUMS` file downloaded via anonymous FTP from debian.org. Since regular FTP does not provide cryptographic integrity checking, a network-based man-in-the-middle could substitute a hash that matched the malicious ISO. However, this hash would be publicly visible in videos of the setup process and might later arouse suspicion.

An attacker who had compromised the DVD burner computer could achieve greater stealth. To demonstrate this, we implemented a custom rootkit that defeats the hash verification. Our rootkit is a kernel module that hooks system calls in order to cause the hash verification to succeed and the original ISO's hash to be printed. Hash checks applied in this way are only a minor speedbump under our threat model.

Vote-stealing payload After passing the hash check, the tainted ISOs are used to install the OS on all election servers, spreading the infection. When the new OS boots, the malware checks whether the machine is configured as the counting server, in which case it launches a vote-stealing payload.

During the counting process, this payload acts as wrapper around the process responsible for using the HSM to decrypt votes. This allows the malware to alter the decrypted votes prior to returning them to the counting application. (In our demonstration, we change 100% of the votes, but it would be straightforward to implement a more subtle algorithm that manipulates an arbitrary fraction.) The altered votes are then counted and released as the official results. Such an attack would be unlikely to be detected, as there is no audit mechanism to check the accuracy of the decryption.

Other avenues for infection What we have described is far from the only means of injecting a malicious payload into the servers. Several other pieces of closed-source software of unknown or untrusted provenance could be vehicles for attacks. These include the `evote_post.sh` script, missing from the server source code repository, which runs on all servers, as well as the driver software for the HSM, which is a closed-source application manually installed to the counting server from a DVD. These programs all touch critical, trusted portions of the I-voting system, yet they are not reviewable by the public and not integrity checked through any visible procedures.

In fact, during the pre-election server setup process in 2013, workers used an incorrect version of the `evote_post.sh` script that failed to install the `evote_analyzer` package on the VFS. Administrators later had to manually install this package during the voting period, after they realized that the server was not reporting all expected log data [56]. This provides a case-in-point example of a failure of the procedural protections to ensure that only the correct software gets installed on the server machines.

Zero-day exploits are yet another potential attack vector, and a source of many "known unknowns." One illustration of this is the OpenSSL Heartbleed bug [34], which was not disclosed until April 2014. The front-end server used during the 2013 election was vulnerable to Heartbleed, and an attacker who knew about the bug likely could have exploited it to extract the server's TLS private key. Then, using a man-in-the-middle attack on connections from voters, they could have selectively prevented certain voters' ballots from being received by the real server.

The key lesson from our server-side attack is that it is extremely difficult to ensure the integrity of code running on a critical system, particularly when faced with the possibility of sophisticated attacks or dishonest insiders. If any element in the lineage of devices that handle the software installed on the counting server is compromised, this could jeopardize the integrity of election results [63].

5.3 Attacking Ballot Secrecy

While our experiments focused on attacks against the integrity of election results, we also considered ballot secrecy issues, since the secrecy of the voter's ballot is a critical defense against voter coercion and vote buying. The I-voting system implements a relatively strong protection against in-person, individual coercion by allowing voters to cast replacement votes online or to cancel their electronic ballots entirely and vote in person on election day. More sophisticated attacks remain possible, however, including spyware on the voter's PC or smartphone, as well as server-side attacks.

Server-side attacks on ballot secrecy are particularly troubling, since preserving ballot secrecy is a main goal of the system's cryptographic double-envelope architecture. The I-voting design attempts to ensure that votes remain private by breaking the association between voters' digital signatures from their plaintext votes. The encrypted ballots are separated from the signatures and copied to an isolated machine before being decrypted and counted. Note that this machine, the counting server, has access to the complete association between the encrypted ballots and the plaintext votes. An attacker who can smuggle this information out through a covert channel can compromise every voter's secret ballot.

Unfortunately, the tabulation procedures offer multiple possibilities for exfiltrating this information. When tabulation is complete, officials use the counting server to burn a DVD containing both vote totals and log files. Suppose for simplicity that the attacker is a dishonest insider with access to this DVD and to the complete set of signed, encrypted ballots (e.g. from a backup disk) and some mechanism for infecting the counting server with malicious code, such as the routes discussed above. The counting server malware can sort the encrypted ballots and leak the voter choices corresponding to each as a sequence of integers in the same order. Since there is typically only one race, only a few bits per ballot are needed to determine the choices of all voters. The malware could steganographically encode this data into the log files through the order of entries, or it could simply write this information to unallocated sectors of the disc. The attacker can then decode this information and use it to associate every voter's digital signature (and hence, their identity) with their vote.

6. DISCUSSION

Though we have spent the majority of this report discussing weaknesses and risks, we would be remiss if we failed to acknowledge the great lengths that the I-voting system developers, security staff, and officials go to in their efforts to protect the election system.

One core strength of the I-voting system is Estonia's national ID card infrastructure and the cryptographic facilities it provides. While the ID cards cannot prevent every important attack, they do make some kinds of attacks significantly harder. The cards also provide an elegant solution for remote voter authentication, something few countries do well.

The Internet Voting Committee's willingness to release source code is a very positive step for transparency. This shows confidence in the software's developers and demonstrates officials' desire to work with the security community at large. Providing access to the source allows many parties to analyze it — not only international researchers like us but also the domestic security community, who have an even greater interest in the system's secure operation. For these reasons, we urge the committee to go further and release the source code to the I-voting client and the missing portions of the server code discussed in Section 4.1.

Finally, we commend the Internet Voting Committee for their dedication to improving the election system. Since its inception in 2005, the system has undergone significant changes. From the switch to a standalone client, to the deployment of the log server that enhances forensic and monitoring capabilities, to the addition of the verification app, the I-voting system has not stood still. Yet as we have argued, even these and an array of other useful safeguards are not enough to secure Estonia's online elections in the face of a determined and well-resourced modern attacker.

Opportunities for innovation While the risks of Internet voting are clear, the benefits are uncertain. Many Estonians support I-voting because they believe there is widespread fraud in the country's paper-based system. Whether or not these concerns are founded, the I-voting system can do little to help, since nearly 80% of votes are still cast on paper. Fortunately, there are safe and effective ways to apply new technology to secure paper-based voting.

In recent years, researchers have developed methods that can dramatically increase the security of paper ballots. Statistical risk-limiting audits [6, 7, 46, 62] can minimize the risk of error or fraud during tabulation. Cryptographic techniques that achieve end-to-end verifiability [5, 9, 59] enable individual voters to verify that every vote has been counted accurately. Estonia has an opportunity to be the first country in the world to adopt these technologies on a national scale.

7. CONCLUSIONS

Compared to other online services like banking and e-commerce, voting is an exceedingly difficult problem, due to the need to ensure accurate outcomes while simultaneously providing a strongly secret ballot. When Estonia's I-voting system was conceived in the early 2000s, it was an innovative approach to this challenge. However, the designers accepted certain tradeoffs, including the need to trust the central servers, concluding that although they could take steps to reduce these risks through procedural controls, "the fundamental problem remains to be solved" [2]. More than a decade later, the problem remains unsolved, and those risks are greatly magnified due to the rapid proliferation of state-sponsored attacks.

As we have observed, the procedures Estonia has in place to guard against attack and ensure transparency offer insufficient protection. Based on our tests, we conclude that a state-level attacker, sophisticated criminal, or dishonest insider could defeat both the technological and procedural controls in order to manipulate election outcomes. Short of this, there are abundant ways that such an attacker could disrupt the voting process or cast doubt on the legitimacy of results. Given the current geopolitical situation, we cannot discount state-level attacks targeting the system in future elections.

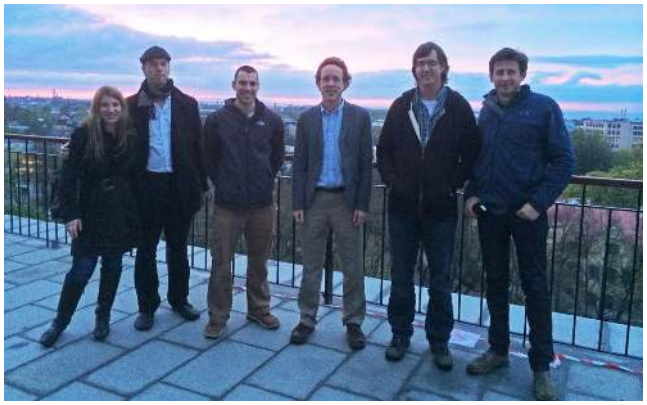
Due to these risks, we recommend that Estonia discontinue use of the I-voting system. Certainly, additional protections could be added in order to mitigate specific attacks (e.g. [48]), but attempting to stop every credible mode of attack would add an unmanageable degree of complexity. Someday, if there are fundamental advances in computer security, the risk profile may be more favorable for Internet voting, but we do not believe that the I-voting system can be made safe today.

Acknowledgments

We thank everyone in Estonia who shared their insights on the I-voting system during our visits, including Sven Heiberg, Andres Hiie, Priit Kutser, Helger Lipmaa, Tarvi Martens, Arnis Parsovs, Jan Willemson, and many others. Of course, the views expressed here (and any errors) are ours alone. We also thank David Jefferson, Brian Krebs, Barbara Simons, Peiter "Mudge" Zatko, and the anonymous reviewers. We are particularly grateful to Rop Gonggrijp and Dominic Rizzo for numerous suggestions and contributions.

We have not accepted any financial support from within Estonia, except for travel and accommodations for the observers during the October 2013 voting period, which were reimbursed by Tallinn City Council. The only requirement for that arrangement was that we observe the election.

This material is based upon work supported by Google/ ATAP, by the U.S. National Science Foundation under grants CNS-1255153 and CNS-1345254, and by an NSF Graduate Research Fellowship under grant DGE-1256260.



— Tallinn, May 2014

8. REFERENCES

[1] B. Adida. Helios: Web-based open-audit voting. In *Proceedings of the 17th USENIX Security Symposium*, Aug. 2008.

[2] A. Ansper, A. Buldas, M. Oruaas, J. Priisalu, A. Veldre, J. Willemson, and K. Virunurm. E-voting concept security: analysis and measures. Technical Report EH-02-01, Estonian National Electoral Committee, 2003.

[3] A. W. Appel. Security seals on voting machines: A case study. *ACM Trans. Inf. Syst. Secur.*, 14(2):18:1–18:29, Sept. 2011.

[4] J. Applebaum, J. Horchet, and C. Stöcker. Shopping for spy gear: Catalog advertises NSA toolbox. Der Spiegel, Dec. 2013. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

[5] J. Benaloh, M. Byrne, P. T. Kortum, N. McBurnett, O. Pereira, P. B. Stark, and D. S. Wallach. STAR-Vote: A secure, transparent, auditable, and reliable voting system. *CoRR*, abs/1211.1904, 2012.

[6] J. Bretschneider, S. Flaherty, S. Goodman, M. Halvorson, R. Johnston, M. Lindeman, R. L. Rivest, P. Smith, and P. B. Stark. Risk-limiting post-election audits: Why and how, Oct. 2012. http://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.

[7] J. A. Calandrino, J. A. Halderman, and E. W. Felten. Machine-assisted election auditing. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, 2007.

[8] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy*, 2(1):38–47, Jan 2004.

[9] D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. Rivest, P. Y. A. Ryan, E. Shen,

A. Sherman, and P. Vora. Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes. *IEEE Transactions on Information Forensics and Security*, 4(4):611–627, Dec. 2009.

[10] M. Clayton. Ukraine election narrowly avoided 'wanton destruction' from hackers. Christian Science Monitor, June 2014. http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

[11] Cybernetica AS. Internet voting solution, 2013. Accessed: May 13, 2014, http://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4_web.pdf.

[12] D. Danchev. Study finds the average price for renting a botnet. ZDNet, May 2010. http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528.

[13] Estonian Certification Authority. Avaleht. In Estonian. http://www.id.ee/.

[14] Estonian Certification Authority. Kasulik tugiinfo mobiil-id kohta. In Estonian. http://mobiil.id.ee/kasulik-tugiinfo/.

[15] Estonian Certification Authority. Mis on ID-tarkvara? In Estonian. https://installer.id.ee/.

[16] Estonian Information System's Authority. Public key infrastructure PKI, May 2012. https://www.ria.ee/public-key-infrastructure/.

[17] Estonian Internet Voting Committee. Dokumendid, 2013. In Estonian. Accessed: March 2014, http://vvk.ee/valijale/e-haaletamine/e-dokumendid/.

[18] Estonian Internet Voting Committee. Ehk videos, 2013. In Estonian. Accessed: March 2014, https://www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ/videos.

[19] Estonian Internet Voting Committee. Statistics about Internet voting in Estonia, May 2014. http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.

[20] Estonian Internet Voting Committee. Using ID-card and mobil-ID, May 2014. https://www.valimised.ee/eng/kkk.

[21] Estonian Ministry of Foreign Affairs. Estonia today, 2012. http://www.euc.illinois.edu/estonia/documents/E-Estonia.pdf.

[22] Estonian National Electoral Committee. Kohaliku omavalitsuse volikogu valimised 2013. In Estonian. http://www.vvk.ee/kohalikud-valimised-2013/.

[23] Estonian National Electoral Committee. Vabariigi valimiskomisjon. In Estonian. Accessed: October 2013, http://www.vvk.ee/.

[24] Estonian National Electoral Committee. Elektroonilise hääletamise süsteemi üldkirjeldus, 2013. In Estonian. http://vvk.ee/public/dok/elektroonilise-haaletamise-systeemi-yldkirjeldus-EH-03-03-1_2013.pdf.

[25] Estonian National Electoral Committee. Valimised: Android Apps on Google Play, Oct. 2013. In Estonian. Accessed: May 13, 2014, https://play.google.com/store/apps/details?id=ee.vvk.ivotingverification.

[26] Estonian National Electoral Committee. Comment on the article published in The Guardian, May 2014. http://vvk.ee/valimiste-korraldamine/vvk-uudised/vabariigi-valimiskomisjoni-vastulause-the-guardianis-ilmunud-artiklile/.

[27] Estonian National Electoral Committee. Valimised on the App Store on iTunes, Apr. 2014. In Estonian. Accessed: May 15, 2014, https://itunes.apple.com/ee/app/valimised/id871129256.

[28] Estonian National Electoral Committee. Valimised: Windows Phone'i rakenduste+mängude pood (Eesti), Apr. 2014. In Estonian. Accessed: May 15, 2014, https://www.windowsphone.com/et-ee/store/app/valimised/11c10268-343f-461a-9c73-630940d8234b.

[29] Estonian National Electoral Committee, Estonian Internet Voting Committee, and Cybernetica AS. Android based vote verification application for Estonian i-voting system, Sept. 2013. https://github.com/vvk-ehk/ivotingverification.

[30] Estonian National Electoral Committee, Estonian Internet Voting Committee, and Cybernetica AS. e-hääletamise tarkvara, Sept. 2013. Accessed: March 2014, https://github.com/vvk-ehk/evalimine.

[31] Estonian Public Broadcasting. Center Party petitions European human rights court over e-voting, Sept. 2013. Accessed: May 14, 2014, http://news.err.ee/v/politics/4ee0c8a2-b9c2-4d28-8ae4-061e7d9386a4.

[32] J. Fleming. EU nations developing cyber 'capabilities' to infiltrate government, private targets. EurActiv, Dec. 2013. http://www.euractiv.com/infosociety/eu-nations-lack-common-approach-news-532294.

[33] A. Greenberg. Shopping for zero-days: A price list for hackers' secret software exploits. Forbes, Mar. 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

[34] The Heartbleed bug, Apr. 2014. http://heartbleed.com/.

[35] S. Heiberg, P. Laud, and J. Willemson. The application of i-voting for Estonian parliamentary elections of 2011. In *VOTE-ID*, pages 208–223, 2011.

[36] G. Hoglund and J. Butler. *Rootkits: Subverting the Windows Kernel*. Addison-Wesley, 2005.

[37] ICT Export Cluster. e-estonia.com: The digital society, Aug. 2014. http://e-estonia.com/.

[38] R. Johnston. The real deal on seals: Improving tamper detection. *Security Management*, 41:93–100, Sept. 1997.

[39] R. Johnston. Some comments on choosing seals and on PSA label seals. In *Proceedings of the 7th Security Seals Symposium*, 2006. http://www.ne.anl.gov/capabilities/vat/pdfs/choosing-seals-and-using-PSA-seals-2006.pdf.

[40] R. Johnston. Insecurity of New Jersey's seal protocols for voting machines, Oct. 2010. http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf.

[41] R. Johnston and A. R. Garcia. Vulnerability assessment of security seals. *Journal of Security Administration*, 20:15–27, 1997.

[42] D. W. Jones and B. Simons. *Broken Ballots: Will Your Vote Count?* Stanford University Center for the Study of Language and Information, 2012.

[43] E. Kain. Report: NSA intercepting laptops ordered online, installing spyware. Forbes, Dec. 2013. Accessed:

May 14, 2014, http://www.forbes.com/sites/erikkain/2013/12/29/report-nsa-intercepting-laptops-ordered-online-installing-spyware/.

[44] J. Kitcat. Source availability and e-voting: An advocate recants. *Commun. ACM*, 47(10):65–67, Oct. 2004.

[45] B. Laxton, K. Wang, and S. Savage. Reconsidering physical key secrecy: Teleduplication via optical decoding. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, pages 469–478, 2008.

[46] M. Lindeman and P. B. Stark. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, 10(5):42–49, 2012.

[47] H. Lipmaa. Paper-voted (and why I did so). Blog post, Mar. 2011. http://helger.wordpress.com/2011/03/05/paper-voted-and-why-i-did-so/.

[48] H. Lipmaa. A simple cast-as-intended e-voting protocol by using secure smart cards, May 2014. http://eprint.iacr.org/2014/348.

[49] Mandiant. APT1: Exposing one of China's cyber espionage units, Feb. 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[50] N. Mediati. How to remotely install apps on your smartphone. TechHive, Nov. 2013. http://www.techhive.com/article/2067005/how-to-remotely-install-apps-on-your-smartphone.html.

[51] U. Oja. Paavo Pihelgas: Elektroonilise hääletamise vaatlemine on lihtsalt võimatu, Mar. 2011. In Estonian. http://forte.delfi.ee/news/digi/paavo-pihelgas-elektroonilise-haaletamise-vaatlemine-on-lihtsalt-voimatu.d?id=41933409.

[52] F. Paget. Hacking summit names nations with cyberwarfare capabilities. McAfee Blog Central, Oct. 2013. http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

[53] A. Parsovs. Practical issues with TLS client certificate authentication, Feb. 2014. https://www.internetsociety.org/sites/default/files/12_4_1.pdf.

[54] B. Plumer. Estonia gets to vote online. Why can't America? Wonkblog. The Washington Post, Nov. 2012. http://www.washingtonpost.com/blogs/wonkblog/wp/2012/11/06/estonians-get-to-vote-online-why-cant-america/.

[55] ptrace(2): process trace. Linux Programmer's Manual.

[56] T. Raidma and J. Kase. Kohaliku omavalitsuse volikogu valimiste e-hääletamise protseduuride hindamise lõpparuanne, Jan. 2014. In Estonian. http://vvk.ee/public/KOV13/lopparuanne_2013.ddoc.

[57] D. G. Robinson and J. A. Halderman. Ethical issues in e-voting security analysis. In *Proceedings of the 2nd Workshop on Ethics in Computer Security Research (WECSR)*, March 2011.

[58] rsyslog: The rocket-fast system for log processing, Apr. 2014. http://www.rsyslog.com/.

[59] P. Y. A. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia. Prêt à voter: A voter-verifiable voting system. *Trans. Info. For. Sec.*, 4(4):662–673, Dec. 2009.

[60] D. E. Sanger. Obama order sped up wave of cyberattacks against Iran. The New York Times, June 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[61] B. Simons. Report on the Estonian Internet voting system. Verified Voting Blog, Sept. 2011. https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/.

[62] P. B. Stark. Super-simple simultaneous single-ballot risk-limiting audits. In *Proceedings of the USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, Aug. 2010.

[63] K. Thompson. Reflections on trusting trust. *Commun. ACM*, 27(8):761–763, Aug. 1984.

[64] I. Traynor. Russia accused of unleashing cyberwar to disable Estonia. The Guardian, May 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

[65] I. Traynor. GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm. The Guardian, Oct. 2013. http://www.theguardian.com/uk-news/2013/oct/03/gchq-eu-surveillance-cyber-attack-belgian.

[66] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp. Security analysis of India's electronic voting machines. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS)*, pages 1–14, 2010.

[67] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman. Attacking the Washington, D.C. Internet voting system. In *Proceedings of the 16th International Conference on Financial Cryptography and Data Security*, Feb. 2012.