webrootsdemocracy.org

Secure Voting

A guide to secure
#onlinevoting in elections.

WebRoots Democracy

Campaigning for online voting in UK elections.

Contents

Forewords

Areeq Chowdhury

Rt Hon John Bercow MP

Chloe Smith MP

Graham Allen MP

Hannah Bardell MP

Rt Hon Tom Brake MP

> “The Government said they wanted assurances of online voting being ‘robust and really hard to hack’ – I believe this report provides those assurances.”

Forewords

Areeq Chowdhury

One of the major challenges I've come across since starting this campaign has been to provide reassurances that modernising our voting system would not make it less secure.

In October last year, the Government said they wanted assurances of online voting being "robust and really hard to hack" – I believe this report provides those assurances.

Secure Voting draws upon decades of experience in secure online voting from leading academics and global providers of online and electronic voting. If you were to seek advice on how to make a car or a boat, you would seek it from those who have years of experience in successfully making cars and boats. This is the approach I have sought when putting together this report.

This report does not shy away from the security challenges of online voting, but addresses them head on. Issues such as cyber-attacks, data security, peer-pressure, and identity verification are all addressed in detail by the contributors. When reading it, I urge you to consider it within the context of the current voting system. A common theme throughout this report is the strength an online voting system has when compared to current methods such as postal voting.

In addition, this report includes research which shows a staggering 95% of the UK's current 19,000+ politicians were elected on turnouts of less than 50%. In a democracy such as ours, we should not turn a blind eye to this.

As highlighted in WebRoots Democracy's Viral Voting report last year, increased voter engagement is one of the many benefits that online voting can deliver in the UK. It is time for the Government to realise these benefits.

In the House of Commons at the end of last year, Nick Boles MP, Minister of State at the Department of Business, Innovation and Skills said that online voting is down to "a matter of time" and that the Government are happy to work with other political parties and groups outside of Parliament "to ensure that eventually we do get there."

This reform could take up to 5 years to enact, and the clock is against us for 2020, so I urge the Government to action this commitment and follow the recommendations set out in this report.

Areeq Chowdhury
Report Editor and Founder of WebRoots Democracy

Rt Hon John Bercow MP

I am delighted to welcome this report on secure online voting by WebRoots Democracy.

As Speaker of the House of Commons, most people will know me – if they have heard of me at all – as the chap who shouts "Order!" a lot in the Chamber. However, when I was elected to the position in June 2009 I said that it should be part of the role of any modern Speaker to act as a champion of, and an ambassador for, Parliament.

The Speaker's Commission on Digital Democracy was a product of this desire to open up Parliament and to improve the way we interact, with a focus on how digital technology could widen participation in politics, with a view to encouraging more effective engagement. Members of the Commission spent a year involved in extensive consultation with a wide range of people from different communities, ethnicities, ages and income brackets. It was this diversity of views that informed the Commissioners, who reported back on 26th January 2015 with five key targets and further recommendations as to how the House might harness the power of the digital revolution to facilitate better dialogue between politicians and ordinary people.

The recommendation that online voting be available by 2020 for all citizens generated a fascinating debate and, perhaps understandably, the most media interest. There are currently two ways of voting in the UK: in person or by proxy in a polling station; and in advance by post. Although online voting has been piloted on a small scale, it was not available at last year's general election. Some people, particularly young people, told the Commission that the inconvenience of having to vote in person put a lot of people off doing so. Similarly, those with disabilities, Britons living abroad and military personnel posted overseas would undoubtedly benefit from a secure online voting system. On the other hand, concerns were raised about the potential for cyber-attacks and hacking, not to mention the possibility that voter impersonation and intimidation could become more commonplace when voting is undertaken online. However, I have always been clear that protecting the integrity of the ballot box is of the utmost importance.

I look forward to the contribution to the discussion the release of the WebRoots Democracy report has, and the debate that will follow.

Rt Hon John Bercow MP
Speaker of the House of Commons

Chloe Smith MP

I am pleased to work once again with WebRoots Democracy to argue for online voting.

The Chinese proverb advises us to have planted a tree years ago. We should have planted this tree already, and there is no time to lose.

I often take a generational view of democracy. It is an extremely unusual thing for Generation Y not to be able to do something online.

We shop, we bank, we date, we chat, we organise with ease. However, we vote entirely on paper. It's alien to young people, and indeed to anyone who appreciates the capability of the internet. It's also ineffective: we communicate online with people all the time but we lack the final "one-click" to clinch the deal in democracy when the time comes.

Of course there are important security and cost considerations, but those pertain to paper voting too. Sensibly legislating and implementing e-voting can be done if politicians admit that it is almost immoral by now to fail to consider it. It is a sizeable project and we should start it.

So I welcome this report, which brings together in-depth knowledge about the practicalities of the reform. Moving voting online does not need to scare us.

This is too obvious an area for reform to ignore if politicians are to think and act anything like the new generation which will grow to dominate. My generation is politically interested, but turned off by traditional politics. That means that today's politicians have to engage today's young people once again in the nuts and bolts of democracy.

Even if we have to plant that tree today, let's do it without delay and make it blossom, not wither.

Chloe Smith MP
Chair of the All-Party Parliamentary Group on Democratic Participation
Conservative Member of Parliament for Norwich North

Graham Allen MP

The growth of the internet and digital technology has enabled individuals to be truly global citizens, connecting them beyond borders with people and cultures at the touch of their fingertips.

It has transformed businesses and not-for-profits, increasing productivity, efficiency, and innovation at a scale not seen before.

The public sector, too, has experienced how the internet can help them save money, foster creativity, and engage with people using methods more reflective of their lives.

Modernising the way we vote, therefore, is an idea that should be taken seriously by the Government.

The introduction of online voting is a reform that was backed by the House of Commons Political and Constitutional Reform Select Committee last year, and it was recommended as a way to boost voter engagement.

It is simply unacceptable for politicians to turn a blind eye to poor levels of voter participation. It is not a problem that should be deferred to future generations.

In our Party's leadership election last year, a record 343,995 voters chose to cast their votes online, representing 81% of the total turnout. This was the largest online voting election in UK history. It is therefore, of no surprise to me that polls show it would be the most popular method if brought in.

I am pleased to welcome this report by WebRoots Democracy. It represents an important collection of work addressing the key security challenges and contains a number of interesting ideas.

Change does not happen overnight, and modernising elections will take time, however, if we are serious about creating a twenty-first century democracy, online voting is a reform that must be given serious attention.

Graham Allen MP
Chair of the Political and Constitutional Reform Select Committee 2010-15
Labour Member of Parliament for Nottingham North

Hannah Bardell MP

Isn't it time for our voting system to reflect the era in which we live?

This issue is not about modernising for modernising's sake: as this WebRoots Democracy report indicates, an electronic voting system would provide acute identity verification, offer confirmation of a citizen's vote cast, and increase voter turnout.

In the 2007 election in Scotland we saw two worlds collide in terms of attempts to modernise the system. Whilst we maintained the manual system of casting our votes, an electronic counting system was put in place. The results were disastrous. Around 100,000 votes were disqualified, around 7% of total votes cast.

So in Scotland, we've felt the pain of modernisation gone wrong. But then we only modernised half the system!

Of course, there are concerns, and these concerns should and have been diligently addressed in this report. It offers the Government's existing online verification tool, GOV.UK Verify, as a particularly encouraging solution to addressing potential voter fraud. The report's 'repeat voting' proposal is a vigorous attempt to avoid coerced voting in the home or elsewhere and should be applauded for its attention to the many new factors which would arise in an electronic voting system.

One of the key offerings is the opportunity for voters to verify their selection and receive confirmation of their choice. Our current voting system experiences thousands of accidentally spoilt ballots in a General Election - each one representing a lost voice in the democratic process. Measures to ensure protection against cyber-attacks, such as incorporating independent third parties to attack the system in order to test it, are more secure than our current system, where posted ballots could be manipulated.

Moreover, this issue is about engagement and confidence in our democratic system. Whilst the voting system is stuck in the same yesteryear of pen to paper and manual counting – society will move on and our democracy will be stuck in the past.

This report suggests that an electronically-voting democracy is a more inclusive and representative democracy. We cannot languish any longer, the UK Parliament and our voting system must develop into the 21st Century.

Hannah Bardell MP
Scottish National Party Member of Parliament for Livingston

Rt Hon Tom Brake MP

Over the last two decades, the arrival and explosion of the Internet has transformed the way in which we live, communicate and share information. Politics has not been immune to this transformation. I still remember my first days as a political activist. The only way to effectively spread our message was by knocking on thousands of doors, pounding the streets delivering leaflets or, if lucky, getting TV or radio coverage for an issue.

Whilst these methods are still widely used, little did I know that in 2016 I would also be having monthly online Facebook video Q&A with local residents, casework Skype calls, or updating thousands of people on an issue by sending an email or posting on social media. In fact, it's quite astonishing that in 2016, people are able to use the Internet to shop online, read the news or make a secure banking transaction, but are not yet able to vote online. It's time for politics to truly enter the 21st century and adopt online voting.

Every election cycle, pundits and politicians criticise voter apathy, disengagement in the political process, and even bad weather for low voter turnouts. In the last General Election only 66% of registered voters actually cast a ballot. The figures are even more depressing when looking at the 2014 local elections in Sutton, the borough in which I live. Only 47% of residents showed up to the polls. I am convinced that online voting could be a major solution to these problems.

As previous research has shown, it has the potential to significantly raise youth voter turnout, improve voting accessibility for vulnerable and disabled residents, and reduce the costs of elections. Of course, the public and the Electoral Commission will need to be reassured that voting online will be safe and secure, and the report extensively addresses this topic.

I welcome this stellar report produced by WebRoots Democracy. It provides an excellent explanation of the effects of online voting and its importance to the future of our political institutions. It satisfies the need to produce a secure, but more accessible means of casting a ballot. We must take this opportunity to push our nation in a direction that allows everyone to exercise their right to vote and exercise it easily.

Rt Hon Tom Brake MP
Liberal Democrat Member of Parliament for Carshalton and Wallington

Executive summary

Purpose and background of this report

Recommendations

Key findings

> There is plenty of political representation, but relatively little political participation at the ballot box.
>
> WebRoots Democracy

Purpose and background of this report

In the UK today, there is plenty of political representation, but relatively little political participation at the ballot box. As analysis in this report shows, an estimated 95% of the UK's over 19,000 elected politicians were elected in elections with less than 50% voter turnout.

One solution to engage 21st century society in the UK is to modernise our method of voting, and to allow the public to be able to vote online in elections and referenda. The benefits to doing so are set out in detail in the Viral Voting report published in March 2015, and include improved voter engagement and education; the elimination of accidentally spoilt ballots; a reduction in the cost-per-vote; and better accessibility for disabled and vision-impaired voters.[1]

One of the challenges of online voting, as with all important online services, is the security of the process and system. With the help of experienced providers of online voting and academics from around the world, this report aims to be a guide to the key questions surrounding online voting security and the potential solutions.

WebRoots Democracy

WebRoots Democracy[2] is a voluntary, youth-led pressure group, campaigning for the introduction of an online voting option in UK elections.

In addition to this, the pressure group intends to reverse growing political apathy and low electoral turnout in the UK, particularly amongst young people.

Whilst political apathy has a variety of causes, we must recognise that we live in an age of distraction and rapid technological advances. As such, WebRoots Democracy is also campaigning for an accessible, informative, and interactive election website to help reach out to new voters.

It was conceived in February 2014, and launched[3] in May 2014 following the European Parliament and Local Council elections.

Summary

Recommendations

1. The Government should invest in a programme to implement an accessible online voting option in elections with a view to the public being able to vote online by the 2020 UK General Election.
2. The Government should run online voting pilots, using a fair and open competition process, across the remainder of this Parliament.
3. All major UK political parties should sign a cross-party commitment to online voting.

Key findings

Voter verification

Ensuring that the correct person is voting in an election is crucial to ensure a true and fair democratic process. A number of solutions are put forward in this report ranging from the use of simple usernames and passwords, special mobile SIM cards, mobile pin-codes, and the use of the Government's existing online verification tool, GOV.UK Verify.

Voter verification is something that is lacking in current voting methods at polling stations and via post due to there being no identification checks at polling stations and with the ability of malicious individuals to steal and forge postal votes.

Safeguards from peer-pressure

The potential of online voting to allow the public to vote wherever they feel most comfortable somewhat reduces the risk of voters being pressured by a partner or another individual to vote in a certain way. A proposal which is mentioned a number of times within this report is to allow "repeat voting" where only the last vote counts. This is in order to devalue coercion altogether.

Ensuring the correct vote is submitted

Offering voters a chance to verify their selection or to receive some unique form of confirmation of their choice is put forward as a solution in this report. Potential barriers to this such as "man-in-the-middle attacks" are examined by some of the contributors.

Confirmation for the voter that the correct vote has been submitted is something that is not offered in current methods of voting. The estimated number of accidentally spoilt ballots in a General Election runs into the thousands, and postal voters receive no confirmation that their vote was submitted to the ballot box.

Ensuring the correct vote is received

Some contributors suggest the use of a block chain based public bulletin board as a method of verifying the votes received are the same as the ones that were cast. This is also highlighted as a benefit of online voting that does not exist in current methods of voting as election administrators have little to no ability to verify whether votes received via post have been tampered with or manipulated.

Safeguards against malware on the voter's device

There are a number of suggestions for safeguards against malware, such as the use of live operating systems, within this report, however an important theme is that any online voting system should be built on the assumption that the voter's device contains malware in order to mitigate any risks prior to the election taking place.

Whilst the details are not contained within this report, the Government may also wish to investigate the recent work of the University of Birmingham's "Du-Vote" system which claims to allow voters to securely cast votes even if their device is infected with viruses.

Safeguards against cyber-attacks

A range of views are presented on this issue, however the key messages are for the Government/online voting provider to have strong defences against distributed denial of service attacks and for voters to be educated on cyber-safety prior to the election. This is something the Government has already been embarking on through its "Cyber Streetwise" initiative.[4]

Contingencies in case of vote-tampering

A number of ideas are suggested within this report for contingencies in case of vote-tampering. Should an individual's vote or an entire election be compromised, reverting to voting via another channel could be an option.

Contingency plans in the current system are difficult to implement for individual voters and a by-election would have to be called if an entire election was compromised. This, however, could carry the exact same issues and risks as the previous, compromised election. In this respect, online voting has a greater number of options with regards to contingency-planning than current methods of voting.

Detecting interferences with the online voting system

Various methods of detecting interferences with an online voting system are presented within this report. In Professor Krimmer's words "monitoring, monitoring, monitoring" is a key theme here.

Maintaining audit trails

The importance of maintaining audit trails and for them to be independently verified are stressed within this report. Suggestions of how audit trails can be maintained include the use of block chain based technologies as well as provider-specific technologies.

It is recommended that every process, interaction, and instruction should be audited.

Ensuring the system is sufficiently secure

A common proposal put forward in this report is to test the online voting system by attacking it. This includes bringing in independent third parties and white-hat hackers to verify the security of the system and highlight potential gaps.

As Dr Curran puts it, the security of the system "should be approached in the same manner as securing any vital resource online."

Securing voter records and personal details

Proper implementation of encryption processes, as well as the use of digital signatures and passwords are put forward as a solution to this issue by a number of the contributors.

It is noted in the chapter by Mi-Voice that "the majority of data breaches are caused due to the poor implementation of the technology – not the technology itself."

Open-sourcing and working in an alliance

There are mixed views on open-sourcing the software due to the advantages and disadvantages of doing so.

Related areas of interest

Recent developments

Other Government projects

Legislation

> Online voting? I mean I don't have any objection to it…
>
> David Cameron

Related areas of interest

Recent developments

UK General Election 2015

Voter turnout

Turnout in the 2015 UK General Election was 66.1%, representing an increase of just 0.3 percentage points on the election in 2010.[5] Turnout in 21st century UK elections therefore continue to be significantly lower (13 percentage points) than elections post-1945.

According to figures from Ipsos Mori, turnout amongst 18 to 24 year olds continues to be below 50%, as it has been since 2001.[6]

Age	Estimated turnout (%)					
	1992	1997	2001	2005	2010	2015
18 - 24	63	51	39	37	44	43
25 - 34	76	64	46	49	55	54
35 - 44	80	73	59	61	66	64
45 - 54	80	79	65	65	69	72
55 - 64	82	80	69	71	73	77
65+	83	79	70	75	76	78

In addition to this, analysis by WebRoots Democracy shows that an estimated 95% of the UK's over 19,000 politicians were elected in elections with less than 50% voter turnout.[7]

	Total	Average voter turnout	Total elected on turnout >50%	Total elected on turnout <50%
Councillors	18100	35.70%		18100
MPs	650	66.10%	650	
Directly elected Mayors	17		6	11
N Irish MLAs	108	54.50%	108	
Welsh AMs	60	41.80%		60
Scottish MSPs	129	50.57%	129	
London AMs	25	40.90%		25
PCCs	41	14.70%		41
MEPs	73	35.60%		73
Total	**19203**	**42.48%**	**893**	**18310**
Proportion elected above/below 50% voter turnout (%)			4.7	95.3

Accidentally spoilt ballots

Analysis by WebRoots Democracy following the election shows that there were an estimated 27,500 accidentally spoilt ballots.[8] Voters who accidentally spoil their ballots are never informed that their vote did not count.

As explained in the Viral Voting report,[9] accidentally spoilt ballots could be made impossible when using an online voting option.

Pre-election comments on online voting

In the run up to the election, during a live television event with young voters on Sky News, Prime Minister David Cameron responded to a question on introducing online voting twice by saying he does not have 'any objection' to it.[10] However, he added that he does not believe introducing online voting would lead to more people voting.

> "Online voting? I mean I don't have any objection to it, but I think in a way we're asking the wrong question. The reason people don't vote is not because it's too complicated to go down to the polling station; the reason that people don't vote is because they don't believe it makes enough of a difference."
>
> "Look, I don't have any great objection to it… but the reason people don't vote is not because it's too complicated to go down to the polling station."
>
> David Cameron

WebRoots Democracy/YouGov poll

More than half (56%) of the British public who are online support the inclusion of an online voting option in the upcoming referendum on the UK's membership of the EU, according to a poll by WebRoots Democracy and YouGov in July 2015.[11]

The sample size of the poll was 1,543 adults in Great Britain.

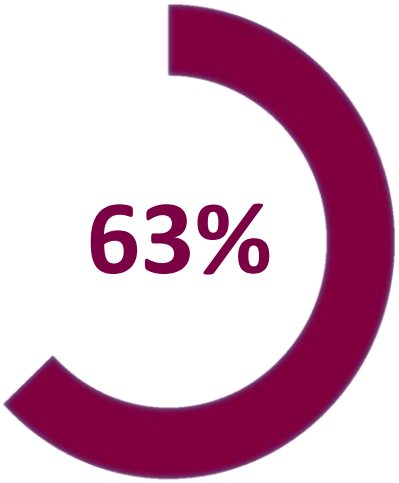
Across the country, support was strongest in London (59%) with each of the other regions (Rest of South, Midlands/Wales, North, and Scotland) also showing support of more than 50%.

Another WebRoots Democracy/YouGov poll released at the same time, found that 59% of Londoners who are online are in favour of introducing online voting for the 2016 London Mayoral Election.[12]

The sample size of this poll was 1,047 adults in London.

Tecmark/YouGov poll

A survey by Mancunian marketing agency, Tecmark and polling company YouGov, in April 2015, found that 63% of adults in the UK believe that the introduction of online voting would boost turnout in elections.[13]

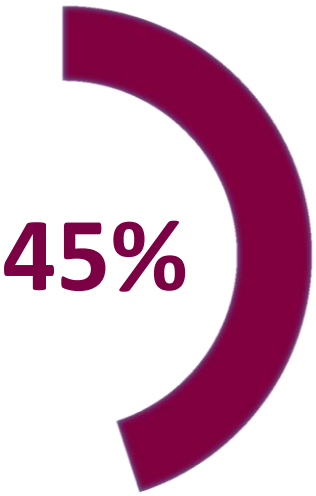


The data shows that support is strongest amongst women, those who live in London, and those aged 25 to 39.

The poll also found that trust in the security of online voting was an issue with 40% of respondents stating that it is their 'biggest concern.'

Opinium poll

Another poll in April 2015, by Opinium, found that, if introduced in the future, online voting would be the most popular method of voting in the UK.[14]



The survey of over 2,000 adults in the UK showed that 45% of respondents would choose to vote online if it was an option in future elections. This compares to 30% who said they would continue to vote at a polling station, 13% who said they would vote by post, and 2% who would vote via proxy.

2015 ONS internet usage data

The latest figures[15] released by the Office for National Statistics (ONS) have shown that in 2015, the proportion of adults in Great Britain that use the internet on a daily basis has more than doubled compared to 2006. The total number of adults that use the internet everyday or nearly everyday is 39.3 million (78%). In 2006, when directly comparable records began, the proportion was 35%.

The data also shows that almost all (96%) of those aged 16 to 24 use the internet 'on the go'.

Most strikingly, smartphones have overtaken laptops and tablets as the most common device to use the internet on the go. Two-thirds of 'on the go' internet users

accessed the internet via their mobile phone, compared with 45% using laptops, and 17% using other handheld devices.

The data shows that sending and receiving emails remains the most common use of the internet with 76% doing so, however the proportion of those reading online news, newspapers, or magazines has increased from 20% in 2007 to 62% in 2015. In addition to this, the proportion of adults using social networks has continued to increase with 61% doing so in 2015, compared to 54% in 2014 and 45% in 2011.

Online shopping has experienced strong growth, too, with 90% of 16 to 24 year olds buying goods online which is an increase on 65% in 2008. The total proportion of adults buying goods online is 76% up from 53% in 2008. 42% made purchases worth between £100 to £500, and 9% made purchases of £2,000 or more.

Online voter registration

Data published by the Government in 2015 shows that since the introduction of online voter registration, more than 7 million people have registered to vote online with 2 million registering via the traditional paper method.[16]

On deadline day for registering before the 2015 Election, a record 485,012 people registered to vote with 97% of these applications being done online.

More than half (51%) of voter registrations, since the online option was introduced, were made by those aged 16 to 34.

On the day of the BBC Election Debate on April 16th, 118,000 people registered to vote with 93% registering online. At the end of the debate, the host, David Dimbleby, read the website link out urging viewers to register.

The highest number of online voter registrations was on the final day with 469,047 registering online, whilst the highest number of paper registrations on any day since last summer was on November 5th with 27,068 paper registrations.

On Bite the Ballot's 'National Voter Registration Day', on February 5th, 166,140 people registered to vote, with 94% online.

Proposed changes to the 1976 EU Electoral Act

In November 2015, the European Parliament voted to adopt a set of reforms to the 1976 EU Electoral Act by 315 votes to 254. The reforms include the need for member states to provide an online voting method for citizens living abroad.[17]

The reforms were proposed in order to remedy some of the differences[18] between countries in the EU relating to European Parliament elections. According to the European Parliament,[19] these 'undermine the notion of European citizenship and the principle of equality.'

> "We want to adjust the Electoral Act of 1976 to the new reality. The elections to the European Parliament continue to be extremely national. We hope to increase citizens' interest in participating in this important element of European decision-making."
>
> Co-rapporteur, Danuta Hübner.

> "The young generation should be encouraged to take part in these elections. The internet generation prefers to vote online, with one click, rather than going to a town hall or a school."
>
> Co-rapporteur, Jo Leinen.

The reforms propose that all EU citizens living abroad should be able to vote in European Parliament elections and that electronic, online and postal methods should be made available in all EU member states, which includes the UK.

The proposed reforms to the 1976 EU Electoral Act will now go to the European Council and must be unanimously endorsed before being approved by all member states.

The Queen's Speech

The Queen's speech[20], following the General Election, hinted at the possibility of introducing an online voting option to make elections more accessible for overseas voters.

The Queen's Speech takes place during the State Opening of Parliament which marks the formal start of the parliamentary year. The Queen's Speech sets out the Government's agenda for the coming session, outlining proposed policies and legislation.

One of the bills, entitled the "Votes for Life" bill, outlined proposals to scrap the current 15-year time limit on UK citizens living abroad voting in Westminster and European elections. It also stated that it will provide for secure and accessible registration of overseas electors.

On electoral administration, the Queen's Speech stated that the bill contains 'provisions to make it easier for overseas electors to vote in time to be counted.'

The bill also referenced a report[21] by the Hansard Society from March 2014 entitled "Our forgotten voters: British citizens abroad" which states as one of its recommendations that 'a feasibility study of electronic voting should be carried out' with the trial being undertaken 'in parts of the world with a high concentration of British expatriates.'

There are an estimated 4.6 million UK citizens currently living abroad.

2015 Labour leadership election

In September 2015, the new Labour leader, Jeremy Corbyn, was elected in the largest online voting election in UK history after 422,871 voters took part in the process.

Figures released by Electoral Reform Services[22], who coordinated the election, showed that 81% of these votes were cast online making it the largest online voting election in UK history. The total number of votes cast online was 343,995.

Conservative London Mayoral candidate selection

In October 2015, Zac Goldsmith, MP for Richmond Park and North Kingston, was elected as the Conservative Party's candidate for London Mayor in 2016 in an online ballot. Goldsmith beat his rivals winning 70% of the 9,227 votes cast. Votes were cast 'predominantly online' with voters also able to take part via post.[23]

Goldsmith's online election means that all main political parties in the UK have adopted online voting for their own party elections. As mentioned, the Labour Party elected their new leader using online voting. In London, the Liberal Democrat candidate Caroline Pidgeon, and the Green Party's candidate Sian Berry were both elected in online ballots. In 2014, the Scottish National Party used online voting to elect their new Deputy Leader, Stewart Hosie.

Barack Obama comments

In August 2015, United States President, Barack Obama, revealed in an interview[24] with tech business magazine 'Fast Company' that he believes online voting should 'absolutely' be a priority.

In the context of using technology to enable better services for the public, Obama said that he wants technology to 'help shape policy' in order to solve some of the challenges facing the country. Ultimately, he stated, Governments should be thinking about how technology can 'enhance the experience of democracy.'

> "I look at my daughters, who are, as every teenage kid is today, completely fluent in technology and social media. They might not go to a town hall meeting physically, the way their grandmother might have around some issue,

> and sit through a two-hour debate. Because they're just used to things moving faster. But we can imagine creating a corollary process for them that is consistent with how they interact generally. We can think of apps that promote engagement and the power of people."
>
> US President, Barack Obama.

He said that he foresees the private sector having a role to play in developing the technology for online voting and believes that online voting is 'something that all of us in every level of public life should be thinking about' and that the goal should be to 'make "we the people" mean something in a 21st century context.'

In his final State of the Union Address[25] in January 2016, Obama re-emphasised the need for modernising democracy saying that we need to "make voting easier, not harder, and modernise it for the way we live now."

John Penrose comments

In an interview[26] with the Local Government Chronicle in October 2015, Constitutional Reform Minister, John Penrose MP, described online voting as an 'intriguing' and 'interesting' idea that the Government is 'keeping a close eye on.'

Acknowledging the potential security risks, Mr Penrose said that the Government wants to see evidence that it would be 'robust' and difficult to hack. He added that online voting would be 'incredibly convenient' for voters.

> "It's intriguing, it's interesting and we're keeping a really close eye on the way the technology develops but we would also want to see really solid evidence in the future of it being robust and really hard to hack."
>
> Minister for Constitutional Reform, John Penrose.

SNP calls for electronic voting in Parliament

In December 2015, the Scottish National Party made fresh calls for MPs to be able to vote electronically in Parliament.[27]

Currently the 650 MPs in the House of Commons spend 15 to 20 minutes queuing up in voting lobbies in the Palace of Westminster.

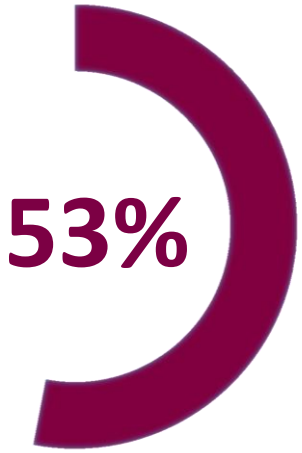
SNP MP, Hannah Bardell, said that the "time wasted" currently would be "much better spent representing our constituents and tackling the issues that impact on their lives."

> "The House of Common's reluctance to modernise its outmoded procedures is part of the reason that parliament is far from family friendly and continues to be considered alien and remote by the public.

> As we move towards the start of 2016, it's well and truly time to create a modern parliament that is fit for a modern democracy."
>
> Hannah Bardell MP.

Trade union strike ballots

Trade unions have used combined online balloting in non-statutory ballots for a number of years, and the Trades Union Congress first called in 2003[28] for this to be extended to those ballots governed by statutory provisions, such as strike votes. Union statutory ballots are governed by the 1992 Trade Union and Labour (Consolidation) Act, which mandates postal-only ballots, and which would need to be revised for online ballots to go ahead.



In March 2015, the previous Business Secretary, the Liberal Democrat, Vince Cable said he supported calls for trade unions to be able to vote online and described it as a 'sensible reform.'

A YouGov poll commissioned by the Trades Union Congress in January 2016, found that the majority (53%) of the British public back online strike ballots.[29]

The proposals to allow online voting for trade union strike ballots were rejected in the House of Commons, however, during the debate, Minister for Skills, Nick Boles, made some positive comments in relation to online voting.[30]

> "From the very first time that was raised, the Secretary of State, the Prime Minister and I have made it clear that we have no objection in principle to online voting or e-balloting, as it is sometimes called. Indeed, I would go further: it would be extraordinary if, in 20 years' time, most elections in most countries in the world on most questions of importance were not decided through electronic means of communication…
>
> …It is a matter of time and human ingenuity. I have no doubt that we will get there, and we are happy to work with all members of the Opposition, and all groups outside Parliament, to ensure that eventually we do get there."
>
> Minister of State, Nick Bowes MP.

University of Birmingham 'Du-Vote' system

In May 2015, computer scientists at the University of Birmingham claimed to have made a 'breakthrough' in secure online voting technology, developing a technique to allow people to cast their election votes online even if their computers are suspected

of having viruses.[31] Led by Professor Mark Ryan, the researchers took inspiration from banks and created a system which allows people to vote by employing independent hardware devices in conjunction with their PCs.

The researchers claim the system could be ready for use in the 2020 or 2025 General Election.

> "This system works by employing a credit card-sized device similar to those used in online banking. It is called Du-Vote, and we have been developing it over the past two years. From the voter's perspective, it's straightforward: you receive a code on the device and type it back into the computer.
>
> The main advantage of this system is that it splits the security between the independent security device and a voter's computer or mobile device. A computer is a hugely powerful, all-purpose machine running billions of lines of code that no one really understands, whereas the independent security device has a much, much smaller code base and is not susceptible to viruses."
>
> Professor Mark Ryan, University of Birmingham.

Other Government projects

Register to Vote (online voter registration)

In June 2011, the Government put forward proposals to introduce individual electoral registration which included the introduction of online voter registration.

Writing in the foreword[32] of the proposal document, then Deputy Prime Minister, Nick Clegg, and then Minister for Political and Constitutional Reform, Mark Harper, wrote:

> "This legislation provides us with an opportunity to look at how we can modernise our system of electoral registration to make it easier, more convenient and more efficient for people to use and administrators to run. The current system has not kept pace with technological advances and is largely paper based."
>
> Nick Clegg MP and Mark Harper MP

The online voter registration tool was launched in June 2014, meaning the project length was an estimated **3 years**.

Announcing the launch[33], then Minister of State at the Cabinet Office, Greg Clark said:

> "This service will bring voter registration into the 21st century and make it easier, simpler and faster for people to register to vote. Putting public

> services online is saving taxpayers money and giving people access to services when and where they need them."
>
> Greg Clark MP

GOV.UK Verify (online identity assurance)

In October 2011, the Government committed an extra £10 million[34] in funding to the Identity Assurance programme, signing the first delivery contracts in September 2013.[35]

GOV.UK Verify went into public beta in October 2014, and the due date for going live is April 2016, making the length of the project an estimated **5 years**.

In a speech[36] in February 2015 about GOV.UK Verify, former Cabinet Office Minister, Francis Maude said:

> "Digital services are 20 times cheaper than over the phone, 30 times cheaper than by post, and 50 times cheaper than face-to-face. But it's also an opportunity to create better services: more responsive to people's needs and more convenient to use. If you can shop online at midnight and bank from your smartphone, then you should be able to renew your passport or view your driving record just as easily.
>
> So we want Government to be digital by default. Our aim is to design services which are so straightforward that all those who can use them will choose to do so, and those who can't are given the support they need."
>
> Lord Francis Maude

Online tax disc renewal

In the Autumn Statement in December 2013, the Government announced[37] plans to replace the tax disc which shows that motorists have paid vehicle excise duty with an online system.

Announcing the plans the Treasury said it showed that the Government was moving "into the modern age" and that it would make "dealing with Government more hassle free."

This service went live in October 2014, meaning the estimated length of the project was just **10 months**.[38] According to the Driver and Vehicle Standards Agency, the estimated saving of moving online will provide annual savings of around £10 million to the taxpayer in addition to removing "an administrative inconvenience for millions of motorists."

Savings for the taxpayer

The Government published figures[39] in 2015 showing that savings from digital and technology transformation have totalled £3.56 billion from 2012 to 2015. Writing in a blog for the Government Digital Service, the Chief Operating Officer, Stephen Foreshaw-Cain said:

> "These savings were only made possible because digital transformation made them so. Digital has helped us rethink the way we do things, but we're only at the start of that journey…
>
> …Over 98% of driving tests are now booked online, 85% of self-assessment filing is done through online channels, and 12 million people have registered to vote using a new digital service."
>
> Stephen Foreshaw-Cain, Government Digital Service

Legislation

In order to introduce an online voting option in elections, a number of legislative changes will need to be made which include amendments to the Representation of the People's Act. This should be done in a similar manner to the amendments made to allow postal voting on demand in the Representation of the People Act 2000 and treated as 'absentee' ballots.[40]

Amendments may also need to be made to this section to allow for suggested measures such as repeat voting.

In order to make an amendment to an existing law, a Bill would need to be introduced in either the House of Commons or the House of Lords for examination, discussion, or amendment. The Bill will then need to receive Royal Assent before becoming an Act of Parliament, and law.[41]

The proposed amendments to allow postal voting on demand were presented in the Representation of the People Bill[42] on the 18th of November 1999 and received Royal Assent on the 9th of March 2000, meaning the process in Parliament took less than **4 months**.

The Act applies to both Parliamentary and Local Government elections, however, specific amendments may be required for elections such as European Parliament elections.

Electoral Reform Services

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Ensuring the correct vote is received

Safeguards against malware on the voter's device

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> "It is possible to provide voters with the opportunity to independently check if their vote has been received and how it has been recorded."

Electoral Reform Services

About

Electoral Reform Services (ERS), based in London, was born out of the campaigning organisation, Electoral Reform Society, in the 1980s.

Last year, over 400 organisations throughout the UK conducted electronic ballots with ERS – whether online, by telephone, or by text.

They are experienced in running elections and providing online voting services for professional bodies, companies, and political parties including the Conservatives, Labour, and the Liberal Democrats.

They notably coordinated the 2015 Labour leadership election which was the largest online voting election in UK history with almost 350,000 votes cast online.

Voter verification

Different methods of authentication can be used to enable voters to cast their electronic votes, e.g. single-use "security codes" or personal ID information such as dates of birth or national insurance numbers. In countries where electronic ID cards are already being used to facilitate access to health services or banking (e.g. Estonia), these can also be used to digitally sign the vote. An electronic voting system must be able to identify that the information being provided to authenticate the voter is the information required to enable a vote to be cast and recorded in that particular ballot and it must be unique to the voter.

The vast majority of organisations working with ERS will issue (by post or email) their voters with randomly generated single-use security codes to enable them to access the electronic voting systems. This is similar to a postal ballot, where a ballot paper number is used to make the ballot paper unique. Other organisations have required voters to provide personal identifiers such as dates of birth, and postcodes (online or by text) or a membership number and a date of birth.

Safeguards from peer-pressure

We discussed above how electronic voting information and security codes can be distributed to the voter by various means and that there are risks associated with any transfer of information that requires a third party carrier. Once delivered, the vote cast must be secret. There is good practice advice for voters on how to cast their vote in secret - often basic advice such as considering their physical location when they cast their vote and the proximity of others to them.

The risks of vote coercion and vote selling (for example a company could bribe or threaten its employees to vote in a certain way, or a landlord threaten their tenants) also need to be addressed. This risk arises with any form of remote voting including

postal ballots or online, telephone and SMS voting. Legislation, with appropriate penalties such as fines or prison sentences, will provide some safeguard against this risk. Another possibility is to allow voters to vote multiple times, with only the last vote being counted. A vote-buyer is unlikely to pay you for your online or postal vote if they know you could later change it online or at a polling station. There are also various techniques which allow a voter to obtain a receipt for their vote, which proves to the voter that their vote has been cast in a certain way, but which would not be accepted as proof by a vote-buyer. This is an active field of research by cryptographers.

Ensuring the correct vote is submitted

It is possible to provide voters with the opportunity to independently check if their vote has been received and how it has been recorded. This is known as a voter-verified audit trail (VVAT). This can be setup in various ways for example by allowing voters to log in and check their receipt on a website "bulletin board", or phone a telephone service to confirm the vote or even get a separate postal receipt sent to a personal postal address. For contentious and high profile ballots the use of VVAT may be an added security measure that enhances the integrity of the ballot. As mentioned above, cryptographic methods may be used to ensure the voter's receipt does not facilitate coercion or vote-selling.

Ensuring the correct vote is received

Again there is a risk with any form of remote voting that the vote might be tampered with after submission but before receipt by the organisation counting the votes. Imagine a postal worker steaming open your postal ballot and altering your vote before putting it back in the post. With online voting this risk is largely addressed by configuring servers to require secure (https) connections, this forces traffic between the browser and server to be encrypted so it cannot be altered during transmission. The use of Extended Validation (EV) SSL/TLS certificates gives the voter greater reassurance that they are submitting their vote to the correct website (an EV certificate is only issued to a website owner after vetting by the certifying authority).

Safeguards against malware on the voter's device

With personal devices there is always a possibility that malicious software is present. If designed specifically in relation to a ballot it could disrupt, change or read and communicate to a third party the voter's vote. Whilst anti-virus software exists, it must be kept up to date and can only protect against known issues. It is important here to ensure voters are aware of the risk of using electronic devices and maintaining personal data security. For example, keeping authentication codes secret, not clicking suspicious links or opening attachments in unexpected emails, and appropriately deleting and destroying voting information.

Safeguards against cyber-attacks

The system should be built and configured according to recognised industry guidelines, such as the server-hardening standards published by the Centre for Internet Security (CIS). The system should also be regularly scanned for vulnerabilities by independent third party such as an ASV (Approved Scanning Vendor i.e. an organisation with internet security expertise which has been approved to conduct testing for compliance with the PCI DSS standards for credit card processing).

Infrastructure supporting the systems should be robust and mitigate against downtime or interruption of service, for example through the use of redundant architecture and system replication. Online voting providers must be able to demonstrate that they have rigorous quality assurance procedures and processes. Evidence such as certification in quality management and information security, e.g. ISO9001 and ISO27001 would be expected.

Contingencies in case of vote-tampering

Suspicious activity needs to be investigated as described below, and if there is evidence of malpractice voters would be invited to cast their vote again. If a multi-channel voting system is used (e.g. if voters can choose to vote online, by post or in person) it also offers the opportunity to compare voting patterns between channels. Depending on the risk assessment for each channel, a threshold or limit could be placed on votes allowed via that channel e.g. elections could include online voting provided no more than 30% of votes are cast online (similar thresholds are currently being used in Switzerland, with the intention of gradually increasing the threshold as and when security requirements are met).

Detecting interferences with the online voting system

ERS has been running postal ballots for over 100 years, and online votes for over 15 years. We currently administer around 2,000 election projects each year, each project may have multiple contests and constituencies, which requires many thousands of individual ballots. As such we have acquired a great deal of experience of monitoring the pattern, timing and frequency of votes being cast, internet protocol (IP) addresses etc., so that suspicious activity can be investigated for evidence of malpractice.

Maintaining audit trails

It should be possible to audit that any submitted vote is correctly included in the count and has not been altered whether by malware on the voter's computer, hackers intercepting traffic between the voter and the webserver, or even corrupt employees at the online voting vendor with access to the stored votes. Ideally the audit should be carried out by the voters themselves although this will be an unfamiliar process as the audit and assurance is currently carried out by other

means. For example a trusted independent body running the election, or political party agents being allowed to witness the sorting and counting of ballot papers on election night. The value of any audit depends on a sufficiently large sample of cases being audited, so voters will need to become familiar with these new processes in order to carry out the audits in sufficient numbers to provide the necessary reassurance in the integrity of the vote.

Ensuring the system is sufficiently secure

Load-testing is an essential phase in the development of online voting sites which need to be able to cope with very high peaks of traffic particularly at the beginning of the voting period immediately after polls open and again just before polls close. ERS has experience in administering online voting projects for some of the largest organisations in the UK, including trade unions, political parties, and building societies and other financial institutions, so we have acquired detailed knowledge of patterns of turnout over the voting period. It might be acceptable for commercial websites, such as those selling event tickets, to hold customers in a queue when the servers get too busy, but this would not be ideal for online voting as voters might just give up and reduce turnout.

Security testing is also critical for the success of an online voting site. ERS' in-house development team will conduct application security tests as part of the development process, but we will also commission an independent third party specialising in web application security to test major releases of our software. Internet security can seem like an "arms race" between developers and hackers, every time a developer fixes a bug or vulnerability, some hacker will discover a new one. It is therefore essential to ensure that experts with the most up to date knowledge of internet security have tested the system.

Securing voter records and personal details

It is good practice to separate, physically and electronically, the system and database used for the distribution of the voter information from the database used to store the votes cast on the electronic voting system. The only commonality between these two systems being the authentication codes used by the voters. This ensures that the voter's identity is separated from their voting preference but, as currently with UK public elections and other postal ballots, this allows, in the event of queries or challenges, for the online voting provider to investigate and if need be invalidate the votes from a particular voter.

It is also possible for the data related to the ballot to be encrypted when stored to further enhance the security and secrecy of the vote, however this is not as straightforward as it sounds. If the data has to be searched or any calculations performed (such as vote-counting), then any encryption can impact performance and make the system unusable. Techniques such as homomorphic encryption (allowing

votes to be counted without decryption) have been developed and may be used on certain types of ballot, but this is another active field of research by cryptographers.

Open-sourcing and working in an alliance

ERS is happy to work in alliance with others and has done so for several public voting and vote-counting projects in the past, including previous pilots of online voting in the UK. Our own software is currently not open source and this is an open question. On the one hand if the code is open source then it gives any would-be hacker full knowledge of how the software works, which might allow them to construct malware specific to that voting system. On the other hand making the code open source means it can be reviewed by a wide audience and give voters greater re-assurance that the software is fit for purpose.

Everyone Counts

Data centre security

Hardware and software security

Enhancing security with an on-demand delivery model

Mitigating tampering and human error

Ballot submission and transport

Audit trails

> “Security is about layer upon layer of protection. Each layer cumulatively increases the safety of the election project.”

Everyone Counts

About

Everyone Counts is an electronic voting provider based in California, USA. They have experience in running electronic and online voting across the USA, in Australia, and during previous pilots of online voting in the UK.

Introduction

More than simple ballot delivery, an election is formulated of many components, one of the most critical being security. An election solution - the infrastructure (hardware, networks, and software) and the actual data (elector information, ballots cast, and results) - must be protected from both intentional and unintentional interference. Security is about layer upon layer of protection. Each layer cumulatively increases the safety of the election project. Everyone Counts accomplishes this is by using military-grade security and Tier 1-accredited data centres; deploying software that has built-in redundancies and requires multiple levels of access; a delivery model that is perpetually state of the art; and a verifiable audit trail.

Data centre security

Security begins with protecting the physical components of the voting system. All hardware systems associated with an election must be stored within a secure facility. This ensures that the systems contained within the data centre are protected from both intentional and unintentional physical risks and environmental incidents. A secure election platform is one that is deployed in an enterprise-class data centre that maintains geo-failover sites.

Hardware and software security

Securing and maintaining the hardware and software on which the election is run and data is stored is paramount in establishing confidence in the results of an election. Redundancies to ensure accessibility; software designed to prevent and, when necessary, detect intrusion; and controlled access to all election hardware and software are each aimed toward ensuring the security of the election content and stored data.

Enhancing security with an on-demand delivery model

A Software as a Service (SaaS) based system is, by definition, continually updated as market requirements, security, and accessibility standards improve, ensuring that the system is perpetually state of the art. When software is run on antiquated technology, security risks are higher and product lifecycle management staffing costs are higher. Most businesses and many government organisations now choose SaaS delivery methods for mission-critical solutions. SaaS is the only viable method proven to continually increase security, reliability, and efficiency, while reducing cost.

Mitigating tampering and human error

Elections are one of the few mission-critical business processes in the world that have not embraced technology, using instead insecure, error-prone paper processes and antiquated, expensive voting machines.

Ballot submission and transport

Simply stated, it is easier to tamper with a vote that has been cast using a single piece of paper than it is to tamper with an online vote that can be verified via multiple audit trails. A single record is a single point of failure. Paper ballots without backup can be torn up, hidden, or re-cast after being stolen from a ballot box. Ballot boxes containing paper ballots, require a chain of custody while being transported, thus making these ballots further susceptible to tampering, damage, or loss. When a ballot is cast using electronic voting, the ballot data is then validated, encrypted, and stored. At the close of the election, quorum members unlock the election jointly to initiate the decryption process, which strips all ballots of identifying information, shuffles them, and finally decrypts the ballots for tabulation.

Audit trails

Well-designed and properly performed post-election audits significantly mitigate the threat of error, and should be considered integral to securing online voting. Hand-marked paper ballots are difficult and costly to count, particularly as ballots become more complicated with multiple offices and propositions in a single election. Additionally, without multiple audit trails that serve as a system of checks and balances, a single, hand-marked paper ballot system makes vote tampering and inaccurate counting increasingly probable. Everyone Counts' eLect Quad Audit online voting system offers up to four independently stored ballots of record and audit trails generated for each cast ballot: encrypted electronic submission, screen image capture, physical paper ballot, and a 2D barcode of vote data available on both the printed paper ballot and screen image capture. Any one of these records can be tallied independently to verify accurate results and provide an efficient, transparent, and risk-limiting audit of election results.

Conclusion

The future of voting requires a secure, scalable, cost-effective solution that enables online voting on laptops, tablets, and mobile devices, and ensures a robust election administration system that authenticates and validates votes while enfranchising voters. A state of the art Software as a Service (SaaS) voting system system that embraces technology advances provides governments and their citizens with a more reliable, secure, and accurate democratic process. Although trustworthy elections are essential to democracy, achieving them requires vision, conviction and, in some cases, courage in order to defeat the "we've always done it this way" mentality. The time is now to choose secure online voting solutions over paper and single purpose

hardware-based solutions or else run the risk of undermining the Citizens' confidence that reported election results accurately reflect the collective will of the voters.

Follow My Vote

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Ensuring the correct vote is received

Safeguards against malware on the voter's device

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> "Due to the decentralised design and the blockchain-based record, it should be impossible to tamper with votes on a large-scale basis."

Follow My Vote

About

Follow My Vote is a public benefit corporation based in Blacksburg, Virginia, USA and was founded in 2012. They are developing an online, open-source voting platform using technologies such as blockchain technology and elliptic curve cryptography.

Voter verification

This question breaks down into two parts: first, how can we verify that a given person is allowed to vote (i.e. they have a right to vote, and they have not voted already); second, how can we determine that a given vote was cast by one of those verified persons, and that it is the only vote on a given issue cast by that person.

The first part does not change substantially in a transition to an online voting system. Voters must register to vote, and receive a certification authorising them to vote when the polls open. In Follow My Vote's online system, this certification takes the form of an identity on a blockchain which has been cryptographically signed by the identity verifiers for the election as being unique and authorised to vote.

The second part is a more difficult problem which, in contemporary paper ballot systems, is largely unaddressed. It is simply assumed that if a ballot is in the box, it is valid and should be counted. There is no possible verification of this assertion later on in the process. In electronic voting systems, the problem is worse as typically audit trails are not preserved, and these systems are frequently designed with no eye towards security, allowing them to be manipulated to alter the votes.

Follow My Vote's voting system will preserve a complete audit trail which provides cryptographic proof that each counted vote was cast by one of the authorised identities, and it was the only one cast by that particular identity, without enabling any party (including election officials) to determine which certified identity cast that vote.

Safeguards from peer-pressure

One of the major benefits of an online voting system is the flexibility it offers to voters in terms of where and when they vote. Voters can vote in a time and place where they feel best enabled to make an honest and informed voting decision. If a voter still feels pressured in any way, our system provides a mechanism by which voters can revoke their online vote and instead vote on a paper ballot at a polling place, without opening up the possibility for a vote to be counted multiple times.

Ensuring the correct vote is submitted

In the Follow My Vote system, all votes are public data available on the blockchain. Because of this, a voter can look up their vote in the public record and verify that it was cast correctly. The voter can do this verification on a public computer to verify that his personal computer is not out of sync with the network, or being fed invalid information about the public record by an attacker. Furthermore, the open source Follow My Vote application will be able to count the votes on the public record, and show the voter the results directly, rather than trusting election officials to tally the votes in secret, so the voter can be completely assured that his vote was cast as intended and counted as cast.

Ensuring the correct vote is received

Due to the inherent trust, fault tolerance, and censorship issues involved in a centralised voting solution, our system leverages a decentralised design. Thanks to this property, our system does not require any online voting provider to verify the votes. This is done by individual voters as they tally the votes as described earlier. This verification is done using the cryptographic audit trail made publicly available on the blockchain. This audit trail proves that the votes were not tampered with after they were cast.

Safeguards against malware on the voter's device

In any electronic voting system, if the operating system the voter uses when casting his votes is compromised with malware, it is possible that an attacker could steal the voter's cryptographic identity, change the votes prior to publication, and determine the real-world identity of the voter. No safeguards do or can exist with modern technology once the malware infection has taken place; therefore, the only defence against this is to prevent a malware infection, or to neutralize the infection for the duration that the voter's private information is held on the device used to vote.

Clearly, the threat of malware is a serious one, and Follow My Vote has hired a malware analyst to help them to harden their software against this threat to the greatest possible extent. The threat of attack is greatest on web-based platforms, and for this reason, Follow My Vote will not provide a web-based voting application unless they can ensure that such an application meets the security standards of their other voting applications. The threat of attack is least on mobile devices, where, due to the security models used by modern mobile operating systems, it is rare to find a malware infection capable of interfering with other applications on the device (most malware on mobile devices can do nothing without first asking the owner's permission and can be trivially removed simply by uninstalling the application containing it). The greatest risk of compromise from malware will be on desktop and laptop computers, where the operating systems do not have as strong of a security model, and malware can be difficult to find and remove. Because of this, Follow My Vote will recommend users only vote from these computers using a live operating

system (a temporary computer operating system which runs in RAM and is used only for voting), which will neutralize the threat of malware on the computer while the Follow My Vote application is running and storing data on the computer. Follow My Vote will provide tutorials and/or software to help voters accomplish this. Voting from a computer running a live operating system is the most secure way to vote, and will protect users from virtually all possible malware.

Safeguards against cyber-attacks

As discussed earlier, there is no centralised system to attack. A custom cyber-attack would have to be levied against each individual voter, which would be prohibitively expensive and time-consuming. Furthermore, attacking voters who are using the live operating system would be nearly impossible.

Contingencies in case of vote-tampering

Due to the decentralised design of the Follow My Vote system and the blockchain-based record, it should be impossible to tamper with votes on a large-scale basis. If such an attack could be found, the same attack could compromise the entire Bitcoin network (an online payment processing network). Since there is already such a great incentive to find such an attack, yet Bitcoin remains secure against large-scale attacks, it is highly unlikely that such an attack will be found.

The difficulty of attacking an individual voter depends on how careful they are to avoid attack, but as described earlier, the Follow My Vote software will be designed to make it easier for voters to protect their security than to compromise it. Nevertheless, if such an attack is successfully levied against a voter, that voter will immediately be able to see on the public record that his vote has been tampered with, and will be able to report the fraud to the election officials. From there, the exact details of how fraud is dealt with will need to be determined on an election by election basis.

Detecting interferences with the online voting system

Because all of the online communications used by the Follow My Vote system will be encrypted and cryptographically signed, any interference with the online communication will be automatically detected and rejected.

Maintaining audit trails

The Follow My Vote online voting system will provide a complete audit trail for the entire election, from identity verification through to the final tally, on the public blockchain record. The open source application will validate this entire audit trail when tallying the results to ensure that no tampering occurred. Since the application is open source, the public can examine its code and verify that it is auditing the election correctly.

Ensuring the system is sufficiently secure

There is only one way to determine if a particular online system is secure, and that is to try to attack it. If no successful attack can be found, it is considered secure. Even formal proofs of correctness can only verify that the software is doing what it was intended to; they cannot verify that the software is invulnerable to an attack its designers failed to foresee.

Because the Follow My Vote system is based on proven blockchain technology, which has been open to attack for several years, it is unlikely that such an attack will be found.

Securing voter records and personal details

The Follow My Vote system will not need to store any voter's personal details, nor does it mandate what details may need to be collected and/or stored. The identity verification agencies chosen for a particular election will likely need to collect some personal details in order to certify within the Follow My Vote system that the voter's on-chain identity is unique and authorised to vote, but it is their responsibility to ensure the confidentiality of any data they require in order to grant this certification.

Open-sourcing and working in an alliance

Follow My Vote's code is open source on GitHub. The entire voting system will be open source, including the voting, tallying, and auditing software. They welcome contributions from all who wish to further the goal of building a secure, open source, end-to-end verifiable online voting system and seeing this system implemented in elections around the world. Anyone wishing to help out with development should visit followmyvote.com/code-contributors.

Dr Kevin Curran

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Ensuring the correct vote is received

Safeguards against malware on the voter's device

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> "Securing an online voting system should be approached in the same manner as securing any vital resource online."

Dr Kevin Curran

About

Dr Kevin Curran BSc (Hons), PhD, SMIEEE, FBCS, CITP, SMACM, FHEA is a Reader in Computer Science at the University of Ulster, Northern Ireland, and group leader for the Ambient Intelligence Research Group.

Dr Curran has made significant contributions to advancing the knowledge and understanding of computer networking systems, evidenced by over 800 published works.

He is a fellow of the British Computer Society (FBCS), a senior member of the Association for Computer Machinery (SMACM), a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE), and a fellow of the higher education academy (FHEA).

He is an IEEE (Institute of Electrical and Electronics Engineers) Technical Expert for Internet/Security matters since 2008 and is a member of the EPSRC (Engineering and Physical Sciences Research Council) Peer Review College.

Voter verification

This is a core question for the success of electronic voting. What if, for instance, an electronic vote is infected with a virus so that when a voter 'opens' it to vote, it then proceeds to vote for its candidate of choice and even disguises the fact to the voter who is none-the-wiser after the e-vote? It is really the nightmare scenario for e-voting as any election system must separate a voter's choice from the identity of the voter to protect ballot secrecy. It follows therefore that the voter would receive verification only that the ballot had been received and not what the actual choice was. The content voter thinks the correct choice has been recorded when in actual fact someone has ‘stolen’ their vote. There is no trivial way of detecting such a ‘theft.’ In this manner, elections could be manipulated wholesale if the virus author was successful in infecting sufficient numbers of computers. Similarly, if the voting is cast through websites, those sites could be spoofed to reveal personal identification numbers and passwords of voters, and then the vote could be automatically recast with those values to a different candidate.

So the core solution is to correctly register people to vote. Since all individuals in most tax-paying countries already have unique ‘keys’ (e.g. National Insurance numbers in the UK), these could be used as an entry to login during an election. As soon as a person comes of voting age, their unique key could automatically be activated to allow them to vote. This would eliminate the process of registration altogether. If every citizen of legal voting age is automatically registered, the first pro-active thing the citizen would need to do is obtain a password so that others could not simply run a brute-force programme to enter every possible unique key

and vote on others' behalf. This password could be sent on the legal-voting-age birthday of the citizen. Once logged-in, the voter would simply vote and the voter's effort would then be finished until the next election. There would be no need to keep tabs on voters' addresses and have voters re-register every time they change their address.

I am not advocating this as a method to follow but rather more as a simplistic overview of the issues involved. A feasible solution might be to build a system based on the blockchain technology which is currently being used for the virtual cryptocurrency Bitcoin. Building a secure electronic voting system is difficult. The US Pentagon dropped their proposed online voting system which would have given overseas military personnel the opportunity to vote in the elections in 2005, citing the inability to ensure the legitimacy of votes as the reason.

Safeguards from peer-pressure

This is a non-technical issue. There is nothing inherently different about computerised voting or traditional voting that would encourage pressure on voting that does not exist at present. Canvassing by all parties is a form of pressurisation and that is expected to continue albeit in a more electronic format as opposed to the knock on the door.

Ensuring the correct vote is submitted

The solution to ensure a voter can verify that they submitted a particular vote is to receive some confirmation of their choice. Whether this happens through email or logging onto a secure online enclave will be up to the implementers of that particular e-voting system.

It is crucial that the voter would receive verification and that this verification is not tampered with. Here we have to worry about what is known as 'man in the middle' attacks. In a man in the middle attack, a voter might believe that they are communicating with a particular e-voting system and receiving a correct verification of their vote cast for candidate X but in reality, an imposter has stolen their vote and cast it for candidate Y but also informs the voter of their original choice.

In effect, the content voter thinks the correct choice has been recorded when in actual fact someone has 'stolen' their vote. This is not a trivial attack and due to the two stage process of voting and verification, does not directly translate to a traditional man in the middle attack but nonetheless, it serves to highlight the fact that an imposter could insert themselves into the verification step as well in order to mask their original fraudulent voting on behalf of another person. When it comes to important processes such as national voting, we cannot underestimate the skills of an adversary in this regard.

Ensuring the correct vote is received

This is one of the easier aspects of managing and providing a secure online voting system. Using well established secure database transaction features and encryption alongside replicated databases, an online voting provider should be able to verify votes received are the one cast at any instant.

Safeguards against malware on the voter's device

There is always the risk that a voter's device can become infected with malware. The safeguards for this are the same as best practice for any computing system.

If a machine becomes infected with malware, then proper step is to wipe the machine and reinstall the operating system. This may sound dramatic but true geeks will spend time setting a machine up safely, reconfiguring it, installing all core applications and then making a snapshot (image) of the machine so that if an infection does occur, then is less work to bring the machine back online. The levels of sophistication being seen in current malware really make this necessary.

The steps to take once an infection has been detected are:

1. Assume the worst about compromised information on your credit cards, bank accounts and PayPal. Therefore use another computer to check the state of these accounts and change the passwords to be safe.

2. Backup all core data. Of course, a cloud service like Dropbox makes this much easier nowadays.

3. Re-install the operating system using original disks or the recovery disk.

4. Make sure to do a complete re-format of the disk when installing the operating system.

5. Re-install all applications. A site such as ninite.com is invaluable in an instance like this. Ninite allows you to select from all the popular freeware applications and it creates an installer so that you only have to run one instance of the software to install multiple applications.

6. Install a firewall and anti-virus tools. Microsoft Security Essentials is useful.

7. Next, make sure the system is fully patched. Make sure you install Windows Updates, Java Updates, Adobe Updates, Apple Updates, etc.

8. Run a complete anti-virus scan to clean the backup from step 2.

9. Restore the backup.

Safeguards against cyber-attacks

The giants of technology in recent times have all suffered disruption from cyber-attacks. The number one cyber-attack threat is a Distributed Denial of Service (DDOS) attack. If most network administrators are honest, they know they can do little to protect themselves against a targeted attack. Most System Admins know that they are only still in their job because no one specifically targeted their poorly patched company servers. In the main, DDOS attacks are hard to stop as free simple to use tools such as Low Orbit Ion Cannon (LOIC) and High Orbit Ion Cannon (HOIC) make it easy to flood sites with overwhelming amounts of dummy traffic created by custom scripts. You simply enter the URL of a website, and watch these free programs generate fake packets so as to overload a site's servers. You can watch the average site being brought to its knees in minutes. Of course a tool like these run from 1 or 1 PCs would not be enough to bring down an Internet giant however other distributed DDOS tools which are built on collections of compromised machines (DDOS botnets) can perform much larger synchronised DDOS flood attacks.

Public voting systems therefore will need to ensure they have robust DDOS flood defences. Some approaches that worked just a few years ago are now basically useless. For instance, in recent years, a common way to defend against these attacks was to try in real-time to identify spikes in traffic and then use a technique called 'blackholing'. This was in conjunction with a sites internet provider so that the incoming fake traffic is rerouted to the 'blackhole' however newer DDOS attacks change their profile much quicker so it becomes more and more difficult to simply identify which packet requests are nefarious. Voting providers should try to deal with DDOS traffic on the edge of their network immediately. They should be able to utilise a cloud solution so in the event of these large-scale flooding attacks, they have enough bandwidth to absorb them. Bandwidth allows space to breathe, cope and react.

A good place to start is to deploy DDOS prevention systems such as Google Project Shield or services like Cloudflare provide. Google shield for instance is a suite of tools for activists and non-profits, including tools for evading web censorship and oppressive regimes. The biggest focus has been on DDOS attacks, a kind of brute-force action that can easily take down a small site without leaving any clues as to the culprits. DDOS has been a persistent problem for small-scale activists on the web, but Google’s Project Shield offers free DDOS mitigation services to sites serving media, elections, and human rights related content. The tool is built on Google's PageSpeed service, a front-end tool that offers developers faster loading times. Sites hosted by Project Shield would sit behind PageSpeed's infrastructure, allowing Google to pool resources if any one site fell victim to an attack. Unless an attack was strong enough to bring down all the PageSpeed sites, it wouldn't be able to bring down any of them. It's a similar model to existing DDOS services like Cloudflare, although the more recently launched PageSpeed service is working from a smaller

base of sites. In addition, some Internet Service Providers offer what is called a "wide channel" which provides again a sort of buffer or safety margin for customers to outstay a DDOS. However, a wide channel and filtering services are only effective if the filtration rules are kept up to date to fight the latest DDOS techniques. In the main, DDOS attacks are being used as a modern day form of resistance. It is akin to the traditional 'Street Protests' except they are now 'Internet Protests' and we can expect to see many DDOS attacks in the future at online voting systems.

Contingencies in case of vote-tampering

The only viable contingency is once identified to allow the affected individual(s) to recast their votes. The recasting may have to take place over a different channel or even revert to traditional voting (hopefully this number of course is very low) but the priority of course is to remove the tampered votes and allow the recasting of genuine votes. Any other approach could be seen as a failure of the e-voting process.

Detecting interferences with the online voting system

A key technology here would be Intrusion Detection & Prevention software (IDS). Intrusion detection is the process of monitoring connections coming to and leaving from a computer or network and then analysing those connections for signs of potential violations or incidents that go against security and acceptable use policies. Causes of these incidents can include attackers gaining unauthorised access to systems, malware such as spyware and Trojan viruses and misuse of system privileges by users or attempts to gain additional privileges. An intrusion detection system is the software that automates this process. An intrusion prevention system has all the same capabilities of an intrusion detection system and also has the capability of preventing possible violations.

When detecting possible incidents, an IDS can take a number of actions. One would be to report the incident to a system security administrator, who could then initiate a response to mitigate the effects of the incident. Alongside alerting an administrator, the IDS could also keep a record of incident that could be referenced at a later date and as a way to help prevent future cases of that particular incident. A key feature will be the anomaly based detection which is the process of comparing the known behaviours of the network against observed events in the same network to identify significant deviations. An anomaly is defined as a deviation to a known or normal behaviour. Profiles are used to represent the normal or expected behaviours of voters. It would be hoped that this would alert the administrators to nefarious voting patterns.

Maintaining audit trails

All web servers should maintain and protect their log files. This is core to identifying attacks and for ascertaining quickly how the service was penetrated. There are well known secure processes for which events should be monitored. These are no

different for an online voting system. Likewise with the audit trails, these can be implemented as they do at present for financial organisations and other who deal with critical information.

Ensuring the system is sufficiently secure

Securing an online voting system should be approached in the same manner as securing any vital resource online. Here a layered security approach is recommended. Some key aspects are to have a Centralised User Management which allows the IP admin team to control all intrusions from a central location. There should of course be a comprehensive password protection at various levels so as to isolate or lock out a user level if needed. Data classification should be established for classification of data. They should regularly hire penetration testers to conduct reviews and adopt a continuous review culture so as to identify and respond at the earliest opportunity to new risks or breaches.

Securing voter records and personal details

Protection against third party hacking involves ensuring the system is securely implemented, that all systems are patched and up to date. It is crucial that only essential services are turned on. Intrusion detection systems need to be in place to identify possible attacks. Log files should be secured and the crucial attack vector events constantly recorded. Encryption is essential for all information and a layered security strategy should be in place in order to ensure the system is safe from the attacks that are certain to unfold.

Properly implemented encryption should prevent the details of a voter from being exposed. If the proper forms of salting and hashing and encrypting online details are followed alongside strong passwords, then details should be safe from modern brute-force password cracking techniques. The key of course is that that the encryption algorithms and techniques are correctly deployed alongside strong passwords.

Open-sourcing and working in an alliance

Yes, I would open-source software and I would be willing to work with others in an alliance.

Mi-Voice

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Safeguards against malware on the voter's device

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> "The majority of data breaches are caused due to the poor implementation of the technology – not the technology itself."

Mi-Voice

About

Mi-Voice, based in Southampton, was established in 2006 by iMeta Technologies; an organisation with a pedigree of developing secure transactional applications for clients such as Virgin Money and top tier investment banks and broker/dealers.

Mi-Voice took part in previous pilots of electronic voting in the UK, and provides online voting for clients such as the Scottish National Party and Oxford University, amongst others.

Voter verification

There are a number of ways that voter verification can be implemented to make it extremely difficult for somebody to impersonate a voter. The two most obvious processes include an independent 'pre-registration' phase whereby individuals who wish to vote electronically need to register to vote by this channel. The second is to have some form of independent verification by a third party government platform to validate the authenticity of the voter.

Both processes can capture/use information that would be outside of the electoral roll data supplied by the public authority, making it much harder for an attacker to have all of the credentials required in order to impersonate a vote.

The downside of both these approaches is that it requires extra effort on behalf of the voter to participate electronically, which feels counter intuitive considering the convenience the channel potentially offers voters – especially given the lack of voter authentication at polling stations.

It should also be stated that as far as voter verification is concerned - any e-voting platform is only as good as the electoral roll data it is using.

Safeguards from peer-pressure

This is one of the most common arguments used against online voting – voter coercion. It is a potential issue; however, it can be overcome depending on how electronic voting is being conducted.

For instance, if electronic voting is open and subsequently closed before polling day individuals who felt that they had been coerced into voting a certain way could be given the right to vote in person and their electronic vote cancelled.

Technology can also be used to counter this issue by implementing a 'last vote' counts capability which means that a voter can vote many times but only their last vote will be counted. Therefore, if somebody is under duress, they can vote one way when being coerced and then vote how they wished at a later date/time.

It is also entirely possible that if it was commonly known that the 'last vote counts', the party attempting to coerce voters may not attempt to do so in the first place.

Ensuring the correct vote is submitted

A man in the middle attack would require an attacker to intercept a vote, decrypt it, alter the original preference and then re-encrypt the ballot in such a way that the receiving server accepted the altered communication. To achieve this would be no simple task, however to mitigate this type of threat completely, a process can be implemented that involves the system providing a response to the voter that is unique only to them and the candidate/preference they have selected. Not only would the attacker need to break the encrypted seal, they would also need to return the correct, unique response code for that voter and the candidate that they have selected. Failure to do so would return the wrong code and alert the voter to the fact that their vote had been manipulated.

Safeguards against malware on the voter's device

I think the premise for this question is misguided. I believe any remote e-voting platform should assume that the device (mobile/pc/tablet) being used to vote is potentially infected and as a consequence should use the appropriate encryption, authentication and operational processes to mitigate key logging, phishing and other types of malware attacks.

The practicality/scale/complexity of attempting to safeguard a voter's device to guarantee that a device was secure and clean would be extremely difficult if not impossible to achieve.

Safeguards against cyber-attacks

There are many different types of cyber-attack and there are just as many mitigation strategies to prevent/offset them. Rather than list them all here, I think it is fair to say that any e-voting provider should be able to demonstrate that they have considered the various different attack vectors and have a response for each type of threat. This risk mitigation strategy should be independently verified and tested.

Contingencies in case of vote-tampering

The response provided earlier highlights one way in which an individual could be alerted to vote tampering. Vote manipulation on a large scale basis is a much bigger threat simply because of its ability to subvert an election.

Large scale tampering is an attack that could be attempted internally or externally throughout the election cycle, from the commissioning of the voting servers through to the declaration of the result. This question is a far reaching one that really needs to be broken down into the constituent parts of an election process. As already mentioned, an e-voting service provider should be able to demonstrate that they

have identified and mitigated against the various types of threat at each stage of the election process. In addition to having the means to identify and prevent such attacks, I would also add that it is essential that there is an extremely robust audit trail that can be independently verified.

Detecting interferences with the online voting system

As discussed previously, response codes are one way to detect interference at the individual voter level. There are also specific services that can be implemented to detect and mitigate against large scale distributed denial of service attacks.

Interference from internal attacks or through attempts to alter data stored on servers should be countered using the appropriate authentication processes and by having a robust audit trail that can be verified by independent parties and that cannot be manipulated.

Maintaining audit trails

This is one of the areas where online systems have an advantage over other voting channels. Every process, interaction and instruction can and should be audited. The audit trail should also be capable of being independently verified.

Ensuring the system is sufficiently secure

Any statutory e-voting platform should be independently reviewed from both a code and process perspective. In addition, external penetration testing should be conducted by the electing authority to ensure that the platform is fit for purpose.

Securing voter records and personal details

There has been a lot of press lately about individual's details being stolen/hacked. There is a simple solution to this issue, ensure your platform is developed and tested properly! The majority of data breaches are caused due to the poor implementation of the technology – not the technology itself.

With regard to how data is stored, it is possible to de-couple the identity of the voter with the vote cast – in fact in some countries this is a legal requirement and represents one of the biggest challenges to e-voting providers.

Open-sourcing and working in an alliance

Yes. I believe that transparency is key to gaining trust. There of course is a commercial consideration for any e-voting company who will want to protect their intellectual property rights and investment, however this needs to be balanced with the ability for code to be independently reviewed, audited and verified.

As an aside, I am also a strong believer in interoperability between platforms as I believe this is another way to install confidence and trust into the process.

Professor Robert Krimmer

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Ensuring the correct vote is received

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> “Voters get a chance to verify whether their vote was cast as intended and recorded as cast.”

Professor Robert Krimmer

About

Professor Robert Krimmer MBA, PhD is Professor of e-Governance at Tallinn University of Technology, Estonia. He focuses on electronic democracy, governance, and related issues.

In the past, he served as Senior Adviser on New Voting Technologies in the Election Department of the OSCE's (Organisation for Security and Co-operation in Europe) Office for Democratic Institutions and Human Rights, in Warsaw, Poland. His role was to co-ordinate and support election-related activities where new technologies are used in elections and contribute to developing the methodology in this respect.

Professor Krimmer founded and chaired E-Voting.CC, and initiated the bi-annual EVOTE conference series held in Bregenz, Austria.

Voter verification

There are basically three forms of identification:

1. Username & passwords which we know from everyday e-mail;
2. Using one-time passwords where we have to make sure that the receiver is actually the eligible voter and
3. The most secure form, electronic signature cards.

While the latter is in use in Estonia, it hardly is available anywhere else in the world and so is its use limited.

Safeguards from peer-pressure

The best safeguard right now is twofold: make internet voting take place in the pre-voting phase and let voters cancel their electronic vote in case they feel pressured by going to a regular polling station. The second way is to allow for repeat-voting, i.e. that you can cast your online vote as often as you wish as long as it takes place in the voting phase.

Ensuring the correct vote is submitted

This can only be guaranteed by systems offering individual verifiability. This means that voters get a chance to verify whether their vote was cast as intended and at least recorded as cast. For this a number of ways how to realise it have been found, including distributing a set of answer codes to the voters and the system having to send the voter after voting a confirmation/return/answer code to their mobile phone to see whether their vote was cast as intended and recorded as cast. Basically it always requires a second independent channel through which some form of information is shared that will allow me to gain a higher level of trust that my vote has not been compromised.

Ensuring the correct vote is received

This can be done through universal verification. This requires complex cryptography to be used and allows us to see that the votes are actually counted as recorded and have not been tampered with nor modified.

Safeguards against cyber-attacks

There is no real prevention against this but one can do to limit the effect of such an attack by installing distributed denial of service prevention boxes and allowing for enough bandwidth etc. In the end if the attacker has a lot of bandwidth at his/her hand, the best way to prevent is to be able to cancel the online voting, and provide regular polling stations. Other ways are of course to include provisions in the electoral code against attackers.

Contingencies in case of vote-tampering

Organisational measures can be the most effective ones in this case. There are a number of measures that you can undertake like limiting access to the servers, using various mechanisms to show that the system has not been interacted with in any unforeseen way.

Detecting interferences with the online voting system

Monitoring, monitoring, monitoring. In addition, the Swiss cantons used to cast test votes that are in a separate constituency which provide at least a higher confidence in the result while actually adding only little to the formal security of level of the system.

Maintaining audit trails

Generally the log files of an online voting system are essential. However it is important that they cannot be altered in order to provide for evidence. Furthermore organisational measures could include public notaries auditing/confirming/certifying the correct behaviour of the authorities.

Ensuring the system is sufficiently secure

This is really tough, as real world election settings cannot really be emulated. One can only come up with as close as possible scenarios and test beds, but as soon as one use digital signatures for user identification, test beds can become really hard to be created.

Securing voter records and personal details

As most online voting systems do not solely rely on organisational measures to protect secrecy of the vote, such a scenario where they record how someone has

voted and leaking their identity is very unlikely. However it cannot be said that it is impossible only that it is very unlikely and very hard to do.

Open-sourcing and working in an alliance

Sharing the source code of election software is a good way to raise the awareness and trust and understanding of educated (IT-literate) people for the respective election software. However it is not a guarantee that the software is secure and prone to any errors. It just makes it easier for third parties to detect. Generally open source is a democratic idea so it should be inherent to elections to be run with as much open source software as possible. But it is also clear that maybe not all can b*e* provided openly.

Scytl

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Ensuring the correct vote is received

Safeguards against malware on the voter’s device

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> “The use of online voting provides a number of measures to detect and prevent individual and large scale vote manipulation.”

Scytl

About

Scytl, based in Barcelona, Spain, was founded in 2001 as a spin-off from a leading research group at the Autonomous University of Barcelona that had pioneered research of security solutions for the electronic voting industry since 1994.

They have delivered electronic voting solutions across the world in countries such as Australia, Canada, France, and Norway. Most notably, they provided online voting in the 2015 New South Wales State Elections which was reported as the largest government binding online voting election worldwide.

Introduction

Scytl works diligently with our Customers (which include electoral commissions, government bodies and so on) to introduce electronic voting in the most safe, secure, transparent and auditable manner within our Customers' political environment and context. The unique challenges associated with online voting are clearly addressed and catered for by Scytl technology as described in this chapter. Scytl works hand in hand with our Customers to select and tailor solutions that suit their specific needs – not all solutions are appropriate for all Customers. As there is no single answer or "out of the box" solution – Scytl consults with officials to recommend electoral technology and process specifics that reflect the technological and cultural environment where the system will be used.

In understanding and reviewing the responses to these questions posed to Scytl regarding our Scytl Online Voting product, you will see a number of terms recur regularly. We strongly encourage the reader to research these terms and characteristics in order to gather a deeper understanding of the functions they perform and their necessity in providing a secure online voting system should your interest be piqued:

- Cast-as-Intended verifiability
- Recorded-as-Cast verifiability
- Cryptographic techniques
- Multiple voting
- Vote integrity based on digital signatures
- Multiple-channel communication – internet, SMS, etc.

Ultimately the technology elements of Scytl Online Voting used are moulded by the legislative environment applicable during the electoral event.

Voter verification

One of the most important challenges in remote voting is how to properly identify a remote voter. Be it a paper based postal or online voting process, the lack of in-

person authentication generates concerns related to the real identity of the voter. Secure and accurate authentication is important at two levels: both the voter registration phase and the actual voting phase.

Unlike postal voting, the introduction of online voting provides strong and secure methods of identifying voters. These methods of identification can include a user identifier, a PIN, an SMS confirmation code, and so on which are multiple factors of authentication – as opposed to a user's ink signature in the paper based equivalent.

Verification that the correct person has voted is linked primarily to three factors – the voter registration process, voter authentication mechanisms, and vote authentication mechanisms.

The vote authentication process is related to the vote validation process prior to putting the ballot into the ballot box. In the case of postal voting this is the equivalent of opening the outer envelope and checking the voter credential inside. If the voter credential is from a valid voter that has not cast any other vote, the inner envelope is put in the ballot box. Both authentication processes are of paramount importance to ensure the accuracy of the results.

Voter registration process

It is important to consider that correct voter authentication starts prior to the voting process, in the voter registration process. In some cases, voters need to register in advance to vote remotely, so it is also important that the authentication and authorisation is done accurately and securely during this initial phase. Scytl technology and processes can be used in the voter registration phase, preventing impersonation attacks that could in many cases go undetected in the voting phase. The Voter Registration System is physically separate to the Scytl Online Voting system.

Voter authentication mechanisms

Voter authentication is related to the login access to the voting system. In many ways it is equivalent to the voter authentication process used when sending a postal ballot using a dual envelope process. Authentication mechanisms are used to identify a voter, and work to ensure that only eligible voters can cast a vote.

Scytl Online Voting can rely on multiple authentication factors that can be further enforced with the use of independent channels in the authentication process - an example being the reception of a one-time access code via a mobile phone. This combination can detect and prevent impersonation attacks where a voter's credential is intercepted, enabling a stronger and more secure voter authentication mechanism than a postal one.

Where possible Scytl looks to accommodate the authentication mechanism to the requirements of the specific election and tries to reuse any pre-existing

authentication mechanism to make the voting process easier. Depending on the strength of the existing authentication mechanism, Scytl provides a second authentication mechanism (like the access code from a mobile phone as mentioned previously) that enables an additional level of security. This is similar in concept to the mechanisms used in online banking, where customers have one user/password credential to access a portal and a second credential for executing higher level operations, such as performing a bank transfer. Since Scytl Online Voting is based on an underlying cryptographic protocol, the use of strong authentication mechanisms, such as digital certificates, is natively supported with the authentication mechanism flexibility available for both the voting and registration processes.

Vote authentication mechanisms

As mentioned above, vote authentication is of paramount importance to ensure that the remote votes in the ballot box have come from eligible voters. In the postal voting scenario this is usually done by adding a voter credential into the postal envelope. In Scytl Online Voting we apply a similar - although far more secure - approach based on digitally signing the encrypted vote via a unique voter digital certificate. By checking the digital signature of the encrypted vote, it is possible to verify that the vote has been issued by a valid voter and can be accepted into the counting process. A valid digital signature also provides an integrity proof of the vote that prevents any undetectable manipulation following the casting of the vote, as a modified vote will automatically contain an invalid digital signature. Placing a digital signature over an encrypted vote does not compromise a voter's privacy, as the link is with formed with the cryptographic vote envelope rather than with the vote content.

In cases where voters have their own digital certificates (e.g. a state or nationwide electronic ID), Scytl technology can use them for digitally signing the encrypted votes. Where this is not the case Scytl Online Voting natively implements a mechanism whereby authenticated users are transparently provisioned with individual digital certificates. This mechanism is completely transparent to the voter and does not require storage or further installation in a user's device that the already existing internet browser. The digital certificates for this mechanism are generated by the election officials during the election configuration process. The certification authority and voter digital certificates are keyed to a specific election and expire following the election. The voter digital certificate can be issued to a voter alias that does not necessarily contain the voter identity (e.g. voter abcXYZ) to prevent the direct link between an encrypted vote and a voter's identity.

During the vote casting process the digital signature is performed within the voter's browser in the same process as the vote encryption. This is important, as once the encrypted and digitally signed vote leaves the voter's computer, it cannot be compromised without detection. In contrast to Scytl Online Voting, other voting systems digitally sign the vote on the voting server, however such a system does not provide this same level of vote authenticity as Scytl Online Voting, as all the votes

are signed by the *same* server key. If all the votes are signed by the *same* key and the server is compromised the whole ballot box could be modified without detection.

Safeguards from peer-pressure

Another concern present in remote voting (it does not matter if based on paper or electronic) is the lack of a controlled environment supervised by election authorities to cast a vote. Coercion or vote buying practices are generally viewed as easier is these environments.

In practice it is necessary for a coercer to be confident that they have successfully influenced the vote, and this is done by either supervising the voting process or by checking the contents of a vote during the transport or counting process.

The introduction of Internet voting opens the door to measures that could mitigate the execution of this practice by enforcing 'vote secrecy and integrity', as well as providing 'multiple voting.'

Vote secrecy

In Scytl Online Voting, votes are encrypted and digitally signed in the voter's browser. The vote decryption key is split into physically separate shares on separate smartcards during the election configuration process removing the possibility that the key can be misused. This prevents a coercer from spying on or changing the votes after being cast.

Multiple voting

If the coercer supervises the voting process then they can be sure that the voter followed their instructions. However multiple voting capability provides a facility to allow a voter to cast another vote later that will be counted, rather than the vote cast earlier in the presence of the coercer. In this way the use of multiple voting prevents a coercer or vote buyer knowing that the supervised vote is actually the counted vote. The introduction of online voting has allowed the implementation of this practice, so coerced voters can cheat the coercer without detection. Scytl Online Voting systems support this mechanism when allowed by legislation.

Ensuring the correct vote is submitted

It is vitally important to the voter and the electoral officials that the vote submitted by the voter is the one received and ultimately counted for the election. This property of the voting system helps create the trust by users and officials alike, and is based on a number of factors such as private key signing of votes and the verifiability properties of the system.

In order for the voter to ensure that the vote they cast is the vote counted the following techniques are applied in Scytl Online Voting:

- Vote integrity with digital signatures
- Cast-as-Intended verifiability
- Recorded-as-Cast verifiability
- Integrity of the votes with digital signatures and SSL

In Scytl Online Voting the encrypted vote is digitally signed within the voter's browser, prior to being transferred across a network and stored at the voting server. In addition to communication-level measures such as SSL security over the network transmission, the signature of the vote prevents it from being modified without detection by the voting server, or by the electoral authorities during the counting phase. In this way voters can be sure that the vote that is leaving their computer cannot be manipulated without detection.

Cast-as-Intended verifiability

Another important concern about remote voting is how to verify that the content of an encrypted vote sent to the voting system, really contains the selection originally made by the voter. In other words, that a bug or security problem did not change the voter intent prior to its encryption.

Cast-as-Intended verifiability allows voters to check that the content of an encrypted vote cast matches their voting intentions. One mechanism for Cast-as-Intended verifiability is based on return codes such as those used in the Norwegian system (where voters received return codes generated by the voting server from the vote they cast, and the voter could check that those codes matched the ones in a paper voting card assigned to their selected options). An alternate mechanism is the one used in the iVote system in NSW Australia for the 2015 State Elections: voters could call a service where, once authenticated and having provided a receipt number obtained from casting their vote, the voter is told the content of their vote by an IVR.

Cast-as-Intended systems are carefully structured to suit the specific culture and requirements of the electorate in which they are to be deployed. By way of example, the tailored receipt number system and delivery process for the Norwegian system would not have been viable in NSW due to the cultural and technical differences between these two electoral environments.

Recorded-as-Cast verifiability

An advantage of online voting is that the voter is aware that the vote has reached the server when it is cast as it's an online transaction. There is however a risk that the confirmation of reception is shown to the voter but the vote is not properly stored in the ballot box.

Recorded-as-Cast verifiability allows voters to check that their votes are correctly stored by the server: usually this verification is implemented via a bulletin board system on a public website where the server publishes the fingerprints of all votes

received and stored in the ballot box. After casting their vote a voter receives a receipt containing their vote fingerprint, which is digitally signed by the voting server to ensure the validity of the receipt. Voters can check that the fingerprint of their vote is present in the bulletin board, and auditors can then check that all the votes stored by the server are published. Any claims raised by the voters can be validated by checking the digital signatures in their receipts to determine if the claims are true or false. Auditors can also crosscheck that the fingerprints published on the bulletin board belong to votes stored in the ballot box and vice versa. This demonstrates the integrity of the ballot box and the bulletin board.

Ensuring the correct vote is received

Audit measures can be implemented in Scytl Online Voting to check that votes have not been altered after being cast by the voter. This is achieved by performing the cryptographic operations in the voter's browser rather than delegating them to a voting server.

Vote signed with a digital signature in the browser

In Scytl Online Voting the vote is digitally signed within the voter's browser, prior to being transferred across a network and stored at the voting server. Communication-level measures such as SSL security protect the vote only during network transmission, but they do not protect the vote in the voting server. The signature of the vote prevents it from being modified without detection by the voting server, or by the electoral authorities during the counting phase.

Scytl provides an online voting solution to electoral organisations which the organisation may operate independently of Scytl. This ensures that Scytl is not directly involved with the running of the election, something generally required by electoral officials.

In light of this, Scytl online voting software provides facility to allow the electoral officials to confirm that the votes received where the same as those submitted by the voter – this functionality leverages that for allowing the voter to confirm their vote was the same as that submitted.

Safeguards against malware on the voter's device

Malware within a voter's device presents a challenge to the voter as well as the electoral authority responsible for the collection of the votes. The possibility of malware on the voters device creates an environment where the voters device is 'not trusted' by the voting system and so Scytl manages this risk by providing methods to gain trust in the vote itself that is cast. Gaining trust in a vote is provided through the Cast-as-Intended verifiability mechanism combined with multiple voting and multiple channel capability.

Cast-as-Intended verifiability

Cast-as-Intended verifiability allows voters to check that the content of the vote cast matches their voting intention – allowing the voter to determine if malware has somehow changed their vote. Scytl Online Voting systems provide for the verification to be passed to the voter through an alternate device than that used to cast the vote, for example a voter may cast the vote from their home PC followed by verification via their mobile phone through email or SMS.

In the event the voter verifies their vote and is not satisfied with the result, Scytl Online Voting system supports multiple voting and multi-channel elections, allowing the voter to re-cast and re-verify their vote using an alternate voting device or channel.

Safeguards against cyber-attacks

The breadth of cyber-attacks to any internet connected system is great by anyone's measure. Many of the means of protecting the online voting systems are methods familiar to all in the computer security field – defence in depth as a concept is used to ensure not only the online voting system itself is protected but the communications and physical infrastructure adjoining it. The safeguards can be thought of in the following ways:

Standard infrastructure-level measures

These are the measures familiar to all with even a passing interest in computer security – DoS and DDoS mitigation strategies combined with firewalls, monitoring systems, access controls both physically and per device, combined with a separation of duties for staff and administrators. Measures are taken based on the form of attack the system is exposed to.

Standard cryptographic techniques: tamper-proof logs, digital signatures, protection of the decryption key

The protections above are intended to detect and prevent external attackers affecting the integrity of the system – insider attacks are also a threat to be mitigated. Insider attacks are detected using cryptographic techniques including technologies such as Scytl's patented tamper-proof logs which monitor the Scytl Online Voting system, as well as ensuring that only valid votes that are digitally signed by voters are included in output from the system.

The decryption key for the election is destroyed when created by splitting it into pieces during the election initiation process– meaning that it does not exist during the whole voting period until the pieces are re-joined following the voting period. The pieces are protected on multiple smart cards distributed amongst multiple electoral officials. The votes can't be decrypted by the system without this key.

Advanced cryptographic techniques: end-to-end verifiability and zero-knowledge proofs

The use of techniques based on advanced cryptography (Cast-as-Intended, Recorded-as-Cast and Counted-as-Recorded) allows a complete audit of Scytl Online Voting. It is possible to find and isolate any attempt to manipulate the election if an attacker can gain access to the system.

These techniques provide what is known as *Software Independence*. Software Independence provides a feature whereby trust is not required in the software to guarantee the accuracy of an audit. It does not matter that someone finds an exploit in the software – as the exploit cannot be used to manipulate an election without detection.

Contingencies in case of vote-tampering

The use of online voting provides a number of measures to detect and prevent individual and large scale vote manipulation. By cryptographically sealing the votes in the browser of the voter's terminal using individual user keys it is possible to ensure that any manipulation of the vote during transport or storage will be detected.

Recognition of a tampered vote is vital, and this is a feature of Scytl Online Voting. This recognition is based on a combination of the following factors:

- Sealing the votes in the voter's browser using cryptography
- Voter verifiability: Cast-as-Intended and Recorded-as-Cast
- Logs and monitoring systems
- Vote structure
- Redundancy

Votes that fail any of the above tests are rejected by the system and available to officials for investigation.

The contingency plans to be taken when dealing with tampered votes are determined by election officials. Scytl Online Voting will highlight those votes which have been tampered with allowing the election administrators to decide on the actions to be taken – in exactly the same way the officials would do in the case of votes that are suspected of tampering in a paper ballot box.

Sealing the votes in the voter's browser using cryptography

Votes are sealed by digitally signing them in the voter's device, prior to sending and storing on the voting server. This sealing process prevents the manipulation without detection of a vote during transport or storage in the Ballot Box. As votes are digitally signed using a unique digital certificate for each voter this requires a person attempting to tamper with the vote to gain access to the private key of that voter whose vote they wish tamper.

Once a person attempting to tamper many votes moves this to a large scale basis this becomes increasingly more difficult as the person must gain access to as many individual private keys as votes they wish to manipulate. In Scytl Online Voting all votes are signed outside the voting server for this reason. When votes are signed outside the online voting server the risk of a trusted system administrator using that access for ill-intent is removed.

The use of cryptographic technology also provides the ability to confirm that a vote stored in the ballot box is the same as the vote that left the voters browser. The facilities provided by SSL, the cryptographic technology normally associated with secure web traffic, are not sufficient to sign the vote, however they provide an additional layer of security to the online voting system through the integrity they provide to the communication channel. These features combine to provide integrity from the time the votes are cast in the browser until they are counted.

Voter verifiability: Cast-as-Intended and Recorded-as-Cast

Sealing the votes within the voter's browser forces an attacker to focus any manipulation attempt onto the voter's browser. In doing so, this significantly increases the difficulty to scale this attack without detection as an attacker must corrupt 101 browsers to corrupt 101 votes – and all without being detected. Comparison of the effort to corrupt 101 different user's browsers with the tampering of 101 postal votes in a mailbag shows the levels of comparative effort to tamper with these votes!

Individual tampering of votes can also be detected by verification methods available to the voter, such as the Cast-as-Intended and Recorded-as-Cast verification features described previously. Cast-as-Intended allows voters to check that the encrypted and digitally signed vote placed in the ballot box contains their voter intent (i.e. it has not been manipulated before encrypted in the same voter terminal). Recorded-as-Cast allows voters to check that the vote has been stored in the ballot box at the voting server and that it is not eliminated before being counted.

Tamper-proof logs and monitoring systems

Generating logs of election activity and monitoring those logs is also important to detect malicious practices during the election. In Scytl Online Voting these logs are protected by cryptographic means to prevent an attacker varying these logs without detection – in this way large scale attacks can be detected via ongoing review of the tamper-proof logs and monitoring systems.

Vote structure – check the vote is 'well formed'

A challenge overcome by the cryptographic toolkit used in Scytl Online Voting is the question of detecting the validity of a vote – without compromising its secrecy or integrity. The system is able to detect whether the vote contents themselves appear

a correctly formed vote without actually decrypting the vote. An interesting and very valuable property of the advanced mathematics built into the system.

Using these cryptographic tools Scytl Online Voting is capable of validating the votes are well formed when they are received at the voting server, again following decryption at the end of the election, and again prior to counting. This provides the ability to detect any poorly formed votes that may be an attempt to corrupt or modify the system.

Redundancy

Another form of attack on an online voting system involves the removal of votes from the electronic ballot fallowing successful casting but prior to their decryption. Scytl Online Voting can be replicated both for availability and disaster recovery to prevent the loss of data from natural as well as nefarious activities. These levels of redundancy mitigate the risks associated with the electronic ballot box being affected during and after the running of the election.

Detecting interferences with the online voting system

Detecting interference with Scytl Online Voting during the election is similar to the detection of interference in other internet connected systems, albeit with additional features. The additional features to enhance the security described in detail above are:

- Tamper-proof logs and monitoring systems
- Voter verifiability: Cast-as-Intended
- Voter verifiability: Recorded-as-Cast
- Multiple-channel communication – internet, SMS, etc.
- Integrity of the votes with digital signatures and SSL

This is in contrast again to postal based voting systems. Postal voters cannot be sure if their votes will arrive to the ballot box or even if they will arrive in time for the count. This inherent reliability problem associated with the postal service is generally undetectable by the voter, as opposed to an online system where the voter receives immediate feedback. Of course in countries such as Australia a voter may find their postal vote was not included in the count when they receive a fine in the mail for failure to vote!

Maintaining audit trails

Audit logs are a strength of Scytl technologies in general and Scytl Voting Systems in particular. The audit logs allow auditors to reliably and confidently review audit data during and after an event in order to determine what has happened to individual votes and the electronic ballot box as a whole. Numerous logs are kept, both within the online voting system and externally. Key audit trails already mentioned are

linked to the tamper proof logs and the bulletin board that contains the voter's receipts.

Cryptographic proofs from the counting phase of the election provide an audit trail that is publicly verifiable to ensure that vote decryption has been executed correctly and that the reported votes are truly the votes collected by the system. This same proof also demonstrates that all the votes registered in the Scytl electronic voting system are taken into account for computing an election result.

All these traces and cryptographic proofs protect the privacy of the voters and can be audited openly without the risk of compromising election secrecy. All these logs and proofs can be stored and audited following the election to again check the integrity of the results.

It is these advanced cryptographic techniques that form the basis of one of the most robust ways to guarantee that an election has been conducted with no undetected incidents and providing a high level of confidence that election results reflect the intentions of the voters.

Ensuring the system is sufficiently secure

Stress testing and verification of an online voting system is the same as the stress testing of any other engineered computing system. Scytl has a Secure Software Development Life Cycle design and implementation methodology that involves the specification of the system, the build and implementation of the system and an ongoing risk management approach to addressing risks relevant to online voting systems.

Security processes during the development of the online voting system

From the design phase, the Scytl online voting system cryptographic protocol is formally checked in order to ensure it provides the required security functionality based on initial risk analysis and Scytl's core voting functionality. This formal check involves consultation with various experts, potentially extending to presentation in conferences for public assessment.

The core cryptographic components, and their linked monitoring systems, are constantly reviewed in order to keep up with technical advancements and ongoing risk analysis, as well as code review by differing teams in order to isolate and address weaknesses.

During system implementation the cryptographic code is reviewed by cryptographic experts to ensure protocols are implemented correctly. Static security analysis of the source code is used to detect and solve any patterns that could be a potential security issue exploitable by an attacker. During system testing, dynamic security analysis tools are used to detect and solve potential exploits that may be present when the system is deployed. As a final step white box security testing is also

performed by a separate team of security experts to detect vulnerabilities that may not exist in the attack pattern database of the previous tools.

Upon implementation in a customer environment Scytl works with the customer to confirm that the system operates in a predictable manner under load and other stress scenarios.

Facilitation of third-party audits

In addition to the works described above Scytl has provided the cryptographic protocol and the online voting system code for inspection by third parties, in agreement with its Customers. The third party auditor will generally check that the code provides the expected security properties, that the protocol has been correctly implemented and that they find no weakness.

Securing voter records and personal details

Scytl Online Voting is designed from the ground up to protect the voter's privacy – from the administrators of the election as well as from the infrastructure itself. In the case that any potential attacker gains access to the system, as is the case with a privileged user, they will not be able to connect voters with their votes.

To further this philosophy Scytl Online Voting contains minimal information about voters and only requires access to a voter identifier – any additional information to this will depend on the characteristics of the particular election, and that information is protected using standard measures for the protection of personal information. These measures include access control mechanisms such as application controls, data encryption, database security, firewalls and so on – as well as minimising the amount of data the system requires to have access to. As described earlier, Scytl Online Voting is designed to allow the electoral administration to provide an external authentication system which again reduces the information available to the voting system.

Protecting the privacy of the vote, ultimately identified through the link between the voter and their actual vote, is crucial to public acceptance of the voting system and is provided by the system through a combination of process and cryptographic means.

Prior to ballot box opening the voters vote and their identification are protected in an encrypted digital envelope. The key to open this digital envelope is the electoral board key and that key is broken into different shares which are stored separately with different individuals – which means that during the election the key to decrypt the electoral votes does not physically exist in any single location. Each individual component of the key is then stored in separate safes or other protective means. At the conclusion of the election the ballot box is closed, a concept from the paper voting system. Once closed the votes go through a process of cleansing, validation, mixing and decryption in a ceremony where the holders of the components of the electoral key come together – a process designed to ensure that each vote is

completely separated from the identity of the voter who cast it as well as to remove malformed votes, duplicate votes and other items that will ultimately be audited.

In order to make hacking more difficult, election configuration and decryption processes can be implemented in air-gapped systems - systems completely isolated from any network. The use of these air gapped systems removes the possibility of online remote attacks during these phases of the election.

Open-sourcing and working in an alliance

Scytl believes that collaboration with third parties for auditing the cryptographic voting protocol and the implementation of that protocol is good practice. For this reason, Scytl's cryptographic protocols have been published in conferences to allow public review of its design and facilitated access to its source code to auditors selected by our Customers.

Scytl has worked in alliance with a number of companies over the years and continues to foster a partnership model for the implementation of its systems.

Scytl considers it good practice to publish code with a license restricting its use to code inspection or testing, providing transparency to the electronic voting process, whilst balancing the wishes of the Customer. It is worth understanding that code publication does not provide a guarantee of the security of the system. Scytl's experience is that in practice few reviewers may participate, and it may be complex to find any weakness without a systematised methodology and organisation for the code review. There are many examples of systems whose code has been publicly available for years, before any weakness has been found such as in OpenSSL. As well as this it is important to allow for bugs that may be found in the future and may have a number of subsystems reliant on that code. For this reason Scytl considers that it is more important for a voting system to be end-to-end verifiable rather than open source. With end-to-end verifiability the verification of the election integrity is independent of the software as it's based on a mathematical proof. Due to this property of Software Independence, should any bug in the system be exploited by an attacker, the end-to-end verifiability properties will allow detection of the attack - thus preventing this from compromising the integrity of the election.

At this stage Scytl does not see a strong value proposition for our Customers in open sourcing Scytl Online Voting as a key feature for security is through providing verifiability which allows for any *misbehaviour* of the system or any attack to be detected – regardless of the system implementation.

It is widely accepted that publishing source code does not ensure that software contains no bugs. In addition to this, if a bug is detected, there is no surety that a bug will not be maliciously exploited by the finder.

Finally, publishing source code does not guarantee that the same source code is used in the real system. This leads to a requirement for additional audit measures to

be implemented that will require direct access to the voting system by additional staff, adding further risks of malicious access.

In summary it is currently the view of Scytl that whilst source code publishing does provide transparency it falls short in providing other security attributes such as being mathematically provable or ensuring that the source code is the same as that used in an election. Scytl recommends a focus on demanding end-to-end verifiability, as it is a more reliable way to audit and gain confidence in the system.

Smartmatic

Voter verification

Safeguards from peer-pressure

Ensuring the correct vote is submitted

Ensuring the correct vote is received

Safeguards against malware on the voter’s device

Safeguards against cyber-attacks

Contingencies in case of vote-tampering

Detecting interferences with the online voting system

Maintaining audit trails

Ensuring the system is sufficiently secure

Securing voter records and personal details

Open-sourcing and working in an alliance

> “The only way to counter the potential influence of coercion is to ‘devalue’ coercion itself.”

Smartmatic

About

Smartmatic, globally headquartered in London, was founded in the USA in 2000 by a small group of young entrepreneurs and engineers. They specialise in electronic voting technology, identity management, and solutions for smart cities.

Smartmatic has run thousands of elections across the world in Argentina, Belgium, Brazil, Estonia, and the USA, amongst others.

It is part of the SGO Group which is chaired by former Deputy Secretary-General of the United Nations, Lord Malloch-Brown.

Voter verification

Ensuring that only the correct, eligible voters are permitted access to cast their ballots is critical to the integrity of the democratic process. One of the strengths of internet voting is that systems can be designed and engineered to include strong authentication schemes which offer eligibility assurance far in excess of the current means of remote (postal) or in-premise (polling station) solution provisions.

These include:

Electronic ID (eID) - These are unique identity documents which are used uniquely identify citizens and provide the eligible owner with secure access to a variety of online governmental services.

In many instances they contain a unique digital certificate which can be used by the owner to securely encrypt and digitally sign transactions to prove their authenticity. eID requires the owner to activate the signing via a secret PIN number (which only they know).

Mobile ID (mID) – This is a more modern replacement of eID in which a unique SIM card is provided to the eligible owner and installed on their mobile phone to enable the owner to securely encrypt and digitally sign transactions. Like eID, mID requires the eligible owner to enter a secret PIN number to activate the system and secure the transactions.

(Both eID and mID are used in Estonia for the purposes of accessing eGovernment services, which include online voting).

Existing sign-on/authentication services – Online voting can be used in conjunction with approved and trusted existing online governmental identity verification services such as GOV.UK Verify.

In addition, private sign-on services (such as banking access systems) can be used to provide secure access and authentication in a similar manner.

Multi-factor based systems – Multi-factor authentication systems offer the most robust method of identity assurance and eligibility. Numerous factors of an individual can be captured (biometric, biographical, behavioural, documental, technical and social) to create a unique 'digital identity' for the eligible user which offers the strongest mechanism for mitigating against unauthorized access, identity theft and fraud. An example of such as system is Your.ID.[43]

It is critical to reinforce that all of the above methods offer considerably more secure and robust mechanisms for ensuring that the correct person can vote, than exist in postal voting and polling station voting. Under the current provisions for postal voting, voters are required to provide a handwritten signature and their Date of Birth. Dates of Birth are not secret and are often known by friend and family members. Signatures, whilst offering a more unique identifier, can be easily copied, resulting in a very insecure and weak method of authentication and eligibility assurance.

In the case of authentication in the polling stations, the current provisions do not require the voter to provide any identifying information other than to state their name.

The current provisions for voting in the UK are therefore highly susceptible to fraud, identify theft and open to allowing ineligible persons cast ballots.

Safeguards from peer-pressure

When voting is taken outside of a controlled environment (polling station), then the risks of voter coercion are increased, due to the fact that there is no 'authority' to reduce the presence or influence of potential coercers. This applies not only to online voting but also to postal voting.

The only way to counter the potential influence of coercion is to 'devalue' coercion itself. This can be achieved by enabling 'multiple session' voting which allows the voter to cast their ballot as many times as they wish, with each successive cast ballot cancelling out the previously cast ballot thereby ensuring the principle of 'one person, one vote'. In such instances, if a voter if influenced by a coercive agent to vote a certain way, they can access the system again (in a coercer free environment) and recast their ballot.

This type of scheme was employed in the Estonian online voting environment since 2005 and is seen as highly effective way of reducing coercion. In Estonia additional measures are taken to reduce the potential and effect of coercion by giving the voter the opportunity to go to the polling station and cast a paper ballot which cancels out any previously cast online votes.

Ensuring the correct vote is submitted

One of the advantages of online voting is that voter verification provides a mechanism for the voter to check that their ballot was cast (received by the digital

ballot box/server) in the state that it was intended and has not been tampered with, changed or deleted.

Voter verification is critical to demonstrating the successful security of the system and can be used to clearly demonstrate the integrity of the online voting platform.

In Estonia 'cast-as-intended' verification has been used since 2013, by means of a smartphone based application which is used by the voter to verify successful receipt of the vote.

(A detailed explanation of 'how vote verification works' is included as an Addendum to this submission).[44]

It is worth reinforcing that the current provisions for remote voting in the UK (postal voting) offer no such mechanisms for the voter to check that their postal ballot was received in the manner in which it was cast and therefore offers no proof that their ballot has not been tampered with.

Ensuring the correct vote is received

The proof of the security of an online voting solution can only be guaranteed through the means of voter verification. Voter verification provides a mechanism to allow the voter to check that their vote was received by the voting server in the state they intended. (This is explained above).

In addition, the use of a 'block chain' based public bulletin board (PBB) allows a comparison to be made that the contents of the digital ballot box, exactly match the encrypted votes and voting receipts that have been committed to the PBB. This provides a robust method of assuring that the votes received by the system were the representative votes cast by eligible voters, which proves the integrity of the online voting platform.

Again, it must be noted that in the case of postal voting, there are no mechanisms to check that the votes which were received are the ones which were cast and that no tampering/manipulation has taken place.

Safeguards against malware on the voter's device

The reality is that the largest number of threats affecting a web based application occurs as a consequence of vulnerabilities affecting an individual's computer. Most of these risks and vulnerabilities can be reduced by following best-practice computer safety procedures[45] such as running up-to-date antivirus software.

However, it is impossible to guarantee that an individual's computer is not infected by viruses and/or malware. A well designed, 'government grade' online voting solution will be designed and engineered with this in mind knowing that it is impossible to fully protect against the threat of malware, but provide mechanisms to:

a) Allow the voter to check if their vote has been manipulated due to malware on their voting computer.

b) Allow the voter to take remedial action if vote manipulation has occurred.

This is achieved by providing a mechanism for 'out-of-band' voter verification, by allowing the voter to check that their vote have been cast-as-intended on a different device than the one they used for voting. If a vote cannot be verified correctly, then the voter should be given the opportunity to log onto the online voting solution (on a different device) and recast their ballot ('multi-session voting').

With these methods used in conjunction with education around general cyber safety it is possible to maintain the security and integrity of the system.

In addition, the use of purpose built, certified voting applications rather than voting from a regular web browser further reduce the risk of malware infection affecting the voting process.

Safeguards against cyber-attacks

In the ever connected and web-centric world, protection against ever evolving cyber-attack is become increasingly important. This obviously extends to the realm of online voting.

Well engineered online voting systems are designed, built and deployed to withstand most common cyber-attacks. The first stage in ensuring that the appropriate safeguards are in place is to understand the threat landscape, model the likelihood and severity of vulnerabilities and to establish the appropriate mitigation strategies to contain and eliminate the threats. This is undertaken using a risk based, proven project management methodology and modelling of 'attack trees'.

The types of cyber-attacks can vary in type and severity and a detailed analysis of this is beyond the scope of this report. However, described below some of the top cyber-attack types and an explanation of how a well-designed online voting system can mitigate vulnerabilities.

Sophisticated DDOS attacks - These attacks flood web application servers with service requests which overwhelm the servers so they are unable to accommodate legitimate requests.

Countermeasure - Defensive responses to denial-of-service attacks typically involve the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate.

Socially engineered Trojans - Socially engineered Trojans are the primary the method of cyber-attack and typically occur when a user browses a website (usually trusted) which prompts them to run a Trojan.

Often, the website tells users they are infected by viruses and need to run fake antivirus software. The user executes the malware, and infection occurs socially engineered Trojans are responsible for hundreds of millions of successful hacks each year.

Countermeasure - Social engineered Trojans are best handled through end-user education and ensuring that up-to-date antivirus software is installed.

Unpatched software - These attacks commonly occur as a result of not installing the most up-to-date version of the software.

Countermeasure - Vulnerabilities through unpatched software are normally mitigated through end-user education and ensuring that all versions of software are kept up-to-date and that up-to-date antivirus software is installed.

Phishing attacks - Phishing attacks typically occur as a result of bogus emails reporting to be sent from legitimate organisations that the individual will know.

Countermeasure - Decreasing risk from phishing attacks is mostly accomplished through better end-user education and with better anti-phishing tools such browsers with anti-phishing capabilities.

Many vulnerabilities and cyber-attacks are targeted at channelling through, or taking advantage of web browsers. In this respect, many of the common threats can be mitigated through the use or purpose built, certified online voting applications which strongly control the security parameters of the client side voting environment. Estonia uses purpose built voting applications in its online voting platform as a mechanism of mitigating against many common cyber vulnerabilities.

Contingencies in case of vote-tampering

A well-engineered ‘governmental-grade’ online voting system will be designed and engineered to protect against both individual and wholesale vote tampering. This is achieved by layering additional ‘application-level’ cryptographic processes on top of standard IT security techniques to provide the strongest level of protection of votes.

Individual vote tampering would typically occur as a result of interception and manipulation of the vote on the voter’s computer or on the internet as the vote is in transit to the vote server. Wholesale tampering could occur as a result of an attack on the digital ballot box (voting server) both by either and external or internal attacker.

The principle means of protection of all forms of manipulation is through strong, end-to-end encryption and through the use of digital signatures which make it practically impossible for voter preferences to be ascertained and changed without having access to the election private key.

To further mitigate against individual manipulation, the use of a certified voting application over a standard web browser makes it possible to strongly enforce the best security principles and reduce the risk of SSL downgrade attacks which could make the vote more vulnerable to manipulation.

In the case of wholesale manipulation, the enforcement of secret sharing schemes which allow 'multi-party' decryption of the votes mean that the decrypted votes cannot be manipulated by a single malicious agent.

Detecting interferences with the online voting system

Any government grade online voting system must have specific counter measures to detect and alert of any attempts to interfere with the online voting system during the election.

The following activities and processes should be present in any well designed system:

Hardware monitoring and alerting – All critical hardware components should have automated processes which detect and alert the presence of any unexpected network traffic and unauthorized attempts to access the system.

This applies to all server, firewalls, network switches and critical hardware components. Suspicious activity can be logged in immutable logs which cannot be tampered with or changed, and triggers to alert network administrators and IT security experts can be configured to investigate at short notice.

Voter verification – As discussed previously, voter verification provides a mechanism for the voter to detect any attempt to interfere with (manipulate) their vote.

Integrity checking with PBB – This provides a mechanism to publicly prove the integrity of the election system and to highlight any attempt to change vote contents, delete valid votes and add bogus votes from non-eligible voters.

Mixing proofs – These mathematical proofs provide evidence that no interference occurred during the critical 'mixing' process and that the encrypted votes which entered the mixing, are the same as those which came out of the mixing and that no votes were deleted, added or changed.

Decryption proofs - These mathematical proofs provide evidence that no interference occurred during the critical decryption process and that the encrypted votes which entered the mixing, are the same as those which came out of the decryption and that no votes were deleted, added or changed.

Maintaining audit trails

The provision of the necessary audit trails and tools are critical in the proof of the integrity of any online voting system, which is key to creating trust in the system.

Audit trails provided by any governmental grade online voting system should at a minimum include:

Proof of logic and accuracy – In this instance a set of pre-defined votes are lodged in the system and the actual results are compared with the expected results to prove the logic and accuracy of the platform.

Voter verification – This provides a mechanism for the voter to 'audit' their own voting session and to confirm that the system has captured their vote in the manner that they intended.

Integrity checking with PBB – Using public bulletin board, auditors, voters and other stakeholders can check the presence of all the encrypted votes that have entered the system and have been successfully cast.

Employing block chain based technologies and 'digital time stamping' allows auditors to confirm that no legitimate votes have been tampered with or deleted and that no ineligible (bogus) votes have been cast. This can take place whilst the election is being run.

Immutable logging – All interactions with the online voting system from an administrative, auditing and voting session perspective can be recorded in immutable logs which preclude the deletion of log entries or the addition of bogus log entries.

Mixing proofs – Mathematical proof of the correct operation of the cryptographic mixing process can be provided via the means of 'zero knowledge proofs' (ZKP) which demonstrate that all of the votes which entered the anonymisation (mixing) process exited the process and that no manipulation, addition or deletion of votes occurred. This is done in a way which never discloses the value of the votes (vote preferences).

Decryption proofs - Mathematical proof of the correct operation of the decryption process can be provided via the means of zero-knowledge proofs which demonstrate that all of the votes that entered the system were successfully decrypted and included in the final tally.

Source code audit – To ensure the highest levels of transparency, we strongly recommend the provision of the system source code for auditing (under confidential Escrow terms). Auditors can verify correct operation of the election protocols and business rules to ensure their correctness.

Software audits – Auditing of installed software components should be undertaken to ensure that the correct versions of the certified election software are the ones that are installed and running the election.

Ensuring the system is sufficiently secure

Testing any online voting system is a critical stage in the proof of the security and integrity of the system. In this respect a wide variety of test scenarios are undertaken as follows:

Quality assurance tests – These are performed as part of the development process to ensure that the software code is of a sufficiently high quality and that the system operates correctly. These are internal tests typically undertaken by the solution provider.

User acceptance tests (UAT) – These are tests undertaken by the customer in conjunction with the solution provider, which test that the system complies with their desired, stated requirements.

Logic and accuracy tests (LAT) – These prove that the system is operating correctly and is undertaken by submitting test scripts with known voting patterns and comparing the results with the test scripts.

Security and penetration tests – These are performed on the software and hardware elements of the election system to ensure that the system is no susceptible to any vulnerabilities that may jeopardise the security, accuracy, integrity and availability of the system.

Tests are performed against a number of threat scenarios and vectors and any potential vulnerabilities are ranked in terms of severity and resolved prior to repeat testing and the going live of the system. Many penetration tests employ the use of 'white-hat hackers' who attempt to hack the system and expose it to variety of cyber-attacks.

Volume tests – These ensure that the system has been correctly scoped in terms of performance to ensure that the system can receive the expected number of votes over the election period.

Independent certification – As part of the testing process, we strongly advocate the engagement with an independent third party who can certify or endorse the system. This provides an additional level of assurance of integrity which as stated previously, helps build trust in the system.

Securing voter records and personal details

The use of strong (end-to-end) encryption and digital signatures offers the most robust method of protecting voter privacy and ensuring the security of the votes. This method uses an electronic 'double envelope scheme' which encrypts the vote on the voting device used (which protects the vote preferences).

The encrypted vote is then digitally signed and then transmitted to the vote server (digital ballot) box over a secure encrypted (TLS 1.2) transport channel.

The digital ballot box is located in a Tier-1 secure data centre which offers physical, logical and procedural protection from ineligible access to provide the strongest levels of security.

After the closing of the election, the cryptographic 'mixing' process strips the digital signature from the encrypted vote to fully anonymize the votes which are randomly shuffled to break the order in which they were cast. At this stage any information regarding the voters' identity is completely removed from the votes which are still encrypted to hide the voting preferences.

Finally, the decryption process takes place in an offline 'air-gapped' environment and is undertaken in a multi-party collaborative environment in which members of the electoral board recreate the election private key.

These specific process steps ensure that voters' personal data are fully protected and the details of who they voted for are similarly secure.

Open-sourcing and working in an alliance

We strongly believe that transparency is critical to the creation of trust in the case of online voting. As part of this process we strongly advocate the full disclosure of system source code to the relevant Election Management Body (EMB) and/or any independent third-party for review and certification.

However, we do not advocate open sourcing election software (including online voting). The definition of 'open-source' involves the copyright holder providing a license for individuals to change, modify and redistribute the software to anyone to use for any purpose.

In this context, we consider that providing the source code of anyone to modify, change and contribute to presents a risk to the integrity of the election system rather than an advantage. Providing the source code in open source may in fact present a security risk and give potential attackers any opportunity to introduce vulnerabilities into the system.

Such situations are commonplace in the open-source domain and only recently the discovery of the 'Heartbleed' bug which affected the popular Open SSL cryptographic software library, realised that thousands of websites and applications worldwide, which were considered secure had in fact been highly vulnerable for many years. This was a direct consequence of the injection of vulnerabilities in the Open SSL libraries due to the open sourcing.

There is a very good reason why most mission critical software systems (power station management, weapon manage systems) do not use open-source software, and for this reason we would strongly advocate 'disclosed source' as the best method of establishing openness, transparency and trust without compromising potential security and creating risk.

Verizon

Voting platform described

Process

Identification

Security

Cost of reconciliation

Verification

System upgrades

> “Individuals who have registered through GOV.UK Verify should be able to use it to vote.”

Verizon

About

Verizon, based in New York, USA, was founded in 1983 and is the largest US wireless communications service provider, as well as being a provider of online identity assurance.

They are currently involved with the UK Government's 'GOV.UK Verify' programme which aims to give citizens a secure and convenient method of accessing Government services online.

The contribution below was provided by Matthew Margetts and has been adapted from his contribution to the Speaker's Commission on Digital Democracy.

Introduction

The task of introducing a voting platform for General, Local and Mayoral elections can be broken down into 4 distinct challenges:

1. Identification

2. Security

3. Adoption

4. Verification – the voting process

Electronic voting is not (initially) seen as a replacement for existing forms of voting but as a compliment to these services and as a means of engaging with a wider voting base, only eclipsing these methods over time as public demand grows.

Voting platform described

The investment needed to introduce and service a voting platform has been based on creating a comparable cost to the postal vote and over time to realize benefits from the need for staffing in ballot stations. A digital voting experience can be introduced in via a Federation of parties acting in concert to deliver a common goal on a common standard (in principle) on a cost-neutral basis.

The intention is to deliver a safe, secure system of voting that allows members of the public to vote by using mobile devices: telephones and tablets, and from personal computers (PCs).

The system is intended to treat each vote – General Election, Local, Mayoral etc. as a separate occurrence and as such whilst the process of Identification, Security, Adoption and Verification will be the same for each occasion the user will be required to re-register for every vote; in effect the Application will close after each vote and a new App created per event.

The platform has been conceived as being politically neutral and will only carry information to the end user concerned with the process of voting.

As such the roll out of digital voting platform can form part a broader transformation process that enables the online citizen – both transactional (passport, driving license etc.) but also social and informational services.

The process

In broad terms the process can be broken down into 4 key headings:

1. Identification

2. Security

3. Adoption

4. Verification

Each heading covers specific, linked challenges and solutions that will provide the foundation for the technical specification documentation that would form part of the ongoing consultation process.

Identification

The challenge for any system is to recognise and verify the identity of the user, unlike other systems that require online registration – voting requires a double guarantee of proof: firstly for the identity of the user and secondly for the user to a specific device.

The risk in meeting this challenge is to look to devise a new set of protocols and inputs around personal data without frustrating the consumer or creating liabilities around management. The solution therefore is not to build a new system but rather adopt existing, trusted processes and adapt them for purpose; the answer is to use retail banking identification processes and scale out to the users.

Over the past 2-3 years the UK banking sector has invested heavily in online account management partly in a bid to save money and partly in order to better manage customers and their information. Whilst the adoption of online account management by customers varies from institution to institution the protocols are in place for millions of individuals to access their accounts digitally.

The coverage of the UK population offered by the banks (approx. 94%) is significant and therefore provides a cornerstone for the roll out of online voting in the UK.

The process would see individuals looking to vote online as being verified through their bank. An individual would on visiting their account details behind the secure firewall of the bank be offered the opportunity to download the voting App – this will

require the Government and the banking sector to agree on the credentials necessary to prove an individual ID is accepted by both parties.

As part of the App download the individual would be sent a text – to their nominated mobile account number by their bank confirming that they were downloading the App and containing a unique password that would act to unlock the application.

The sending of the text in addition to being an added level of security will also act to verify the device. Furthermore if the voter is tied to this one device then the system is additionally secure – they have 2 factors – the password and the device. If they lose the device then they need to go through registering another or be passed directly to the Electoral Commission for reinstatement of the in person option.

The individual can only download the App once.

As the App is downloaded and activated, a message, synchronized through the bank's systems is sent to the Electoral Register notifying them of the individual's decision to vote electronically.

As a matter of choice the user may opt to change the user name and password on the front of the App but the unique identifier of the data package would be set: individual, individual address.

The federated approach of using the banks to validate and transmit the App acts both to reassure the consumer on the integrity of the system and to provide validation that the person and device are genuine.

Moreover, the approach provides a benefit to banks and a further benefit to Government; for the banks it provides an enhancement to their services and encourages the further adoption of online services – for example Barclays Digital Eagles programme. For Government, it provides an engagement opportunity around the digital passport and a protocol for mass adoption.

For example the Government's introduction of the Digital ID for vehicle licence renewal already sees the use of an ID albeit provided by a third party provider – Experian, Callsign etc. The concept is to evolve this process and recognise that a bank acts as the primary custodian of an individual's identity and as agreed with the consumer support the delivery of services.

Security

As the responsibility for the identification of the voter lies within the banking system the security issues are around the safe transfer and recording of the vote itself.

The process of voting, is based on the download of an App which, with the text security message, acts to lock down the voter to the device. As the device is being used as a second factor to bolster security, it makes for excellent security with a

slight loss of usability. The App itself will only display candidate information relevant to the individual's address as recorded on their bank statements.

The function of the App is therefore limited to candidate information and the ability to vote – a period which will correspond to the timelines set out for postal votes. The screen is therefore open to vote for a specific timeframe.

Once a vote has been cast, the data packet is transferred to a secure data area - the recommendation would be to work with an existing government supplier, housed on a proprietary server.

The assumption made is that the key used to decrypt the results is managed and only released on the day of the election. This requires a trusted party, ideally external to the development of the process who provides the other half of the key. This is standard public/private asymmetric key.

The mathematical puzzle of being able to time-lock encryption does not have a useful solution from reading the literature.

As with the Identification leg of the process the opportunity is to use existing suppliers and systems such as Azure Mobile Services that manage denial of service to ensure that the data is transmitted from device to server in a way that is safe from hacking. The data transfer is encrypted and should also be signed to prove validity.

As with the Postal Vote system the public will be made aware of how to approach the voting process, ensuring that their vote is a private affair and that they do not allow access to the system to third parties.

Cost of reconciliation

The benefits realised through the removal of cost at both the local ballot level and the cost of supplying and monitoring postal voting should act to make the system cost neutral.

An electronic vote is automatically machine counted removing the cost of human error and is directly auditable. Equally the cost of posting out and returning a vote is removed.

Whilst for the most part the aim is to reduce cost within the election process some unique costs will be generated such as the cost of raising awareness of the platform to the electorate.

A further consideration will have to be made for the cost of establishing the design of the voting interface. Whilst the design of the App is relatively simple it will require a design house to set out the experience and will have to be built to work across all devices: Android, Blackberry, IOS and Microsoft.

Furthermore, it is likely that the overall party responsible for hosting the delivery of the platform (recommendation: Electoral Commission) will have to provide both a web based Q&A as well as a call centre support – again it is probable that the cost of these services can be met within existing budgets as the platform acts to remove costs in the existing system.

The voting App will have to be designed to work on the principle mobile and devices platforms: IOS, Android, and Win 8. In respect to functionality, the recommendation again is to borrow from existing banking payments systems, and to make the App work around 4-5 screens:

- Sign up and pass word screen
- Candidate list
- Vote
- Vote confirmation – confirming vote
- Despatch and thank you

The App would be live for an agreed period prior to the General Election.

In the case of a lost device – mobile or PC once the App had been downloaded, a protocol notification could be introduced that would allow the individual to vote in person. The technology to link to the Electoral Register is again proven and it would be a matter of mapping out the process. Again it is likely that the circumstances would require a period of at 24 hours prior to the election in order to qualify.

As with the Postal Vote all notices would stress the idea of privacy and responsibility of the individual to take charge of the matter and act in way that did not make their vote the property of others.

Verification

The voting process is straightforward and follows a proven pathway of using an encrypted message - the vote - that is then consolidated at a secure location and finally unlocked.

The vote is sent via a private key – embedded in the App at the individual device level, and using a public key read by a government-vetted, yet independent party (Logica, Fujitsu, etc.) who allocate the vote to the corresponding party.

As with the identification process the intention is to make use of existing, trusted partners who operate under agreed protocols and who have worked with the government. The safeguards are, in effect built, into the voting process by using existing norms.

Moreover, it would, under current circumstances be a challenge for anyone to download the App on the day of voting or at least 36 hours prior as the registrant has

to be accounted for on the electoral roll. Over time, the vote timings can be extended to allow votes to be cast on the day.

Whilst the description of the process has tended to be built around the use of smartphone apps, the service can be extended to PCs on the basis that using an ordinary mobile phone to download a pin the App can be accessed online.

Votes would only be unlocked and recorded after the closure at 10pm of Ballot Offices or in line with agreed timeframes.

System upgrades

The process is built around natural redundancy, after each election the App is scrapped, and learnings around consumer experience taken into account and put into practice for the next time.

The benefit of this system is that it removes the need to continually manage legacy systems and invest in technology that might be supplanted by a better provider in the 4 years between elections. The optimum is to devise a system whereby the delivery is scaled up to suit and that investment is focused on building an interface API that is compatible across devices and mobile operators.

Additional comments

Currently Verizon is part of the Verify programme, the Government's digital ID standard. The Verify system has been built through industry consultation through the OIX (Open Identity Exchange) forum that has seen submissions from corporates, government bodies as well as foreign nationals, sharing best practice. The debate has been open and effective in creating a framework agreement and a deliverable outcome.

The process is 98% secure - the extra 2% is being covered off in the beta that is currently being run. Once the pilot is complete in April the system will be rolled out. The Government stands behind Verify and over 50 government agencies will use the protocol to process driving licences, tax returns etc. There are 9 providers of verification standards, and the group cannot be altered for 2 years.

It is my contention that individuals who have registered through Verify should be able to use it to vote.

The voting process itself in terms of technical design is covered off above. This could be expanded to look at emerging technologies such as blockchain, which are capable of guaranteeing a voting process but again there are proven capabilities that are used by government that work, at scale, just as well.

It is safe to conclude that the process of introducing digital democracy to the UK is not impeded by technology, nor is the cost of implementing a technological solution prohibitive; it exists at scale. If the Verify process was used as the cornerstone of the registration process the application could act to remove the need for a postal vote

and achieve a higher level of integrity than the postal vote as the system is tamper proof - for example ballot papers cannot be bulk voted.

Conclusion

> “I have no doubt that we will get there, and we are happy to work with all members of the Opposition, and all groups outside Parliament, to ensure that eventually we do get there.”
>
> Nick Boles

Conclusion

Next steps

As set out in the Viral Voting report, the case for online voting has been clearly made and the benefits are plenty. This Secure Voting report has set out how an online voting option can be secured, answering many of the concerns raised by decision makers who have been cautious in supporting the reform.

The next steps will be to continue the push for cross-party support, of which much progress has been made. The focus, however, will be on making requests from the Government to introduce this reform over the course of this current Parliament.

Get involved

If you agree that it's time for the UK to modernise elections and you would like to find out more about the campaign for online voting, there are a number of ways to do so.

The best way to stay up-to-date is to follow WebRoots Democracy on social media:

- Like us on Facebook at http://facebook.com/WebRootsUK.
- Follow us on Twitter at http://twitter.com/WebRootsUK.
- Join our Instagram following at http://instagram.com/webrootsdemocracy.
- Subscribe to our YouTube channel at http://youtube.com/WebRootsUK.

To join the mailing list for email updates, follow the instructions here.

If you are a keen writer or blogger, why not blog for webrootsdemocracy.org? Blogs on our website are based around issues of voter apathy, young people, disabilities, participation, digital democracy, and, of course, online voting.

Since launching in May 2014, **webrootsdemocracy.org** has received thousands of hits from over 100 countries.

If you would like to become a blogger for WebRoots Democracy, send an email to hello@webrootsdemocracy.org.

E-petitions are a great way to show demand and make a collective voice heard. WebRoots Democracy has set one up on Change.org. If you haven't already, help spread the message by signing, tweeting, and sharing our e-petition.

To keep up to date with upcoming events and actions, join our mailing list here. If you are interested in getting involved or collaborating with WebRoots Democracy in another way, contact Areeq Chowdhury at areeq@webrootsdemocracy.org.

Acknowledgements

Special thanks for this report goes to all who have supported WebRoots Democracy since its inception. As an independent campaign that is run voluntarily, every contribution of support is greatly valued and goes a long way.

Particular thanks for helping put together the report go to Luke Ashby, Alex Sunkler, Will Long, Dr Kevin Curran, Ben Thomas, Professor Robert Krimmer, Sam Campbell, Sandra Guasch, Jordi Puiggali, Mike Summers, Sonya Anderson, David Melville, Matthew Margetts, and John Wood.

Enquiry details

WebRoots Democracy

Website: www.webrootsdemocracy.org
Email: hello@webrootsdemocracy.org
Twitter: @WebRootsUK

Electoral Reform Services

Website: www.electoralreform.co.uk
Email: enquiries@electoralreform.co.uk
Twitter: @ERSvotes

Everyone Counts

Website: www.everyonecounts.com
Email: adam.tesan@everyonecounts.com
Twitter: @EveryoneCounts

Follow My Vote

Website: www.followmyvote.com
Email: contact@followmyvote.com
Twitter: @FollowMyVote

Dr Kevin Curran

Website: www.scisweb.ulster.ac.uk/~kevin
Email: kj.curran@ulster.ac.uk
Twitter: @drkevincurran

Mi-Voice

Website: www.mi-voice.com
Email: enquiries@mi-voice.com
Twitter: @MiVoice

Professor Robert Krimmer

Website: www.robert.krimmer.ee
Email: robert.krimmer@ttu.ee
Twitter: @robertkrimmer

Scytl

Website: www.scytl.com
Email: contactus@scytl.com
Twitter: @Scytl_SA

Smartmatic

Website: www.smartmatic.com
Email: info@smartmatic.com
Twitter: @smartmatic

Verizon/AOL

Website: www.verizonwireless.com
Email: matthew.margetts@teamaol.com
Twitter: @verizon

Glossary of terms

Algorithm - A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer

API (application programming interface) - A set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service.

Attack vector - A path or means by which a hacker can gain access to a computer or network server in order to deliver a malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities.

Audit trail - A record of the changes that have been made to a database or file

Bandwidth - The transmission capacity of a computer network or other telecommunication system

Biometric - Relating to or involving the application of statistical analysis to biological data

Blackholing - An anti-spam technique in which an Internet service provider (ISP) blocks packets coming from a certain domain or address. Blackholing can also refer to an individual who sets up a similar barrier up for his or her personal network. Blackholing of specific domains can prevent certain types of malware and denial of service attacks.

Blockchain - A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly

Botnets - A group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.

Brute-force attack - A trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

Cryptocurrency - A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Cryptography - Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is

unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored.

Custom scripts - Scripts are lists of commands executed by certain programs or scripting engines. They are usually text documents with instructions written using a scripting language. They are used to generate Web pages and to automate computer processes.

Cyber-attack - An attempt by hackers to damage or destroy a computer network or system.

Data centre - A large group of networked computer servers typically used by organisations for the remote storage, processing, or distribution of large amounts of data.

Database transactions - A series of operations performed within a database management system against a database such that, once completed, the data is left in a reliable and consistent state. If any step of the transaction fails, then all steps are reversed so that data integrity can be maintained.

Decryption - Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

Digital signature - A mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

Distributed denial of service - a type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash. This type of denial-of-service attack is perpetrated by hackers to target large-scale, far-reaching and popular websites in an effort to disable them, either temporarily or permanently. This is often done by bombarding the targeted server with information requests, which disables the main system and prevents it from operating. This leaves the site's users unable to access the targeted website.

Double envelope scheme - A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.

Dummy traffic – Randomly generated packets injected in the network to make the perception of real traffic difficult.

Elliptic curve cryptography - a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys.

Encryption - The process of converting information or data into a code, especially to prevent unauthorized access

End user - The person who actually uses a particular product.

End-to-end encryption - A method used for securing encrypted data while it is moving from the source to the destination. The objective of end-to-end encryption is to encrypt data at the Web level and to decrypt it at the database or application server.

Escrow - A bond, deed, or other document kept in the custody of a third party and taking effect only when a specified condition has been fulfilled.

Extended validation SSL certificate - This is a type of secure sockets layer (SSL) certificate solution. Designed to eradicate online transaction fraud, these certificates help organisations gain consumer trust by providing secure transaction processes.

Failover - A backup operation that automatically switches to a standby database, server, or network if the primary system fails or is temporarily shut down for servicing. Failover is an important fault tolerance function of mission-critical systems that rely on constant accessibility. Failover automatically and transparently to the user redirects requests from the failed or down system to the backup system that mimics the operations of the primary system.

Fault tolerance - Fault tolerance is the way in which an operating system (OS) responds to a hardware or software failure. The term essentially refers to a system's ability to allow for failures or malfunctions, and this ability may be provided by software, hardware or a combination of both. To handle faults gracefully, some computer systems have two or more duplicate systems.

Front-end - A front-end system is part of an information system that is directly accessed and interacted with by the user to receive or utilize back-end capabilities of the host system. It enables users to access and request the features and services of the underlying information system. The front-end system can be a software application or the combination or hardware, software and network resources.

Hardware - The machines, wiring, and other physical components of a computer or other electronic system

Hashing - Hashing is generating a value or values from a string of text using a mathematical function. Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only.

A formula generates the hash, which helps to protect the security of the transmission from unauthorized users.

HTTPS (Hypertext Transfer Protocol Secure) - This is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection. HTTPS enables encrypted communication and secure connection between a remote user and the primary web server.

Immutable logs – a tamper-resistant recording of how a system how a system has been used.

Key logging - A computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.

Load testing - This is a software testing technique used to examine the behaviour of a system when subject to both normal and extreme expected load conditions.

Log files - A file that lists actions that have occurred. For example, Web servers maintain log files listing every request made to the server.

Malware - Software which is specifically designed to disrupt or damage a computer system.

Man-in-the-middle attack - A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own.

Notaries - A person authorised to perform certain legal formalities.

Open-source - Denoting software for which the original source code is made freely available and may be redistributed and modified.

Operating system - The low-level software that supports a computer's basic functions, such as scheduling tasks and controlling peripherals.

Packet - A data packet is a unit of data made into a single package that travels along a given network path. Data packets are used in Internet Protocol (IP) transmissions for data that navigates the Web, and in other kinds of networks.

Patched - A patch is a software update comprised code inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package.

PBB - Public bulletin board.

PCI DSS (Payment Card Industry Data Security Standard) - A standard that all organisations, including online retailers, must follow when storing, processing and transmitting their customer's credit card data.

Phishing - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Point of failure - A single point of failure (SPOF) is a critical system component with the ability to cease system operations during failover. SPOFs are undesirable to systems requiring reliability and availability, such as software applications, networks or supply chains.

RAM (random access memory) - A type of data storage used in computers that is generally located on the motherboard. This type of memory is volatile and all information that was stored in RAM is lost when the computer is turned off.

Redundancy - A system design in which a component is duplicated so if it fails there will be a backup.

Salting - Password salting is a form of password encryption that involves appending a password to a given username and then hashing the new string of characters.

Scripts - Scripts are lists of commands executed by certain programs or scripting engines. They are usually text documents with instructions written using a scripting language. They are used to generate Web pages and to automate computer processes.

Software - The programs and other operating information used by a computer.

SSL (secure sockets layer) - A standard protocol used for the secure transmission of documents over a network.

TLS (transport layer security) - A protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet.

Trojan viruses - A Trojan horse is a seemingly benign program that when activated, causes harm to a computer system.

White box testing - A methodology used to ensure and validate the internal framework, mechanisms, objects and components of a software application. White box testing verifies code according to design specifications and uncovers application vulnerabilities.

White-hat hackers - A white-hat hacker is a computer security specialist who breaks into protected systems and networks to test and assess their security. White-hat

hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white-hat hackers have permission to employ them against the organisation that has hired them.

Zero knowledge proofs - In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

References

[1] Viral Voting: Future-proofing elections with an #onlinevoting option – WebRoots Democracy, 3 March 2015.
[2] WebRoots Democracy – http://webrootsdemocracy.org.
[3] 'The campaign for online voting starts here…', Huffington Post, 27 May 2014.
[4] Cyber Streetwise – HM Government.
[5] Voter turnout data for the United Kingdom – International IDEA.
[6] How Britain voted in 2015 – Ipsos Mori.
[7] With the exception of the directly elected Mayors, these figures are based on the average turnout for each overall election. All figures are based on the most recent elections for the respective roles. Directly elected Mayor turnouts: Bedford (66%); Bristol (28%); Copeland (64%); Doncaster (28%); Hackney (40%); Leicester (59%); Lewisham (37%); Liverpool (31%); London (38%); Mansfield (58%); Middlesbrough (53%); Newham (40%); North Tyneside (32%); Salford (26%); Torbay (60%); Tower Hamlets (37%); Watford (37%).
[8] Figures reveal thousands of ballots rejected due to voter confusion – WebRoots Democracy, 9 May 2015.
[9] Viral Voting: Future-proofing elections with an #onlinevoting option – WebRoots Democracy, 3 March 2015.
[10] David Cameron says he has 'no objection' to online voting – WebRoots Democracy, 3 February 2015.
[11] WebRoots Democracy/YouGov poll shows majority want online voting implemented in the EU referendum – WebRoots Democracy, 21 July 2015.
[12] WebRoots Democracy/YouGov poll shows majority want online voting implemented in the 2016 London Mayoral Election – WebRoots Democracy, 21 July 2015.
[13] Brits back smartphone voting in general elections new Tecmark/YouGov poll reveals – Tecmark.
[14] Online voting by 2020? – Opinium, 16 April 2015.
[15] Internet access – Households and individuals, 2015 – Office for National Statistics, 6 August 2015.
[16] Figures show 7 million using online voter registration, whilst less than a quarter register by paper – WebRoots Democracy, 21 April 2015.
[17] European Parliament: EU citizens living abroad 'must be able to vote online' – WebRoots Democracy, 14 November 2015.
[18] 2014 European elections: national rules – European Parliamentary Research Service, 10 April 2014.
[19] EP elections: "Spitzenkandidaten", mandatory thresholds, right to vote abroad – European Parliament, 11 November 2015.
[20] The Queen's Speech 2015 – HM Government, 27 May 2015.
[21] Our forgotten voters: British citizens abroad – Hansard Society, 20 March 2014.
[22] Electoral Reform Services – Twitter, 14 September 2015.
[23] Luke Ashby, Electoral Reform Services – Twitter, 2 October 2015.
[24] President Obama: The Fast Company Interview – Fast Company, 15 June 2015.
[25] President Obama's 2016 State of the Union Address – Medium, 13 January 2016.
[26] Penrose says digital voting is "interesting" and "intriguing" – John Penrose MP, 26 October 2015.
[27] SNP calls for Commons electronic voting – BBC News, 21 December 2015.

[28] Union e-Day: 7 million to win from online voting – Trades Union Congress, 20 January 2003.
[29] Majority of British people say electronic balloting to vote for strikes is appropriate – Trade Union Congress, 6 January 2015.
[30] Trade Union Bill – UK Parliament, 22 October 2015.
[31] Online voting a step closer thanks to breakthrough in security technology – University of Birmingham, 1 May 2015.
[32] Individual Electoral Registration – GOV.UK, June 2011.
[33] Register to vote: new online service launched – GOV.UK, 10 June 2014.
[34] Government commits £10m for Identity Assurance as directory of Trusted Services projects published – Technology Strategy Board, 2 November 2011.
[35] Identity Assurance: First delivery contracts signed – Government Digital Service, 3 September 2013.
[36] Francis Maude on GOV.UK Verify – GOV.UK, 3 February 2015.
[37] Car tax disc to be axed after 93 years – BBC News, 5 December 2013.
[38] Renew your tax disc online – GOV.UK, 7 July 2014.
[39] How digital and technology transformation saved £1.7bn last year – GOV.UK, 23 October 2015.
[40] Representation of the People's Act 2000 – HM Government.
[41] Bills – Parliament.uk.
[42] Representation of the People Bill – Parliament.uk.
[43] Your.ID
[44] To download a copy of Smartmatic's addendum on voter verification, please visit webrootsdemocracy.org/secure-voting.
[45] Protecting your computer – Get Safe Online.

webrootsdemocracy.org

For enquiries, please email
hello@webrootsdemocracy.org

WebRoots Democracy

Campaigning for online voting in UK elections.