



OPEN RIGHTS GROUP

Issues around e-Voting in Student Union elections

For more information contact:
Open Rights Group
7th floor, 100 Grays Inn Road
London WC1X 8AL
+44 (0) 20 7096 1079
<http://www.openrightsgroup.org>
info@openrightsgroup.org

Introduction

This pamphlet is designed to inform the debate around the use of e-voting and online voting technology in student elections.

Electronic voting

Electronic voting means voting or counting votes using computer technology. Voting is a uniquely difficult problem for computer science. In order to comply with human rights legislation e-voting systems, when used in local, regional and national elections, must:

- Verify that you are eligible to vote
- Ensure that you vote only once
- Ensure you can vote anonymously
- Ensure you can vote privately
- Allow for meaningful recounts
- Allow for audit and oversight

There are currently no practical solutions which tackle all of these fundamental requirements simultaneously.

Evidence from elections in the UK and around the world shows that e-voting technology is vulnerable to significant error and fraud. Systems fail on election day, software bugs prevent votes being recorded, voters find the interfaces hard to use, and recounts turn out to be impossible. The testing, certification and audit processes designed and implemented so far have been quite unsatisfactory.

Thus far, every commercial e-voting system evaluated by independent researchers has been found to contain fundamental security flaws¹. Malicious or fraudulent attacks are not the only concern: errors caused by software bugs can also alter results. All election counts are affected by human error. But human error is random, and small scale. Introducing computers into the process means errors become systematic.

For example, votes were counted electronically for the May 2007 Scottish Parliamentary election. In one constituency, as the returning officer was going to declare the result for Labour, the result was questioned on the basis that the Scottish National Party had received zero votes. On examination it was found that a whole column of votes, on the far side of an Excel spreadsheet, had not been counted because they had 'fallen off the screen'. The spreadsheets were checked, the vote recounted and the result declared for the Scottish National Party, which caused the Scottish Parliament to change hands².

If an e-voting system doesn't register any votes for one candidate, or counts

¹ For the most recent example of this, see the University of California, Santa Barbara's Top to Bottom review of the electronic voting systems used in California, available at <http://www.cs.ucsb.edu/~seclab/projects/voting/> Also see <http://avirubin.com/vote/analysis/index.html>

²http://news.bbc.co.uk/2/hi/uk_news/scotland/6627657.stm and page 50 of http://www.openrightsgroup.org/wp-content/uploads/org_election_report.pdf?page=50 For more international examples, see the ORG briefing pack on elections: <http://www.openrightsgroup.org/uploads/evoting-briefing-pack.pdf>

backwards for one candidate whilst counting forwards for another, then the errors are not evenly distributed and the election result is no longer a fair representation of voters' intentions³.

Remote e-voting

In addition to the problems associated with electronic voting, remote e-voting – online voting – brings with it another set of issues. This is because systems based around the internet and PCs are vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc). These attacks may disrupt the process of voting or bring the results into question.

In 2004 a panel of academics were asked to evaluate an online absentee voting system designed for the US military, called SERVE. Their conclusions were stark:

“We regret that we are forced to conclude that the best course is not to field the SERVE system at all. Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear.”⁴

This advice led to US Government to abandon SERVE in 2004⁵.

What's more, elections held using online voting are vulnerable to manipulation of very traditional kinds, because it is difficult to verify that the voter is who they claim to be – and because others can watch the voter vote. This opens the door to voter coercion and vote buying.

With many systems, meaningful recounts are not possible as all the authorities have is a database of votes, with no paper trail for audit. As renowned cryptographer and computer security expert Bruce Schneier, has stated:

“a secure internet voting system is theoretically possible, but it would be the first secure networked application ever created in the history of computers.”⁶

Remote e-voting in student elections

This is all very well for *real* elections, but do elections at Students' Unions (SUs) really matter as much? We believe they do. SUs are a traditional springboard to local and national government. Encouraging acceptance of lax electoral arrangements in students sets a poor example and will likely make them less vigilant when they vote or stand in political elections. And election fraud at any level can lead to disaster.

"Take it from me, elections matter" - Al Gore

At London Metropolitan University's SU, paid staff took the place of elected students in office between July and December 2008 because the incidence of online voting

³ For more on these issues, see

<http://www.wired.com/politics/security/commentary/securitymatters/2006/11/72124>

⁴ See <http://servesecurityreport.org/>

⁵ See http://www.theregister.co.uk/2004/02/06/pentagon_cans_internet_voting_system/

⁶ See <http://www.schneier.com/crypto-gram-0012.html#1>

fraud had been so great⁷. The election was eventually rerun in November. Around the same time, detection of online voting fraud at the University of Essex Students Union resulted in the instatement of a new President there. These two cases were only detected after complaints were made, and could only be identified because fraudulent votes were cast from a small number of computers. Because fraud is so hard to detect, many more incidents could have gone unnoticed.

Most SUs run online elections without adequate or audited human and technical resources. Even where there is a serious attempt to do things properly, systems will suffer from all of the fundamental problems that are inherent in online elections:

- They are susceptible to systematic error
- They are vulnerable to undetectable attack
- They open the door to voter coercion
- They are vulnerable to vote buying
- They do not allow for meaningful recounts

It is therefore impossible to really trust that the results are correct the way that anyone can in a paper election.

Campaigning dynamics and online voting

Online voting changes campaigning dynamics. Elections are rarely won or lost on polling day. Campaigns for candidates, parties and slates are run with the specific aim of convincing the voter that, when they are alone in their polling booth, they will feel privately compelled to cast their vote a particular way. Online voting fundamentally alters the way that campaigns are run and that votes are cast.

The traditional door-knocking approach takes on a new dimension when candidates and/or their supporters can “guide” voters through the voting process. There is nothing to stop a candidate / supporter watching over a voter, suggesting other votes that they might like to cast. This is especially insidious when, through membership to a particular party or group, a voter is under pressure to publicly conform to certain voting expectations.

University halls of residence house thousands of students in close proximity, all with network access. A single day’s concerted campaigning drive, with the emphasis on “guided” voting, could elicit more votes than a consistent month-long campaign though which candidates meet their constituency and refine their policies.

Online voting is often introduced to improve voter turn-out and student engagement in Union politics. Yet, by moving polling beyond the SU Building, the visibility of campaigns, and the elections themselves, is dramatically reduced. Unmissable banners and physical interaction with candidates are replaced by emails that can be deleted unread. Elections become detached from the SU.

The impetus of a campaign can turn from being active across the University buildings over the course of many weeks and engaging with students, to targeting individual inboxes, primarily on polling days. Those with access to large mailing lists, sending out a message around the same time as the voting instructions go out, stand to make huge gains following this simple strategy devoid of interaction.

⁷http://www.londonmet.ac.uk/londonmet/library/f78122_3.pdf

While there is much anecdotal evidence that online voting can increase turnout initially, what does increase turnout much more is an actively contested election with candidates who engage the imagination and enthusiasm of voters. While this may be somewhat of a rarity, the voting system should not be compromised to accommodate insipid candidates. Evidence from UK e-voting and remote e-voting pilots showed little or no lasting effect on turnout⁸.

Summary

This pamphlet has presented some of the technical and practical issues associated with online elections, with a specific focus on Students' Unions (SUs) in the UK. It is clear that there are many ways in which online voting significantly increases the risk of error, fraud and voter coercion. Online voting may not, as is often intended, increase student engagement with SUs and boost voter turnout.

While around half of the current Cabinet served as a SU officer at or after university, the incidence of SU officers is much higher amongst younger MPs who start on the political career ladder straight from university. Student candidates now generally seek to become the elected officials and special advisers of the near future. As a result, any policy belief that elections should run without carefully considered checks and balances can have serious ramifications.

The problems associated with online voting, both technical and practical, therefore demand attention at all levels.

About the Open Rights Group

The Open Rights Group is a grassroots technology advocacy organisation. Our core operations are funded by hundreds of tech-literate UK citizens who want their voices heard in national debate around technology issues. We speak out against the poor regulation and implementation of digital technology with the aim of protecting people's civil, human and consumer rights. In May 2007 and May 2008 we fielded volunteer teams of officially accredited election observers to monitor pilots of e-voting and remote e-voting technologies in local and regional elections. You can find out more about our work on e-voting here:

<http://www.openrightsgroup.org/category/issues/evoting-issues/>

⁸See <http://www.jasonkitcat.com/h/n/WRITING/evoting/ALL/34/>