Handout 2 (E-Voting)

In security engineering, there are many counter-intuitive phenomena: for example I am happy (more or less) to use online banking every day, where if something goes wrong, I can potentially lose a lot of money, but I am staunchly against using electronic voting (lets call it e-voting for short). E-voting is an idea that is nowadays often promoted in order to counter low turnouts in elections[1] and generally sounds like a good idea. Right? Voting from the comfort of your own home, or on your mobile on the go, what could possibly go wrong? Even the UK's head of the Electoral Commission, Jenny Watson, argued in 2014 in a Guardian article that the UK should have e-voting. Her plausible argument is that 76% of pensioners in the UK vote (in a general election?), but only 44% of the under-25s. For which constituency politicians might therefore make more favourable (short-term) decisions is clear. So being not yet pensioner, I should be in favour of e-voting, no?

Well, it turns out there are many things that can go wrong with e-voting, as I like to argue in this handout. E-voting in a "secure way" seems to be one of the things in computer science that are still very much unsolved. It is not on the scale of Turing's halting problem, which is proved that it can never be solved in general, but more in the category of being unsolvable with current technology. This is not just my opinion, but also shared by many security researchers amogst them Alex Halderman, who is the world-expert on this subject and from whose course on Securing Digital Democracy I have most of my information and inspiration. It is also a controversial topic in many countries:

- The Netherlands between 1997–2006 had electronic voting machines, but "hacktivists" had found they can be hacked to change votes and also emitted radio signals revealing how you voted.
- Germany conducted pilot studies with e-voting, but in 2007 a law suit has reached the highest court and it rejected e-voting on the grounds of not being understandable by the general public.
- UK used optical scan voting systems in a few trail polls, but to my knowledge does not use any e-voting in elections.
- The US used mechanical machines since the 1930s, later punch cards, now DREs and optical scan voting machines.
- Estonia used since 2007 the Internet for national elections. There were earlier pilot studies for voting via Internet in other countries.
- India uses e-voting devices since at least 2003. They use "keep-it-simple" machines produced by a government owned company.

[1] In my last local election where I was eligible to vote only 48% of the population have cast their ballot. I was, I shamefully admit, one of the non-voters.

- South Africa used software for its tallying in the 1993 elections (when Nelson Mandela was elected) and found that the tallying software was rigged, but they were able to tally manually.

The reason that e-voting is such a hard problem is that we have requirements about the voting process that conflict with each other. The five main requirements for voting in general are:

- **Integrity**
  - By this we mean that the outcome of the vote matches with the voters' intend. Note that it does not say that every vote should be counted as cast. This might be surprising, but even counting paper ballots will always have an error rate: people after several hours looking at ballots will inevitably miscount votes. But what should be ensured is that the error rate does not change the outcome of the election. Of course if elections continue to be on knives edges we need to ensure that we have a rather small error rate.
  - There might be gigantic sums at stake and need to be defended against. The problem with this is that if the incentives are great and enough resources are available, then maybe it is feasible to mount a DoS attack agains voting server and by bringing the system to its knees, change the outcome of an election. Not to mention to hack the complete system with malware and change votes undetectably.
- **Ballot Secrecy**
  - Nobody can find out how you voted. This is to avoid that voters can be coerced to vote in a certain way (for example by relatives, employers etc).
  - (Stronger) Even if you try, you cannot prove how you voted. The reason for this is that you want to avoid vote coercion, but also vote selling. That this can be a problem is proved by the fact that some jokers in the recent Scottish referendum tried to make money out of their vote.
- **Voter Authentication**
  - Only authorised voters can vote up to the permitted number of votes (in order to avoid the "vote early, vote often").
- **Enfranchisement**
  - Authorised voters should have the opportunity to vote. This can, for example, be a problem if you make the authorisation dependent on an ID card, say a driving license. Then everybody who does not have a license cannot vote. While this sounds an innocent requirement, in fact some parts of the population for one reason or another just

do not have driving licenses. They are now excluded. Also if you insist on paper ballots you have to have special provisions for blind people. Otherwise they cannot vote.

- **Availability**
  - The voting system should accept all authorised votes and produce results in a timely manner. If you move an election online, you have to guard agains DoS attacks for example.

While these requirements seem natural, the problem is that they often clash with each other. For example

integrity vs. ballot secrecy
authentication vs. enfranchisement

If we had ballots with complete voter identification, then we can improve integrity because we can trace back the votes to the voters. This would be good when verifying the results or recounting. But such an identification would violate ballot secrecy (you can prove to somebody else how you voted). In contrast, if we remove all identification for ensuring ballot secrecy, then we have to ensure that no "vote-stuffing" occurs. Similarly, if we improve authentication by requiring a to be present at the polling station with an ID card, then we exclude absentee voting.

To tackle the problem of e-voting, we should first have a look into the history of voting and how paper-based ballots evolved. Because also good-old-fashioned paper ballot voting is not entirely trivial and immune from being hacked. We know for sure that elections were held in Athens as early as 600 BC, but might even date to the time of Mesopotamia and also in India some kind of "republics" might have existed before the Alexander the Great invaded it. Have a look at Wikipedia about the history of democracy for more information. These elections were mainly based on voting by show of hands. While this method of voting satisfies many of the requirements stipulated above, the main problem with hand voting is that it does not guaranty ballot secrecy. As far as I know the old greeks and romans did not perceive this as a problem, but the result was that their elections favoured rich, famous people who had enough resources to swing votes. Even using small coloured stones did not really mitigate the problem with ballot secrecy. The problem of authorisation was solved by friends or neighbours vouching for you to prove you are elegible to vote (there were no ID cards in ancient Greece and Rome).

Starting with the French Revolution and the US constitution, people started to value a more egalitarian approach to voting and electing officials. This was also the time where paper ballots started to become the prevailing form of casting votes. While more resistant against voter intimidation, paper ballots need a number of security mechanisms to avoid fraud. For example you need voting booths to fill out the ballot in secret. Also transparent ballot boxes are often used in order to easily detect and prevent vote stuffing (prefilling the ballot box with false votes).

Another security mechanism is to guard the ballot box against any tampering during the election until counting. The counting needs to be done by a team potentially involving also independent observers. One interesting attack against completely anonymous paper ballots is called *chain vote attack*. It works if the paper ballots are given out to each voter at the polling station. Then an attacker can give the prefilled ballot to a voter. The voter uses this prefilled ballot to cast the vote, and then returns the empty ballot back to the attacker who now compensates the voter. The blank ballot can be reused for the next voter.

The point is that paper ballots have evolved over some time and no single best method has emerged for preventing fraud. But the involved technology is well understood in order to provide good enough security with paper ballots.

E-Voting

If one is to replace paper ballots by some electronic mechanism, one should always start from simple premise taken from an Australian white paper about e-voting:

> *"Any electronic voting system should provide at least the same security, privacy and transparency as the system it replaces."*

Whenever people argue in favour of e-voting they seem to be ignore this basic premise.