Towards an inter-disciplinary dependability analysis of an e-voting system

Jeremy W. Bryans and Peter Y. A. Ryan
School of Computing Science
University of Newcastle upon Tyne
Newcastle upon Tyne, NE1 7RU

1. Introduction

The idea of using digital technology to facilitate the democratic process is an attractive one. Such technology holds out the possibility of fast, efficient and convenient voting. In principle it may even be possible to deploy systems that provide higher levels of assurance of accuracy, secrecy and availability, i.e., more assurance. However, on the downside, a poorly designed e-voting system could open up the possibility of election fraud on a massive scale. Furthermore, without adequate auditing facilities, such fraud might be totally undetectable. It is worrying that there appears to be a serious possibility that just such "thank you for your vote, have a nice day" style voting machines may be deployed in the upcoming US elections.

Every dependable, computer-based system must be designed with careful attention to socio-technical aspects. Even if the technical components are superbly designed and verified, the system may still be prone to failure due to badly designed procedures. This is true even for those most technical of systems: cryptographic systems. The Enigma cipher was, from a purely cryptanalytic point of view, a very strong system. It was badly let down by various poor procedures such as the selection of message indicators and the widespread use of stereo-typed plaintext.

E-voting systems are no exception.

2 Goal of the workshop

We must evaluate the dependability of systems within their contexts. We seek to extend the technique of dependability analysis to consider the socio-technical context within which a technical system is embedded. E-voting systems are a very clear example of technical systems embedded in rich social contexts. In this workshop we will seek to reach a consensus on what an interdisciplinary dependability analysis of an e-voting system should include.

3 *Prêt à Voter*

In this workshop we will focus on one proposed scheme due to David Chaum. This scheme has a number of striking features:

- it allows voter verification,
- it requires minimal trust to be placed in the technical components.

In place of trust in the technical components, the scheme provides the possibility for minute auditing of the actions of the booths and tellers. The probability of malfunctions or corruption of these components going undetected falls off exponentially with the number of votes affected.

The assurance argument comprises two key steps:

First, evaluation of the cryptographic core of the scheme to derive assurance of the effectiveness of the checking mechanisms. That is, we need to be confident of the claims that any attempts by the booths or tellers to corrupt votes will be detectable with the appropriate probability.

Secondly, careful examination of the error handling and recovery procedures. The latter is critical. Even if the technical aspects of the scheme are perfectly designed, if there are procedure failures in handling the errors that are flagged, the system could still fail.

In the workshop we present the key ingredients of a simplified version of Chaum original scheme (that we have dubbed the " *Prêt à Voter*" system) along with the dependability goals that it claims to provide. We will then outline some possible error handling and recovery mechanisms and indicate some vulnerabilities inherent in these procedures that could lead to possible attacks.

The Chaum digital voting system[3] is a cryptographic tour de force, combining visual cryptography, Chaum anonymising mixes and partial random checking. It provides voters and auditors with many checks and balances designed to ensure that the implementation adheres to the specification. Of course, this technical system must be deployed with a wider socio-technical system, and social recovery mechanisms for the technical failure modes must be defined and examined.

In this presentation, we will outline the technical mechanisms that alert the user or election official to the possibility of foul play. For example, the Chaum scheme requires some participation by the voter, over and above the action of casting their vote. Part of the voting process requires the voter to make a "random" choice between two parts of a receipt, labelled upper and lower. Later on they must retain either the upper or the lower half, according to their earlier choice. The voter should then run a well-formedness check on the retained ballot receipt. This mechanism is designed to make it very difficult for a booth to corrupt a vote undetected. We refer the reader to the description on [1] for details.

This mechanism does depend however on the voter performing certain tasks reasonably assiduously:

- They should make their choice of strip to retain in an unpredictable way.
- They should check that the booth accurately reflects their choice in what it prints on the strips.
- They should perform the well-formedness checks after leaving the booth.

Failing in these procedures could open up vulnerabilities. Thus, for example, humans are notoriously bad at simulating random choices. Surveys have shown that when people are asked to choose between "heads" and "tails", approximately 80 % chose heads. A significant proportion of voter are likely not to be sufficiently alert to notice if a booth tried to fool them about their choice. Even when they do notice, they have to take appropriate action to ensure that a fraudulent booth is identified and taken out of service.

During the workshop, we propose some goals and requirements for an e-voting system. We will then present the essential features of the (simplified) Chaum scheme and propose some error handling and recovery strategies.

4 Some relevant URLs

We suggest that the reader check out the following urls:

`www.verifiedvoting.org`

The home page of a campaign initiated by David Dill among others, seeking compulsory voter-verifiable (paper?) audit trails for US elections.

`www.truemajority.org/ComputerAteMyVote/index.cfm`

"The Computer Ate My Vote" is the name of a campaign initiated by Ben Cohen, seeking to prohibit computerised voting until better security assurances are given.

Computer scientists with a particular interest in electronic voting include

`lorrie.cranor.org/voting/`

and

`www.notablesoftware.com/evote.html`.

We will focus our discussions around the "*Prēt a Voter*" electronic voting scheme. A brief description of this scheme can be found at the tutorial website

`homepages.cs.ncl.ac.uk/jeremy.bryans/home.formal/`

This scheme is a simplification of the scheme proposed by David Chaum in [3]. An in-depth analysis of the Chaum scheme is provided in [2].

5 Questions

We suggest that attendees ponder the following questions that will be discussed during the workshop:

- Requirements for an e-voting system
- Who are the stakeholders for a voting system?
- How might their interests conflict?
- What are the assets and risks?
- What assumptions
- Would the electorate as a whole be fairly confortable using such a system?
- Would they find it useable, understandable?
- Would they trust such a system?
- How would one best go about assuring the public of the trustworthiness of such a system?
- Is it just too technically complex?
- How might trust be undermined?
- How might the system be improved?

References

[1] `http://homepages.cs.ncl.ac.uk/jeremy.bryans/home.formal/` .

[2] Jeremy Bryans and Peter Ryan. A Dependability Analysis of the Chaum Voting Scheme. Technical Report CS-TR-809, Newcastle University School of Computing Science, 2003.

[3] David Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Security and Privacy*, 2(1):38–47, Jan/Feb 2004.