Chapter 7
Modeling Threats of a Voting Method

Sven Heiberg
Cybernetica AS, Estonia, & Software Technology and Applications Competence Centre, Estonia

Jan Willemsen
Cybernetica AS, Estonia, & Software Technology and Applications Competence Centre, Estonia

ABSTRACT

In Estonian Parliamentary elections held in 2011, the percentage of Internet voters among all the voters was as high as 24.3%. At the same time a student implemented a proof-of-concept malware which demonstrated the effective disenfranchisement of the voter from the right to vote. The chapter gives an overview of risk assessment and threat modeling of Estonian Internet voting after the events of 2011. The chapter presents a classification of attacks against the voting method, distinguishing between manipulation attacks, revocation attacks and attacks towards public confidence.

INTRODUCTION

Several countries have looked into some form of electronic voting for various reasons. It is hoped that remote electronic voting improves the availability of elections especially for citizens abroad and increases voter turnout (Madise & Martens, 2006; Driza-Maurer, Spycher, Taglioni, & Weber, 2012; Pinault & Courtade, 2012). Electronic tallying is seen as a way to speed up the process to provide accurate election results (Mirau, Ovejero, & Pomares, 2012). For disabled people, electronic voting is a possibility to vote without assistance (Loide & Lepp, 2007). It is even claimed that without online voting segments of society will stay completely absent from voting (The world’s five biggest cyber threats, 2012).

Opponents of electronic voting point out that the application of new technology opens new ways to tamper with elections (Jefferson, Rubin, Simons, & Wagner, 2004). The basic threats are the same for all voting methods – selective voter disfranchisement, privacy violation, vote buying, etc., but the technology of electronic voting allegedly allows attacks to be carried out more efficiently than ever before.

Estonia has implemented a specific form of remote electronic voting – Internet voting – as a method to participate in various types of legally binding elections since 2005. In Parliamentary
Modeling Threats of a Voting Method

elections held in 2011, the percentage of Internet voters among all the voters was as high as 24.3%. In parallel to the rise of popularity, the amount of attempts to question the security or suitability of the Internet voting increased. For example, in 2011 a student implemented a proof-of-concept malware which demonstrated effective disenfranchisement of the voter from the right to vote, although the victim was left with an impression that his vote was cast as intended and accepted as cast. This proof-of-concept malware was used as a tool in an attempt to revoke the results of Internet voting altogether (Heiberg, Laud, & Willemsen, 2011).

Today in Estonia, Internet voting is not a niche method anymore. Successful attacks against the method might have significant influence on the election result. In this evolved situation we have performed threat modeling of the Estonian Internet voting method. We have used attack-trees as a modeling tool. Building upon existing works and combining it with the experience from Estonian elections, we have reached an extended classification of attacks against the voting method. We distinguish between manipulation attacks, revocation attacks and attacks on public confidence. We show how the technology of the voting method can be abused to achieve an election specific goal.

BACKGROUND

From Paper Voting to Internet Voting

By election we understand a formal process of selecting a person for public office by voting. Election depends on the voting methods available in the society to precisely gather preferences of those eligible to vote. The most widely applied voting method nowadays is voting on paper by secret ballot. Voting on paper usually takes place in the controlled environment of a polling station. A voter is authorised by the election officials; she receives a ballot paper and enters a polling booth, where she secretly marks her preferences on the ballot. The voter then inserts the ballot into a ballot-box guarded by election officials. The ballot-box is opened by the election officials after the voting period and the votes are tabulated by hand. All steps of the process, besides the actual act of voting, can be subject to monitoring by observers.

A remarkably different voting technology was applied in the United States before the American Revolution. Voters called their votes out loud, so that the clerk could write them down adjacent to the voters’ names in the poll book (Jones & Simons, 2012). Voice vote was an easily observable voting method, which allowed observers directly to verify the count, but the transparency of the method came with the price of bribery and coercion.

Voting by secret ballot hinders the coercion, provided that the act of voting is carried out privately and the cast vote contains no information to link it back to the original voter. On the other hand, ballot secrecy reduces the transparency of the tabulation and introduces new ways to manipulate the voting results by ballot box stuffing for example.

Harris (1934) observed and identified various types of voting fraud in the US elections. Harris (1934) also analysed mechanical voting machines, already present at that time, and reached a conclusion, that “where election frauds prevail there should be no question about the advisability of adopting voting machines” (Harris, 1934, p. 280). The new technology was seen as an effective countermeasure against fraud in the paper-based elections. Decades later the National Bureau of Standards (1988) strongly recommended the elimination of the Votomatic-type of mechanical systems due to technological problems. The same report identified major vulnerabilities in electronic tallying systems. In 2000, a bad ballot design in the Votomatic system caused a scandal in the US Presidential election.

The advent of electronic voting methods took place in the 1960s with the electronic tabulation of paper-ballots. In the 1970s, electronics were used for vote recording by direct-recording electronic