Chapter 8
Software Vulnerabilities in the Brazilian Voting Machine

Diego F. Aranha
University of Brasília, Brazil

André de Miranda
University of Brasília, Brazil

Marcelo M. Karam
University of Brasília, Brazil

Felipe B. Scarel
University of Brasília, Brazil

ABSTRACT

This chapter presents a security analysis of the Brazilian voting machine software based on the experience of the authors while participating in the 2nd Public Security Tests of the Electronic Voting System organized by the Superior Electoral Court (SEC), the national electoral authority. During the event, vulnerabilities in the software were detected and explored to allow recovery of the ballots in the order they were cast. The authors present scenarios where these vulnerabilities allow electoral fraud and suggestions to restore the security of the affected mechanisms. Additionally, other flaws in the software and its development process are discussed in detail.

INTRODUCTION

The Brazilian Superior Electoral Court (SEC) has been increasingly adopting electronic elections since 1996, culminating in the current scenario where nearly all votes are collected by voting machines and a considerable fraction of the machines have fingerprinting devices for voter identification. Important milestones in the history of the initiative were the first purely electronic elections in 2000, the transfer of full responsibility for software development to the SEC in 2006 and the migration to the GNU/Linux operating system in 2008. Although security testing by independent parties should be a part of the process from the start, as a natural way to improve reliability of elections and reassure that the system provides sufficient ballot secrecy and integrity, it only received significant attention after the software components and human procedures for electronic voting became stable. An important movement in this direction has been the public and periodic testing of the voting systems organized by the SEC since 2009. Despite some undesirable restrictions, these tests allow teams
of specialists from industry and academia to independently evaluate the security mechanisms adopted by the Brazilian voting system.

The main goal of this work is to present the observations collected by the authors during their participation in the 2nd iteration of the Public Security Tests organized by the SEC in 2012. Our previous official report of the event was jointly written with the SEC and does not contain sufficient information regarding other security issues not directly attacked by the authors during the event. Our intention is to point out several limitations of the Brazilian electronic voting system and to contribute to its security process. Following standard practices in the security field, we present self-contained descriptions of the observed software and development process flaws with multiple suggestions for correction or mitigation. This way, the interested parties are in an adequate position to implement effective countermeasures. In particular, the main design and implementation problems detected on the security mechanisms of the voting machine software are detailed. An overview of such issues can be found below:

- **Inadequate Protection of Ballot Secrecy:** Votes are stored out of order, but it is trivial to recover them in order only from the public data produced by a voting machine and superficial knowledge of the software source code, which is also made public to the political parties. This vulnerability fully compromises ballot secrecy when associated to a partial or complete ordered list of electors.

- **Inadequate Use of Encryption:** The same encryption key is shared among all voting machines for encrypting the critical portions of their memory cards. These include the voting machine software and other cryptographic keys required for authenticating election results. Using the classical abstraction of a locker as an encryption technique, this is equivalent to using half a million lockers with exactly the same key, since this is the approximate number of voting machines in operation. This encryption key is also stored in the plain text portion of the memory cards. Using the same analogy, this is compatible to hiding the locker key under the carpet and trusting the secrecy of this location to protect the confidentiality of the key.

- **Obsolete Cryptographic Algorithms:** The SHA-1 cryptographic hash function used for computing digital signatures and integrity verification is demonstrably not collision-resistant. These specific applications of the chosen hash function have been deprecated for 6 years already. A sophisticated collision in this hash function would allow an insider attacker to construct fake voting software capable of producing election results indistinguishable from the correct outcome.

- **Inappropriate Attacker Model:** Significant emphasis is put on the design of security features resistant only to outsider attackers, when insider threats present a much higher risk.

- **Faulty Software Development Process:** Bad engineering practices allow the accidental or malicious insertion of software vulnerabilities, clearly attesting that the software development process is immature from a security point of view.

- **Insufficient Integrity Verification:** The voting software verifies its own integrity during its initialization process, but all of the information needed to subvert this verification is contained inside the voting machines, with different attack surfaces depending on the presence of a hardware security module. In the older voting machine models without this module, the problem of software authentication is reduced to itself, with no external source of trust. In this case, digital signature-based