CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Bulletin - Volume 3, Number 9, September/2018

Publication of the source code for Brazilian electronic voting machines

Lucas Lago

With the announcement of the publication of the source code used in Brazilian electronic voting machines (EVM) by the Superior Electoral Court (Tribunal Superior Eleitoral - TSE), a new chapter in the discussions on the safety of voting machines will begin.

It is a known fact in information security that all systems have vulnerabilities that can be exploited by eventual attackers; no computational system is invulnerable. Security planning is developed considering the environments of these computational systems, contemplating other elements, such as the people involved, the physical structure where the system is located, as well as several other elements.

> "The design of the system should assume that all attackers already know the system in the smallest details and despite this knowledge, security must be guaranteed.".

It is important to stress that, yes, there are vulnerabilities in the Brazilian EVMs, which does not directly imply vulnerability in the electoral system as a whole, and more than that, it is necessary to show that the exposure of the source code used in the EVM is not one of those vulnerabilities.

Brazil adopted Electronic Voting Machines since 1996, when they were used in some municipal elections. This technology allowed Brazil to achieve, even though it is a country of continental proportions, the tally of its elections a few hours after the closing of the voting.

However, the use of this technology suffers harsh criticism from researchers from many different areas, as well as from society. In the 2014 elections, a request for an audit of the voting machines was made, because the small difference in the result of the elections fueled the suspicions that already fall on the technology. However, it is necessary to separate baseless criticisms from critics who rely on serious research, which should be seen by the TSE as contributing to the development of a safer electoral process for the country.

Despite being updated over the years, Brazilian EVMs are still considered first generation models, which are characterized by being voting machines that make the election dependent on software. The Brazilian electoral process depends on the quality and honesty of the code developed by TSE. Models of voting machines of later generations use printed votes to allow a software-independent audit, carried out by manually counting the votes.

This text intends to show that the opening of the source code, contrary to what may seem in a superficial analysis, does not increase the vulnerabilities in the Brazilian elections. TSE willingness to open this (and, if possible, the opening of the EVMs hardware architecture) shows that the court is acting in accordance with information security principles, concerned with the creation of a safer election process for the country.

The information security discipline and the creation of secure systems capable of keeping information in a secretive manner have been widely developed in the military sphere.

In 1883, Auguste Kerckhoff - Dutch cryptographer - published two articles that presented six principles for the development of cryptographic systems. Although modernization is necessary for some points of these principles, they serve as a guide for any system that needs security, as follows:

1. The system must be practically, if not mathematically, indecipherable;

2. The system should not be required to be secret, and should not be a problem if the system falls into enemy hands;

3. One must be able to communicate and remember his keys without using written notes, and correspondents should be able to change their keys if they wish;

4. The system must be able to perform communication via telegraphs;

5. It should be portable, and should not require too many people to operate;

6. And finally, given the circumstances in which it should be used, the system should have good usability and should not be stressful or require the user to learn or complete a long list of steps.

Bringing some of the principles of this list to the present, we can ignore principle 4 that at the time was an element related to the future. The telegraph was a novelty at the end of the 19th century.

Another aspect to be updated is the expression "enemy hands" in the second principle. It must be interpreted in a broader way, because at the time the author was publishing in a magazine specializing in military cryptography and in the current context, we can consider 'enemy hands' anyone interested in corrupting the system

Turning now to the principles and analyzing the Brazilian electronic voting machines, there are some items that the EVM complies with. Principle 6, for example, was part of the basic specification of the electronic voting machines since its inception and the choice of its architecture and functionalities allowed the visually impaired and illiterate to exercise their right to vote with more quality and confidence. The adoption of electronic voting contributed to the reduction of null votes in the country.

Principle 5, which says a single person must be able to operate the system, is an obvious requirement when it comes to a voting machine, after all, voting in Brazil is secret and must be done independently by the citizen.

Principles 1 and 3 require their own texts to be detailed as they refer to how information is encrypted in the EVM. And it is not imagined that votes are transferred via telegraph today as suggested by principle 4.

Regarding principle 2, which says that secrecy cannot be a requirement of the system, we notice that it was directly affected by the open source policy and the free software movement initiated by the Free Software Foundation. When Kerckhoff proposed that secrecy may not be a necessity, he was not advocating that the project should be public. This came from the influence of free software - a modern reading of this principle.

This principle emerges as a counterpoint to security by obscurity, which proposes the secrecy of the project as one of the security tools of a system. The main flaw that happens here is that, since secrecy is a necessity for security, there is an obvious way for an attacker to achieve his goal, that is, to break the confidentiality of the project; this is something that can easily be achieved with infiltrated people or corrupting people who have this project.

So Kerckhoff - and, independently, Claude Shannon - proposed that the design of the system should assume that all attackers already know the system in the smallest details and despite this knowledge, security must be guaranteed.

All the major cryptographic protocols go one step further, not only do the developers assume attackers might know their algorithm but also, they publish implementations of their algorithms, and invite people and entities to test them and look for vulnerabilities. This process increases the reliability of systems in two ways: first by showing that they were developed with Kerckhoff's 2nd principle in mind; and, secondly, allowing other developers to show potential flaws and improvement points in their system.

The TSE, with the publication of the source code of Brazilian electronic voting machines, takes an important step toward creating a more transparent, reliable and secure electoral process. However, there are still other steps to be considered, such as the adoption of open architecture hardware and upgrading the existing EVMs to second or third generation systems, but above all, it is necessary to abandon the mentality that the system currently used is 100% secure because this belief is the main vulnerability of the system.

Lucas Lago *is a PhD student in Computer Engineering at Escola Politécnica da Universidade de São Paulo, and researcher at CEST-USP.*

Coordinator: Edison Spina

This article is a result of the authors' ascertainment and analysis, without compulsorily reflecting CEST's opinion.