CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Boletim - Volume 3, Número 9, Setembro/2018

Disponibilização do código fonte da urna eletrônica

Lucas Lago

Com o anúncio da abertura do código fonte utilizado nas urnas eletrônicas brasileiras pelo Tribunal Superior Eleitoral (TSE), um novo capítulo nas discussões sobre a segurança das máquinas de votação irá se iniciar.

É um fato conhecido na segurança da informação que todos os sistemas possuem vulnerabilidades que podem ser exploradas por eventuais atacantes; nenhum sistema computacional é invulnerável. O planejamento de segurança é pensado então considerando os entornos desses sistemas computacionais, contemplando outros elementos como as pessoas envolvidas, a estrutura física onde o sistema se encontra, além de diversos outros elementos.

> "O projeto do sistema deve partir do pressuposto que todos os atacantes já conhecem o sistema em seus mínimos detalhes e a segurança deve ser garantida apesar desse conhecimento."

Então é importante frisar que sim, existem vulnerabilidades na urna atualmente usada, o que não implica diretamente em vulnerabilidade no sistema eleitoral como um todo, e mais do que isso é necessário mostrar que a exposição do código fonte utilizado na urna não é uma dessas vulnerabilidades.

As urnas eletrônicas são adotadas no Brasil desde o ano de 1996, quando foi utilizada em algumas eleições municipais. Essa tecnologia permitiu que o Brasil conseguisse, mesmo sendo um país de proporções continentais, totalizar as suas eleições poucas horas após o encerramento das votações.

Porém, o uso dessa tecnologia sofre duras críticas de pesquisadores das mais diversas áreas, bem como da sociedade. Nas eleições de 2014, foi realizado um pedido de auditoria das urnas, pois a diferença pequena no resultado das eleições alimentou as suspeitas que recaem sobre a tecnologia. Entretanto é necessário separar críticas sem embasamento realizadas a respeito das urnas eletrônicas das críticas que se apoiam em pesquisas sérias, as quais devem ser vistas pelo TSE como contribuições para o desenvolvimento de um processo eleitoral mais seguro para o país.

As urnas brasileiras - apesar de terem passado por atualizações ao longo dos anos - ainda são modelos considerados de primeira geração, que são caracterizadas por serem máquinas de votação que tornam a eleição dependente de software, isso significa que o processo eleitoral brasileiro depende da qualidade e lisura do código desenvolvido pelo TSE. Modelos de máquinas de votação de gerações posteriores trazem a impressão do voto que permite que seja realizada uma auditoria independente de software, com a contagem manual dos votos.

O que se pretende nesse texto é mostrar que a abertura do código fonte, ao contrário do que possa parecer em uma análise superficial, não aumenta a chance de vulnerabilidades nas eleições brasileiras. Pelo contrário, a disposição do TSE de realizar essa abertura (e, se possível a abertura da arquitetura de hardware da urna) mostra que o tribunal está agindo de acordo com princípios da segurança da informação, preocupado com a criação de um sistema eleitoral mais seguro para o país.

A disciplina de segurança da informação e a criação de sistemas seguros capazes de manter informações de forma sigilosa tiveram amplo desenvolvimento no âmbito militar.

Em 1883 Auguste Kerckhoff - criptógrafo holandês - publicou dois artigos onde apresenta 6 princípios para o desenvolvimento de sistemas criptográficos. Apesar de ser necessária uma modernização de alguns pontos desses princípios, eles podem ser usados como guia para qualquer sistema que necessita de segurança, sendo eles:

1. Deve ser praticamente, se não matematicamente, indecifrável;
2. Não deve ter como requisito ser secreto, e não deveria ser um

problema se o sistema cair em mãos inimigas;
3. Deve ser capaz de se comunicar e lembrar de suas chaves sem utilizar notas escritas, e correspondentes devem ser capazes de alterar suas chaves, caso queiram;
4. Deve ser capaz de realizar a comunicação via telégrafos;
5. Deve ser portátil, e não deve necessitar de muitas pessoas para operar;
6. E, por último, dadas as circunstâncias em que ele deve ser utilizado, o sistema deve ter boa usabilidade e não deve ser estressante ou requerer que o usuário saiba ou complete uma longa lista de passos.

Contextualizando alguns dos princípios dessa lista para a atualidade, podemos ignorar o princípio 4 que na época tratava de um elemento de pensar no futuro, afinal o telégrafo era novidade no final do século 19.

Outro aspecto a ser atualizado é a expressão "mãos inimigas" do princípio 2 que deve ser interpretada de uma forma mais abrangente, pois na ocasião o holandês estava publicando em uma revista especializada em criptografia militar e no contexto atual pode-se considerar 'mãos inimigas' qualquer pessoa interessada em corromper o sistema.

Olhando agora para os princípios e analisando a urna eletrônica brasileira, há alguns itens que a urna cumpre com louvor. O princípio 6, por exemplo, foi parte da especificação básica da urna eletrônica desde sua concepção e a escolha de sua arquitetura e funcionalidades permitiu que deficientes visuais e analfabetos também pudessem exercer seu direito de voto com mais qualidade e confiança. A adoção da votação eletrônica contribuiu para a diminuição de votos nulos no país.

O princípio 5 que diz que o sistema deve ser operado por uma única pessoa, é um requisito óbvio quando se trata de uma máquina de votação, afinal o voto no Brasil é secreto e deve ser feito de forma independente pelo cidadão.

Os princípios 1 e 3 necessitam de textos próprios para serem detalhados, já que dizem respeito à forma como as informações são criptografadas na urna. E não se imagina que os votos sejam transferidos via telégrafo nos dias de hoje, como sugere o princípio 4.

Em relação ao princípio 2, o que diz que o segredo não pode ser um requisito do sistema, nota-se que este foi diretamente afetado pela política de código aberto e *software* livre iniciada pela Free Software Foundation. Quando Kerckhoff propôs que o segredo não pode ser uma necessidade, ele não está defendendo que o projeto deva ser público, isso vem da influência do *software* livre em uma leitura moderna desses princípios.

Esse princípio surge como um contraponto à segurança por obscuridade, que propõe o sigilo do projeto como uma das ferramentas de segurança de um sistema. A principal falha que acontece aqui é que, sendo o sigilo uma necessidade à segurança, existe um caminho óbvio para um atacante conseguir o seu objetivo, ou seja, a quebra do sigilo do projeto; isto é algo que pode ser facilmente conseguido com pessoas infiltradas ou corrompendo pessoas que possuem esse projeto.

Então Kerckhoff - e, de forma independente, Claude Shannon - propõe que o projeto do sistema deve partir do pressuposto que todos os atacantes já conhecem o sistema em seus mínimos detalhes e a segurança deve ser garantida apesar desse conhecimento.

Todos os principais protocolos criptográficos dão um passo além, não só assumem que seus algoritmos serão conhecidos por atacantes eventualmente, como publicam as implementações de seus algoritmos e convidam pessoas e entidades para testá-los e procurar vulnerabilidades. Esse processo aumenta a confiabilidade dos sistemas de duas formas: primeiro mostrando que eles foram desenvolvidos a partir do 2º princípio de Kerckhoff em mente; e, segundo, permitindo que outros desenvolvedores mostrem eventuais falhas e pontos de melhoria em seu sistema.

O TSE, com a publicação de código fonte das urnas eletrônicas brasileiras, toma um passo importante na direção da criação de um processo eleitoral mais transparente, confiável e seguro. Entretanto, ainda existem outros passos que devem ser considerados, como, por exemplo, a adoção de arquitetura de *hardware* aberta e a atualização das urnas atuais para sistemas de segunda ou terceira geração, mas, principalmente, é necessário abandonar a mentalidade de que o sistema de votação usado atualmente é 100% seguro, porque essa crença é a principal vulnerabilidade do sistema.

Lucas Lago é Doutorando em Engenharia de Computação na Escola Politécnica da Universidade de São Paulo e pesquisador do CEST-USP.

Coordenador Acadêmico: Edison Spina
Este artigo resulta do trabalho de apuração e análise das autoras, não refletindo obrigatoriamente a opinião do CEST.