Novos Rumos para o Ecossistema da Urna Eletrônica

José Monteiro, Lucas Guimarães, Saulo Lima, Marcus Amorim, Rodrigo Coimbra

[1]Tribunal Superior Eleitoral (TSE)
Brasília, DF

sevin@tse.jus.br

Abstract. *The embedded systems of Brazilian Electronic Voting machines (UE) and the infrastructure for pooling systems (UE Ecosystem) evolves for the inclusion of new tecnological and security advancements. In this paper we show the topics to be incorporated to the UE Ecosystem in next years.*

Resumo. *Os sistemas embarcados da Urna Eletrônica e a infraestrutura de segurança (Ecossistema da Urna) evoluem para incluir avanços tecnológicos e de segurança. Neste trabalho mostramos os tópicos a serem incorporados ao Ecossistema da Urna nos próximos anos.*

1. Introdução

O Ecossistema da Urna é constituído do equipamento em si e de todo o software e firmware necessários à sua operação, configuração e programação.

A partir de 2019, a segurança do Ecossistema da Urna foi construída com uma combinação de algoritmos e implementações diversas presentes nos Módulos Criptográficos e no software [Monteiro et al. 2019]. Com o descarte das urnas sem Módulos Criptográficos, passou-se a usar preferencialmente as assinaturas providas pelos Módulos Criptográficos MSD ou MSE, que armazenam chaves privativas de cada urna. Dessa forma, foi possível reduzir o número de bibliotecas de software utilizadas nos sistemas, o que satisfaz a observadores externos que apontavam a dificuldade de análise de múltiplas bibliotecas criptográficas. Hoje as operações de assinatura digital e criptografia na urna são feitas Módulos Criptográficos, libharpia e OpenSSL.

As últimas alterações do Ecossistema da Urna, particularmente em relação ao modelo introduzido em 2020 (UE2020) e posteriores, incluíam novo hardware com processadores Intel Atom E3940, tela *touch screen* para o mesário, mídias em USB e NVMe e o novo Módulo Criptográfico (Módulo de Segurança Embarcada - MSE) em substituição aos antigos *Main Secure Devices* - MSDs da urnas anteriores. A arquitetura da Cadeia de Segurança proposta por [Gallo et al. 2010] foi mantida, mas com algoritmos renovados.

A nível de software, em 2022, a segurança foi alterada pela inclusão da biblioteca libharpia, desenvolvida pelo Cepesc [Pacheco et al. 2022], que trouxe algoritmos com tecnologia pós-quântica aos sistemas eleitorais para as eleições gerais daquele ano. A biblioteca implementa uma proposta de assinaturas híbridas, com algoritmos clássicos (ED448) e pós-quânticos. A nova biblioteca inclui modernos algoritmos de assinatura (Dilithium) e de envelopamento (Kyber), que agora fazem parte da suíte do NIST para Criptografia Pós-Quântica (PQC).

Em seguimento à inovação e à atenção permanente com a segurança, os trabalhos estão sendo orientados a 3 linhas principais: 1) difusão do uso de PQC na UE (seção 2); 2) uso de *Multi-Party Computation* (MPC) com *Secret Sharing* (SS), para aumentar a segurança dos aplicativos desktop do Ecossistema da Urna (seção 3), e; 3) uso de protocolo de votação fim-a-fim (seção 4). Esses itens serão abordados em mais detalhe a seguir.

2. Difusão do uso de PQC na UE

Depois do trabalho de Shor [Shor 1994] e com o avanço das técnicas criptográficas pós-quânticas — biblioteca libharpia [Pacheco et al. 2022] e definição de algoritmos padrão pelo NIST [NIST 2024b, NIST 2024a] —, o TSE iniciou trabalhos para permitir que as urnas, por meio do MSE e outras bibliotecas possam utilizar um modelo híbrido em suas assinaturas. As assinaturas pós-quânticas feitas com libharpia se mostraram bem rápidas, mais que as clássicas atualmente usadas, o que também serve de incentivo para a atualização das bibliotecas de assinaturas.

O módulo MSD possui restrições severas de armazenamento, o que inviabiliza a inclusão de novos algoritmos e chaves em seu firmware. Por outro lado, o mais recente MSE possui margem para uma atualização de firmware que permita a inclusão de um algoritmo de assinatura pós-quântica (Dilithium) para as três fases de operação da urna — desenvolvimento, simulado e oficial [Monteiro et al. 2019].

Uma dificuldade para esse trabalho é a escala necessária e os custos associados para se alterar o firmware das cerca de 445.000 urnas com MSE espalhadas por todo o país, além de envolver a perda de certificação obtida para a versão atual do firmware, que precisará ser modificado.

Outra dificuldade é a necessidade de definição das cadeias de certificação. Existem ACs-Raízes para os algoritmos clássicos do ITI, mas não existe AC-Raiz para algoritmos pós-quânticos. Há notícias de que o ITI está trabalhando em uma AC-Raiz puramente pós-quântica, mas ainda sem datas. Uma solução temporária seria certificação com cadeias cruzadas, mas esse encadeamento de criptografia pós-quântica e clássica pode trazer problemas futuros, quando os computadores quânticos surgirem de fato. Para esse caso, uma solução seria re-certificar a raiz da uma cadeia pós-quântica do TSE com uma cadeia pós-quântica oficial, quando fosse lançada, e revogar a cadeia antiga usada.

3. Segurança para os aplicativos desktop

Uma parte importante do Ecossistema da Urna são os aplicativos necessários à preparação das urnas para a eleição e suporte aos processos de auditoria. Uma parte importante da preparação consiste na carga de dados e programas que serão usados diretamente nas urnas. Esse conjunto de software é crítico e precisa de medidas de segurança adequadas pois são executados em desktops com Windows. Atualmente, a plataforma desktop conta com módulo de segurança que gerencia o controle de acesso a programas e arquivos.

Além disso, há uma infraestrutura própria (driver monitor e serviço) para proteger o acesso às chaves necessárias para assinatura dos programas e dados. Em essência, essa infraestrutura usa o processador de segurança TPM para gerar e armazenar chaves, bem como executar protocolos de autenticação de dispositivos e suas chaves — os chama-

dos de protocolos de atestação. Os algoritmos baseados em Curvas Elípticas, pode possuir vulnerabilidades devido à implementação dos fabricantes de TPMs. Considerando a dificuldade técnica e financeira para padronização do parque de estações de trabalho, optou-se pelo uso do algoritmo RSA de 2048 bits, com chaves distintas para assinatura e cifração.

O uso do algoritmo RSA de 2048 bits pelo TPM traz preocupações e aponta para o de uso de uma tecnologia pós-quântica. Dessa forma, serão implementadas assinaturas híbridas também nos desktops, mas ainda resta uma outra preocupação com as chaves armazenadas nos TPMs e sua vinculação natural ao algoritmo de assinatura usado. A solução a ser usada consiste no uso de tecnologias de MPC com SS para o compartilhamento e distribuição de chaves pela rede de computadores desktop da Justiça Eleitoral.

4. Protocolo de votação fim-a-fim

Desde 2021 o TSE tem parceria com a USP para a análise de segurança do Ecossistema da Urna e pesquisa de novos recursos para a votação. Como resultado, a USP fez uma proposta de uso de uma tecnologia fim-a-fim (*End to End* - E2E), através da qual se busca maior confiança na lisura e segurança do processo de votação com uma menor dependência do software e hardware usados na implementação dos sistemas eleitorais.

Para tanto, foram buscadas garantias criptográficas adicionais para as seguintes propriedades [EAC 2022]:

(i) Voto é lançado como pretendido pelo eleitor (*"cast-as-intended"*) — permite que o eleitor verifique que seu voto foi corretamente interpretado pelo sistema de votação enquanto estiver no local de votação;

(ii) Voto é gravado como foi lançado (*"recorded-as-cast"*) — permite que o eleitor verifique que seu voto foi corretamente gravado pelo sistema de votação e incluído em um registro de votos público;

(ii) Voto é apurado como foi gravado (*"tallied-as-recorded"*) — o sistema eleitoral providencia um método público de apuração que utiliza o registro de votos público.

Com estas propriedades, cada eleitor é capaz de verificar, de maneira individual, que sua escolha foi corretamente gravada e utilizada pelo sistema para produzir a apuração da eleição. Portanto, um sistema E2E é capaz de prover segurança e confiança, teoricamente, sem depender do hardware e software que o implementaram.

Para a implementação estuda-se, entre outras, o uso de duas novidades: a entrega de um recibo ao eleitor, o Código de Rastreio (CR), que permite conferir se o voto foi apurado corretamente; e um desafio à urna, que que permite conferir se a urna está registrando o voto corretamente.

5. Conclusões

O TSE mantém o Ecossistema da Urna em permanente evolução para dar segurança e confiança aos eleitores. As próximas atualizações envolverão principalmente o uso de Criptografia Pós-Quântica e *Multi-Part Computation*. As implementações das técnicas serão desenvolvidas e incorporadas aos sistemas conforme suas necessidades e com cuidado de sempre se considerar a escala dos trabalhos necessários.

Referências

EAC (2022). End to End (E2E) Protocol Evaluation Process. Technical report, USA Government. https://www.eac.gov/votingequipment/end-end-e2e-protocol-evaluation-process.

Gallo, R., Kawakami, H., Dahab, R., Azevedo, R., Lima, S., and Araujo, G. (2010). T-DRE: A hardware trusted computing base for direct recording electronic vote machines. In *ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference*, pages 191–198, New York, NY, USA. ACM.

Monteiro, J., Alessandre, S., Rodrigues, R., Alvarez, P., Meneses, M., Mendonça, F., and Coimbra, R. (2019). Protegendo o sistema operacional e chaves criptográficas numa urna eletrônica do tipo T-DRE. In *Anais do XIX Simpósio Brasilieiro de Segurança da Informação e Sistemas Computacionais*, São Paulo, SP. https://sbseg2019.ime.usp.br/anais/197131.pdf.

NIST (2024a). Module-lattice-based digital signature standard. Federal Information Processing Standards Publication FIPS 204, U.S. Department of Commerce, Washington, D.C. https://doi.org/10.6028/NIST.FIPS.204.

NIST (2024b). Module-lattice-based key-encapsulation mechanism standard. Federal Information Processing Standards Publication FIPS 203, U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203.

Pacheco, R., Braga, D., Passos, I., Araújo, T., Lagrota, V., and Coutinho, M. (2022). libharpia: a New Cryptographic Library for Brazilian Elections. In *Anais do XXII Simpósio Brasilieiro de Segurança da Informação e Sistemas Computacionais*, pages 250–263, Santa Maria, RS.

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.