LARC-PCS-EPUSP
TSE

Relatório de Testes de Segurança UE 2020
Resumo Executivo

Projeto LARC – TSE

10 de Agosto de 2022

Resumo Executivo

Este relatório compila os resultados dos testes de vulnerabilidades e análises de segurança realizados pela equipe do Laboratório de Arquitetura e Redes de Computadores (LARC) da Escola Politécnica da Universidade de São Paulo (EP-USP) sobre a urna eletrônica modelo 2020 (UE2020).

Esta análise de segurança busca identificar vulnerabilidades, pontos de atenção ou melhorias que possam interferir ou contribuir para melhorar a operação do sistema eletrônico de votação. Entende-se por **Vulnerabilidade** do sistema alguma situação que possa comprometer o sigilo ou a integridade dos votos de uma eleição. Por outro lado, entende-se por **Pontos de Atenção** as situações em que se observa que um sistema não esteja de acordo com sua especificação ou com recomendações de melhores práticas de segurança, por levarem a um potencial comportamento indevido ocasionado por uma imperfeição (defeito) em um arquivo de configuração, software ou hardware; o resultado disso é um funcionamento que, embora incorreto ou não ideal, não interfere na destinação, integridade e/ou anonimato dos votos dos eleitores. Adicionalmente, podem ser identificadas **Melhorias** que, embora não caracterizem pontos de atenção e nem vulnerabilidades podem, de alguma forma, contribuir para aprimorar as funcionalidades a elas relacionadas.

Um dos objetivos principais do conjunto de testes que se buscou aplicar à UE2020 foi o de fazer com que ela fosse exposta à maioria dos ataques relevantes que aconteceram em Testes Públicos de Segurança (TPS) realizados pelo TSE no passado. Deste modo, as principais fontes utilizadas para definição dos casos de testes neste estudo foram:

a) Levantamento histórico e análise sistemática das estratégias de ataques adotadas pelos investigadores que participaram em Testes Públicos de Segurança anteriores, dando atenção particular àquelas que tenham obtido algum grau de sucesso;

b) Levantamento e identificação das estratégias comuns na literatura científica e técnica para avaliação de segurança de sistemas computacionais;

c) Estratégias adicionais propostas e executadas pela equipe USP para o modelo de urna 2015, como parte de parceira USP-TSE iniciada em 2021;

d) Sugestões de testes feitas por diversos pesquisadores e investigadores brasileiros, parceiros da USP, locados em outras instituições, cujas

implementações eram compatíveis com os prazos e os recursos desta atividade de avaliação.

O conjunto de testes assim definido pode ser considerado comparável ao que seria obtido se a UE2020 tivesse participado de todos os TPS anteriores, e é composto pelos seguintes 9 grupos de testes:

1) Análise de segurança dos processos de gestão e proteção de chaves criptográficas;
2) Avaliação do uso de chaves junto com os respectivos algoritmos de assinatura digital;
3) Verificação de quebra de sigilo de voto pela porta de áudio;
4) Análise estática de código com foco em falhas de gerenciamento de memória: Flawfinder e CppCheck;
5) Identificação de uso de algoritmos criptográficos inadequados;
6) Teste de mecanismos de verificação de integridade de código e dados carregados na urna;
7) Análise de segurança do Registo Digital do Voto (RDV): ordenação, criptografia e recuperação de parciais;
8) Análise de Segurança da Zerésima;
9) Análise de Segurança do processo de carga e certificação da urna 2020.

Os detalhes e resultados da aplicação de cada um desses testes encontram-se em no relatório completo.

Os principais achados e suas correspondentes ações ou sugestões encontram-se resumidos na tabela a seguir:

Teste		**Vulnerabilidade/ Ponto de Atenção/ Melhoria**
1	Análise de segurança dos processos de gestão e proteção de chaves criptográficas	Vulnerabilidade: 0 Ponto de Atenção: 1 Melhoria: 3
2	Avaliação do uso de chaves junto com os respectivos algoritmos de assinatura digital	Vulnerabilidade: 0 Ponto de Atenção: 1 Melhoria: 4
3	Verificação de quebra de sigilo de voto pela porta de áudio	Vulnerabilidade: 0 Ponto de Atenção: 0 Melhoria: 3
4	Análise estática de código com foco em falhas de gerenciamento de memória: Flawfinder e CppCheck	Vulnerabilidade: 0 Ponto de Atenção: 3 Melhoria: 1
5	Identificação de uso de algoritmos criptográficos inadequados	Vulnerabilidade: 0 Ponto de Atenção: 1 Melhoria: 2
6	Teste de mecanismos de verificação de integridade de código e dados carregados na urna	Vulnerabilidade: 0 Ponto de Atenção: 0 Melhoria: 1
7	Análise de segurança do Registo Digital do Voto (RDV): ordenação, criptografia e recuperação de parciais	Vulnerabilidade: 0 Ponto de Atenção: 0 Melhoria: 3
8	Análise de Segurança da Zerésima	Vulnerabilidade: 0 Ponto de Atenção: 0 Melhoria: 2
9	Análise de Segurança do processo de carga e certificação da urna 2020.	Vulnerabilidades: 0 Ponto de Atenção: 0 Melhoria: 0

Vale ressaltar que os testes foram executados com as versões do software da urna eletrônica disponibilizadas pelo TSE durante o período de realização destes testes.

Tendo passado por esse conjunto de testes sem que qualquer vulnerabilidade ou falha tenha sido identificada, pode-se inferir que a urna eletrônica modelo 2020 preserva todas as proteções existentes nos modelos anteriores das urnas eletrônicas dotadas de hardware de segurança, criando assim um cenário similar de resistência a ataques quando utilizadas. Com relação aos pontos de atenção e melhorias, sugere-se que eles sejam implementados em uma oportunidade conveniente de atualização do sistema.

Como esse modelo de urna possui um processador mais veloz que os anteriores, notou-se também que as funções tradicionais do sistema de votação normalmente são realizadas com maior celeridade.

De forma mais detalhada, e em consonância com essa constatação, os achados obtidos ao longo da execução dos testes permitem à equipe executante tirar as seguintes conclusões com relação ao software e hardware da UE2020:

- Em termos de segurança, a base de código encontra-se em bom estágio de maturidade. Essa constatação se baseia tanto no fato de não terem sido encontrados problemas óbvios ou graves no software como pela verificação de que a navegação pelo código fonte realizada em busca de respostas para dúvidas específicas pôde, em geral, ser realizada com certa facilidade. Apesar disso, cabe notar que a investigação realizada ainda se fez desafiadora por conta: (1) do tamanho da base de código; (2) de alguma heterogeneidade de estilo nele observada; e (3) de trechos que parecem conter código legado e que, portanto, poderiam ser refatorados para melhor legibilidade e manutenibilidade;
- As primitivas criptográficas adotadas para proteger ativos e recursos do sistema são usadas de forma apropriada. Uma única ressalva é que alguns pontos parecem ter sido também combinados com técnicas de ofuscação, reduzindo a clareza do código sem necessariamente trazer benefícios de segurança. Como essa característica parece ser herança de uma época em que a urna eletrônica ainda apresentava chaves secretas embutidas em seu código, questão suplantada pela disponibilidade de hardware de segurança nos modelos atuais, sugere-se considerar novamente a refatoração do código buscando aumentar a sua clareza e remover pontos de complexidade desnecessária;
- O processo de ativação de uma urna recém-saída da fábrica é baseado nos princípios de segregação de funções e privilégio mínimo. Uma urna ainda não ativada não consegue executar os softwares de uma eleição sem passar por todo o processo de certificação inicial, onde a ativação completa depende tanto de recursos computacionais do TSE/TRE, bem como da participação de múltiplos agentes do TSE e de um TRE. Tais fatores minimizam a chance de uma ativação

indevida, sem um conluio extenso. Além disso, mesmo se uma urna for indevidamente ativada, ainda há controles adicionais que previnem que os dados gerados por ela sejam indevidamente usados em uma eleição, sem serem detectados.