Relatório Final da Comissão Avaliadora

1. Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 601 de 7 de agosto de 2019, tem como atribuição validar a metodologia e os critérios de julgamento definidos no Edital do TPS e avaliar e homologar os resultados obtidos durante o teste. Cabe a ela, ao final, produzir relatório conclusivo contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes porventura identificadas.

A Comissão é composta de 10 membros, representantes dos seguintes órgãos:

1. TSE – ROGÉRIO AUGUSTO VIANA GALLORO
2. MPF – LUIS OTÁVIO DE COLLA FURQUIM
3. Congresso Nacional – FREDERICO QUADROS D´ALMEIDA
4. OAB – JOSÉ RORILSON VIEIRA ARAÚJO
5. PF – PCF MARCELO ANTONIO DA SILVA
6. CONFEA – RODRIGO DE SOUZA BORGES
7. SBC – PAULO LÍCIO DE GEUS
8. Comunidade Acadêmica – MAMEDE LIMA MARQUES
9. Comunidade Acadêmica – OSVALDO CATSUMI IMAMURA
10. Comunidade Acadêmica – JAMIL SALEM BARBAR

O propósito deste relatório é apresentar os resultados dos testes dos investigadores e grupos de investigadores.

2. Metodologia de Avaliação dos Testes

Foram mantidos os critérios de análise do TPS 2017, ou seja:

- Pontos de intervenção: elementos do processo eleitoral atacados;
- Impacto: quais propriedades de segurança foram violadas;
- Extensão: granularidade, extensão geográfica (ex. urna, seção etc.);
- Contexto: procedimentos, atores, circunstâncias do processo eleitoral.

Foi mantida a classificação dos resultados dos Planos de Teste como:

- Não realizados;
- Realizados sem contribuição para melhoria do sistema;
- Realizados com contribuição para melhoria do sistema.

3. Planos de Teste

Foram recebidos 14 planos de teste e aprovados 13. Compareceram 5 grupos de investigadores e 2 investigadores individuais, sendo executados efetivamente 10 planos de teste. Os objetos das propostas foram os seguintes:

3.1) Grupo de Investigadores: ***Fellipe Ribeiro Silva Abib (Coordenador)***

- Componentes do Grupo: Alan Papafanurakis Heleno, Caio Henrique de Aquino, Vicente Charles Willian Biesseki.
- Plano de Teste: identificação do eleitor e de seu voto a partir das informações gravadas no Registro Digital do Voto (RDV) e tentativa de manipulação do Boletim de Urna (BU).

3.2) Grupo de Investigadores: ***Jairo Simão Santana Melo (Coordenador)***

- Componentes do Grupo: Felipe Pradera Resende, Luiz Fernando Sirotheau Serique Junior, Leonardo de Almeida Ramos.
- Plano de Teste: identificação da operação eletrônica da urna, analisando os sinais elétricos nos circuitos entre o teclado e a placa mãe, empregando técnicas de inteligência artificial para identificação de cada tecla pressionada.

3.3) Grupo de Investigadores: ***Luis Antonio Brasil Kowada (Coordenador)***

- Componentes do Grupo: Gabriel Cardoso de Carvalho, Victor Faria de Souza, Igor Palmieri Antunes (ausente), Ramon Rocha Rezende.
- Plano de Teste 1: obtenção de chaves criptográficas e verificação do correto uso da criptografia para a garantia da integridade, confidencialidade e autenticidade.
- Plano de Teste 2: verificar a proteção de programas pré-construídos (denominados de bibliotecas), necessários ao sistema da urna.

3.4) Grupo de Investigadores: ***Luís Fernando de Almeida (Coordenador)***

- Componentes do Grupo: Fábio Rosindo Daher de Barros, Gabriel Ferrari Carvalho, Josinei Rodrigues Lopes Silva, Fernando Nogueira da Silva.
- Plano de Teste: tentativa de uso de Machine Learning para reproduzir o padrão de geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.

3.5) Grupo de Investigadores: ***Paulo César Herrmann Wanner (Coordenador)***

- Componentes do Grupo: Ivo de Carvalho Peixinho, Galileu Batista de Souza.
- Plano de Teste 1: recuperação de senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos.
- Plano de Teste 2: quebra da criptografia da proteção (SIS) do sistema gerador de mídia das urnas eletrônicas (GEDAI).
- Plano de Teste 3: domínio do sistema de geração de mídia a fim de adulterar dados de preparação da urna da seção eleitoral.

3.6) Investigador Individual: ***José Fellipe de Moraes Albano***

- Plano de Teste: identificação de componentes da rede computacional do TSE de forma a identificar possíveis alvos e disparar ataques específicos contra serviços disponibilizados na rede.

3.7) Investigador Individual: ***Leonardo Cunha dos Santos***

- Plano de Teste: quebra do sigilo do voto por meio de detecção de padrões de comportamento elétrico durante o pressionamento de teclas.

4. Avaliação dos Planos de Teste

Os planos de teste apresentados em consequência ao edital de Testes Públicos de Segurança do Sistema Eletrônico de Votação foram todos avaliados pela Comissão Avaliadora. Os resultados da realização dos planos são apresentados a seguir:

4.1) Planos de teste não realizados

Grupo Paulo César Herrmann Wanner: o Plano de Teste 3, descrito como “recuperar senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos”, não foi executado por não ter obtido sucesso na tentativa de execução do programa de transmissão em um ambiente virtual para a sua manipulação. Os esforços técnicos foram dedicados aos seus planos de teste 1 e 2.

4.2) Planos de teste realizados sem contribuições

a. Grupo Fellipe Ribeiro Silva Abib: identificação do eleitor e seu voto a partir do posicionamento dos votos gravados no RDV.

   Justificativa: Os investigadores verificaram os código-fontes dos programas de votação e geração de Boletim de Urna, realizaram algumas votações na urna para verificação da lógica implementada, mas não conseguiram passar pelos mecanismos de segurança para identificar o voto e efetuarem as alterações desejadas.

b. Grupo Jairo Simão Santana Neto: levantar a influência da operação eletrônica da urna, em decorrência de se pressionar suas teclas.

   Justificativa: Os investigadores tiveram acesso aos circuitos elétricos da urna para conectar um osciloscópio para leitura dos sinais elétricos gerados pelo teclado, mas não conseguiram identificar padrões, nesses sinais observados, no intuito de obter as informações necessárias com objetivo de identificar as teclas pressionadas e, consequentemente, o voto.

c. Grupo Luis Antonio Brasil Kowada (Plano de Teste 1): obtenção de chaves criptográficas e avaliar o uso da criptografia para a garantia da integridade, confidencialidade e autenticidade.

   Justificativa: Os investigadores tentaram obter as chaves criptográficas empregando as técnicas utilizadas no TPS anterior e atestaram que os ajustes de segurança implementados não possibilitaram concluir os objetivos propostos.

d. Grupo Luis Antonio Brasil Kowada (Plano de Teste 2): verificar a proteção de programas pré-construídos, necessários ao sistema da urna.

   Justificativa: Foram observados que todos os programas e dados carregados na urna estavam protegidos, não permitindo realizar ou introduzir qualquer alteração.

e. Grupo Luis Fernando de Almeida: analisar a possibilidade de criar rotinas inteligentes, utilizando as técnicas de Machine Learning, capazes de reproduzir o padrão de geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto.

   Justificativa: Os investigadores realizaram uma sequência de votação conhecida para identificar alguma correlação com o registro dos votos na urna. No entanto, não lograram sucesso.

f. Investigador José Fellipe de Moraes Albano: identificação de componentes da rede computacional do TSE de forma a identificar possíveis alvos e disparar ataques específicos contra serviços disponibilizados na rede.

   Justificativa: Os testes ficaram limitados aos enlaces de comunicação para a transmissão do Boletim de Urna. Todas as tentativas de intervenção nos sistemas de conectividade à rede não foram concluídas.

g. Investigador Leonardo Cunha dos Santos: quebra do sigilo do voto por meio de detecção de padrões de comportamento elétrico durante o pressionamento de teclas.

   Justificativa: O investigador realizou algumas intervenções na urna para realizar uma leitura dos sinais elétricos do teclado e, apesar de não ter obtido sucesso no processo de identificação da tecla digitada pelo eleitor, identificou que a urna fica inoperante quando o teclado é desconectado. No entanto, a urna não reporta explicitamente o motivo da falha, muito embora seu sistema operacional continue atuante e registrando eventos.

4.3) Planos de teste realizados com contribuição

a. Grupo Paulo César Herrmann Wanner (Plano de Teste 1): quebrar a criptografia da proteção do sistema gerador de mídia das urnas eletrônicas.

   i. Contribuição:
   O GEDAI (Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica) é responsável por gerar os cartões de instalação das urnas eletrônicas. Quando o GEDAI é executado no ambiente do sistema operacional Windows ele fica sob um programa chamado SIS (Subsistema de Instalação e Segurança) que tem o objetivo de proteger o computador utilizado pela Justiça Eleitoral. O SIS cifra a unidade de armazenamento onde o GEDAI está instalado, utilizando o programa TrueCrypt, constituindo um primeiro nível de barreira de segurança. Neste volume cifrado estão contidos todos os programas, arquivos de configuração e algumas chaves criptográficas utilizadas pelo GEDAI. A chave utilizada para abrir a unidade de armazenamento cifrado é gerada no momento da instalação, por meio de um algoritmo proprietário do TSE.
   Como o equipamento é preparado de forma a ser replicado e instalado em todos os ambientes da Justiça Eleitoral para preparação da urna eletrônica, a cifra não pode ser atrelada ao usuário do sistema em cada

instância da máquina, já que os usuários são da ordem de centenas a milhares, com inevitável rotatividade, tornando inviável a administração de senhas individuais neste cenário. Sendo assim, a senha é gerada durante a instalação e configuração do equipamento, e por princípio fica armazenada no próprio dispositivo de armazenamento da máquina. É fato, portanto, que um invasor, dispondo dos conhecimentos e das técnicas necessárias, poderá obter a chave de cifragem. A eficácia desta proteção é limitada, mas exerce seu papel de barreira suplementar inicial, exigindo tempo e trabalho técnico em uma eventual tentativa de ataque.

Tendo eliminado a barreira da cifragem, a equipe abriu um caminho para tentar ataques contra o próprio SIS para ter o acesso ao GEDAI e as informações associadas.

A equipe demonstrou a esperada viabilidade de se recuperar a senha, gastando pouco mais de um dia de trabalho para seu êxito. Há de se ressaltar que a equipe já atuou nos eventos anteriores do TPS e conhecia com profundidade o sistema a ser atacado, o que contribuiu de sobremaneira o processo.

ii. Impactos:

A cifra da mídia de armazenamento foi comprometida, eliminando uma barreira que dificulta ataques contra o sistema de segurança SIS, fazendo com que haja acesso ao GEDAI.

iii. Extensão:

O ataque expõe o sistema gerador de mídia, sem a proteção do sistema hospedeiro, ou, em outras palavras, expõe o sistema que grava o software da urna na mídia utilizada para instalação, normalmente pertencentes a uma zona eleitoral, que pode abranger um município de pequeno porte ou parte de um município de grande porte.

iv. Contexto:

A inseminação do software das urnas ocorre nas dependências da Justiça Eleitoral (TRE e Cartórios Eleitorais) por pessoal qualificado e autorizado pelo TRE. O evento é previsto no calendário eleitoral, em um ritual público e com a presença de testemunhas de partidos políticos e da sociedade, além de gerar uma ata e relatório eletrônico das urnas inseminadas durante o processo.

b. Grupo Paulo César Herrmann Wanner (Plano de Teste 2): recuperar senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos.

i. Contribuição:

Após o sucesso na execução do plano de teste precedente, a equipe passa à tentativa de ataque ao sistema SIS propriamente dito, de forma a tentar neutralizá-lo e assim o acesso total à aplicação GEDAI, que seria o alvo principal para conseguir alterar o software e os dados que serão instalados no conjunto de urnas de uma zona eleitoral.

Desprovido da cifragem, o conteúdo da mídia de armazenamento do equipamento que roda SIS/GEDAI foi executado como máquina virtual e a equipe concentrou-se em manipular o Registro do sistema operacional Windows, local onde se armazena diversas configurações deste sistema operacional e de suas aplicações, para conseguir neutralizar o SIS. Após conveniente manipulação do registro, a equipe teve sucesso em iniciar a máquina virtual com o sistema SIS neutralizado e assim o acesso direto à aplicação GEDAI.

O SIS faz uma validação de assinatura digital de todos os programas que são executados, mas como ele foi neutralizado, esta validação não foi mais realizada, de modo que foi possível realizar alterações no executável do GEDAI.

A equipe conseguiu executar a aplicação GEDAI sob seu controle, porém as tentativas de gerar alterações no conteúdo a ser inserido na mídia de inseminação das urnas, a própria aplicação GEDAI rejeitou os código/dados alterados, gerando uma condição na urna de não inicialização ou execução correta do seu sistema.

Restringindo severamente as modificações nos arquivos a equipe finalmente conseguiu gerar uma versão de dados que a urna conseguiu executar. A urna, assim configurada, gerou uma zerézima e após a execução dos procedimentos de votação e da finalização gerou um Boletim de Urna (BU) aparentemente válido, sob o aspecto visual do mesário.

As alterações realizadas se limitaram ao nome do município e à Unidade da Federação (UF). No entanto, tais informações são impressas na zerézima e no BU apenas para o controle humano, sendo que os dados efetivamente utilizados na totalização são os códigos numéricos que identificam estes atributos, os quais não puderam ser alterados em função dos mesmos fazerem parte do conjunto de dados

assinados digitalmente pelo TSE e TRE. A Alteração desses códigos gera uma rejeição dos mesmos pelo software da urna em sua verificação inicial, uma vez que a urna realiza a verificação de assinatura dos mesmos.

ii. Impactos:
Os dados de nome do município e da UF que são impressos na zerézima e no BU foram alterados, mas não impactaram no sigilo e contabilização do voto. Esta pequena alteração descritiva dos dados não reflete em uma alteração real do município e UF, onde o voto é registrado, já que a integridade do código se manteve. O sistema de verificação prévia da assinatura de dados da urna não permitiu alteração que pudesse ser prejudicial à contabilização e ao sigilo do voto. O comportamento observado da urna nesta situação é a sua completa inatividade, sem nenhuma condição de operação visível, do ponto de vista do observador externo.

iii. Extensão:
O escopo do ataque é limitado às urnas da zona eleitoral pertinente, contudo há diversos pontos de verificação no processo eleitoral em que a verificação visual ocorre, a começar pelo próprio dia da inseminação. Eventualmente, falhas humanas em tais processos poderiam permitir a preparação de uma urna adulterada chegar à seção eleitoral no dia da eleição, o que certamente atrairia a atenção dos mesários, gerando substituição imediata da urna. Em última análise, caso nem mesmo os mesários notem a adulteração no nome do município e na UF, a votação será realizada sem problemas, com a contabilização correta dos votos e posterior "upload" ao sistema de totalização, sem gerar pendências. Apenas a versão da zerézima e do BU impressas pela urna trarão os nomes do município e UF adulterados.

iv. Contexto:
Há diversos procedimentos públicos, com testemunhas, desde a preparação da urna até o próprio dia da eleição. Diversos agentes dos procedimentos devem contribuir na verificação de conformidade comportamental e visual da urna, mas mesmo que todos falhem sequencialmente na detecção da anomalia, a votação em si não será afetada e tecnicamente a fraude não será consumada.

4.4) Contribuição extra-plano registrada pelos investigadores

a. Alteração do som emitido pela urna eletrônica para os eventos não relacionados à conclusão do voto.

Contribuição:

O investigador reporta que, durante seus testes, notou que a urna, durante sua preparação do início da votação, emite muitas vezes aquele já tradicional som, que aqui chamaremos “som padrão de término de votação”. Tal som é aquele emitido também quando um eleitor conclui o seu voto, que pode ser ouvido pelos mesários e pelos eleitores que estejam relativamente próximos ao local da votação.

O investigador sugere que a emissão desse “som padrão” durante os estágios de preparação, ou manuseio das urnas, no dia da votação pode sugerir aos eleitores eventualmente aguardando na fila o início da votação, de que algum tipo de manipulação de voto na urna possa estar ocorrendo, até mesmo que um conluio de mesários esteja proporcionando uma inserção de votos ilegalmente.

A Comissão Avaliadora concorda com a observação e recomenda que o som emitido durante a inicialização no dia da votação, término da votação, e mesmo nos procedimentos que precedem o dia da votação, seja alterado por um outro absolutamente diferenciado do “som padrão de término de votação”.

b. Remoção do cabo do teclado.

Contribuição

O investigador, durante testes internos da urna, observou que a remoção do cabo do teclado causa o "travamento" da urna. Muito embora a urna continue operando internamente, como pode ser comprovado pelo registro de eventos do sistema, o software atualmente falha em não reportar externamente, no display, a falha específica de mau contato do cabo do teclado. Dentre as falhas observadas em campo, possivelmente alguns casos são devidos ao eventual mau contato deste cabo, especialmente no caso das urnas que têm que ser transportadas a locais remotos para votação.

A sugestão é de que a urna registre no display este caso específico de problema, o que poderá auxiliar as equipes de manutenção no futuro. A urna deverá continuar inoperante, apesar do aviso, mas sem mostrar apenas uma tela branca, o que é bastante desconcertante quando acontece no dia da votação.

5. Recomendações dos Testes Anteriores

As recomendações contidas no Relatório Final da Comissão Avaliadora do TPS/2017 foram objeto de análise dessa comissão, inclusive com realização de reunião com representantes da Secretaria de Tecnologia da Informação/DG/TSE. Após a apresentação da secretaria mencionada, foi fornecida informação atualizada com as providências tomadas, conforme segue abaixo.

5.1) Alterar o nome do Termo de Confidencialidade para Termo de Responsabilidade

O TSE atendeu esta recomendação.
O documento agora é chamado "Termo de Responsabilidade", conforme expresso em edital. Resta pendente ajuste na Resolução, cujo processo (2019.00.000004566-6) está em tramitação.

5.2) Alterar a frase do item 3 do termo de confidencialidade de "bem como obter acesso aos sistemas com o objetivo de copiá-los" para "bem como obter acesso aos sistemas sob análise com o objetivo de copiá-los e/ou transportá-los"

O TSE atendeu esta recomendação.

O Termo de Responsabilidade do TPS/2019 apresenta a redação proposta.

5.3) Alterar a frase do item 7 do termo de confidencialidade de "ou qualquer outro dispositivo de computação móvel" para "ou qualquer outro dispositivo computacional"

O TSE atendeu esta recomendação.

O Termo de Responsabilidade do TPS/2019 apresenta a redação proposta.

5.4) Instituição de um Comitê de Assessoria Perene

O TSE não atendeu esta recomendação.

O tema foi submetido à Comissão Reguladora e esta entendeu que a decisão pela criação da Comissão de Assessoria Perene é de competência da alta administração do TSE. O tema foi submetido. No processo SEI 2019.00.000004566-6, foi incluído o Relatório da Comissão Avaliadora do Teste Público de Segurança 2017 (SEI 1030110) e nele consta, como recomendação, a "Instituição de um Comitê de Assessoria Perene".

5.5) Tornar o exame do software da urna perene e constante, mas mantendo o TPS no formato em que está

O TSE não atendeu esta recomendação.

Existe um projeto novo para abertura do código-fonte, o software da urna, que está em avaliação quanto à viabilidade jurídica. A Portaria TSE nº 444, de 10 de junho de 2019, institui comissão para realizar estudos relativos à viabilidade da publicação do código-fonte do conjunto de software do ecossistema da urna eletrônica na Internet. Para esta eleição, os investigadores poderão acompanhar as alterações dos códigos-fonte após o reteste.

5.6) Estender o TPS para cobrir não apenas ataques computacionais, mas também ataques de engenharia social

O TSE não atendeu esta recomendação.

A Comissão Reguladora entende que o TPS se presta ao exercício dos sistemas eleitorais.

5.7) Estender o TPS para testar elementos em maior profundidade, removendo barreiras existentes de forma a tornar mais eficientes os testes, dado o curto período de tempo disponível

O TSE não atendeu esta recomendação.

A Comissão Reguladora poderá estudar meios de facilitar a realização dos testes pelos investigadores. Não haverá alterações quanto às barreiras de segurança, a flexibilização dessas é desnecessárias para a realização dos ataques.

5.8) Realização de auditorias cientificamente embasadas

O TSE atendeu esta recomendação.

Existe um grupo do TSE (GT – Auditoria, instituído pela Portaria TSE nº 1056, de 05 de dezembro de 2018) realizando estudos para a melhoria das fiscalizações e auditorias do processo eleitoral para o pleito de 2020. As propostas, uma vez concluídas, serão

submetidas ao Ministro relator das resoluções e também submetidas à audiência pública.

5.9) Garantia do acompanhamento das correções do software

O TSE atendeu esta recomendação.

Além da realização do reteste, caso a proposta seja acatada pelo Ministro relator, os investigadores poderão acompanhar a evolução do código-fonte. O reteste está previsto na Resolução TSE nº 23.444, de 30 de abril de 2015, e a minuta de Resolução de Fiscalização e Auditoria, processo SEI 2019.00.000011039-5, prescreve o acesso aos códigos-fonte, nos 6 meses que antecedem o pleito.

5.10) Estudo de ataques via artefatos no processo de compilação

O TSE atendeu esta recomendação.

Foi incluída, na minuta de Resolução de Fiscalização e Auditoria (processo SEI 2019.00.000011039-5), previsão para procedimento de análise dos binários produzidos durante a compilação, com vistas a verificar a sua correspondência ao código-fonte analisado. Além disso, os compiladores utilizados na lacração são de código aberto e amplamente utilizados pela comunidade. Os compiladores são lacrados com o software produzido pelo TSE.

5.11) A lacração dos sistemas deve ocorrer antes do TPS

O TSE atendeu esta recomendação.

Os sistemas submetidos ao TPS são lacrados um mês antes da realização dos testes.

5.12) O TPS deve abranger os sistemas de totalização e biometria

O TSE não atendeu esta recomendação.

As sugestões, no momento, não poderão ser acatadas, haja vista que o sistema RecBU está sendo reescrito para as eleições de 2020 e deverá estar disponível para o TPS 2021. Quanto ao sistema de biometria, da mesma forma, ainda há uma indefinição quanto ao software a ser utilizado nas próximas eleições: Bozorth ou Griaule.

5.13) Eliminar a restrição etária para participação no TPS

O TSE não atendeu esta recomendação.
A responsabilidade penal do participante impossibilita esta opção. Esta questão foi apresentada à Administração (processo SEI 2019.00.000004566-6 – Informação ASSEC nº 23/2019, SEI 1135984).

6. Recomendações

6.1) Atender as recomendações apresentadas por esta Comissão Avaliadora em seus Relatórios de Avaliação elaborados ao final dos Testes Públicos de Segurança anteriores.

6.2) Instituir um Comitê de Assessoria Perene. Tendo em vista que os ajustes nos sistemas eleitorais são realizados de forma continuada por conta das atualizações tecnológicas e informes de segurança apresentados, seria recomendável que houvesse uma avaliação técnica acompanhando as decisões de modificações propostas, não se limitando ao evento do TPS. Desta forma, poderia haver uma contribuição mais significativa para as propostas para o TPS.

6.3) Realizar reunião virtual e presencial previamente ao TPS, bem como após o mesmo, contando com a participação da Comissão Reguladora e dos investigadores. Os investigadores novos no processo necessitam muito tempo para conhecer o sistema eleitoral e os seus componentes (hardware, software e procedimentos). Uma reunião técnica poderia acelerar o processo de esclarecimento, permitindo aos investigadores um conjunto maior de oportunidades para identificar as possíveis vulnerabilidades e elaborar planos mais precisos.

6.4) Quanto ao processo de desenvolvimento:

a. implantar processo de desenvolvimento seguro de software (apontado como recomendação já no TPS/2017). O ciclo de vida do desenvolvimento seguro é um processo que consiste na inserção de várias atividades e produtos relacionados a segurança na fase de desenvolvimento de software como modelagem de ameaças, análise estática do código com uso de ferramentas, revisão de código, testes de segurança direcionados e uma revisão final de segurança, minimizando o surgimento de vulnerabilidades.

b. Obter certificados com consultorias independentes e reconhecidas internacionalmente para processo de desenvolvimento seguro de software fará com que o TSE seja publicamente credenciado em práticas adequadas e reconhecidas internacionalmente.

c. Realizar auditorias cientificamente embasadas. Auditorias cientificamente fundamentadas são a base da forense computacional, especialidade de segurança computacional voltada para a verificação do funcionamento esperado de um sistema e da detecção de eventuais comportamentos estranhos ao mesmo, com base nos rastros (não limitados a arquivos de log) que toda execução de software provoca em um sistema computacional, seja em sistemas

de arquivos, seja em memórias internas a dispositivos computacionais. Princípio fundamental do processo é o exame de dispositivos de armazenamento não no sistema sob análise, mas sim em sistema de confiança. Semelhantemente, a análise de dispositivos internos deve utilizar o processador do sistema sob análise, mas rodando sistema operacional e utilitários confiáveis, portanto externos ao mesmo. Em contraste, as rotinas de verificação hoje disponíveis na urna não obedecem tais princípios.

d. Tornar o exame do software da urna perene e constante, mas mantendo o TPS no formato em que está. Esta comissão entende que o processo de análise e busca de vulnerabilidades devem ser contínuos, com organizações acadêmico-científicas que demonstrem competência e disponibilidade de recursos humanos (tipicamente alunos de pós-graduação e pesquisadores experientes). A extensão natural do mesmo seria a disponibilização do código-fonte de forma aberta, entretanto a maioria dos testes exige também o acesso ao hardware, algo que é mais facilmente viabilizado em instituições de ensino e pesquisa. Somente com o aumento do tempo de exposição ao código e entendimento do sistema é que é possível elaborar testes mais complexos que permitam descobrir vulnerabilidades mais sofisticadas. O TPS em si poderia ser utilizado como uma ocasião para demonstração de provas de conceito e troca de experiências entre equipes de investigadores.

6.5) Quanto ao código fonte:

a. Disponibilizar o código fonte dos sistemas eleitorais, objeto deste TPS/2019, para consulta pública logo após a cerimônia de lacração do código.

   Foi observado que os investigadores dispõem de escasso tempo para familiarizar-se com o código fonte dos sistemas objeto dos testes. Considerando-se que isto pode ser fator determinante do fracasso de planos de ataque, mascarando, assim, o devido diagnóstico da segurança dos sistemas eleitorais e, portanto, gerando falsa sensação de segurança, recomenda-se que as inscrições para o TPS possam ocorrer antes do pleito anterior, possibilitando sua participação nos eventos da abertura dos sistemas das Eleições a partir de 180 dias antes do primeiro turno, além de permissão de consulta aos códigos-fonte nas dependências da unidade da Justiça Eleitoral mais próxima.

b. Convidar para participar da cerimônia de lacração do código, inclusive colocando suas assinaturas digitais, aqueles investigadores que obtiverem sucesso, ainda que parcial, em algum de seus planos de ataque e que

retornarem para verificar e atestar se o problema apontado foi devidamente corrigido.

6.6) Quanto ao processo de inscrição e de seleção:

Realizar levantamento nas redes sociais, antes da abertura das inscrições em cada TPS, questionando se há vulnerabilidades no sistema eleitoral eletrônico para que aqueles que apresentarem razões minimamente consistentes sejam convidados a participar do próximo TPS, pré-vinculando seus planos de ataque ao teor de suas alegações na mídia. Oferecer-se-ia, inclusive, a opção de montagem de grupo com integrantes de sua livre escolha, respeitadas as vedações constantes do edital (idade, nacionalidade etc).

6.7) Quanto à ampliação do objeto do TPS:

a. Estender o TPS para testar elementos em maior profundidade, possibilitando a remoção prévia das barreiras existentes de forma a tornar mais acessível o ponto específico dos testes. Em razão do exíguo tempo disponível durante o TPS, para se realizar uma análise de segurança em profundidade, propõe-se que parte das barreiras de segurança existentes sejam seletivamente removidas, de forma a expor subsistemas mais internos à ação dos investigadores. Como segurança computacional é normalmente obtida com várias camadas ou níveis de profundidade, assim também os testes de segurança deveriam ser capazes de verificar individualmente cada barreira, de forma a que se possa aperfeiçoá-la, independentemente das demais existentes. Um sistema assim aperfeiçoado estará muito mais eficaz para resistir a ataques mais elaborados e complexos, ou seja, aqueles em que os atacantes disponham de mais tempo de análise do sistema-alvo e de preparação do ataque.

b. Estender o TPS para cobrir não apenas ataques computacionais, mas também ataques de engenharia social. Muitos sistemas computacionais acabam sendo atacados com sucesso justamente através das pessoas que detêm acesso mais privilegiado aos mesmos. Efetivamente são ataques indiretos, contra o que se convenciona chamar o elo mais fraco, no caso as pessoas. A literatura é plena de exemplos de casos assim, sob o nome de phishing scam ou spear phishing. Trata-se de se desferir ataques que tentam convencer pessoas a involuntariamente executar código estranho malicioso, comprometendo a máquina de um usuário interno à infraestrutura do TSE/TREs e estabelecendo uma "cabeça de ponte" para o atacante elaborar ataques precisos e sofisticados contra alvos internos geralmente desprotegidos das ferramentas usuais de defesa.

c. Ampliar o objeto de testes do TPS, incluindo os sistemas elencados no edital do TPS/2019 Art. 2º §2º incisos I a VII e IX, a saber: identificação e verificação biométrica do eleitor; preparação e infraestrutura para o Kit JE Connect; processamento dos arquivos de urna (fase posterior às fases de transmissão e

de recebimento dos arquivos gerados pela urna eletrônica após o encerramento da votação na seção); totalização (TOT) e gerenciamento da totalização (GER); acesso às máquinas servidoras; acesso aos bancos de dados; ataques de negação de serviço; sistema de geração de chaves criptográficas.

6.8) Quanto ao ambiente de realização do TPS:

a. Organizar as baias e mesas de trabalho dispondo os monitores de forma privativa para os investigadores, em conformidade com os termos de confidencialidade por eles assinados. Os testes devem ser realizados de forma reservada, possibilitando um ambiente mais controlado, o sigilo e a tranquilidade para o seu procedimento, o qual deverá ser acompanhado pela equipe reguladora.
b. Melhorar o sistema de registro de solicitação de apoio técnico. Considerar a possibilidade de que a equipe de apoio técnico disponha de tablets para abrir vídeo-chamadas, ou chats, para que os investigadores prontamente entrem em contato com o responsável técnico. A Comissão Avaliadora deverá ter acesso em tempo real (em meios digitais ou em papel) às solicitações realizadas pelos investigadores e às respectivas respostas.

c. Disponibilizar para Comissão Avaliadora acesso WiFi através de SSID próprio e não pelo SSID TSE-EVENTOS. A estrutura computacional destinada à Comissão Avaliadora deverá estar pronta e disponível com antecedência.

d. Permitir a troca de informação ('brainstorm') entre os investigadores para maximizar o potencial criativo. Para tanto, determinar horários específicos para curtos intervalos, com deslocamento físico a ambiente adequado, acompanhados do apoio técnico, que registre tal intercâmbio e certifique-se de que constem os devidos créditos naqueles planos de ataque que alcancem sucesso com o auxílio de tal intercâmbio.

6.9) Quanto às modificações nos sistemas objeto do TPS

a. O ataque à cifragem da mídia de armazenamento do sistema GEDAI revelou que a barreira implementada pelo sistema proteção SIS e de criptografia (TrueCrypt) e o método de armazenamento de chaves não é muito eficaz. Portanto, recomenda-se uma revisão profunda do ambiente operacional e dos mecanismos de proteção necessários para que o GEDAI possa estar instalado de forma segura e confiável para cumprir a sua função de preparação de mídias para a urna eletrônica. Evitar o uso de produtos descontinuados, como é o caso do TrueCrypt, ou aqueles que não estejam validados especificamente e que sejam comprovadamente seguros e confiáveis. As chaves de criptografia devem ser armazenadas usando equipamentos de segurança para armazenamento de chaves, como HSM (Hardware Security Modules).

b. Diferenciar o som de aviso, emitido durante a inicialização no dia da votação, bem como ao término da votação, e também nos procedimentos que precedem o dia da votação, seja selecionado para um outro distinto do som padrão de aviso emitido quando o eleitor conclui o seu voto. O objetivo é de que a emissão dos referidos avisos de inicialização e término, entre outros, não seja confundida com o aviso de que foi inserido novo voto na urna, visto que a população já assimilou tal som como sendo o de término de inserção do voto.

c. Mostrar, no display, aviso de que o cabo do teclado "se desconectou", caso a urna identifique mau contato no cabo do teclado. Contudo, a urna deve continuar inoperante.

6.10) Publicar, em formato físico e eletrônico, compêndio da documentação produzida e conclusões desta Comissão Avaliadora, conforme disposto no inciso II do artigo 20 da Resolução 23.444/2015 do TSE.

Brasília/DF, 10 de dezembro de 2019.

COMISSÃO AVALIADORA DO TESTE PÚBLICO DE SEGURANÇA 2019