

Relatório da Comissão Avaliadora do Teste Público de Segurança 2017

1.Introdução

A Comissão Avaliadora designada pela Portaria TSE 565, de 3 de agosto de 2017, possui as atribuições de validar a metodologia e os critérios de julgamento definidos para o Teste de Segurança.

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

2.Metodologia

Foram disponibilizados equipamentos e componentes de software para a realização do teste cujas versões podem ser encontradas a seguir:

- Equipamento: Computador SIS¹ utilizado para execução dos softwares GEDAI-UE²

- Softwares instalados:
 - Windows 7 64 bits
 - SIS versão 1.60
 - GEDAI-UE versão “A Hora da Estrela”

- Equipamento: Computador Dual Boot³ para uso genérico dos investigadores

- Softwares instalados:
 - Windows 7 64bits
 - Linux Ubuntu 16.04 64bits

- Equipamento: Computador utilizado para inspeção e consulta de códigos fontes

- Softwares instalados:
 - Windows 7 64bits, ○ Linux Ubuntu 16.04 64bits ○ Elipse CDT versão Neon 4.6.0 ○ Astah versão 6.9.0 ○ Cppcheck versão 1.72
 - Flawfinder versão 1.31

- Equipamento: Computador para acesso à Internet

- Softwares instalados:

¹ Computador SIS: Computador com sistema operacional Windows 7 64bits e Sistema de Gerenciamento de Segurança (SIS) da Justiça Eleitoral.

² GEDAI-UE: Sistema de geração de mídias para a urna eletrônica.

³ Computador Dual Boot: Computador preparado para iniciar com o sistema operacional Windows 7 64bits ou Linux Ubuntu 16.04 64bits.

- Windows 7 64bits

- Equipamento: Kit JEConnect⁴

- Softwares instalados:
 - SO Linux versão 2017.9.29.SP ○ APP JEC versão 2017-1795-BSB
 - Transportador versão 17.9.6

- Equipamento: Servidor utilizado para execução dos softwares RecArquivos⁵ e InfoArquivos⁶

- Softwares instalados:
 - RecArquivos versão 17.9.3 ○ InfoArquivos versão 17.9.0

Os critérios de análise utilizados na avaliação dos testes foram:

- 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.

3. Planos de Teste

Foram apresentados planos de teste de 4 investigadores individuais e 3 grupos de investigadores. As propostas foram as

seguintes: **3.1) Investigador Individual:**

Cassio Goldschmidt

- Proposta: encontrar erros e vulnerabilidades no software responsável pela carga das urnas eletrônicas (GEDAI-UE) que possibilitem a inserção de código dentro desse sistema, a fim de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados e dos sistemas responsáveis pela votação eletrônica.

3.2) Investigador Individual: José Carlos Gama Quirino

- Proposta: ataques genéricos à urna eletrônica, na tentativa de comprometer a integridade e o anonimato do voto.

⁴ Kit JEConnect: Conjunto de aplicativos para a transmissão de dados extraídos da urna eletrônica.

⁵ RecArquivos: Sistema de recebimento de arquivos transmitidos.

⁶ InfoArquivos: Sistema de registro de arquivos recebidos.

3.3) Investigador Individual: **Marcelo dos Anjos**

- Proposta A: Atacar o hardware de segurança da urna eletrônica com a intenção de extrair desse dispositivo informações confidenciais do sistema de votação eletrônico.
- Proposta B: Alterar dados de votação da urna eletrônica por meio de ataque ao sistema responsável pela transmissão dos arquivos de urna.

3.4) Investigador Individual: **Rodrigo Cardoso Silva**

- Proposta A: Invadir o sistema responsável pela recepção dos arquivos de urna eletrônica a partir de ataques ao sistema de transmissão desses mesmos arquivos.
- Proposta B: Explorar vulnerabilidades do sistema operacional que roda na urna eletrônica, podendo por meio dele alterar ou prejudicar os sistemas e os dados contidos na urna.

3.5) Grupo de Investigadores: **Diego de Freitas Aranha (Coordenador)**

- Componentes do Grupo: Caio Lúders de Araujo, Paulo Matias, Pedro Yóssis Silva Barbosa, Thiago Nunes, Coelho Cardoso.
- Proposta A: Capturar a chave secreta da urna eletrônica, por meio de ataques ao cartão de memória utilizado para fazer carga nas urnas.
- Proposta B: Atacar os equipamentos e sistemas responsáveis pela recepção e transmissão dos arquivos de urna eletrônica.
- Proposta C: Encontrar vulnerabilidades no algoritmo de aleatoriedade do Registro Digital do Voto (RDV), buscando fragilizar o sigilo do voto.
- Proposta D: Atacar a urna eletrônica executando sistema malicioso, por meio das entradas USB do equipamento.
- Proposta E: Execução de código estranho de impressão na urna eletrônica.
- Proposta F: Violação do sigilo do voto individual sensível.
- Proposta G: Violação da integridade do software de votação.

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

- Componentes do Grupo: Gabriel Cardoso de Carvalho, Ramon Rocha Rezende e Victor Faria de Souza.
- Proposta: Avaliar se os procedimentos de gerenciamento da chave secreta da urna eletrônica garantem a confidencialidade e a autenticidade necessárias.

3.7) Grupo de Investigadores: **Ivo de Carvalho Peixinho (Coordenador)**

- Componentes do Grupo: Fábio Caus Sicoli e Paulo Cesar Hermann Wanner.

- Proposta: Executar o software da urna eletrônica em um computador e, a partir daí, tentar extrair a chave secreta da urna eletrônica.

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 foram classificados em: não realizados, realizados sem contribuição e realizados com contribuição para melhoria do sistema e apresentados a seguir.

a) Planos de teste não realizados

- a.1. Investigador Marcelo dos Anjos: Teste invasão hardware/software (Proposta A);
- a.2. Investigador Marcelo dos Anjos: Alteração de dados da votação (Proposta B);
- a.3. Grupo Diego Aranha: Execução remota de código na plataforma web (Proposta B);
- a.4. Grupo Diego Aranha: Tentativa de violação do sigilo do voto (Proposta C);
- a.5. Grupo Diego Aranha: Inserção de dispositivo USB malicioso (Proposta D);

b) Planos de teste realizados sem contribuições

- b.1. Investigador Rodrigo Cardoso Silva: Programa Transportador de Arquivos – “teste Doodle” e Uenux e softwares básicos Metamorfose (Kafka).
 - . Justificativa: O investigador não conseguiu cumprir o objetivo nestes dois planos de testes propostos e não houve nenhuma contribuição.
- b.2. Investigador José Carlos Gama Quirino: Ataque aos sistemas dos hardwares e softwares da urna eletrônica.
 - . Justificativa: O investigador não conseguiu cumprir o objetivo nos testes propostos, e não houve nenhuma contribuição.
- b.3. Grupo Luís Antonio Brasil Kowada: Análise do uso dos procedimentos criptográficos.
 - . Justificativa: O investigador não conseguiu cumprir o objetivo nos testes propostos, e não houve nenhuma contribuição.

c) Planos de teste realizados com contribuição

c.1. Investigador Cássio Goldschmidt: Revisão de código e teste dinâmico de geração das mídias para a preparação da urna eletrônica (GEDAI-EU).

. Contribuição: O investigador não conseguiu cumprir o objetivo proposto neste plano de teste. No entanto, apontou alguns itens de não conformidade com boas práticas do mercado, que, no entender da comissão avaliadora, devem ser considerados pela equipe técnica do TSE na revisão dos processos adotados.

c.2. Grupo Diego Aranha (Proposta A): Capturar a chave secreta da urna eletrônica, por meio de ataques ao cartão de memória utilizado para fazer carga nas urnas.

. Pontos de Intervenção: ataque à criptografia do sistema de arquivos do cartão de memória. Os resultados obtidos da execução do plano de teste não violaram a destinação e/ou anonimato dos votos.

. Impactos: Obtenção da chave criptográfica do cartão de memória que realiza a carga do sistema da urna devido ao acesso à chave que estava no código-fonte de testes e também em porção desprotegida do sistema de arquivos do cartão. A decifração do cartão de memória de carga permite a inspeção de partes críticas do software e vazamento de outras chaves criptográficas sensíveis.

. Extensão: Aplica-se ao sistema eletrônico de votação em caso de obtenção de todas as chaves de proteção do sistema.

. Contexto: Um eventual atacante precisa se valer de dois momentos de intervenção, um durante a pós-lacração de códigos-fonte, um em instante após geração de mídias e antes do processo de carga.

c.3. Grupo Diego Aranha (Proposta E, apresentada durante o teste): Execução de código estranho de impressão na urna eletrônica.

. Pontos de Intervenção: ataque a biblioteca de registro de histórico de atividades (*log*) contida no sistema eletrônico de votação após verificação que esta não estava assinada.

. Impactos: possibilidade de alteração de parâmetros e de funcionalidades da biblioteca, onde foi alterado o formato de mensagem de log e inserido um texto anômalo na inicialização do sistema. Os resultados obtidos da execução do plano de testes não violaram a destinação e/ou anonimato dos votos.

. Extensão: Aplica-se ao sistema eletrônico de votação podendo impedir que o sistema continue operando.

. Contexto: Um eventual atacante precisa se valer de dois momentos de intervenção, um durante a pós-lacração de códigos-fonte, um em instante após geração

de mídias e antes do processo de carga. Também se faz importante relatar que sistemas de verificação de assinaturas dos sistemas instalados como Verificador Pré-Pós eleição poderiam identificar a adulteração nas bibliotecas.

c.4. Grupo Diego Aranha (Proposta F, apresentada durante o teste): Violação de sigilo de voto individual sensível.

. Pontos de Intervenção: ataque a biblioteca utilizada para cifrar o arquivo RDV contida no sistema eletrônico de votação após verificação que esta não estava assinada.

. Impactos: possibilidade de decifração do arquivo RDV possibilitando uma possível quebra do sigilo do voto se for possível acumular sucessivas versões do arquivo, antes e depois de cada voto.

. Extensão: Aplica-se ao sistema eletrônico de votação, em especial ao sigilo do voto.

. Contexto: em que se pese a demonstração de factibilidade de execução das etapas propostas, faz-se importante notar que no contexto de um processo eleitoral real, um eventual atacante precisa se valer dos seguintes momentos de intervenção—que são aqueles que permitem interferência no processo eleitoral: (a) pós-lacração de códigos-fonte e geração de chaves criptográficas, para entendimento das lógicas dos processos criptográficos e obtenção de chaves; (b) instante após geração de mídias e antes do processo de carga para comprometimento de arquivo binário específico; (c) sessão eleitoral durante o processo eleitoral. Também se faz importante relatar que sistemas de verificação de assinaturas dos sistemas instalados como Verificador Pré-Pós eleição poderiam identificar a adulteração nas bibliotecas.

c.5. Grupo Diego Aranha (Proposta G, apresentada durante o teste): Violação da integridade do software de votação.

. Pontos de Intervenção: ataque a biblioteca utilizada no sistema eletrônico de votação após verificação que esta não estava assinada.

. Impactos: possibilidade de interferência no funcionamento do sistema eletrônico de votação através da alteração de uma mensagem constante na tela da urna.

. Extensão: Aplica-se ao sistema eletrônico de votação.

. Contexto: em que se pese a demonstração de factibilidade de execução das etapas propostas, faz-se importante notar que no contexto de um processo eleitoral real, um eventual atacante precisa se valer dos seguintes momentos de intervenção—que são aqueles que permitem interferência no processo eleitoral: (a) pós-lacração de códigos-fonte e geração de chaves criptográficas, para entendimento das lógicas dos processos criptográficos e obtenção de chaves; (b) instante após geração de mídias e antes do processo de carga para comprometimento de arquivo binário específico; (c) sessão eleitoral durante o processo eleitoral. Também se faz importante relatar que

sistemas de verificação de assinaturas dos sistemas instalados como Verificador Pré-Pós eleição poderiam identificar a adulteração nas bibliotecas.

c.6. Grupo Peixinho: Executar o software da urna eletrônica em um computador e, a partir daí, tentar extrair a chave secreta da urna eletrônica.

. Pontos de Intervenção: ataque ao sistema de inicialização da urna e obtenção da chave criptográfica utilizada pelo módulo do *kernel*.

. Impactos: possibilidade teórica de construção de programa que assine os produtos de uma urna (modelo anterior a 2009, sem MDS⁷), que provavelmente seria aceito pelo totalizador.

. Extensão: Aplica-se ao sistema eletrônico de votação.

. Contexto: em que se pese a demonstração de factibilidade de execução das etapas propostas, faz-se importante notar que no contexto de um processo eleitoral real, um eventual atacante precisa se valer dos seguintes momentos de intervenção—que são aqueles que permitem interferência no processo eleitoral: (a) pós-lacração de códigos-fonte e geração de chaves criptográficas, para entendimento das lógicas dos processos criptográficos e obtenção de chaves; (b) instante após geração de mídias e antes do processo de carga para comprometimento de arquivo binário específico; (c) sessão eleitoral durante o processo eleitoral. Também se faz importante relatar que sistemas de verificação de assinaturas dos sistemas instalados como Verificador Pré-Pós eleição poderiam identificar a adulteração nas bibliotecas.

5.Recomendações

1) Alterar o Termo de Confidencialidade para Termo de Responsabilidade:

- a. Alterar o nome do Termo de Confidencialidade para Termo de Responsabilidade;
- b. 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”;
- c. Alterar a frase do item 7 do termo de confidencialidade de “ou qualquer outro dispositivo de computação móvel” para “ou qualquer outro dispositivo computacional”.

2) Instituição de um Comitê de Assessoria Perene:

- a. Esta recomendação é uma reiteração de recomendação de 2016;

⁷ MDS: Módulo de segurança em hardware.

- b. Recomenda-se que este Comitê seja formado por membros da comunidade (não apenas científica) com o objetivo de propor novos mecanismos de segurança e maneiras possíveis de se implementá-los;
- c. Esta comissão terá necessidade de uma interface dentro do TSE para viabilizar o trânsito necessário de informações e, para tanto, terá a incumbência de indicar um grupo de apoio dentro do TSE;
- d. Terá como atribuições a avaliação do processo eleitoral, observando a aplicação das recomendações de segurança propostos, e o aprimoramento da transparência de todo o processo;
- e. Além dos desafios supracitados, resgata-se aqui uma recomendação de 2016 com relação à certificação do processo seguro de desenvolvimento de software, que já havia sido apontada inclusive por volta de 2002.

3) Aprimoramento dos Testes Públicos de Segurança:

- a. Tornar o exame do software da urna perene e constante, mas mantendo o TPS no formato em que está. Incentivar via workshops e campanhas o pré-estudo com acesso completo ao software (idealmente disponível via Internet, mas em não se conseguindo isso, da maneira como é, com acesso físico apenas). Assim, as equipes poderiam vir mais bem preparadas para os dias do teste, sendo muito mais eficazes durante os poucos 3 dias de contato com os sistemas físicos e software real em operação. Este procedimento serve também para que a Justiça Eleitoral analise o processo como um todo e possibilite o aprimoramento contínuo do sistema. Disponibilizar o histórico completo de software do SVE desde sua concepção, acessível via controle de versões.
- b. Estender o TPS para cobrir não apenas ataques computacionais, mas também ataques de engenharia social. A ideia seria disponibilizar um diagrama completo de toda a hierarquia de pessoas/funções envolvidas na produção do software, no registro nos TREs, na inseminação das urnas, na operação do dia da votação e na apuração. A descrição da hierarquia e procedimentos estaria disponível bem antes, de forma que durante os dias do TPS os testes sejam mais eficientes. O laboratório para testes de engenharia social deveria oferecer equipamentos e rede montados e operacionais, assim como pessoas treinadas em cada função. As equipes contariam com o auxílio de seus componentes para ajudar a cumprir os diferentes papéis concebidos para experimentação e ataque. Em cada etapa ou cada ação enfraquecedora da cadeia de confiança do sistema, as ações possíveis e/ou suposições válidas, como por exemplo cooptar alguma pessoa em algum papel, devem ser registradas, de forma a se obter no resultado a descrição completa da superfície de ataque e de seus facilitadores de penetração.
- c. 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. Um exemplo prático é disponibilizar versões da urna operando com mídia em texto claro.

Motivação: do jeito como está, os testadores perdem tempo precioso dos três dias subvertendo as primeiras barreiras, sobrando muito pouco tempo ao final para desferir ataques em maior profundidade, dessa forma impedindo testes necessários para os casos em que atacantes reais consigam subverter previamente as barreiras existentes.

4) Realização de Auditorias Cientificamente Embasadas:

- a. Aprimorar a realização de auditorias do ponto de vista científico. Hoje a auditoria de 2% de urnas com eleição aberta impõe, por questões de logística, uma janela significativa de tempo que, somada aos relatos de precariedade dos lacres e de falsa sensação de segurança dada pela assinatura física dos juízes, suscita grande desconfiança da opinião pública em geral e dos especialistas em segurança em particular.
- b. Garantir independência da equipe de auditoria em relação ao TSE.

5) Garantia do Acompanhamento das Correções dos Softwares:

- a. Garantir acompanhamento na implementação de correções decorrentes do TPS ou de eventuais bugs descobertos internamente, de forma que haja ciência por parte das equipes das modificações realizadas entre o TPS e a assinatura do SVE, com sessão de diffs⁸ entre arquivos, processo de compilação e nova assinatura.

6) Estudo de Ataques via Artefatos no Processo de Compilação:

- a. No dia da assinatura do código, instanciar um sistema operacional padrão de repositório bem conhecido, instanciar um toolkit de compilação com versões de componentes bem reconhecidos pela comunidade e daí proceder à compilação e assinatura.

7) A Lacração dos Sistemas Deve Ocorrer Antes do TPS:

- a. Reitera-se recomendação de 2016;
- b. Recomenda-se que o tempo de inspeção de código seja da ordem de seis meses antes do TPS.

8) O TPS deve Abranger os Sistemas de Totalização e Biometria:

- a. Reitera-se recomendação de 2016.

9) Eliminar a Restrição Etária para Participação no TPS:

- a. Reitera-se a recomendação de 2016;
- b. Deve existir um Termo de Responsabilidade específico.

6. Comentários adicionais

⁸ diffs: diferenças observadas nos arquivos manipulados.

Abstraindo-se dos detalhes de cada teste, pode-se tecer comentários sobre as causas das vulnerabilidades encontradas, suas implicações e especulações sobre os motivos que levaram às suas presenças nesta instância do TPS.

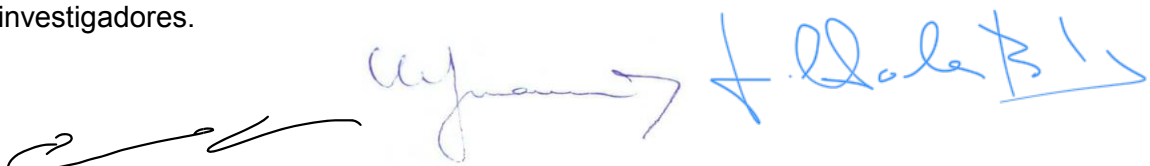
Em primeiro lugar, o fato de a chave criptográfica do sistema de arquivos estar disponível em arquivo componente do código fonte evidencia apenas uma falha na preparação do ambiente de teste (TPS), que não traz nenhuma implicação com o SVE como um todo e seu uso nas eleições propriamente ditas.

Em segundo lugar, devido ao fato de que nem todas as urnas dispõem de HSM (Hardware Security Module), é necessário que o software da urna—que é único para todas as versões de hardware da urna—contenha a chave criptográfica em "texto claro" em alguma localização na mídia de execução na fase de boot da urna, durante pelo menos algum período dessa fase. Apesar da cifragem do sistema de arquivos ser uma técnica eficaz para dificultar a ação de intrusos em várias aplicações computacionais, o cenário de utilização da urna eletrônica impõe limitação em sua eficácia, sendo condição conhecida do sistema. Mesmo assim, constitui-se em primeira linha de defesa a eventuais ataques, requerendo tempo/esforço extra aos atacantes. Questões de logística também trazem muitas implicações à operação das urnas, visto que elas são frequentemente substituídas por variados motivos técnicos e procedimentais (tais como a realização da eleição aberta como mecanismo de auditoria), o que sugere que a diferenciação de chaves no sistema de arquivos não deva ser mais granular que uma chave por local de votação.

Em terceiro lugar, as demais vulnerabilidades exercitadas com sucesso—omissão de assinatura digital ou sua verificação em arquivos chave do sistema, ou possivelmente de sua totalidade—ou vulnerabilidades apenas indicadas pelos investigadores—como a não-conformidade com algumas boas práticas do mercado—evidenciam duas conclusões:

- 1) A urna eletrônica atual dispõe de mecanismos de software capazes de prover elevada segurança e integridade ao seu funcionamento. Tais mecanismos são bastante reforçados quando acoplados a mecanismo de segurança de hardware (HSM) disponível na maior parte das unidades (urnas pós2009).
- 2) O processo de desenvolvimento de software do SVE tem ainda um longo caminho até ser considerado seguro segundo as boas práticas do mercado, em geral, e segundo as recomendações as boas práticas científicas de aplicações críticas como esta, em particular.

Resumidamente, pode-se afirmar que nenhuma das vulnerabilidades apontadas neste TPS poderia ser exercitada com o atual estado tecnológico de desenvolvimento do software da urna, caso o TSE tivesse seguido com maior rigor as boas práticas do mercado. É conveniente ressaltar que os resultados apresentados não eximem a possibilidade da existência de outras vulnerabilidades não identificadas pelos investigadores.

The image shows two handwritten signatures. The first is a black ink signature on the left, and the second is a blue ink signature on the right. The blue signature appears to be 'Walter B.' with a stylized arrow pointing to the right.