1 Introdução

A democracia brasileira, retomada na recente História pátria e consolidada com as práticas recompostas sob o legítimo império da Constituição “cidadã” de 1988, apresenta, como ponto de apoio central, o momento da votação. Neste, cada cidadão no exercício de seus direitos políticos pode manifestar sua opinião político-partidária na escolha de representantes, em um processo eleitoral que alcança, no Brasil, mais de 130 milhões de pessoas.

Considerando que esse delicado e importante momento de uma nação é realizado, no Brasil, por sistemas eletrônicos, e visando ao seu aprimoramento e transparência,

o Excelentíssimo Senhor Presidente do Tribunal Superior Eleitoral, Ministro Carlos Ayres Britto, comunicou aos interessados, por meio do edital publicado no DOU de 4 de setembro de 2009, que seriam realizados testes públicos de segurança no sistema eletrônico de votação, informando, ainda, que,

> CAPÍTULO I - DO OBJETO
>
> Art. 1º Constitui objeto do presente edital a realização de testes públicos de segurança no sistema eletrônico de votação a ser utilizado nas eleições gerais no ano de 2010.
>
> CAPÍTULO II - DO OBJETIVO
>
> Art. 2º Os testes de segurança têm como objetivo o aperfeiçoamento do sistema eletrônico de votação.
>
> Parágrafo único - Constitui escopo dos referidos testes verificar a segurança dos seguintes elementos do processo eletrônico de votação: dispositivos de segurança agregados aos produtos emitidos pela urna eletrônica; procedimento da geração de mídias; etapas de preparação das urnas eletrônicas, do hardware das urnas eletrônicas, do lacre físico, dos dispositivos de logística que protegem as urnas, das mídias eletrônicas,

do conteúdo das mídias de dados e do software de votação usado nas seções eleitorais.

CAPÍTULO III - DAS DEFINIÇÕES

Art. 3º Para fins deste edital considera-se:

I - Teste de segurança: conjunto de métodos e técnicas utilizados para atacar o sistema eletrônico de votação, com vistas a explorar eventuais vulnerabilidades do sistema, com o objetivo de violar a integridade e/ou o sigilo do voto;

II - Falha: evento em que se observa que um sistema violou sua especificação por ter entrado em um estado inconsistente e imprevisto ocasionado por uma imperfeição (defeito) em um software ou hardware que impede seu bom funcionamento, porém sem interferir na destinação e/ou sigilo dos votos dos eleitores;

III - Fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou sigilo dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis.

E, no mesmo, constou também, como atribuição da Comissão Avaliadora,

III - Produzir o relatório final, que conterá a descrição dos testes, os resultados obtidos, a análise dos resultados e as conclusões.

2 Descrição dos Testes e Resultados Alcançados

Visto que o objetivo dos testes é o aperfeiçoamento do sistema eletrônico de votação, foi solicitado que todos os interessados em participar como investigadores preenchessem um formulário descrevendo seu plano de teste. Essa medida visa ao rigor científico, à reprodutibilidade dos testes, avaliação de competência da equipe, aderência da proposta ao edital, bem como permitir ao TSE documentar o processo judicial, a preparação do ambiente e a disponibilização dos recursos necessários para sua execução.

Do plano de teste (vide formulário anexo) consta seu escopo, fundamentação, a janela de atuação, durante o ciclo do processo eleitoral, na qual as ações associadas seriam realizadas, o resultado esperado e os recursos necessários.

A seguir são relacionados resumidamente os planos de testes executados e seus resultados, sendo que as descrições detalhadas encontram-se anexas.

2.1 Investigador: Sérgio Freitas da Silva

Objetivo:

Demonstrar a interceptação da radiação eletromagnética emitida pelo teclado da urna eletrônica através de receptores de rádio específicos. Esta radiação será rastreada, capturada, digitalizada e armazenada num arquivo digital para comprovar a materialidade do fenômeno e o risco de quebra do sigilo do voto.

Sistemas afetados: urna eletrônica

Resultados:

O investigador obteve sucesso nos ensaios tais quais propostos no ambiente de testes (vide plano de testes respectivo).

2.2 Investigador: Carlos Eduardo Negrão de Oliveira (Tribunal Superior do Trabalho)

Objetivo:

Demonstrar a alteração do boletim de urna substituindo a impressora da urna eletrônica.

Sistemas afetados: urna eletrônica

Resultados:

O investigador não obteve sucesso nos ensaios na forma constante da proposta original.

2.3 Investigador: Divailton Teixeira Machado (Superior Tribunal de Justiça)

Objetivos:

1. Executar ataque de negação do serviço em uma determinada urna eletrônica;
2. quebrar o sigilo do voto por meio da análise de logs dos sistemas eleitorais.

Sistemas afetados: Gerador de mídia e urna eletrônica.

Resultados:

O investigador não obteve sucesso na sua tentativa de quebra de sigilo eleitoral, sobrepujando os mecanismos de aleatoriedade do preenchimento do registro digital dos votos.

2.4 Investigador: Valter Monteiro Jr. (Marinha do Brasil)

Objetivo:

Introduzir o código malicioso em mídias digitais, na urna eletrônica ou em qualquer servidor do sistema de votação.

Sistemas afetados: Procedimentos, gerador de mídia, urna eletrônica.

Resultados:

Os investigadores não obtiveram sucesso nas suas tentativas de inserção de código malicioso no ambiente de geração de mídias e na urna eletrônica.

2.5 Investigador: Thiago de Sá Cavalcanti (Departamento de Polícia Federal)

Objetivo:

Subverter a geração das mídias e o programa de votação.

Sistemas afetados: Gerador de mídia e urna eletrônica.

Resultados:

O investigador não obteve sucesso nas suas tentativas de inserção de código malicioso visto que o procedimento de validação do Subsistema de Instalação e Segurança não permitiu.

2.6 Investigador: Fernando Andrade Martins de Araujo (Controladoria Geral da União)

Objetivo:

Avaliar as vulnerabilidades das normas e dos procedimentos formais que disciplinam as eleições.

Sistemas afetados: Procedimentos.

Resultados:

A auditoria dos procedimentos proposta no plano de testes revelou algumas fragilidades que podem ser corrigidas por meio do aperfeiçoamento das práticas de segurança já adotadas no processo eleitoral.

2.7 Investigador: Antonio Gil Borges de Barros (Cáritas Informática Ltda.)

Objetivo:

Avaliar os mecanismos de identificação do eleitor na urna eletrônica por meio de inserção de eleitores não cadastrados na seção para permitir o seu voto e possibilitar a vinculação do eleitor ao seu voto.

Sistemas afetados: Gerador de mídias, urna eletrônica e procedimentos.

Resultados:

Os investigadores não obtiveram sucesso no comprometimento dos sistemas em cenário real de votação em nenhum dos testes propostos. Entretanto, no processo de realização dos testes foi constatado que é possível violar o lacre do envelope de transporte do *flash* de carga, sem deixar vestígios facilmente perceptíveis.

2.8 Investigador: Nelson Murilo de Oliveira Rufino (*Information Systems Security Association* - ISSA)

Objetivo:

Aplicar alteração nos arquivos de entrada de eleitores para manipular o resultado de uma eleição e permitir que os eleitores cadastrados possam votar em duas ou mais seções diferentes.

Sistemas afetados: Gerador de mídia e urna eletrônica.

Resultados:

O investigador não obteve sucesso em transpor os mecanismos de validação utilizados na urna eletrônica.

2.9 Investigador: Mauro César Sobrinho (Procuradoria Geral da República)

Objetivos:

1. Substituir o núcleo sistema operacional Linux da urna; 2. resgatar a chave pública contida no *compact flash* e reassinar todos os arquivos binários presentes na urna.

Sistemas afetados: urna eletrônica.

Resultados:

Apesar do sucesso na decifração, alteração e recifração de núcleo do sistema operacional, os investigadores não conseguiram ultrapassar a etapa de validação do núcleo.

3 Análise dos resultados

Os testes realizados mostraram que o sistema eletrônico de votação brasileiro resistiu a todos os ataques executados à sua base de software, não permitindo a violação das condições fundamentais do voto.

É fato que alguns dos ataques permitiram a modificação ou inserção de arquivos na base, mas não tiveram maior consequência em virtude das defesas construídas em camadas no sistema. Exemplos destes são as modificações no núcleo do sistema operacional da urna e ataques contra o gerador de mídia. É importante mencionar que na execução desses ataques foram relaxados alguns controles que impedem sua realização em situação operacional real.

O ataque mais bem sucedido ao sistema ocorreu pela via de um canal conhecido como secundário, ou colateral, consistindo na medição de radiações emitidas pelo equipamento, e não pela suas interfaces usuais de entrada e saída. Tais radiações permitem acompanhar o acionamento de diferentes teclas o que, em princípio, pode levar à identificação do voto de um eleitor. As medidas de mitigação propostas para esse ataque são de implementação simples.

Também dignas de nota são as considerações contidas na análise dos procedimentos adotados no sistema eletrônico de votação, que revelaram a possibilidade de aperfeiçoamento das práticas de segurança já adotadas no processo eleitoral.

Desta forma, além de ter demonstrado a robustez do sistema, os ataques cumpriram exemplarmente o objetivo de suscitar discussões para a melhoria dos processos e certos trechos do sistema de software. Alguns investigadores puderam contribuir com a realização de testes adicionais, não previstos nos planos originais, o que ampliou sua abrangência, além de evidenciar o comprometimento do TSE na busca de um efetivo aproveitamento dos testes.

4 Premiação

De acordo com os critérios constantes no Edital de Premiação dos Testes de Segurança, publicado no Diário Oficial da União, Seção 3, de 9 de setembro de 2009, os testes receberam as seguintes pontuações:

Investigadores	Duração do Teste (Dt)	Pontos de Intervenção	Tipo de Ataque	Extensão do Ataque	Solução Aceita	Nota Final
Sérgio Freitas da Silva	3	1	10	1	2	6,6667
Fernando Andrade Martins de Araújo (CGU)	15	3	10	20	2	2,9630
Antonio Gil Borges de Barros (Cáritas)	9	2	10	5	1	1,3889
Valter Monteiro Junior (Marinha)	15	2	10	5	1	0,8333
Mauro César Sobrinho (PGR)	15	2	10	5	1	0,8333
Thiago de Sá Cavalcante (INC/DPF)	7	3	10	5	1	0,7937
Carlos Eduardo Negrão de Oliveira (TST)	4	2	10	1	1	0,6250
Nelson Murilo (ISSA)	5	2	10	1	1	0,5000
Divailton Teixeira Machado (STJ)	9	3	10	1	1	0,1235

5 Conclusões

As peculiaridades do processo eleitoral brasileiro e as complexidades inerentes a qualquer sistema de votação eletrônico têm exigido do TSE melhorias contínuas na busca por maior transparência e confiabilidade do sistema brasileiro de votação, de forma a satisfazer o cidadão, os partidos políticos e o público em geral, no anseio legítimo de plena confiança no processo eleitoral.

Em consonância com esse processo de evolução, os testes públicos, aqui relatados, constituem um passo valioso em direção a um sistema mais aberto, auditável e moderno, ao mesmo tempo em que submetem os diversos atores envolvidos com a preparação, desenvolvimento e aplicação do modelo brasileiro de votação, a uma maior prestação de contas à sociedade.

Esta Comissão entende que a prática de realização de testes públicos deva ser mantida e considera que a adesão dos partidos políticos é de fundamental importância para o enriquecimento do repertório de testes e maior respaldo do processo.

Brasília, 20 de novembro de 2009.

COMISSÃO AVALIADORA

Mamede Lima-Marques - Universidade de Brasília

Antonio Montes Filho - Centro de Tecnologia da Informação Renato Archer

Ricardo Dahab - Universidade de Campinas

Osvaldo Catsumi Imamura - Instituto de Estudos Avançados/Centro Tecnológico da Aeronáutica

Claudio Salvador Lembo - Universidade Mackenzie

André Ramos Tavares - Pontifícia Universidade Católica de São Paulo

Patrícia Maria Landi da Silva Bastos - Supremo Tribunal Federal.

ANEXO I

Formulário do Plano de Testes (em branco)

Plano de Teste do Sistema Eletrônico de Votação

1 Informações gerais

Título da Plano de Teste	
Instituição Proponente	
Responsável (nome, e-mail e telefone do autor ou responsável)	
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança ☐ Gerador de Mídias ☐ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor ☐ Lacres ☐ Mídias **Procedimentos**: ☐ Geração de mídias ☐ Etapas de preparação da urna ☐ Votação
Duração Estimada do Teste (em minutos)	
Extensão do ataque	☐ Urna ou seção eleitoral ☐ Local de votação

	☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Conhecimentos necessários	*[Mínimos conhecimentos técnicos necessários para a realização do teste]*

Observações:
- O teste a ser realizado deve ser, obrigatoriamente, reproduzível.
- Este plano deverá ter no máximo 10 páginas em formato A4 ou Carta.

2 Reservado ao TSE

Protocolo	Data	
	Resultado	☐ Aprovado ☐ Aprovado com ressalvas ☐ Reprovado

3 Detalhamento do teste

3.1 Resumo do teste

O proponente deverá apresentar um resumo geral e sucinto do teste informado.

.

3.2 Fundamentação

O proponente deverá explanar, detalhadamente, a fundamentação teórica em que se baseia o teste de ataque simulado, cobrindo todos os componentes afetados.

Sempre que possível, o proponente deverá basear suas asserções em normas, artigos, publicações ou outros trabalhos técnicos e científicos.

3.3 Precondições para o teste

Deverá ser apresentada lista de todas as informações, recursos materiais (inclusive software e respectivas versões) e recursos humanos necessários para a realização do teste por parte da proponente. A listagem deve incluir a qualificação dos recursos humanos citados.

O proponente deverá ainda, obrigatoriamente, mencionar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

3.4 Escopo – Superfície de Ataque

O proponente deverá informar exatamente quais componentes do sistema de votação eletrônica sofrerão atuação/alteração por parte da equipe executora do teste, incluindo:

- *Material (e.g. urna, gerador de mídias, mídias, lacres...),*
- *Ambiental (e.g. condições de operação, sala, alimentação...)*
- *Procedural (e.g. verificação, emissão de zerésima...)*

3.5 Janela de atuação simulada do atacante

O proponente deverá delinear precisamente qual a janela temporal de atuação do atacante, isto é, em quais instantes será necessária a atuação do atacante, correlacionando com as precondições estabelecidas.

Algumas janelas de atuação exemplo são: (a) acesso a mídias no armazenamento fora do período eleitoral, (b) acesso ao software da urna eletrônica na pós-votação no local de votação, (c) acesso à urna eletrônica, (d) acesso à máquina que gera as mídias, (e) acesso à flash de carga gerada.

3.6 Pontos de intervenção

O proponente deverá listar todos os pontos de intervenção nos quais atuará.

Pontos de intervenção, para o teste de segurança no sistema eletrônico de votação, são as barreiras de segurança que devem ser superadas pelo teste proposto, tais como software (e.g. programas assinados), hardware (e.g. extensão de BIOS proprietária), procedimentos (e.g. armazenamento de urnas), mídias (e.g. assinatura e criptografia do Boletim de Urna), lacres.

3.7 Passos a serem realizados e Material Necessário

O proponente deverá listar todos os passos a serem realizados pelo atacante durante a realização dos testes, incluindo passos condicionais. O detalhamento deve chegar ao nível de comando.

A seguir, uma lista de passos exemplo:

1. *Atacante tem acesso físico à mídia de votação*
2. *Atacante, utilizando um computador portátil, lê a mídia de votação*
3. *Caso a mídia de votação esteja em branco, o atacante volta ao passo 1.*
4. *Fim*

Os passos deverão ser detalhados. Durante os testes não serão permitidos desvios (acréscimos, remoção, modificações) em relação aos passos propostos. Os passos devem conter obrigatoriamente o(s) critério(s) de parada do teste, os quais devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração estimada em minutos para cada passo do teste e o tempo total estimado resultante.

O proponente deverá listar também o material necessário à realização dos testes, especificando quais serão os de responsabilidade do TSE e quais os que serão trazidos pelo investigador.

3.8 Possíveis resultados e impacto

O proponente deve apresentar os resultados que espera obter com as ações realizadas. Em especial, a descrição dos resultados esperados deve conter:

- *Tipo do resultado esperado:*

    - *Alteração do destino do voto;*
    - *Quebra do sigilo do voto;*
    - *...*
- *Extensão do ataque:*
    - *Urna ou seção eleitoral;*
    - *Local de votação;*
    - *Zona eleitoral;*
    - *Município;*
    - *Unidade da Federação;*
    - *País.*

O documento deverá ainda conter uma probabilidade esperada de sucesso do ataque, se possível fundamentada.

3.9 Rastreabilidade

O plano de teste deve conter informações sobre a rastreabilidade do ataque simulado, ou seja, discorrer e fundamentar as condições e probabilidades de se:

- *Não detectar o ataque;*
- *Detectar o ataque.*

3.10 Solução proposta

O plano de teste poderá conter uma solução. Nesse caso, o investigador deverá demonstrar que a solução proposta é viável e extingue a(s) vulnerabilidade(s) explorada(s) no ataque descrito. A solução deverá estar em conformidade com o processo eletrônico de votação, respeitando os procedimentos previstos nas resoluções aplicáveis.

ANEXO II

Relatórios de acompanhamento de execução do plano de teste

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.449/2009
Instituição Proponente	Cáritas Informática LTDA
Responsável pela equipe de investigadores	Antonio Gil Borges de Barrros
Data	10/11/2009
Horário de início (para efeito de premiação)	09:40 (manhã) e 14:30 (tarde)
Horário de término (para efeito de premiação)	12:40 (manhã) e 18:00 (tarde)
Sistemas Afetados	**Software**: √ Subsistema de Instalação e Segurança √ Gerador de Mídias √ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor √ Lacres √ Mídias **Procedimentos**: √ Geração de mídias

	√ Etapas de preparação da urna √ Votação
Extensão do ataque	√ Urna ou seção eleitoral √ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☐ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro √ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	A flash de carga antes do carregamento efetivo da urna.
Critério(s) de parada	

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**
	1. Antonio Gil B. Barros	

	2. Arlei de Almeida O. Junior	
	3. Edison Emilio Alonso	
	4. Gislaine Lirian Bueno de Oliveira	
	5. Clarissa Manuchaguian de Moraes	
	6. Matteo Nava	
	7.	
	8.	
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Vitor Monte Afonso	
	2. Ricardo Nobuyoshi dos Santos Makino	
	3. Roberto Alves Gallo Filho	
	4. Marcélio Gonçalves Pereira	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Gladiston da Silva Costa Débora Nery Silva Wilson Henrique Veneziano	**Assinaturas**:
Comissão Avaliadora	Ricardo Dahab	**Assinaturas**:

4 Observadores externos

Conforme lista de presença.

5 Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

1 (uma) flash de carga Apacer 2008;
1 (uma) flashes de votação – Unisys 16MB;
2 (dois) disquetes;
2 (duas) urnas eletrônicas mod 2008 (Pat. 872670 e Pat. 871387);
1 (um) computador com WindowsXP (Pat. 031201) e Ubuntu 9.04 (Pat. 025826)
1 (um) computador com WindowsXP e Sis 3.06
1 (um) CD com o backtrack 4.0 beta
1 (um) CD com o idapro e sua chave de ativação + chave de ativação do winhex
1 (um) CD com a versão 15.0 do winhex
1 (um) CD com a versão 3.0.10 do VirtualBox (Instaladores para WinXP e Ubuntu 9.04 e 9.10
1 (um) leitor de flash com entrada USB

6 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

Permissão de programas adicionais
Permissão de procedimentos não previstos no plano

7 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

10/11/2009
Testes de GM e mídias
Foram entregues aos investigadores as listas de eleitores das seções 5 e 6.
Eles trabalharam com a seção 5.
Foram entregues as mídias: disquetes, flash carga, flash de votação.
Executaram o "Verificador de Autenticação de Programas", o GM 1º turno
Os investigadores solicitaram a instalação do idapro com a licença fornecida por eles, com a intenção de alterar as mídias.
Os investigadores solicitaram também a instalação da licença deles do winhex para ter acesso a mais funcionalidades da versão completa do winhex.
E ainda os investigadores solicitaram o CD do backtrack 4 para fazer o boot com o live-cd na maquina no GM.
Embora não estivesse previsto no plano de teste o atendimento das comissões à solicitação dos investigadores, a comissão gravou em um CD os programas fornecidos pelos próprios investigadores.
Foram entregues o CD com o idapro e sua licença e o CD do backtrack 4.0.
Instalaram o idapro e seu update colocando uma senha de ativação na máquina de investigador.
Gerado no GM a flash de carga, a flash de votação e o disquete de votação.
Considerando que tiveram acesso as mídias, iniciaram operação nas mesmas.
Colocaram no Windows e informaram só terem visto a partição FAT, notando a presença do arquivo unisys.je.
A máquina dos investigadores foi reiniciada no sistema GNU/Linux Ubuntu, pois não identificaram nada substancial que pudesse ser utilizado no ataque no ambiente Windows.
O Ubuntu montou automaticamente as partições e os investigadores informaram ter visto os

nomes dos arquivos.
Informaram terem copiado os arquivos da flash para a partição do Windows
Informaram avaliar os binários copiados e não terem visto nada
Na máquina que gera mídias, colocaram o CD do Backtrack para analisar o Windows.
Ainda no Windows, tiveram acesso ao Windows Explorer, e informaram visualizar o diretório c:\windows\system32\config e todos os arquivos do Windows.
O Windows Explorer demora a mostrar os arquivos, mas logo mostra os arquivos.
Durante o setup não foi requisitada senha e por isso foi possível a escolha da mídia de inicialização.
Informaram montar a partição do Windows.
Usaram o comando chntpw para zerar a senha do administrador
Reboot no sistema e entraram no Windows
Não conseguiram logar com o usuário administrador
Voltaram para o Backtrack
Montaram a partição do Windows.
Mudaram a senha de administrador para 123e45678
Tentaram mover o arquivo Ultiman.exe para Utilman.old. O prompt de comando retornou erro porque não existia arquivo Ultiman.exe (maiúsculo)
Perguntaram se existe uma documentação descrevendo que é necessário colocar senha no setup.
Foi apresentado pelo TSE a documentação descrevendo o item anterior.
Voltaram para o Windows e não conseguiram logar como administrador
Logaram como 10191.
Tentaram copiar o arquivo c:\windows\system32\config\SAM e não conseguiram
Voltaram para o backtrack
Fizeram um backup do arquivo c:\windows\system32\config\SAM utilizando o Linux.
Utilizando o comando chntpw elevaram os privilégios do usuário 10191.

Trocaram o utilman.exe pelo cmd.exe
Voltaram para o Windows
Logaram com 10191, com privilégios de administrador, mas foi requerida uma contra-senha.
Voltaram para backtrack, montaram a partição do Windows e leram alguns arquivos.
Retornaram o arquivo c:\windows\system32\config\SAM para a versão original.
Voltaram para o Windows e executaram o programa AuditoriaXP do GM e leram os logs.
Tentaram instalar o idapro como usuário 10191, mas não foi possível.
Tentaram rodar o chkdsk, mas não foi possível.
Montaram a flash de carga.
Criaram um arquivo teste.txt com conteúdo "teste".
Iniciaram a urna com a flash modificada.
Fizeram a carga normalmente.
Regeraram a flash de carga.
Alteraram o arquivo eleitor.dat.
Iniciaram a urna com essa flash.
A urna detectou a modificação e parou a inicialização.
Regeraram a flash de carga.
Finalizaram o dia 10/11/09.
Testes de lacre do envelope
Realizaram alguns testes de rompimento do lacre do envelope que transporta as mídias.
Testaram em quatro lacres e destruíram estes lacres.
Colocamos as mídias dentro do envelope e tentaram romper o lacre anexo ao envelope. Destruíram o lacre e não obtiveram resultados.
Apresentaram duas alternativas para violar o lacre: 1 – destravar o lacre e não deixar evidências. 2 – tirar o lacre de um outro envelope e usá-lo no envelope original.

Na primeira alternativa não obtiveram sucesso.
Na segunda alternativa, pegaram o envelope 0253645 como original e lacraram as mídias neste envelope.
Pegaram um segundo envelope, de número 0431262, retiraram seu lacre intacto com um bisturi, cortando onde tinha as colas e ficaram com o lacre disjunto do envelope.
Em seguida, no envelope original os investigadores cortaram com o bisturi e retiraram o lacre original sem que restassem vestígios facilmente identificáveis no envelope, obtendo assim acesso à mídia. Durante o processo de retirada do lacre original foi necessário cortar com bisturi os dois pontos de cola do mesmo.
Colocaram o lacre intacto, do envelope número 0431262, no envelope original. A inspeção visual mostra diferenças entre o lacre original e o adaptado, nominalmente: i) a cola do fecho do lacre com o envelope não está presente. Entretanto, essa diferença não é facilmente percebida e demanda atenção.
Testes de lacre da urna
Rafael da Logística, trouxe os lacres (versão preliminar) para a urna.
Foram lacradas as partes da urna: microterminal, gabinete da urna, entrada da flash externa, entrada do disquete, entrada USB, entrada de teclado da urna.
Os investigadores esperaram 24 horas para fazer o teste.
Pegaram o restante dos lacres e assinaram sobre eles. Tentaram remover as assinaturas com álcool isopropílico. Não obtiveram sucesso, as assinaturas permaneceram. Ficou visível que foi aplicado algo no lacre e que este teve sua rugosidade reduzida.
Utilizaram uma borracha para tentar apagar a assinatura. Não obtiveram sucesso.
Fizeram testes com o lacre da urna, tentando removê-lo com ferramentas, tais como, bisturi e álcool isopropílico. Não obtiveram sucesso.
11/11/09.
Testes de GM e mídias

Os investigadores solicitaram a instalação dos seguintes softwares: - Cain e Abel; - WinHex versão full.
Logaram na máquina do GM.
Localizaram a chave de registro: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\RUN.
Viram algumas chaves do diretório C:\Seguranca: HKEY_LOCAL_MACHINE\System\ControlSet001\Services\SISSVC; HKEY_LOCAL_MACHINE\System\ControlSet001\Services\SISTarefas.
O investigador Matteo Nava compareceu no presente dia.
Os investigadores tentaram buscar no registro onde é iniciado o SIS.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Installer.
Tentaram acessar regedit e regedw32.
Entraram no cmd: net user /add gislaine 12345678 sucesso. net user - lista usuários. net localgroup – lista grupos. net localgroup Administradores gislaine /add – acesso negado net localgroup SisLAvancado /add – acesso negado net localgroup System /add – acesso negado net localgroup Sistema gislaine /add – acesso negado net localgroup Kernel gislaine /add – acesso negado net localgroup AutLAdmin gislaine /add – acesso negado net group AutLAdmin /add – acesso negado tasklist – lista tarefas

kill e psfile – erro – não existe dir d: dir d:\usuarios dir d:\usuarios\000000010191 dir d:\Aplic dir d:\Aplic\sispki
Foi possível criar usuário por meio do prompt de comando.
Entraram no SIS registry.
No cmd digitaram systeminfo.
Fizeram logout.
Tentaram logon com o usuário gislaine – acesso negado
Acessaram com 10191 novamente
Abriram o diretório XP para ver logs (registros de auditoria)
No cmd digitaram urnas – acesso negado
No registro: HKEY_LOCAL_MACHINE\Softwares\SistemasEleitorais\Aut\Ferfil
No cmd: net use \\127.0.0.1\\Aplic2k$ localhost\administrador – erro de sistema net use \\127.0.0.1\\config localhost\administrador – erro de sistema
net share
Foi gravado o instalador do WinHEX full em um CD.
Foi permitido executar o software WinHEX. Foi executado sem necessidade de instalação.
Com isso eles conseguiram acessar a memória de todo o sistema.
Reiniciaram a máquina.
Sugeriram que "se fosse verificado todos os executáveis que são possíveis de execução na máquina geradora de mídia e proibir a execução de qualquer outro software não permitido,

mesmo que esse software não necessite instalação. Usar técnica de hash negativo".
Abriram novamente o WinHEX.
Buscaram informações do SISDesktop.
Sugeriram não permitir criar usuários pela linha de comando.
Executam o GM juntamente com o WinHEX.
Geram a flash e inspecionaram a memória de todo o computador.
A comissão disciplinadora liberou a entrada de uma pistola de ar quente e um termômetro laser digital. - Pistola de ar quente "Hot Air Tool Type Weldy"; - Termômetro "Fluke 62 mini IR thermometer".
Investigaram o conteúdo da memória.
Foram para a máquina do investigador montaram a flash a procura do bootloader.
Desmontaram a flash de carga.
Fizeram um dump da flash usando o comando dd.
Copiaram o dump para a partição do Windows.
Reiniciaram e foram para o Windows.
Executaram o WinHEX e verificaram o dump da flash.
Compararam várias sequências de 32 bytes para servirem como possíveis chaves.
Procuraram pela chave no início da flash (bootloader). Não houve sucesso.
Reiniciaram a máquina de investigação com o sistema GNU/Linux Ubuntu.
Tentaram decifrar o kernel com openssl usando as possíveis chaves eleitas anteriormente, para identificar a chave hexadecimal na flash. Não houve sucesso.
Converteram o uenux para base64 e tentaram decifrá-lo. Não obtiveram sucesso.
Fizeram alguns testes com o openssl para identificar quais os parâmetros deveriam ser utilizados.
Fizeram imagens das partições /dev/sdb1, /dev/sdb2, /dev/sd3 e /dev/sdb4.

Reiniciaram a máquina de investigação com o sistema WindowsXP.
Copiaram os arquivos do CD para a máquina dos investigadores.
Instalaram o Cain&Abel e o Winpcap.
Abriram o dump da flash com o winhex.
Mudaram o valor do parâmetro init do bootloader dentro do dump da flash para "/bin/initrd".
Copiaram o dump alterado para a flash.
Substituíram o init da flash pelo init padrão da distribuição Linux utilizada e o renomearam para initrd.
Copiaram o /bin/sh do Linux utilizado para o /bin da flash.
Iniciaram a urna com a mídia modificada. Não obtiveram sucesso: o SAVD detectou que ela estava modificada.
Copiaram o initrd em cima do initje utilizando o comando cp.
Iniciaram a urna e ocorreu kernel panic.
Restauraram a flash.
Trocaram initje pelo init do Linux utilizado.
Iniciaram a urna e ocorreu erro porque o init não foi localizado.
Voltou initje para flash.
Iniciaram a urna e o SAVD detectou um problema (erro relacionado à chave.jez).
Voltaram dump original para flash.
Urna carregou normalmente.
Testes de lacre da urna
Realizado teste de remoção do lacre da urna eletrônica, utilizando bisturi cirúrgico e álcool isopropílico. A equipe não obteve êxito. O adesivo sofreu modificações no seu material adesivo, apresentando vestígios de violação.
Tentaram remover mais alguns lacres para fins de treino da metodologia. Com lacres

aplicados sobre substratos e após decorridas 24 horas, realizaram novas tentativas de remoção destes lacres. Estas tentativas acabaram deixando evidências de violação. Não obtiveram sucesso. Na tentativa de recolagem do lacre ele não permaneceu íntegro, evidenciando que foi violado. O teste foi feito em uma urna que possuía pedaços de lacres aplicados no dia anterior.
Num segundo teste foi aplicado um lacre em superfície de caixa de CD com tempo de colagem inferior a 24 horas. Com uma pistola de ar quente e termômetro digital, iniciaram tentativa de retirar o lacre da superfície da caixa do CD. O tempo decorrido após a aplicação dos lacres inferior a 24 horas caracteriza um relaxamento das condições de teste.
No início a temperatura do lacre era de 24°C.
Foi aplicada a pistola de ar quente e a temperatura foi sendo elevada.
Elevaram a temperatura do lacre até 47°C e tentaram retira-lo da caixa do CD com o bisturi e pinça, mas o mesmo não saiu.
Continuaram a elevar a temperatura.
Elevaram a temperatura até 80°C e tentaram novamente retirar o lacre da caixa de CD. Retiraram o lacre da tampa de CD deixando pequenas evidências. Elevaram a temperatura até 95°C, sendo esta a máxima temperatura aplicada.
Utilizaram uma tampa do microterminal para aferir em qual temperatura o material da urna se deforma.
Por volta de 89°C a peça da urna eletrônica deformou, mostrando que o material da urna não suporta temperaturas superiores à aferida.
Colocaram dois lacres, um na tampa do disquete e outro na tampa do microterminal, para atingir o tempo de cura necessário e ser testado no dia seguinte.
12/11/2009
Testes de GM e mídias
Iniciaram no ubuntu
Fizeram cópia das partições 4, 3, 2, 1 e de toda flash de carga para o HD da máquina.
Solicitaram o software Virtualbox para instalação na tentativa de executar a flash de carga no

PC.
Copiaram a libgcc_s.so.2 do ubuntu para o diretório lib da flash
Refizeram o seguinte link: ln –s libgcc_s.so libgcc_s.so.2
Desmontaram a flash
Ligaram a urna e não foi detectada a alteração pelo SCUE.
Segundo informações do Saulo, os executáveis são linkados com as bibliotecas finais e não com os links, assim os links não são utilizados, sendo validados somente pelo VPP.
Apagaram o link libgcc_s.so
Colocaram a libcrypt.so.11 e fizeram um link de libgcc_s.so para libcrypt.so.11.
Receberam CD com virtualbox.
Iniciaram a urna com a flash modificada. A urna carregou normalmente porque o link que foi modificado não foi utilizado pelo sistema.
Foram para o ubuntu e tentaram instalar o virtualbox, mas ocorreu um erro de falta de pacotes.
Instalaram o Virtualbox no Windows.
Executaram o Virtualbox.
Criaram um novo projeto, com características de Linux e com HD do dump da flash.
Tentaram iniciar a máquina virtual e ocorreu o erro: "Fatal: No bootable media found! System halted"
Não estavam conseguindo colocar o dump da flash como disco da máquina virtual pois o Virtualbox não suporta o uso de imagens.
Tentaram mapear a flash para o disquete.
Quando iniciaram a máquina virtual a seguinte mensagem foi apresentada: "Erro no boot".
A partir de um arquivo vdi (padrão do virtualbox) eles anexaram o dump da flash para tentar utilizar como disco, por meio do WinHex.
Ao tentar executar, o Virtualbox acusou "invalid header".
Foram suspensos os testes com o Virtualbox.

Reiniciaram a máquina dos investigadores no sistema GNU/Linux Ubuntu.
Renomearam o libgcc_s.so.1 para libgcc_s.so.3.
Criaram o link libgcc.so.1 para libgcc_so.3.
Iniciaram a urna e não ocorreu nenhum erro de validação, pois o link estava apontado para o arquivo certo, libgcc_so.3.
Removeram o link libgcc_s.so.1.
Criaram o link apontando para libgcc_s.so.3.
Erro ao executar o SAVD: "Invalid ELF header. Error while loading shared library".
Removeram o link libgcc_s.so.1.
Criaram o link para libgcc-s.so.3 novamente.
Pessoal da logística abriu a urna para mostrar aos investigadores.
Criaram um diretório teste no diretório /lib.
Moveram libgcc_s.so.2 e libgcc_s.so.3 para o diretório teste.
Apagaram o link libgcc_s.so.1.
Executaram "ln –s teste libgcc_s.so.1".
Moveram libgcc_s.so.3 para libgcc_s.so.1.
Apagaram o link libgcc_s.so.1.
Executaram "ln –sn teste libgcc_s.so.1".
Iniciaram a urna e ocorreu erro no SAVD: "Cannot read file data: Error 23".
Apagaram o link libgcc_s.so.1.
Executaram "ln –s teste libgcc_s.so.1".
Reiniciaram a máquina dos investigadores no sistema Windows para fazer uma nova tentativa com o Virtualbox.
Executaram comando para converter o dump em um arquivo do virtualbox. "vboxmanager convertfromraw dump urna.vdi".
Inseriram arquivo convertido na máquina virtual, desta vez o processo de boot iniciou mas parou com o erro no loader: "Esta flash pertence a JE e só pode ser utilizada na urna

eletrônica".
Desabilitaram rede, USB, disquete e CDROM.
Selecionaram drive HD ICM6.
Habilitaram PAE/NX no CPU.
Iniciaram a máquina virtual e ocorreu o mesmo erro: "Esta flash pertence a JE e só pode ser utilizada na urna eletrônica".
Tentaram iniciar a flash de carga em um computador comum através de um leitor USB de flash card.
Ocorreu o mesmo erro: "Esta flash pertence a JE e só pode ser utilizada na urna eletrônica".
Foi constatada a não possibilidade de realizar boot com Virtualbox ou em um computador convencional.
Retomaram os testes com flash.
Voltaram a libgcc original.
Alteraram o conteúdo do arquivo avboot.vst de uenux para tenux.
Iniciaram a urna com a flash.
Foi detectado um erro de integridade do sistema [tenux].
Voltaram o arquivo avboot.vst para o original.
Fizeram cd uenux/app/ttf
mkdir bkp
cp * bkp
cp ../chave/* .
rm freesans.ttf
Link freesans.ttf -> ue.pri
rm avusrttf.vst
Iniciaram a urna e a tela fica vazia sem aparecer nada, por conta que a fonte foi removida, não sendo possível verificar o estado da urna.
Restauraram o arquivo de fonte e apagaram os arquivos copiados anteriormente

Fizeram bkp dos arquivos da pasta disk/jez
Copiaram os arquivos uenux/app/ttf/* para a pasta jez
Criaram link ln –s freetype.ttf vota_img.jez
Iniciaram a urna e o SAVD detectou um erro no arquivo libgcc_s_so.1
Restauraram o estado da flash.
A urna foi iniciada, ela carregou normalmente.
Criaram diretório jez/bkp/.
Moveram arquivos vota_img.* para jez/bkp/.
Criaram link vota_img.jez apontando para vota_bin.jez.
A urna foi iniciada.
SAVD detectou erro de integridade [vota_img.vst].
Criaram link vota_img.vst apontando para vota_bin.vst.
A urna foi iniciada e a carga foi feita normalmente.
Inseriram a flash de votação.
A urna foi iniciada e o GAP detectou erro: "Erro verificando assinaturas contidas no arquivo /uenux/app/dado/avusrimg.vmt".
Retornaram os arquivos do diretório jez/bkp/.
Moveram arquivos chave.* para bkp/.
A urna foi iniciada.
SAVD detectou erro de integridade [chave.vst].
Criaram link chave.jez apontando para avpart.jez.
Criaram link chave.vst apontando para avpart.vst.
A urna foi iniciada.
SAVD detectou erro de integridade [vota_img.jez].
Restauraram a flash usando o dump da flash original.
Criaram link chave.jez apontando para vota_img.jez.

Criaram link chave.vst apontando para vota_img.vst.
Ligaram a urna e fizeram a carga normalmente.
Ligaram novamente com a flash de votação e ocorreu o seguinte erro: "erro durante a carga do estado geral da urna". Porque não tinha chave para validar.
Copiaram o diretório chave para o diretório jez da flash de carga.
Moveram vota.of* para diretório de backup.
Criaram link vota_ofi.jez apontando para vota_opl.jez.
Criaram link vota_ofi.vst apontando para vota_opl.vst.
A urna foi iniciada.
SAVD detectou erro de integridade [chave.jez].
Restauraram flash utilizando dump da flash original.
Moveram vota_ofi* para diretório de backup.
Criaram link vota_ofi.vst apontando para vota_opl.vst.
Criaram link vota_ofi.jez apontando para vota_opl.jez.
Carga ocorreu normalmente.
Iniciaram urna com flash de votação.
GAP apresentou a seguinte mensagem de erro: "vota.of não foi encontrado".
Geraram disquete do VPP e iniciaram a urna.
O auto-teste foi executado com sucesso.
Testes de lacre da urna
Não houve.
13/11/2009
Testes de GM e mídias
Não houve.

Testes de lacre da urna
Utilizando bisturi e pistola de ar quente, chegando a temperatura de 65°C, removeram a parte plástica do lacre que estava colado há mais de 24 horas na tampa do microterminal, não sendo possível colá-lo novamente. A integridade do lacre não foi preservada.
Tentaram retirar novamente outra amostra do lacre aplicado sobre a tampa do disquete, chegando a temperatura de 75°C, com a ajuda do bisturi. O lacre evidenciou marcas de violação.
Tentaram retirar novamente o lacre da tampa do disquete, utilizando bisturi e pistola de ar quente, chegando a temperatura de 71°C. O lacre evidenciou novamente marcas de violação.
Tentaram retirar o lacre de outra tampa, utilizando bisturi e pistola de ar quente, chegando a 75°. O lacre ficou com marcas de violação.
Em outra amostra, aplicada há mais de 24 horas sobre a superfície da urna, tentaram efetuar a remoção do lacre com bisturi e álcool isopropílico inicialmente, na seqüência procedendo com a pistola de ar quente e pinça. O lacre evidenciou marcas de violação.
Ao final destas diversas tentativas a equipe considerou os testes do lacre por encerrado.

8 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

Os investigadores não obtiveram sucesso nos testes originalmente propostos (vide respectivo projeto de testes).

Os investigadores não obtiveram sucesso do comprometimento dos sistemas de votação em cenário real de votação em nenhum dos demais testes propostos durante o evento de testes. Algumas notas:

- Os investigadores relacraram envelope com mídia de votação sob ambiente relaxado (tiveram acesso a um segundo envelope, não disponível em votação). O envelope produzido não é idêntico ao original. A percepção da diferença demanda atenção.
- O teste cujo objetivo era causar uma falha da urna no final do processo de votação causando assim a perda dos votos realizados, não foi bem sucedido. A fase de carga, com flash sem programas de votação foi bem sucedida. A urna falhou no processo de preparação para votação. Em específico, o teste proposto falhou na fase de verificação do gerenciador de aplicativos com o disquete de votação, tendo passado pelo auto-teste.

O motivo do não sucesso das tentativas dos investigadores é o amplo repertório de contramedidas de segurança técnicas e procedimentais adotadas pelos sistemas de votação.

9 Observações

Não há observações.

10 Apêndices

Não há apêndices.

Sugestões do(s) Investigador(es) para Melhoria

O investigadores sugeriram:

1. Deram a sugestão de que se fossem verificados todos os executáveis que são possíveis de execução na máquina geradora de mídia e proibir a execução de qualquer outro software não permitido, mesmo que esse software não necessite instalação. Usar técnica de *hash* negativo;
2. Publicação (através de instrumento de resolução) de uma Política de Segurança a ser adotadas pelo TSE e pelos TREs;
3. Dentre outros elementos, sugere-se que Política de Segurança deva versar sobre: i) estabelecimento de critérios para adoção de senhas seguras, ii) adoção de procedimentos de configuração segura para os sistemas utilizados para os geradores de mídias, iii) restringir o acesso às funções administrativas para os usuários não-administrativos que utilizam o sistema gerador de mídias, como por exemplo, o comando "net use", iv) reforçar o controle de acesso da pasta do sistema operacional;
4. Elaboração de fluxograma dos procedimentos adotados para todas as fases do processo eleitoral;
5. Sugere-se gravar o número do registro impresso no envelope também no lacre dos mesmos;
6. No sistema de verificação de integridade da urna, teste da existência de todos os arquivos que compõem o sistema completo da urna, assim como arquivos adicionados. Realizar os mesmos testes para links simbólicos.

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.455/2009 23.456/2009 23.457/2009 23.458/2009 23.453/2009 23.454/2009 23.459/2009
Instituição Proponente	CGU
Responsável pela equipe de investigadores	Fernando Andrade Martins de Araújo
Data	12/11/2009
Horário de início (para efeito de premiação)	15h45
Horário de término (para efeito de premiação)	16h30
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança ☐ Gerador de Mídias ☐ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor

	☐ Lacres ☐ Mídias **Procedimentos**: ☒ Geração de mídias ☒ Etapas de preparação da urna ☒ Votação
Extensão do ataque	☐ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☒ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☐ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☒ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	*O teste proposto não contém pontos de intervenção propriamente ditos, uma vez que seu foco está nos procedimentos que envolvem a preparação das eleições e votação.*
Critério(s) de parada	*Descrédito no sistema eletrônico de votação brasileiro.*

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**

	1. Fernando Andrade Martins de Araújo	
	2. Ricardo Nagamine Motta	
	3. Gustavo Fleury Soares	
	4. Fabio Leonel Orsi	
	5. Ricardo Silva Melo Fernandes	
	6. Eduardo Soares de Paiva	
	7.	
	8.	
	Nome completo	**Assinatura**
Apoio técnico da Comissão Disciplinadora	1. Ricardo Nobuyoshi dos Santos Makino	
	2.	
	3.	
	4.	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Wilson Henrique Veneziano Gladiston da Silva Costa Débora Nery Silva José de Melo Cruz	**Assinaturas**:
Comissão		**Assinaturas**:

Avaliadora	Mamede Lima-Marques	

4 Observadores externos

Relatório de Exame dos Processos de Preparação da Votação e da Votação Eletrônica.

INTRODUÇÃO

O presente relatório apresenta os resultados do exame dos processos de preparação da votação, bem como do próprio sistema de votação eletrônica. Pela proposição inicial da equipe responsável pelos testes, dadas as limitações de tempo, o escopo dos exames se limitou à avaliação de vulnerabilidades das normas e procedimentosformais que regulamentam as eleições.

Para execução das atividades dos exames foram seguidos os seguintes passos:

a) Análise de conteúdos do sítio do Tribunal Superior Eleitoral – TSE, de parte da legislação e normativos pertinentes ao processo de votação eletrônica e seus antecedentes, especialmente: Lei Federal 9.504/97, Instrução TSE nº 114 (Resoluções 22.712 e 22.713) e Instrução TSE nº 117 (Resolução 22.714);

b) Entrevistas com servidores do TSE, responsáveis pelo desenvolvimento e pela condução do processo eleitoral;

c) Inspeção Física de uma Urna Eletrônica, por meio de demonstração conduzida por servidores do TSE, apresentando, em linhas gerais, os procedimentos iniciais, votação e encerramento da votação, com geração do boletim de urna.

A seção seguinte apresenta os resultados do exame dos processos destacando as vulnerabilidades mais relevantes que foram detectadas, apresentado análises e eventuais recomendações para minimização de sua probabilidade de ocorrência ou de seus efeitos.

RESULTADOS

1. Procedimento para Guarda e Proteção das Chaves

Objeto:

Na análise da Resolução n.º 22.714 da Instrução n° 117, que dispõe sobre a fiscalização do sistema eletrônico de votação, a votação paralela e a cerimônia de assinatura digital, foi observada uma carência de procedimentos que especifiquem e formalizem como é feita a proteção e guarda das chaves utilizadas na criptografia dos diversos módulos dos sistema de votação eletrônica. Neste contexto o Art. 21 estabelece que:

"Art. 21. As assinaturas digitais dos representantes do TSE serão executadas por meio de programa próprio, cujos códigos e mecanismos poderão ser objeto de auditoria na oportunidade prevista no art. 4º e deverão seguir, no que couber, a regulamentação expedida pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil). "

E ainda, o Art. 22 estabelece:

"Art. 22. As chaves privadas e públicas utilizadas pela Justiça Eleitoral serão geradas pelo TSE, sempre pelo próprio titular, a quem caberá o seu exclusivo controle, uso e conhecimento."

Análise:

Entende-se que estes dois artigos são insuficientes para documentar a guarda e proteção das chaves, carecendo de detalhamento de informações, como, por exemplo, quem (cargo/função) terá acesso às chaves; especificações do ambiente onde as chaves ficarão custodiadas; especificação do dispositivo/hardware em que as chaves ficarão armazenadas;

definição da proteção contra ameaças e ações não-autorizadas às estações de trabalho onde as chaves serão utilizadas; dentre outras.

Conclusões / Recomendações:

Por se tratarem de peças fundamentais no que tange a segurança do processo de votação, e visando proporcionar mais transparência ao processo, sugere-se a formalização desses procedimentos, especificando as características mínimas de segurança para a guarda e proteção destas chaves, seguindo os padrões definidos pela ICP-Brasil.

2. Representatividade da conferência por amostragem das urnas eletrônicas

Objeto:

Representatividade da conferência por amostragem das urnas eletrônicas, por representantes dos Partidos Políticos, Coligações, Ministério Público e Ordem dos Advogados do Brasil, conforme previsão do Art. 66 da Lei 9.504/97 e do parágrafo 1º do Art. 31 da Resolução 22.712 do Tribunal Superior Eleitoral.

Análise:

O parágrafo 1º do art. 31 da Resolução 22.712 define que a conferência por amostragem será realizada em até 3% das urnas preparadas para cada zona, observado o mínimo de uma urna por município.

Para a análise e cálculos que seguem foram utilizados como referência:

2

- Consulta denominada "Eleitorado Web", disponível no sítio do TSE, no endereço eletrônico http://www.tse.jus.br/internet/eleicoes/muni_zona_blank.htm, selecionando-se a

Consulta por Município/Zona, que oferece o quantitativo de eleitores cadastrados, por município, até setembro de 2009;

• Foi estimado, por informação do TSE, um total de 450.000 urnas eletrônicas em todo o Brasil, sendo, desse montante, 10% utilizado como urnas de contingência. Observadas as regras acima, tem-se algo entre 5.564 e 12.600 urnas na amostra. É importante notar que não se trata de uma amostra simples de urnas, pois há uma diretriz de no mínimo uma por município. Trata-se, então, de uma amostra estratificada, cuja precisão depende não apenas de seu tamanho, mas também da alocação da amostra nos estratos. Nesse caso, cada município é um estrato. Assim, no pior caso, conferindo-se apenas uma urna por município, ter-se-ia uma margem de erro máxima de 8,2 pontos percentuais, arbitrando-se 95% de confiança. No entanto, nessa mesma condição de amostragem, se não forem observadas quaisquer falhas nas urnas examinadas, será possível afirmar, com 95% de confiança, que o percentual de urnas com falhas no Brasil é inferior a 2,1%.

Por outro lado, supondo-se outro cenário, onde os 3% máximos de amostragem sejam alcançados, implicaria em que no município de São Paulo (capital) haveria mais de 750 urnas na amostra e no Rio de Janeiro (capital) mais de 420. Mas assim, a margem de erro cairia para menos de um ponto percentual, com 95% de confiança. Nesse cenário, se houver falhas em menos de 1% de urnas, seria possível afirmar, novamente com 95% de confiança, que o percentual de urnas com falhas é inferior a 1,16%.

Simulando-se ainda um cenário intermediário, em que o número de urnas por município respeite os 3% mas não ultrapasse 5 urnas, ter-se-ia cerca de 3,7 pontos percentuais de erro máximo, e menos de 1% de falhas na amostra implicaria menos de 1,7% de falhas no universo, com 95% de confiança.

Conclusões / Recomendações:

É importante ressaltar, no entanto, que esses números são válidos para o Brasil como um todo, e percentuais mais altos de defeitos verificados em determinadas regiões (ou Unidades da Federação) podem não ter significância estatística. Por exemplo, Roraima ficaria com uma amostra de 15 a 29 urnas (vide suposições acima), o que dificilmente permitiria comparar o seu percentual de defeitos com o resto do Brasil. Por exemplo, ainda no melhor caso, em que os 3% são atingidos, supondo-se que a amostra como um tenha apresentado 1% de defeitos, mas em Roraima esse índice tenha sido registrado em 5%.

Mesmo assim, essa diferença não seria estatisticamente significativa. E no pior caso, com apenas 15 urnas na amostra de Roraima, somente se a estimativa estadual ficasse acima de 15% seria significativa em relação a uma média nacional de 1%. Em Minas Gerais, estado com maior número de municípios, que conta com no mínimo 800 urnas, esse problema não ocorre.

Em resumo, a amostragem está bastante adequada, tanto para demonstrar que a porcentagem de urnas defeituosas no Brasil é pequena, quanto para apontar diferenças grosseiras entre Regiões, caso existam. O único detalhe é que nas regiões com poucas urnas na amostra, se os 3% de amostragem de urnas não forem atingidos, a significância estatística da diferença entre média regional e média nacional pode ficar comprometida.

3. Padronização de Procedimentos dos TREs

Objeto:

Procedimentos do Tribunal Superior Eleitoral - TSE destinados a orientar e padronizar os processos dos Tribunais Regionais Eleitorais - TREs com relação à preparação e realização do processo eleitoral do ano de 2008.

Análise:

Na análise dos normativos que regularam as eleições do ano de 2008, verificou-se a inexistência de procedimentos padronizados para os Tribunais Regionais Eleitorais com relação ao processo de preparação das urnas eletrônicas de votação, de operacionalização das mesmas durante o processo eleitoral e de posterior recolhimento e guarda durante o período entre uma eleição e outra.

Conclusões / Recomendações:

Deve-se buscar uma padronização de forma a aumentar a transparência e reduzir a variabilidade do processo de trabalho sem, no entanto, prejudicar a flexibilidade necessária aos Tribunais Regionais Eleitorais para adaptarem-se as suas peculiaridades locais. Seria conveniente que a padronização englobasse pelo menos os seguintes tópicos:

- Quanto à guarda e acondicionamento das urnas:
  - A forma de acondicionamento e guarda das urnas eletrônicas no processo eleitoral;
  - Prazo limite para o recolhimento e acondicionamento nos respectivos depósitos das urnas eletrônicas.
- Quanto à preparação das urnas:
  - Uma data que defina a partir de quando os Tribunais Regionais Eleitorais poderão começar o processo de preparação das urnas eletrônicas para as eleições seguintes;
  - A data limite para que esse processo de preparação das urnas esteja finalizado;
  - A forma como se dará esse processo de preparação das urnas eletrônicas (se será permitido o acompanhamento do público interessado ou não, e no caso, como se dará esse acompanhamento);
  - Em que condições de segurança devem ser feita a distribuição das urnas.
- Quanto à distribuição das urnas:
  - A partir de quando poderá ser iniciada a distribuição das urnas;
  - Prazo limite para o fim da distribuição das urnas;
  - Definição do processo de instalação das urnas no dia das eleições (quem deve efetuar a instalação, qual a sequência de passos a serem seguidos,...).
- Quanto ao processo de votação:
  - Definição do número mínimo de técnicos necessários para dar suporte no manuseio, operação e correção de eventuais falhas das urnas eletrônicas;
  - Procedimentos a serem adotados durante a impressão dos relatórios da urna eletrônica no início do dia da votação;
  - Procedimento dos mesários durante o processo de votação eletrônica (sequência de passos que o mesário deve seguir no processo de votação de cada eleitor);
  - Definição dos procedimentos a serem adotados no caso de eventuais contingências nas urnas eletrônicas;
  - Procedimentos a serem adotados durante a impressão dos relatórios da urna eletrônica no fim do dia da votação.

4. Representatividade estatística da amostragem da Votação Paralela

Objeto:

Representatividade estatística da amostragem da Votação Paralela, prevista no parágrafo 6º do Art. 33 da Lei 9.504/97 e no Capítulo VI da Resolução 22.714 do Tribunal Superior Eleitoral

Análise:

O Art. 40 da Resolução 22.714 do TSE estipula as regras para amostragem, da seguinte forma:

"Art. 40. Para a realização da votação paralela, deverão ser sorteadas, em cada unidade da Federação, seções eleitorais, sendo uma entre as da capital, no seguinte quantitativo:

I – no primeiro e segundo turnos:

a) duas nas unidades da Federação com até 15.000 seções no cadastro eleitoral;

b) três nas unidades da Federação que possuam de 15.001 a 30.000 seções no cadastro eleitoral;

c) quatro nas demais unidades da Federação.

Parágrafo único. Não poderá ser sorteada mais de uma seção por zona eleitoral".

Para a análise e cálculos que seguem foram utilizados como referência:

- Consulta denominada "Eleitorado Web", disponível no sítio do TSE, no endereço eletrônico http://www.tse.jus.br/internet/eleicoes/muni_zona_blank.htm, selecionando-se a Consulta por Município/Zona, que oferece o quantitativo de eleitores cadastrados, por município, até setembro de 2009;
- Foi estimado, por informação do TSE, um total de 450.000 urnas eletrônicas em todo o Brasil, sendo, desse montante, 10% utilizado como urnas de contingência;
- Pelo quantitativo eleitoral levantado e pela quantidade aproximada de urnas eletrônicas informada pelo TSE, chegou-se a uma média aritmética de 325 eleitores por seção / urna.

Pela interpretação do texto normativo, entende-se que seriam sorteadas uma urna da capital mais uma, duas ou três urnas do interior. Efetuando-se os cálculos com as suposições acima, somente nos estados de São Paulo e Minas Gerais seriam sorteadas urnas do interior, e somente nos estados da Bahia, de Pernambuco, Paraná, Rio de Janeiro e Rio Grande do Sul teriam duas. Para o restante das Unidades da Federação aplicar-se-ia a alínea "a" do inciso I do art. 40 da Resolução 22.714. Assim, a amostra fica muito pequena, pois apenas 62 urnas seriam sorteadas, o que resulta em uma margem de erro de até 16,8% (95% de confiança). Se nenhuma dessas urnas da amostra apresentar erros de contagem, seria possível afirmar que o percentual de urnas com esse tipo de defeito no universo é inferior a 8,4%, com 95% de confiança, o que expressa uma margem de erro de baixa confiabilidade. Por outro lado, se 10% das urnas da votação paralela apresentar falhas, ao extrapolar essa estimativa para o universo, ter-se-ia um intervalo de confiança variando de 4,12% a 21,2% (com nível de confiança de 95%).

Conclusões / Recomendações:

Em resumo, as regras atuais de amostragem parecem pouco adequadas para se identificar possíveis erros, pois mesmo que nenhum seja encontrado, não seria razoável afirmar que esse percentual é menor do que 8,4%, o que ainda é alto. Para permitir rejeitar qualquer percentual de erro acima de 5% no universo (caso nenhuma urna da amostra apresente erro de contagem), bastaria retirar uma amostra de 58 urnas de forma aleatória simples, sem as restrições do inciso I. Nesse cenário hipotético, não haveria prejuízo em se impor uma restrição de no mínimo uma urna por UF. Caso fosse necessário, além disso, contemplar no mínimo uma urna na capital e uma no interior, seria necessário amostrar 78 urnas no total, de acordo com a

distribuição da tabela 1 abaixo. Para baixar o percentual de 5% para 2%, seria necessário amostrar 149 urnas, de forma aleatória simples, ou 159, com restrições, de acordo com a tabela 2 abaixo.

Tabela 1 – Amostragem para permitir rejeitar percentuais de falhas acima de 5%

Estrato Urnas Tamanho da amostra

AC – Interior 751 1
AC – Capital 629 1
AL – Interior 4.522 1
AL – Capital 1.575 1
AM – Interior 2.647 1
AM – Capital 3.307 1
AP – Interior 514 1
AP – Capital 685 1
BA – Interior 22.942 3
BA – Capital 5.471 1
CE – Interior 12.778 2
CE – Capital 4.643 1
DF 5.329 1
ES – Interior 6.805 1
ES – Capital 753 1
GO – Interior 9.376 1
GO – Capital 2.651 1
MA – Interior 10.841 1
MA – Capital 1.984 1
MG – Interior 37.958 5
MG – Capital 5.482 1
MS – Interior 3.435 1
MS – Capital 1.587 1
MT – Interior 5.065 1
MT – Capital 1.141 1
PA – Interior 11.092 1
PA – Capital 2.978 1
PB – Interior 6.802 1
PB – Capital 1.384 1
PE – Interior 15.306 2
PE – Capital 3.429 1
PI – Interior 5.208 1
PI – Capital 1.533 1
PR – Interior 18.726 2
PR – Capital 3.901 1
RJ – Interior 20.720 3
RJ – Capital 14.077 2
RN – Interior 5.130 1
RN – Capital 1.556 1
RO – Interior 2.393 1
RO – Capital 794 1
RR – Interior 272 1
RR – Capital 498 1
RS – Interior 21.253 3
RS – Capital 3.202 1
SC – Interior 12.549 2
SC – Capital 936 1
SE – Interior 3.113 1
7

Estrato Urnas Tamanho da amostra

SE – Capital 1.112 1

SP – Interior 65.064 9
SP – Capital 25.403 3
TO – Interior 2.418 1
TO – Capital 397 1
Total: 404.117 78

Tabela 2 - Amostragem para permitir rejeitar percentuais de falhas acima de 2%

Estrato Urnas Tamanho da amostra
AC - Interior 751 1
AC - Capital 629 1
AL - Interior 4.522 2
AL - Capital 1.575 1
AM - Interior 2.647 1
AM - Capital 3.307 1
AP - Interior 514 1
AP - Capital 685 1
BA - Interior 22.942 8
BA - Capital 5.471 2
CE - Interior 12.778 5
CE - Capital 4.643 2
DF 5.329 2
ES - Interior 6.805 2
ES - Capital 753 1
GO - Interior 9.376 3
GO - Capital 2.651 1
MA - Interior 10.841 4
MA - Capital 1.984 1
MG - Interior 37.958 14
MG - Capital 5.482 2
MS - Interior 3.435 1
MS - Capital 1.587 1
MT - Interior 5.065 2
MT - Capital 1.141 1
PA - Interior 11.092 4
PA - Capital 2.978 1
PB - Interior 6.802 2
PB - Capital 1.384 1
PE - Interior 15.306 6
PE - Capital 3.429 1
PI - Interior 5.208 2
PI - Capital 1.533 1
PR - Interior 18.726 7
PR - Capital 3.901 1
RJ - Interior 20.720 8
RJ - Capital 14.077 5
RN - Interior 5.130 2
RN - Capital 1.556 1
8
Estrato Urnas Tamanho da amostra
RO - Interior 2.393 1
RO - Capital 794 1
RR - Interior 272 1
RR - Capital 498 1
RS - Interior 21.253 8
RS - Capital 3.202 1
SC - Interior 12.549 5
SC - Capital 936 1
SE - Interior 3.113 1

SE - Capital 1.112 1
SP - Interior 65.064 24
SP - Capital 25.403 9
TO - Interior 2.418 1
TO - Capital 397 1
Total: 404.117 159

5. Cerimônia de Assinatura Digital e Lacração dos Sistemas
Objeto:
Evidências de correspondência entre programas-fonte analisados anteriormente e apresentados na Cerimônia de Assinatura Digital e Lacração dos Sistemas, prevista no Capítulo III da Instrução nº 117 (Resolução nº 22.714).
Análise:
A partir de 6 meses antes do primeiro turno, técnicos indicados pelos partidos políticos, pela Ordem dos Advogados do Brasil e pelo Ministério Público poderão acompanhar as fases de especificação e desenvolvimento dos sistemas em ambiente específico e controlado para esse fim.
Esse procedimento, descrito no Art. 3º, Capítulo II da Instrução nº 117, dá oportunidade aos interessados para tirar dúvidas e questionar aspectos técnicos antes da cerimônia de assinatura digital e lacração dos sistemas.
A referida cerimônia tem duração de cinco dias e representantes das mesmas entidades que acompanharam o processo de especificação e desenvolvimento dos sistemas estarão presentes.

Nesse período, esses representantes poderão analisar o programa-fonte e acompanhar a compilação e assinatura digital dos programas feita por servidor designado pelo TSE.
Dada a complexidade e tamanho dos programas desenvolvidos e a duração da cerimônia, é dificultada a tarefa de um representante externo de obter evidências sólidas de que os programas-fonte apresentados são os mesmos que ele analisou previamente nas dependências do TSE.
Outro ponto crítico são os meios facultados a um representante externo para evidenciar para que o programa-fonte apresentado na cerimônia é, realmente, o que está sendo compilado. Ao ser privado de operar os computadores responsáveis pela compilação máquina, fica prejudicada a capacidade do representante externo assegurar , a plena correspondência entre programas-fonte previamente analisados e os programas executáveis resultantes do processo de compilação.

Conclusões / Recomendações:
Para evitar questionamentos acerca da correspondência entre os programas fonte analisado antes da cerimônia e os programas-fonte utilizados para compilação, o TSE poderia facultar aos interessados uma análise dos programas assim que os mesmos estiverem finalizados.
Nessa análise, os interessados (por exemplo, os representantes do Ministério Público, Ordem dos Advogados do Brasil e dos Partidos Políticos) poderiam gerar códigos “hash” desses programas-fonte, preservando-os em seu poder até a ocasião da Cerimônia de Lacração. Paralelamente, o TSE poderia publicar, antes da cerimônia, esses códigos “hash”, na Internet.
Dessa maneira, ao calcular os códigos “hash” dos programas-fonte na cerimônia, seria possível compará-los aos códigos “hash” gerados previamente. Isso garantiria que os programas-fonte analisados são os mesmos que serão compilados.

Quanto a garantia de correspondência entre o programa-fonte apresentado na cerimônia e o programa-executável gerado na compilação, poderiam ser disponibilizados computadores aos interessados para compilação paralela. Durante a cerimônia, nas dependências do TSE, os representantes das entidades realizariam compilações paralelas, utilizando os mesmos programas-fonte, bibliotecas, compiladores e demais ferramentas necessárias.

Assim, seria possível o cálculo dos códigos “hash” dos programas-executáveis gerados e tais códigos poderiam ser comparados aos seus equivalentes, gerados a partir da compilação oficial dos programas-fonte realizada pelo TSE.

CONSIDERAÇÕES FINAIS

Os exames foram realizados com o objetivo de auxiliar o Tribunal Superior Eleitoral na melhoria contínua do Sistema de Votação Eletrônica. As propostas sugeridas neste documento visam contribuir principalmente com a transparência e a padronização dos procedimentos executados durante o período eleitoral. Tal padronização de procedimentos tem o intuito de mitigar o risco operacional inerente à sua execução e de aumentar a transparência do processo como um todo, visando fornecer à sociedade um modelo de Sistema Eleitoral ainda mais claro e definido.

Ressalva-se a condição de que as limitações de tempo imposta aos exames realizados, impossibilitaram o prévio conhecimento dos resultados intermediários deste trabalho por parte do Tribunal Superior Eleitoral. Sendo assim, é possível que algumas recomendações não sejam plenamente aplicáveis, ou que processo semelhante já tenha sido adotado, ou ainda que normatizações sugeridas já tenham sido elaboradas ou estejam em processo de elaboração.

Eduardo Soares de Paiva
Fábio Silva Vasconcelos
Fábio Leonel Orsi
Fernando Andrade Martins de Araújo
Gustavo Fleury Soares
Ricardo Silva Melo Fernandes
Ricardo Nagamine Mota

Conforme lista de presença

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.445/2009
Instituição Proponente	Marinha do Brasil
Responsável pela equipe de investigadores	Valter Monteiro Junior
Data	10/11/2009 e 11/11/2009
Horário de início (para efeito de premiação)	Em 10/11/2009: 9:30h Em 11/11/2009: 14:00h
Horário de término (para efeito de premiação)	Em 10/11/2009: 18:00h Em 11/11/2009: 17:30h
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança ☒ Gerador de Mídias ☒ Software de votação usado nas seções eleitorais **Hardware**: ☒ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor ☐ Lacres ☒ Mídias

	Procedimentos: ☒ Geração de mídias ☒ Etapas de preparação da urna ☐ Votação
Extensão do ataque	☒ Urna ou seção eleitoral ☐ Local de votação ☒ Zona eleitoral ☒ Município ☐ Unidade da Federação ☒ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☐ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☒ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	*O ponto de intervenção escolhido pelo investigador foi a modificação das mídias que são produzidas pelo Gerador de Mídias, com vias à introdução de arquivos maliciosos na urna eletrônica. A introdução dos arquivos maliciosos se daria nas seguintes etapas: geração das mídias (flash de carga, flash de votação e disquetes); interceptação das mídias após a geração e antes da preparação das urnas eletrônicas.*
Critério(s) de parada	

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**

	1. Valter Monteiro Junior	
	2. Cláudia Abreu da Silva	
	3. José Antônio de Mello Bartasevicius	
	4. Juliana da Costa Garret	
	5. Thiago Ferreira Tavares da Silva	
	6.	
	7.	
	8.	
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Rodrigo Carneiro Munhoz Coimbra	
	2. Marcus Guilherme de Amorim	
	3. Roberto Alves Gallo Filho	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Débora Nery Silva Gladiston da Silva Costa Wilson Henrique Veneziano	**Assinaturas**:
Comissão Avaliadora	Prof. Mamede Lima-Marques	**Assinaturas**:

4 Observadores externos

Conforme lista de presença

5 Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

4 (quatro) Disquetes
2 (duas) Flash Cards de 64Mb
1 (um) Computador HP (Pat. 030895) com SIS e Gerador de Mídias instalados
1 (um) Computador Positivo (Pat. 025818) dual boot, com Windows e Linux
1 (uma) Urna Eletrônica modelo 2008 (Pat. 446172)
Documentação dos arquivos das mídias
Documentação dos arquivos de entrada do Gerador de Mídias
Base de dados do Gerador de Mídias, arquivos o1sp00000.jez e o1sp707500174.jez
1 (um) Relatório de eleitores da seção 03, zona 174, município de São Bernardo do Campo
Instalação do MinGW com GCC 4.4 no computador Positivo (Windows)
Instalação do LILO no computador Positivio (Linux)

6 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

As mídias geradas não foram lacradas para transporte do local de geração de mídias para o local de

preparação das urnas eletrônicas.

7 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

Dia 10/11/2009
A equipe de apoio técnico forneceu informações sobre o funcionamento do processo eleitoral, do software Gerador de Mídias e da urna eletrônica (criptografia utilizada, sistema operacional e aplicativos).
Foram executados os seguintes procedimentos: A1) Criação de um arquivo executável na partição de dados da flash de carga, para verificar se o sistema da urna o identifica. A2) Foi feita a carga na urna, que não alertou sobre o arquivo estranho. B1) Modificação do arquivo eleicao1.dat, na flash de carga, para verificar o comportamento da urna. B2) Foi feita a carga na urna com a flash de carga alterada. B3) Foi emitido o aviso de erro pela urna (erro de assinatura do arquivo eleicao1.dat). C1) Formatação de um disquete a partir do Windows e cópia dos arquivos normalmente esperados no disquete, de modo a verificar se é possível gerar disquetes sem o Gerador de Mídias. C2) Urna ligada com o disquete gerado sem o Gerador de Mídias e a flash de votação. C3) A urna eletrônica acusou erro, já que a flash utilizada (de carga) havia sido alterada. C4) Realizada nova carga com nova flash de carga. C5) Urna ligada com a nova flash e o disquete. C6) Aplicativos de urna iniciados normalmente.
Dia 11/11/2009
Foi executado o seguinte procedimento:

1) Uma flash de carga gerada pelo Gerador de Mídias foi modificada, efetuando-se a instalação do LILO, ou seja, um outro boot loader (copiado na primeira partição), para verificar se seria possível iniciar outro sistema operacional na urna. 2) Feita a carga e o novo boot loader não foi executado, sendo feita a carga normalmente, pelo sistema do TSE.
A equipe de apoio técnico forneceu mais informações sobre o funcionamento do processo eleitoral, do software Gerador de Mídias e da urna eletrônica (criptografia utilizada, sistema operacional e aplicativos), sobretudo sobre o sistema de carregamento do sistema operacional (boot loader).

8 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

Os investigadores não obtiveram sucesso na execução do plano de testes tal como originalmente proposto (vide respectivo plano de testes do grupo).

Os investigadores não obtiveram sucesso nas suas tentativas técnicas de inserção de código malicioso, visto que sua conjectura sobre a possibilidade de inserção de tais arquivos, no ambiente de geração de mídias e na urna eletrônica não se confirmou devido ao emprego de mecanismos criptográficos e de segurança nos sistemas de votação (encriptação de partições no computador de geração de mídias e nas partições das flashs utilizadas nas urnas eletrônicas), comportamento dos softwares da urna eletrônica com relação aos disquetes (não é feita a cópia de arquivos não assinados do disquete para a urna) e por toda a cadeia de confiança (baseada em assinatura digital) estabelecida entres os aplicativos da urna eletrônica.

9 Observações

10 Apêndices

Estão apensos o relatório de eleitores e os demais documentos emitidos pela urna eletrônica.

11 Sugestões do(s) Investigador(es) para Melhoria

Não há sugestão dos investigadores do momento.

12 Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

1 (um) Cópia da resolução 22.712
1 (um) Cópia da resolução 22.713
1 (um) Cópia da resolução 22.714

13 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

Nenhum.

14 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

15h45 – Início dos Trabalhos
15h46 – Entrega e exposição do "Relatório de Exame dos Processos de Preparação da Votação e da Votação Eletrônica"
16h30 – Fim dos Trabalhos

15 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

O investigador obteve sucesso de acordo com a sua proposta original (vide respectivo projeto de testes).

16 Observações

17 Apêndices

Está apenso o "Relatório de Exame dos Processos de Preparação da Votação e da Votação Eletrônica".

18 Sugestões do(s) Investigador(es) para Melhoria

Os investigadores apresentaram sugestões que estão em anexo a este documento.

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	22.732/2009
Instituição Proponente	ISSA Capítulo Brasil
Responsável pela equipe de investigadores	Nelson Murilo de Oliveira Rufino
Data	11/11/2009
Horário de início (para efeito de premiação)	16h30
Horário de término (para efeito de premiação)	16h45
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança ☐ Gerador de Mídias ☐ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor ☐ Lacres ☐ Mídias **Procedimentos**: ☐ Geração de mídias ☐ Etapas de preparação da urna ☐ Votação

Extensão do ataque	☒ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☒ Alt. da vontade do eleitor ☒ Alt. da vontade do eleitor sem rastro ☐ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	*O ponto de intervenção escolhido pelo investigador foi a modificação das mídias utilizadas no processo eleitoral, mídias de carga, mídias de votação e disquetes de votação. Afim de que se fosse estudada a possibilidade de adulteração da tabela de eleitores.*
Critério(s) de parada	*Adulteração do arquivo de eleitores para que eleitores votem mais de uma vez em seções diferentes.*

2 Equipe de execução dos testes

	Nome completo	**Assinatura**
Investigador(es)	1. Nelson Murilo de Oliveira Rufino	
	2.	
	3.	

	4.	
	5.	
	6.	
	7.	
	8.	
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Marcelio Gonçalves Pereira	
	2. Hélio Luiz Alves Rodrigues	
	3. Ricardo Nobuyoshi dos Santos Makino	
	4. Roberto Alves Gallo Filho	
	5. Saulo Alessandre de Lima	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Gladiston Costa	**Assinaturas**:
Comissão Avaliadora	Antonio Montes Filho	**Assinaturas**:

4 Observadores externos

Conforme lista de presença

5 Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

2 (dois) Disquetes;
2 (dois) Flash cards, uma utilizada para votação – Unisys 32MB
1 (uma) Flash card utilizada como flash de carga - Apacer 2008 64 MB Código: 542042128-2
2(dois) Relatórios de eleitores das seções 09 e 10, zona 0174, município de São Bernardo dos Campos;
1 (um) Leitor USB de Flash Card;
1 (um) Micro-computador com habilidade para geração de mídias de carga, votação e disquetes Número de Série: BRB45002HS;
1 (um) Micro-computador para o desenvolvimento da proposta de teste. Contendo: Uma instalação dual boot com Windows XP e GNU/Linux Ubuntu. Código de patrimônio: 031.024;
2 (dois) Urna eletrônica modelo 2006 para realização de uma votação em modo oficial Códigos de patrimônio: 872670 e 871387
1 (um) Especificação do formato de arquivos de flash de carga
1 (um) Especificação do formato de arquivos de resultado de votação

6 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

A compact-flash de carga foi disponibilizada não se considerando os mecanismos lógicos e físicos envolvidos, como lacres, processos e procedimentos usualmente utilizados. Ou seja, o investigador obteve acesso à mídia sem que se demonstrasse como este acesso poderia ser realizado em um caso real.

7 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

DIA 10/11 – Início das atividades às 10h00m.

10h05 – É gerada uma *Compact Flash* de Carga

- CF: 64 MB – 542042128-2 – Flash de Carga.

10h10 – São geradas duas *Compact Flashes* de Votação

- CF: 32 MB – S/N – Flash de Votação.

10h13 – São gerados dois Disquetes de Votação

10h20 – Investigador analisa conteúdo da *Flash de Carga*

11h00 – Urna Eletrônica é carregada com Sistema Operacional oficial com a seção 09 e a votação é iniciada

11h30 – É entregue o arquivo de especificação do formato de arquivos da flash de carga

11h50 – É definido pelo investigador o processo para realizar uma votação, foram definidos os eleitores da seção 09, zona 0174, município de São Bernardo dos Campos de números 01 e 47. Que votaram da seguinte forma:

Eleitor 01	Eleitor 47
11001	11001
1101	1101
111-121	111-121
11	11
11	11

12h00 – Votação simulada encerrada com dois eleitores votantes

12h01 – Disquete e documentos emitidos pelas urnas entregues ao investigador para análise do conteúdo
13h30 – É explicado o processo de assinatura e verificação dos arquivos binários e de dados da urna eletrônica e da votação
15h15 – Entregue arquivo de especificação do formato de arquivos de resultado da votação
15h45 – Foi entregue ao investigador o disquete de verificação pré e pós eleição para ser executado na urna eletrônica e verificação dos logs
15h50 – O investigador analisa os logs da urna eletrônica
16h30 – Investigador duplica os primeiros 512 bytes do arquivo "eleitor.mnt" e concatena com o final deste mesmo arquivo
16h35 – A urna eletrônica é inicializada com a *flash* de carga modificada
16h38 – A urna retorna num erro de integridade no arquivo "eleitor.mnt"
18h45 – Atividades encerradas

8 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

O investigador não obteve sucesso de acordo com a sua proposta original (vide respectivo projeto de testes).

Os principais motivos do seu insucesso são os mecanismos de segurança utilizados no sistema operacional da urna eletrônica.

9 Observações

10 Apêndices

Estão apensos o relatório de eleitores e os demais documentos emitidos pela urna eletrônica.

11 Sugestões do(s) Investigador(es) para Melhoria

O investigador não apresentou sugestões de melhorias.

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.434/2009
Instituição Proponente	Superior Tribunal de Justiça - STJ
Responsável pela equipe de investigadores	Divailton Teixeira Machado
Data	10/11/2009 e 11/11/2009
Horário de início (para efeito de premiação)	Em 10/11/2009: 9:45h Em 11/11/2009: 11:00h
Horário de término (para efeito de premiação)	Em 10/11/2009: 15:30h Em 11/11/2009: 12:30h
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança √ Gerador de Mídias √ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal ☐Terminal do eleitor ☐ Lacres √ Mídias

	Procedimentos: √ Geração de mídias ☐ Etapas de preparação da urna √ Votação
Extensão do ataque	☐ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo √ Quebra de sigilo sem rastro ☐ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☐ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	*O ponto de intervenção escolhido pelo investigador foi a modificação das mídias que são retornadas para as juntas de apuração, incluindo a compact-flash de votação. Afim de que se fosse estudada a possibilidade de Negação de Serviço e de Quebra de Sigilo Eleitoral.*
Critério(s) de parada	

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**
	1. Divailton Teixeira Machado	
	2.	
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Marciano de Oliveira Meneses	
	2. Luiz Otávio Duarte	
	3. Ferrucio de Franco Rosa	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	André Siqueira	**Assinaturas**:
Comissão		**Assinaturas**:

Avaliadora	Antonio Montes Filho	

4 Observadores externos

Conforme lista de presença

5 Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

3 (três) Disquetes;
2 (duas) Flash cards, uma utilizada para votação – Unisys 16MB Códigos: 150035872-1 e 150035592-8;
1 (uma) Flash card utilizada como flash de carga - Apacer 2008 64 MB Código: 542063205-3
1 (um) Relatório de eleitores da seção 03, zona 174, município de São Bernardo dos Campos;
1 (um) Leitor USB de Flash Card "PQI";
1(um) Micro-computador com habilidade para geração de mídias de carga, votação e disquetes Código de patrimônio: 030.732;
1(um) Micro-computador para o desenvolvimento da proposta de teste. Contendo: Uma instalação dual boot com Windows XP e GNU/Linux Ubuntu. Código de patrimônio: 030.764;
1(uma) Urna eletrônica modelo 2004 para realização de uma votação em modo oficial Código de patrimônio: 132057
1(um) CD-ROM contendo a distribuição BackTrack 4.0 (live CD) – provido pelo proponente
1(um) CD-ROM contendo a distribuição Helix forense 3.0 (live CD) – provido pelo proponente

6 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

Retirada do lacre físico que é acomodado na compact-flash externa (de votação) e é mantido durante o período de "sessentena" (60 dias). Ou seja, relaxou-se a necessidade de uma eventual necessidade de se romper de forma a não restarem vestígios este lacre, visto que não era esse o intuito do teste.
A compact-flash de carga foi disponibilizada não se considerando os mecanismos lógicos e físicos envolvidos, como lacres, processos e procedimentos usualmente utilizados. Ou seja, o investigador obteve acesso à mídia sem que se demonstrasse como este acesso poderia ser realizado em um caso real.

7 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

DIA 10/11 – Início das atividades às 9h45m.
9:45h – Marciano, faz uma explicação inicial sobre o processo de carga do sistema eleitoral: - Compact flash de carga; - Processo de apuração, totalização local e estadual;
9:45h – Investigador: Inicia o sistema com o CD-live Helix 3.0, com a finalidade de observar se o sistema é carregado corretamente.
9:50h- Investigador: Solicita informações sobre os arquivos de *log* do sistema, que é explicada por Marciano.
9:50h – Divailton: Inicia o sistema com o CD-live BackTrack 4 beta para verificar seu correto carregamento.
10:00h – Marciano inicia a máquina geradora de mídias e explica o processo de escalamento de problemas do processo de geração de mídias de carga.
10:00h – Marciano explica o processo de lacração, incluindo o processo de assinaturas.
10:15h – Marciano explica o processo de contingenciamento de urnas no dia das eleições.
10:24h – Marciano gera uma *Compact Flash* em 2:08m para geração - CF: 64 MB – 542063205-3 – Flash de Carga.
10:30h – Marciano explica os propósitos dos diversos tipos de disquetes: - Gera uma *Compact Flash* de votação. - Gera um disquete de votação.
11:02h – Foi realizada a carga da UE: 132057 - Cod. Carga: 280.930.617.765.078.243.528.868
11:09h – Foram inseridos os disquetes de votação e flash de carga a UE foi iniciada pelo Marciano para auto-teste.

11:18h – Auto-teste com sucesso terminado.

É definido pelo investigador o processo para realizar uma votação, foram definidos os eleitores da seção 03, zona 174, município de São Bernardo dos Campos de números 1, 15, 30, 45, 60, 75. Que votaram da seguinte forma:

Eleitor 01	Eleitor 15	Eleitor 30	Eleitor 45	Eleitor 60	Eleitor 75
11001	11002	11003	11004	11005	11006
1101	1102	1103	1104	1105	1106
111-121	121-151	151-171	171-111	111-121	121-151
11	12	13	20	11	12
11	12	14	17	11	12

12:00h – Foi iniciado o software Adepto por parte do investigador para realizar a cópia das mídias de carga, votação e disquete. Entretanto, as cópias foram realizadas utilizando o comando "cat" para a partição sda5 da máquina utilizada pelo investigador, como no exemplo:

mount /dev/sda5 /home/ubuntu/imgs

cat /dev/sdb1 > sdb1.img

A compact flash de votação não pode ser lida pelo leitor IDE instalado na estação do investigador. Dado o horário, os procedimentos foram adiados para após o almoço.

14:30h Retorno dos trabalhos.

14.57h Em uma segunda tentativa com um leitor de cartões USB foi realizada a cópia da compact-flash de votação.

Marciano Explica os mecanismos de criptografia no sistema de arquivos.

15:14h O investigador vê que sua conjectura sobre a relação dos eleitores votantes e o registro digital do voto não pode ser sustentada, dados os mecanismos de aleatoriedade do

preenchimento do registro digital dos votos.
DIA 11/11 – Início das atividades às 11h.
11:00h O investigador faz uma busca nas imagens criadas no dia anterior, utilizando como argumentos de pesquisa as informações dos eleitores (nome, número); com o objetivo de correlacionar as informações.
11:30h O investigador analisa o sistema de arquivos buscando informações sobre os aplicativos que são iniciados durante o processo de inicialização da UE.
12:00h O investigador conclui a impossibilidade de inserção de arquivos maliciosos no processo de inicialização.

8 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

O investigador não obteve sucesso na sua tentativa de quebra de sigilo eleitoral, visto que sua conjectura sobre a relação dos eleitores votantes e o registro digital do voto não pode ser sustentada, dados os mecanismos de aleatoriedade do preenchimento do registro digital dos votos.

Em adicional não foi possível a inserção de códigos maliciosos, dada às camadas de segurança aplicadas no processo.

9 Observações

10 Apêndices

Estão apensos o relatório de eleitores e os demais documentos emitidos pela urna eletrônica.

11 Sugestões do(s) Investigador(es) para Melhoria

O investigador não apresentou sugestões de melhorias.

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	22.814/2009
Instituição Proponente	Pessoa Física
Responsável pela equipe de investigadores	Sérgio Freitas da Silva
Data	10/11/2009
Horário de início (para efeito de premiação)	11:13
Horário de término (para efeito de premiação)	11:42
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança ☐ Gerador de Mídias ☐ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal √ Terminal do eleitor ☐ Lacres ☐ Mídias **Procedimentos**: ☐ Geração de mídias ☐ Etapas de preparação da urna √ Votação

Extensão do ataque	√ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo √ Quebra de sigilo sem rastro ☐ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☐ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	*O único ponto de intervenção é a captação pelo receptor de rádio da radiação eletromagnética emitida pelo teclado da urna. Durante o teste, o receptor deve estar localizado o mais próximo possível do teclado da urna para simplificar o teste e dispensar a utilização de equipamentos especiais, tais como: osciloscópios e antenas especiais*
Critério(s) de parada	*Detectar, gravar e reproduzir a radiação eletromagnética do teclado da urna eletrônica.*

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**
	1. Sergio Freitas da Silva	
	2.	
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Fausto Carvalho Marques Silva	
	2. Ricardo Nobuyoshi dos Santos Makino	
	3. Roberto Alves Gallo Filho	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Gladiston da Silva Costa	**Assinaturas**:
Comissão Avaliadora	Antônio Montes Filho	**Assinaturas**:

4 Observadores externos

Conforme lista de presença

5

6 ,Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

2 (duas) flash de carga Apacer 2008;
2 (duas) flashes de votação – Unisys 16MB;
2 (dois) disquetes de votação;
2 (duas) urnas eletrônicas mod 2006 (Pat. 872670 e Pat. 871387);
1 (um) computador com Windows (Pat. 030745) e software Audacity – v 1.2.6.

7 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

Nenhum.

8 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

11h13min – Início dos testes;
11h13min – Investigador busca ajuste de frequência AM em um rádio analógico;
11h15min – Investigador informa não detectar nenhuma modificação no espectro AM e muda para FM;
11h16min – Investigador busca ajuste de frequência FM em um rádio analógico;
11h21min – Investigador informa detectar modificação no espectro em 90 MHz FM utilizando rádio analógico;
11h22min – Investigador busca ajuste de frequência AM em um rádio digital;
11h23min – Investigador informa detectar modificação no espectro em 89,1 MHz FM utilizando rádio digital;
11h29min – Investigador informa que foi executado ajuste fino na frequência para 89,2 MHz FM no rádio digital;
11h35min – Investigador inicia a gravação da radiação emitida no pressionamento da tecla "1" no terminal do eleitor na frequência de 89,1 MHz FM através de um rádio digital a uma distância de 5 (cinco) cm da face frontal da urna eletrônica em um computador utilizando o software Audacity;
11h40min – Investigador inicia a gravação da radiação emitida no pressionamento das teclas "1 e 7" no terminal do eleitor na frequência de 89,1 MHz FM através de um rádio digital a uma distância de 5 (cinco) cm da face frontal da urna eletrônica em um computador utilizando o software Audacity;
11h42min – Teste encerrado.

9 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

O investigador obteve sucesso nos ensaios tais quais propostos no ambiente de testes (vide plano de testes respectivo).

Entretanto, os testes como propostos não comprometem o sigilo do voto no ambiente de produção.

A razão do não comprometimento em produção deriva do fato de que a captura das emanações eletro-magnéticas propostas pelo investigador requerem distâncias bastante reduzidas do aparato de captura (rádio) para com a urna (nos testes, 5 a 10 centímetros).

Considerando que em um ambiente de votação, tal dispositivo deverá ser disposto fora da sala onde é realizada a votação (em distâncias típicas de alguns metros), e que a relação sinal-ruído deteriora-se rapidamente com a distância, os resultados obtidos pelo investigador não comprometem o sistema de votação atual com os recursos utilizados.

10 Observações

Qualquer observação ou resultado que não se encaixar nos tópicos acima, deverão ser informados neste item. Ex: descrição de equipamentos que foram usados durante o teste e não foram especificados no plano de teste; atrasos; problemas encontrados ou justificativas que prejudiquem ou inviabilizem o teste.

11 Apêndices

Foram gerados pelo investigador 3 arquivos de áudio no formato "wav" gravados no computador utilizado.

12 Sugestões do(s) Investigador(es) para Melhoria

O investigador sugeriu:
"Para solucionar o problema identificado no plano de teste sugerem-se as seguintes alternativas:

Solução 1) Emissão de ruídos aleatórios para confundir o inimigo e proteger o sigilo do voto;

- Esta solução poderia ser desenvolvida na própria uma para emular a radiação eletro magnética do teclado;

Solução 2) Blindagem do teclado ou de toda a urna eletrônica;

- Esta solução evitaria a interceptação da radiação eletromagnética provinda da urna ou do teclado;

Solução 3) Mudança da interface para tela sensível ao toque ("touch screen");

- Esta solução evitaria a radiação do teclado e permitiria a geração de teclados virtuais dinâmicos que aumentariam a segurança do processo de votação;"

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.448/2009
Instituição Proponente	Instituto Nacional de Criminalística / Departamento da Polícia Federal
Responsável pela equipe de investigadores	Thiago de Sá Cavalcanti
Data	13/11/2009
Horário de início (para efeito de premiação)	11h30
Horário de término (para efeito de premiação)	17h30
Sistemas Afetados	**Software**: ☒ Subsistema de Instalação e Segurança ☒ Gerador de Mídias ☐ Software de votação usado nas seções eleitorais **Hardware**: ☒ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor ☐ Lacres ☐ Mídias **Procedimentos**: ☒ Geração de mídias ☐ Etapas de preparação da urna ☐ Votação

Extensão do ataque	☐ Urna ou seção eleitoral ☐ Local de votação ☒ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☒ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☒ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	*O Principal ponto de intervenção desse teste é o Subsistema de Instalação e Segurança para permitir a alteração do sistema Gerador de Mídias.*
Critério(s) de parada	*Modificar o Subsistema de Instalação e Segurança para permitir a alteração do Sistema de Geração de Mídia e gerar mídia válida alterada.*

2 Equipe de execução dos testes

Investigador	**Nome completo**	**Assinatura**
	1. Thiago de Sá Cavalcanti	
Apoio técnico da Comissão	**Nome completo**	**Assinatura**
	1. Marcelo Henrique Pinto de Almeida	

Disciplinadora	2. Hélio Luiz Alves Rodrigues	
	3. Rodrigo Carneiro Munhoz Coimbra	
	4. Márcio Carneiro Rodrigues	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Wilson Henrique Veneziano Débora Nery Silva Gladiston da Silva Costa	**Assinaturas**:
Comissão Avaliadora		**Assinaturas**:

4 Observadores externos

Conforme lista de presença

5 Equipamentos, softwares, hardwares e demais materiais fornecidos pelo TSE

Listar todos os materiais disponibilizados

1 (um) Computador HP com SIS e Gerador de Mídias instalados

6 Relaxamentos nos mecanismos e procedimentos de segurança

Listar todos e quaisquer eventuais relaxamentos nos mecanismos e procedimentos de segurança padrão adotados pelo TSE e TREs e necessários para o sucesso do teste proposto.

A senha do usuário suporte foi concedida ao Investigador, e também a contra-senha para acesso completo à máquina do sistema Gerador de Mídias.

7 Passos realizados

Listar todos os passos realizados pelo investigador durante a realização dos testes, incluindo passos condicionais.

11h30 – Início dos trabalhos
11h35 – Investigador efetua o *login* com o usuário suporte
11h36 – O computador gerador de mídias solicita contra-senha para liberar acesso ao ambiente de suporte
11h37 – A contra-senha "lm2rjdxr" é passada ao investigador
11h40 – Investigador insere DVD com ferramentas de análise no computador gerador de mídias
11h42 – Investigador executa o *software PEBrowser Professional* e iniciou a análise do aplicativo PreVAD.exe
11h45 – Investigador executa o *software IDAPro Demo*
11h46 – Análise do da codificação do aplicativo PreVAD.exe
11h50 – Durante a análise investigador inicia *Debugger* do Windows "Win32"
11h52 – Investigador analisa estrutura de pastas do gerador de mídias
11h53 – Iniciou a análise da codificação do aplicativo VerificadordeAssinaturas.exe no *IDAPro*
11h56 – Busca aplicativo protfxp.sys no disco "C:"
12h01 – *IDAPro* travou
12h02 – Novamente iniciou a análise da codificação do aplicativo VerificadordeAssinaturas.exe no *IDAPro*
12h28 – Durante a análise o investigador inicia *Debugger* do Windows "Win32"
12h30 – Investigador dá controle total para o administrador na pasta "C:\Seguranca"
12h32 – Investigador inicia análise da codificação do aplicativo protfxp.sys no *IDAPro* e inicia o *debugger*
13h00 – Pausa para almoço

14h12 – Investigador efetua novo *login* com o usuário suporte
14h12 – O computador gerador de mídias solicita contra-senha para liberar acesso ao ambiente de suporte
14h14 – A contra-senha "25l0iqmc" é passada ao investigador
14h15 – Investigador continua a análise do aplicativo protfxp.sys no *IDAPro*
14h20 – Investigador efetua backup do aplicativo protfxp.sys na pasta "D:/Comum"
15h00 – Investigador altera o assembly do protfxp.sys para verificar as conseqüências
15h10 – Investigador reinicia o computador com as modificações do protfxp.sys
15h12 – Computador travou na inicialização
15h17 – Investigador reinicia o computador com DVD do WindowsPE
15h19 – Investigador restaura o aplicativo protfxp.sys
15h21 – Sistema Operacional reiniciou normalmente após restauro
15h22 – Investigador reinicia o computador com DVD do WindowsPE
15h25 – Investigador inicia nova análise do protfxp.sys
16h00 – Investigador instala o *software wingate*, que permite que se faça *login* no Windows com qualquer usuário registrado na máquina e senha arbitrária
16h05 – Investigador efetua *login* com o usuário suporte com senha arbitrária
16h06 – O computador gerador de mídias solicita contra-senha para liberar acesso ao ambiente de suporte
16h08 – Investigador efetua *login* com o usuário 10191 com senha arbitrária
16h09 – Sistema Operacional aceita senha arbitrária
16h20 – Investigador reinicia o computador com DVD do WindowsPE
16h25 – Investigador modifica permissões do usuário "10299" para administrador
16h30 – Investigador efetua *login* com usuário "10299"
16h35 – O computador gerador de mídias solicita contra-senha para liberar a modificação de grupo do usuário "10299"

16h45 – Investigador efetua *login* com usuário supervisor
16h47 – Investigador modifica permissões do usuário "10191" para administrador do sistema Gerador de Mídias
16h49 – Investigador efetua *login* normalmente no sistema com usuário "10191"
16h54 – Investigador reinicia o computador com DVD do WindowsPE
16h59 – Investigador demonstrou as ferramentas utilizadas durante a quebra da senha do Windows
17h03 – Investigador faz o login como suporte e recebe nova contra-senha
17h08 – Investigador tenta instalar o root kit, porém o antivírus impede a instalação
17h13 – Investigador desabilitou os serviços do antivírus
17h14 – Investigador instala com sucesso o root kit
17h20 – Os ataques propostos pelo Investigador seriam, segundo ele, facilmente detectáveis por auditoria nas mídias geradas pela máquina subvertida. O Investigador afirma que também é possível detectar a subversão em auditorias nas próprias máquinas.
17h30 – Investigador encerra seu procedimento de teste sem haver logrado sucesso na geração de mídia válida e incorreta

8 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

O Investigador não obteve sucesso na execução do plano de testes tal como originalmente proposto (vide respectivo plano de testes do grupo).

O investigador não obteve sucesso nas suas tentativas técnicas de inserção de código malicioso, visto que sua conjectura sobre a possibilidade de alteração da validação realizada pelo Subsistema de Instalação e Segurança não pode ser totalmente testada e se mostrou infrutífera. Ademais, a instalação do root kit só se mostrou viável após a desativação do antivírus.

9 Observações

O Investigador declara que os testes não foram abrangentes, uma vez que o ambiente de desenvolvimento e os sistemas de totalização não foram submetidos a escrutínio. E, devido ao seu formato, os testes não foram exaustivos.

10 Apêndices

Está apenso o CD com o Live XP utilizado pelo Investigador.

11 Sugestões do(s) Investigador(es) para Melhoria

O Investigador sugere que seja oficializada a política de segurança de bloqueio de boot por dispositivos quaisquer que não sejam o disco rígido da máquina. O Investigador ressalta que auditoria não deve ser considerada procedimento excepcional e, sim, rotineiro, pois é ela que garante a detecção de qualquer violação. Finalmente, o Investigador sugere que o acesso do usuário "supervisor" seja protegido por contra-senha.

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.289/2009
Instituição Proponente	Pessoa Física
Responsável pela equipe de investigadores	Mauro César Sobrinho
Data	10/11/2009
Horário de início (para efeito de premiação)	10/11/2009 – 14:00 horas
Horário de término (para efeito de premiação)	13/11/2009 – 18:00 horas
Sistemas Afetados	**Software**: ☒ Subsistema de Instalação e Segurança ☐ Gerador de Mídias ☒ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☐ Microterminal ☐ Terminal do eleitor ☒ Lacres ☒ Mídias **Procedimentos**:

	☐ Geração de mídias ☒ Etapas de preparação da urna ☐ Votação
Extensão do ataque	☒ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☒ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☐ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	Mídias geradas, arquivos assinados e lacres
Critério(s) de parada	Assinatura de binários com novas chaves e geração de nova mídia corrompida que seja considerada válida pela urna, carregando o sistema.

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**
	1. Patrícia Sumie Hayakawa	
	2. Lucas Brasilino da Silva	
	3. Charles Henrique Gonçalves Santos	
	4. ----------	----------
	5. ----------	----------
	6. ----------	----------
	7. ----------	----------
	8. ----------	----------
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Alberto Rios Júnior	
	2. Hélio Luiz Alves Rodrigues	
	3. Marcélio Gonçalves Pereira	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Gladiston da Silva Costa Débora Nery Silva Wilson Henrique Veneziano	**Assinatura**:

Comissão Avaliadora		**Assinatura**:

4 Observadores externos

Conforme lista de presença

5 Equipamentos, software, hardware e demais materiais fornecidos pelo TSE

1. 7 (sete) flash de Flash card Apacer 2008 64MB. Códigos: 542044192-1, 542106478-5, 542043190-8, 542043420-6, 542042555-6, 542043208-0 e 542045796-0.
2. 1 (um) disquete de votação;
3. 1 (uma) urna eletrônica, modelo 2000 (Patrimônio 222264);
4. 1 (um) computador (Patrimônio 031171) com Sistema Operacional Windows e software Gerador de Mídias e SIS instalados;
5. 1 (um) computador (Patrimônio 031127) com Sistema Operacional GNU/Linux Debian 5.0 instalado;
6. 1 (um) HD Externo de 250GB, contendo os seguintes aplicativos:
6.1. Repositório de Software do Linux Debian 5.0;
6.2. Código fonte do Kernel 2.6.16.62;
6.3. GCC 4.1.2;
6.4. GLIBC;
6.5. Biblioteca OpenSSL;
6.6. NASM;
6.7. Source Navigator;

6.8. Indent;
6.9. Script do site jukie.net (detalhado nas pré-condições);
7. Relatório de eleitores da seção 02, zona 174, município de São Bernardo do Campo;
8. *FIM*

6 Relaxamentos nos mecanismos e procedimentos de segurança

1. Acesso físico às mídias e disquete utilizados na eleição fora dos lacres.

7 Passos realizados

DIA 10/11/2009
1. 14:00 horas – Início dos testes com 4 investigadores; Ausentes os senhores Lucas Brasilino da Silva (chegou 10 minutos depois) e Mauro César Sobrinho (ausente o dia todo);
2. Geração de flash de carga (seção 3, mesa 2442);
3. Verificação e viabilização de pré-condições para o teste;
4. Análise da mídia gerada;
5. Solicitado código fonte da urna para que seja usado no teste;
5.1. Comissão disciplinadora é consultada sobre a possibilidade de disponibilizar o código; 5.2. Comissão disciplinadora decide não liberar acesso ao código fonte durante os testes;
5.2.1. Motivo 1: TREs não possuem os códigos fonte, tornando o teste artificial (Wilson); 5.2.2. Motivo 2: Regras dos testes publicadas anteriormente e critério de isonomia (outros grupos não puderam usar) (Amandio).

5.2.3. Lucas Brasilino entende e concorda com o procedimento, dando continuidade ao teste.
6. 14:30 horas – Lucas Brasilino sai com técnico do TSE para providenciar itens de pré-condição (Repositório Debian e código fonte do Kernel 2.6.16.62) para os testes que não estavam instalados na máquina;
7. Como o repositório disponibilizado possui aplicativos que não foram solicitados na pré-condição da proposta de teste, a equipe foi orientada a não usar aplicativos não relacionados na proposta. Caso haja a necessidade de utilização de algum aplicativo não listado na relação, a comissão técnica e a comissão disciplinadora deverão ser avisadas para que este aplicativo conste do relatório de acompanhamento dos testes;
8. Utilização do Repositório Debian, fornecido pela Justiça Eleitoral, para instalação de aplicativos a serem utilizados nos testes;
9. Tentativa de interpretação de UNISYS.JE;
10. Tentativa de interpretação de Setor de boot;
11. Tentativa de decifrar o ue.pub usando rotinas em linha de comando da biblioteca OpenSSL;
12. Desenvolvimento, por parte da equipe, de um aplicativo (em linguagem C) para buscar um padrão em um arquivo;
13. Identificação de um padrão e tentativa de decifrar arquivos utilizando a biblioteca OpenSSL (função aes-256-ecb);
14. 18:00 horas – Primeiro dia de testes encerrado.
15. *FIM*
DIA 11/11/2009

16. Equipe Ausente o dia todo.
17. *FIM*
DIA 12/11/2009
18. 13:30 horas – Início dos testes com 4 investigadores; Ausentes o senhor Mauro César Sobrinho (ausente o dia todo);
19. A equipe trouxe material para tentativa de abertura de lacre sem deixar vestígios.
19.1. Material: 19.1.1. Estilete; 19.1.2. Adesivo universal para artesanato, transparente e sem Tolueno, marca PEGAMIL.
20. A equipe se dividiu entre a codificação (desenvolvimento de um aplicativo para buscar um padrão em um arquivo) e a tentativa de rompimento do lacre;
21. Tentativa por parte da equipe de decifrar o Kernel;
22. Criação de um script para facilitar a tentativa de decifrar o Kernel;
23. Tentativa de dar carga na urna com uma compact flash orginal; 23.1. A urna não carregou – falha operacional.
24. Geração de flash de carga (seção 3, mesa 2442) com o aplicativo gerador de mídias;
25. Carga na urna com flash não-modificada, com objetivo de testar a flash e verificar os passos quando se carrega a urna normalmente com o sistema oficial;
26. Paralelamente ao passo anterior, a equipe faz pequeno corte no verso do lacre para retirar a

flash de carga. Este corte é perceptível se analisado o lacre individualmente. Se o lacre for visto somente pela frente e junto a um conjunto grande de outros lacres iguais, pode ser que não seja percebido o corte. Dessa forma, a equipe de apoio técnico decidiu relatar e tirar fotografias dos lacres e do corte feito no lacre. Essas imagens irão compor o relatório no item apêndice. Decidiu-se em conjunto com a equipe de investigadores que esse registro visual do lacre será feito no dia seguinte.
27. 18:00 horas – Terceiro dia de testes encerrado.
28. *FIM*
DIA 13/11/2009
29. 14:00 horas – Início dos testes com 3 investigadores; Ausentes os senhores Mauro César Sobrinho e Ricardo Selling de Oliveira (ausente o dia todo);
30. Equipe gerou um software que fez uma varredura em todo o sistema de arquivo, separando blocos de 32 bytes (/root/chaves-all-hdc-classificado.txt), para serem posteriormente utilizados;
31. A partir dos blocos de 32bytes, foi submetido ao software desenvolvido no local (parte em C – find22.c e findall.c - e outra parte em bash script – chaves.sh. Todos os arquivos foram retidos nas estações utilizadas para os testes) e fez o teste indicando a chave a ser utilizada (chave que está na linha 55 do arquivo citado);
32. Decifraram o Kernel e procuraram sequencias de caracteres conhecidas que existem dentro do Kernel. (processo de decriptografia OK e em seguida procura das strings);
33. Modificaram algumas strings conhecidas dentro do Kernel e cifraram novamente utilizando a mesma chave utilizada para decifrar. ID da flash modificada: 542043190-8. Apace de 64MB.
34. Equipe se prepara para testar a inicialização do Kernel.
35. Equipe testou mídia de carga modificada na urna.

36. O Kernel foi inializado com sucesso, porém o SAVD, durante a execução do SCUE, detectou a modificação realizada não executando a carga da urna eletrônica. mensagem: Erro na integridade do sistema / Ocorrência: SAVDi-TSE(113-[uenux]) / Erro: -19
37. Outro teste realizado foi a remoção da assinatura do uenux dentro do avboot.vsg, porém o SAVD, dentro da execução do SCUE, detectou a modificação do avboot.vsg e remoção da assinatura do uenux.
38. 18:00 horas – Quarto e último dia de testes encerrado.
39. *FIM*

8 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

Os investigadores não obtiveram sucesso nos testes propostos (vide respectivo projeto de testes).

As intervenções dos investigadores centraram-se na decifração do kernel do sistema, modificação do kernel e cifração. Apesar de obterem sucesso na decifração, alteração e recifração, o investigadores não obtiveram sucesso na carga do sistema.

A razão do insucesso é a da detecção de adulteração pela urna eletrônica da modificação dos arquivos por meio do sistema SAVD. O mesmo detectou a modificação já no teste inicial de integridade (durante a execução do SCUE)

Adicionalmente ao proposto no plano de testes, a equipe executou o rompimento de um lacre de mídias por meio de corte. A adulteração é perceptível. A percepção da adulteração demanda atenção. Em apêndice constam fotos dos lacres.

9 Sugestões dos Investigadores para Melhoria

Os investigadores sugerem:

1. Aumento do controle de acesso físico aos locais de carga das urnas e equipamentos utilizados nesse procedimento, independente de horário;

2. Normas padronizando os controles mínimos de acesso físico nas dependências da Justiça Eleitoral (em todo o país) para execução da carga nas urnas (CFTV, tempo mínimo de armazenamento das fitas CFTV, controle de entrada e saída de equipamentos eletrônicos (inclusive celulares, smart phones, pen drives e outros dispositivos de armazenamento), entrega das mídias de carga com lacre aos técnicos responsáveis com notas de recebimento etc);

3. Fazer uma análise aprofundada dos procedimentos relacionados a lacre de urnas, mídias etc.

4. Que seja feito um trabalho para definir controles para todos os locais de armazenamento e operação de equipamentos relacionados diretamente com o sistema eleitoral brasileiro e que estes locais sejam homologados (certificados) para operar dentro do sistema eleitoral;

5. Como o sistema de voto eletrônico é classificado como de segurança nacional, é recomendável que estações usadas no desenvolvimento do sistema possuam controles mais rígidos de utilização, principalmente com relação à navegação na Internet, uso de dispositivos de mídia removível, controle das interfaces diversas dos equipamentos, manuseio de códigos fonte (cópia, impressão etc);

6. Repositório dos códigos fonte com rastreamento (log) de acesso aos arquivos (seja via sistemas de controle de versão, seja via sistema de arquivos). Envolver nesse processo tanto os administradores de rede que têm total acesso ao servidor, quanto aos desenvolvedores. Esses controles visam salvaguardar a TI em caso de vazamento indevido de informação;

7. Adotar política de segregação de informação (need to know) no processo de desenvolvimento de sistemas e também um controle via assinatura por parte do desenvolvedor dos códigos desenvolvidos pelo mesmo, para atribuição de responsabilidades e homologação do software desenvolvido;

8. Reavaliação do Kernel usado, visto que o Kernel do Linux é regido pela licença GPL, que preconiza acesso livre ao código fonte e todas as modificações feitas no Kernel irrestritamente. A equipe entende que não seguir essa determinação é uma violação da licença GPL. Assim, recomenda-se a utilização de um Kernel regido pela licença BSD.

9. Armazenamento da chave deveria ser em regiões não contíguas no sistema de arquivo ou através de um conjunto de chaves executar uma operação para extrair a chave utilizada.

10. A publicação do hash do kernel em claro, que abre a possibilidade de utilizar várias chaves para cifrar o Kernel.

10 Observações

1. A equipe não compareceu aos testes durante os seguintes períodos:

    1.1. 10/11/2009 – Período da manhã;

    1.2. 11/11/2009 – Período da manhã;

    1.3. 11/11/2009 – Período da tarde;

    1.4. 12/11/2009 – Período da manhã;

    1.5. 13/11/2009 – Período da manhã;

2. A equipe trouxe o seguinte material que não foram especificados no plano de teste:

    2.1. Estilete comum;

    2.2. Adesivo universal para artesanato, transparente e sem Tolueno, marca PEGAMIL.

        2.2.1. O referido material não foi utilizado em nenhum momento e a equipe preferiu não deixar a cola fazer parte dos autos, levando a mesma.

3. A equipe entende que dificulta (prejudica, mas não inviabiliza) os testes a impossibilidade de acesso ao código fonte dos aplicativos a serem testados, alegando que seria possível conseguir os códigos por meio de artefato malicioso, "Engenharia Social", suborno, extorsão etc.

4. FIM

11 Apêndices

Foram geradas pela equipe de investigadores e pela equipe de apoio técnico 03 imagens (frente, verso e corte), como apresentado a seguir.

Figura 1 – Lacre de mídia (frente)

Figura 2 – Lacre de mídia (verso)

Figura 3 – Lacre de mídia (corte)

Acompanhamento da execução do Plano de Teste

1 Informações gerais

Protocolo do Plano de Teste	23.432/2009
Instituição Proponente	TST
Responsável pela equipe de investigadores	Carlos Eduardo Negrão de Oliveira
Data	13/11/2009
Horário de início (para efeito de premiação)	13/11/2009 – 11:00 horas
Horário de término (para efeito de premiação)	13/11/2009 – 13:20 horas
Sistemas Afetados	**Software**: ☐ Subsistema de Instalação e Segurança ☐ Gerador de Mídias ☐ Software de votação usado nas seções eleitorais **Hardware**: ☐ Microcomputador para geração de mídias ☒ Módulo Impressor ☐ Microterminal ☐ Terminal do eleitor ☐ Lacres ☐ Mídias **Procedimentos**:

	☐ Geração de mídias ☒ Etapas de preparação da urna ☐ Votação
Extensão do ataque	☒ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Provável Impacto	☐ Quebra de sigilo ☐ Quebra de sigilo sem rastro ☒ Alt. da vontade do eleitor ☐ Alt. da vontade do eleitor sem rastro ☒ Desacreditação do sistema
Lista de pontos de intervenção apurada durante a realização do teste	Local de armazenamento da urna após procedimento de carga antes da impressão da zerésima.
Critério(s) de parada	Impressão dos relatórios.

2 Equipe de execução dos testes

Investigador(es)	**Nome completo**	**Assinatura**
	1. Carlos Eduardo Negrão de Oliveira	
	2. ----------	----------
	3. ----------	----------
	4. ----------	----------
	5. ----------	----------
	6. ----------	----------
	7. ----------	----------
	8. ----------	----------
Apoio técnico da Comissão Disciplinadora	**Nome completo**	**Assinatura**
	1. Saulo Alessandre de Lima	
	2. Gilmar Leal da Silva	
	3. Ferrucio de Franco Rosa	

3 Equipe de acompanhamento dos testes

Comissão Disciplinadora	Gladiston da Silva Costa Débora Nery Silva Wilson Henrique Veneziano	**Assinatura**:

Comissão Avaliadora	Ricardo Dahab	**Assinatura**:

4 Observadores externos

Instituição	**Nome**	**Cargo**	**Telefone e e-mail**	**Assinatura**
Sigla da instituição	*Nome completo do expectador*	*Cargo do expectador*	*Telefone e e-mail do expectador*	*Assinatura do expectador*
Conforme lista de presença.	...	...	...	...
...	...	...	...	...

5 Equipamentos, software, hardware e demais materiais fornecidos pelo TSE

9. 1 (uma) Urna Eletrônica (modelo 2004 / patrimônio-132057);
10. 1 (uma) flash de carga (série-542042186-2);
11. 1 (uma) flash de votação (série-542037904-0);
12. 1 (um) disquete de votação;
13. *FIM*

6 Relaxamentos nos mecanismos e procedimentos de segurança

2. Acesso físico a urna eletrônica;
3. Acesso ao código fonte com algoritmo do hash do código de verificação do boletim de urna (possível durante a auditoria do código fonte) para criação de um boletim adulterado aparentemente verdadeiro;
4. Acesso a uma bobina oficial ou tempo para utilizar a disponível na urna;
5. *FIM*

7 Passos realizados

DIA 13/11/2009
40. 11:00 horas – Início dos testes com 1 investigador;
41. Verificação e viabilização de pré-condições para o teste;
42. Explanação do processo eleitoral;
43. Geração de flash de carga (seção 7), de flash de votação e disquete;
44. Preparação da urna (carga da urna, autoteste);
45. Impressão de zerésima;
46. Votação com 4 eleitores;
47. Encerramento da seção;
47.1. Impressão dos boletins de urna; 47.2. Análise dos boletins;
48. 12:40 – Preparação da urna (carga da urna; autoteste);
49. Preparação de um boletim previamente impresso para inserir no módulo impressor;
50. Concatenação de várias vias de BU com fita adesiva objetivando simular a impressão de várias vias.
51. Inserção dos boletins juntos com fita adesiva previamente impressos no módulo impressor de forma invertida (face que imprime termicamente virada para o lado oposto);
52. Impressão de zerésima (previamente impressa);
53. Votação com 4 eleitores;
54. Encerramento da seção;
54.1. "Impressão" (apenas foram expelidos) dos boletins de urna (previamente impressos), com diferença no tamanho do boletim gerado em relação ao pré-impresso, devido à

	impossibilidade de prever o tamanho do relatório a ser gerado (o atacante não conseguiria prever quantos candidatos receberam realmente os votos e, portanto, a margem de erro do tamanho do BU é muito grande, inviabilizando a previsibilidade do comprimento). Os cortes dos Boletins de Urna pré-impressos foram distantes das posições ideais, evidenciando a violação;
FIM DO TESTE	

8 Sugestões dos Investigadores para Melhoria

O investigador sugere:

11. Inserir uma impressão de assinatura digital no Boletim de Urna, para garantia da integridade e autenticidade do boletim;

12. Alterar o procedimento de impressão dos relatórios das urnas para incluir a seguinte recomendação:

    a. Verificar o lado do papel que foi impresso. Isto deverá ser feito para cada modelo de urna, pois existem diferenças entre os modelos atuais;

13. Durante a impressão, via software, questionar o operador sobre o lado do papel no qual o relatório está sendo impresso.

14. FIM

9 Observações

5. O objetivo do teste foi melhor detalhado pelo investigador, após melhor conhecimento do processo eleitoral, consistindo de:

   5.1. O objetivo principal do teste é a substituição do módulo impressor após o relatório de carga e antes da impressão da zerésima. Assim, a unidade de impressão teria a zerésima e todas as vias de impressão do BU já impressas e durante a impressão pela urna seriam impressos os relatórios já armazenados, resultando na impugnação da urna devido à divergência entre os votos impressos e os votos digitais.

   5.2. A grande variabilidade do comprimento do BU em função da impossibilidade de o atacante prever quantos candidatos receberão votos, torna inviável o ataque, pois o atacante não teria controle do comprimento dos BUs o que implicaria no corte em pontos não previstos e evidenciando a fraude.

   5.3. O ataque em geral é pré-condicionado a uma série de fatores (acesso à urna, não emissão de vias adicionais do BU, não percepção do mesário da impressão na face invertida, etc.) sendo, portanto, teoricamente possível, mas impossível na prática. Com a implementação da assinatura digital na impressão o ataque fica impossibilitado.

6. FIM

10 Apêndices

Foi gerado pelo investigador 1 conjunto de impressões da urna (comprovante de carga, comprovante de autoteste, zerésima, 5 vias obrigatórias e uma via adicional de boletins de urna).

11 Avaliação Preliminar do Teste

Avaliação preliminar do teste indicando se houve sucesso ou não e demais informações relevantes obtidas.

1. O investigador não obteve sucesso nos ensaios tais quais os constantes na proposta de testes; 2. A razão do insucesso dos testes propostos alegada pela equipe foi: 2.1. Impossibilidade de danificar ou reprogramar a impressora da urna para realizar o teste. Mas, se o papel for invertido, esta barreira pode ser superada; 2.2. Necessidade de uma impressão idêntica à impressa pela urna ou impossibilidade de viabilizar cortes pela grande variabilidade de tamanhos nos relatórios a serem gerados; 3. A sugestão feita pelo investigador é viável e recomendável que seja implementada;