



## Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

### Relatório dos resultados da realização dos Testes Públicos

#### Grupo 06

##### Representando a Universidade do Ceará

André Luis Moura dos Santos – Doutor em Ciência da Computação – UC/EUA

Márcio André Souto Correa – Mestrando em Computação Aplicada – UECE

Luiz Gonzaga Mota Barbosa – Graduando em Ciência da Computação – UECE

Saulo Rangel Ferreira Hachem – Graduando em Ciência da Computação - UECE

#### Plano de Teste G6PT1

Teste de Segurança do Sistema Eletrônico de Votação do TSE

#### Conteúdo deste relatório

1. Plano de Testes original, submetido pelos Investigadores
2. Acompanhamento dos fatos pela Equipe de Apoio
3. Resultados do Teste
4. Conclusões
5. Futuras Possibilidades

**TSE/SRCOR****7.002.067/2012**

15/03/2012 - 15:20



## Plano de Teste do Sistema Eletrônico de Votação

### 1 Informações gerais

Título do plano de teste	Teste de Segurança do Sistema Eletrônico de Votação do TSE
Instituição proponente (se aplicável)	INSERT/UECE
Responsável	nome: André Luiz Moura dos Santos e-mail: <a href="mailto:andre@dossantos.org">andre@dossantos.org</a> telefone (do autor ou responsável): (085) 9933-5729
Sistemas afetados	<b>Software:</b> <i>Software de votação usado nas seções eleitorais.</i>  <b>Hardware:</b> <input type="checkbox"/> Microterminal <input type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacres <input checked="" type="checkbox"/> Mídias  <b>Procedimentos:</b> <input type="checkbox"/> Carga da urna <input checked="" type="checkbox"/> Votação
Duração estimada do teste (em minutos)	60
Extensão do ataque	<input checked="" type="checkbox"/> Urna ou seção eleitoral <input checked="" type="checkbox"/> Local de votação <input checked="" type="checkbox"/> Zona eleitoral <input checked="" type="checkbox"/> Município <input checked="" type="checkbox"/> Unidade da Federação <input checked="" type="checkbox"/> País
Conhecimentos necessários	[Mínimos conhecimentos técnicos necessários para a realização do teste] <i>Software Básico, Estrutura de Dados, Segurança</i>

**Observações:**

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

### 2 Reservado ao Tribunal Superior Eleitoral (TSE)

Protocolo	Data
	<b>Resultado</b> <input type="checkbox"/> Aprovado <input type="checkbox"/> Aprovado com ressalvas <input type="checkbox"/> Reprovado



A large, thin, curved line, possibly a signature or a mark, spans across the middle of the page.

A small, stylized signature or mark in the bottom left corner.



### 3 Detalhamento do teste

#### 3.1 Resumo do teste

Será avaliada a possibilidade de relacionar o voto a um eleitor. Para isso, serão analisadas a lista de eleitores votantes com o RDV - Registro Digital de Voto.

#### 3.2 Fundamentação

Dependendo do tipo de estrutura de dados utilizada para armazenar estes dados, pode ser possível inferir o voto do eleitor dada a forma sequencial de gravação destas estruturas. Por exemplo, o caso mais simples poderia ser o seguinte. Uma lista sequencial armazena os eleitores que votaram, e outra lista também sequencial armazena os votos dos eleitores. Embora não haja nenhuma ligação direta do eleitor com o voto, podemos inferir com probabilidade de 100% de acerto que o eleitor que ocupa a posição de índice "i" da lista de votantes é o responsável pelo voto de índice também "i" da lista de votos computados daquela urna.

#### 3.3 Precondições para o teste

Grupo de investigadores:

- ▲ Prof. PhD. André Luiz Moura dos Santos - Professor do Departamento de Ciência da Computação da Universidade Estadual do Ceará e diretor do grupo de pesquisa em Segurança da Informação Information Security Research Team - INSERT.;
- ▲ Márcio André Souto Correia, mestrando em Computação Aplicada pela UECE e membro do INSERT;
- ▲ Luiz Gonzaga Mota Barbosa, graduando em Ciência da Computação pela UECE e membro do INSERT e
- ▲ Saulo Rangel Ferreira Hachem, também graduando em Ciência da Computação pela UECE e membro do INSERT.

Como os dados relacionados aos eleitores votantes e o RDV estão criptografados no ambiente da urna e na MR - Memória de Resultado, consideramos que o atacante pode ter acesso a essas informações em texto claro em algum momento, seja na sessão, na zona, no TRE ou no TSE. Assim, para a execução deste teste será necessário acesso aos dados gerados por nosso grupo na urna de teste em texto claro.

#### 3.4 Escopo - Superfície de Ataque

Os componentes do sistema de votação eletrônica que sofrerão atuação/alteração por parte da equipe executora do teste, serão:

- ▲ Material : urna eletrônica, mídias, lacres, código fonte do software da urna;
- ▲ Ambiente : ambiente de teste promovido pelo TSF e
- ▲ Procedimento : análise do processo de gravação do RDV e respectivas mídias envolvidas.





### 3.5 Janela de atuação simulada do atacante

As janelas de atuação que serão necessárias são:

- ▲ Acesso às mídias de armazenamento.
- ▲ Acesso à urna eletrônica
- ▲ Acesso à memória flash de carga gerada

### 3.6 Pontos de intervenção

Pontos de intervenção que serão analisados são:

- ▲ software
- ▲ hardware
- ▲ procedimentos
- ▲ mídias
- ▲ lacres.

### 3.7 Passos a serem realizados e material necessário

Lista de passos:

1. O Atacante tem acesso aos dados de uma ou mais urnas em texto claro referente aos eleitores que votaram
2. O Atacante também tem acesso ao dados de uma ou mais urnas em texto claro referente ao RDV
3. O Atacante verifica a posição de um eleitor votante na estrutura de dados. (15 min)
4. O Atacante infere a posição do respectivo voto daquele eleitor na estrutura de dados da RDV, baseado na posição do eleitor na estrutura de dados dos eleitores votantes. (30 min)
5. O Atacante acessa a posição inferida no RDV e tem acesso ao voto do eleitor. (15 min)
6. Fim

Recursos necessários:

1. Equipe do INSERT
2. Computador Pessoal
3. Leitor de Compact Flash
4. Urna Eletrônica
5. Dados do MR – Memória de Resultado em Texto Claro

### 3.8 Possíveis resultados e impacto

O resultado esperado é a quebra do sigilo do voto. O ataque pode se estender a toda uma região (TRE) ou até mesmo ao país (TSE), caso o atacante faça parte da contabilização dos votos em um destes tribunais. Caso a estrutura de dados para armazenamento dos eleitores que votaram e o RDV sejam preservadas desde a geração na urna até sua totalização no TSE, e essa estrutura de dados não grave essas informações de forma realmente aleatória, a probabilidade é de 100% de sucesso caso exista motivação do atacante.

### **3.9 Rastreabilidade**

Embora os dados necessários para a realização do ataque sejam exportados da urna criptografados, em algum momento eles terão que ser acessíveis em texto claro para a apuração dos votos. Partindo do pressuposto que a possibilidade de ligar o eleitor a um voto deve ser completamente nula, a ínfima possibilidade de que tal situação possa ocorrer já é motivo suficiente para a mitigação do ataque. Quanto a rastreabilidade do ataque, provavelmente ele passaria despercebido se fosse realizado por alguém que participa do processo de apuração e tem acesso aos dados que foram gerados nas urnas referentes aos eleitores votantes e o RDV.

### **3.10 Solução proposta**

Para tornar o sistema resistente ao ataque proposto as estruturas de dados utilizadas para armazenar os eleitores que votaram e os seus votos propriamente dito devem utilizar funções randômicas ou pseudo-randômicas. Tais funções teriam como objetivo impossibilitar a correlação destes dados por meio da inferência da posição dos elementos com base na sua ordem de inserção na estrutura de dados utilizada.



## CAPÍTULO VII

### DAS INSCRIÇÕES DO(S) INVESTIGADOR(ES) E/OU GRUPO(S) DE INVESTIGADORES

**Art. 10.** As inscrições do(s) investigador(es) e/ou do(s) grupo(s) investigadores deverão ser realizadas no período de **2 a 17 de fevereiro de 2012**, observando-se:

I - o formulário de inscrição estará disponível no sítio eletrônico do TSE na internet ([www.tse.jus.br](http://www.tse.jus.br)), durante o período citado no *caput* deste artigo;

II - ao formulário de inscrição, impresso e preenchido, deverão ser anexados os documentos comprobatórios do investigador ou, em se tratando de grupo de investigadores, de todos os seus integrantes, de acordo com as informações que forem declaradas no formulário;

III - o formulário de inscrição e os documentos comprobatórios deverão ser:

a) encaminhados por SEDEX ou carta registrada, postados até o dia **17 de fevereiro de 2012**, endereçados à Secretaria de Tecnologia da Informação do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF, CEP 70.070-600); ou

b) protocolizados no Protocolo Administrativo, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF), até as **19h do dia 17 de fevereiro de 2012**.

**Parágrafo único.** O(s) investigador(es) e/ou componentes do(s) grupo(s) de investigadores declara(m) ter ciência que:

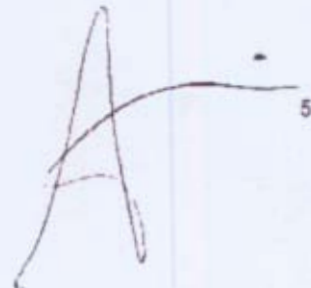
I - deve(m) disponibilizar à Comissão Disciplinadora dos Testes Públicos de Segurança toda a documentação sobre os materiais utilizados e seus procedimentos durante as atividades, independente do resultado obtido nos testes públicos de segurança;

II - deve(m) apresentar à Comissão Disciplinadora dos Testes Públicos de Segurança todos os materiais utilizados e seus procedimentos durante as atividades; e

III - autoriza(m) o uso de sua imagem pela Justiça Eleitoral, com a finalidade de divulgar o processo de testes públicos de segurança realizado pelo TSE, entendendo-se como imagem qualquer forma de representação, inclusive a fotográfica, bem como o processo audiovisual que resulta da fixação de imagens, com ou sem som, que tenha a finalidade de criar, por meio de sua reprodução, a impressão de movimento, independentemente dos processos de sua captação, do suporte usado inicial ou posteriormente para fixá-lo e dos meios utilizados para sua veiculação.

**Art. 11.** Poderão participar na condição de investigador(es) ou de grupo(s) de investigadores cidadãos brasileiros maiores de dezoito anos que preencham os requisitos constantes do formulário de inscrição.

§ 1º É permitida a participação individual de investigador(es) que não participar(em) de grupo de investigadores.







## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G6PT1</b>	Coordenador:	André Luiz Moura dos Santos	
	Investigador 1:	Marcio André Souto Correia	
	Investigador 2:	Luiz Gonzaga Mota Barbosa	
	Investigador 3:	Saulo Rangel F. Hachem	

Informações do Acompanhamento					
Data:	22/03/2012	Hora de Início:	15:30	Hora de Término:	15:55
Resp. Acomp.:	Marco Constantino			Rubrica:	

Dados do Teste			
Título do teste:	Teste de Segurança do Sistema Eletrônico de Votação do TSE		
Início do teste (Data/Hora):	22/03/2012	15:30	
Termino do teste (Data/Hora):	22/03/2012	15:55	
Critério de Parada:			

Relaxamento nos mecanismos e procedimentos de segurança
Para este teste não foram necessários relaxamentos de segurança.

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Procedimento de votação para simulação de um conjunto de votos	
2	Procedimento de fechamento da seção eleitoral	
3	Acesso a mídia de resultado	
4	Leitura dos arquivos "rdv.dat" e "el.dat"	
5	Reconstrução das estruturas de dados	
6	Correlação dos registros do arquivo "rdv.dat" e "el.dat"	

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
15:35	Simulação de um montante de votos, no caso 9 votos. Após o fechamento da seção eleitoral o investigador teve acesso a Mídia de resultado. Com ela em mãos, foi realizada a leitura dos arquivos rdv.dat e el.dat. Após o acesso ao arquivo os investigadores foram informados sobre as estruturas encontradas nestes e as funções de randomização utilizadas Os investigadores solicitaram acesso ao código fonte para identificar as



	rotinas responsáveis pela geração do arquivo rdv.dat. Foram verificadas as especificações referentes aos arquivos binários do rdv.dat e el.dat.
15:45	Os investigadores não obtiveram sucesso na análise proposta e encerraram o teste.

#### Conclusões sobre o teste

Segundo explicações da equipe do Tribunal Superior Eleitoral (TSE) ficou evidente a utilização de uma função de randomização para alocação dos elementos na estrutura do arquivo rdv.dat.
As explicações davam conta que a função de randomização estava sendo utilizada de forma a garantir a difícil reconstrução da sequência de votos realizados.
Por outro lado, não foi possível verificar com maior profundidade os arquivos gerados por estes procedimentos afim de buscar formas de reprodução da sequência dos votos e a devida correlação com os eleitores votantes.

#### Considerações do grupo investigador

O acesso antecipado as estruturas dos arquivos, bem como a arquivos populados com votos de eleitores segundo esses procedimentos, permitiriam resultados mais precisos e conclusivos.
---

#### Considerações do grupo de apoio

Devido à ausência na fase de pré-teste o grupo não estava totalmente ambientado no sistema e nos processos da urna eletrônica. Sendo assim, houve dificuldades na execução dos planos uma vez que a premissa maior para um ataque bem sucedido seria o pleno conhecimento das funcionalidades do sistema.
---

#### Futuras Possibilidades

Adulteração do compilador;
Adulteração da BIOS;
Comprometimento da chave privada presente na Flash Interna da urna;
Um relatório que explicará em maiores detalhes essas novas possibilidades;
identificadas está anexado ao fim deste relatório.

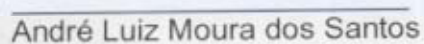
#### Alinhamento do PT

Não há.

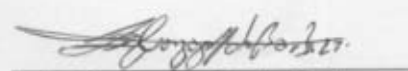
#### Informações Adicionais

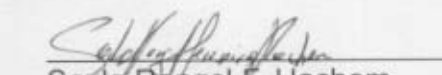
Não há.



  
André Luiz Moura dos Santos

  
Marcio André Souto Correia

  
Luiz Gonzaga Mota Barbosa

  
Saulo Rangel F. Hachem

  
Marco Constantino





## - Adulteração do Compilador

Verificamos que o TSE tem procedimentos para auditoria dos códigos fontes e autenticação dos executáveis que serão instalados nas urnas e utilizados em uma eleição. Por outro lado, não foi encontrado nenhum procedimento semelhante para o compilador utilizado na geração destes executáveis.

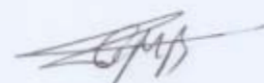
Alterações nos códigos fontes do compilador oferecem riscos com potencial igual ou maior que a alteração dos códigos fontes da urna. Mesmo que seja realizada uma auditoria nos códigos fontes da urna eletrônica, a ausência de uma auditoria do código do compilador utilizado levanta a possibilidade da criação de um compilador malicioso de tal forma que este gere um executável que contenha trechos de códigos que viabilizem o comprometimento do processo eleitoral.

Como exemplo, vamos supor que o TSE use para compilar os executáveis que serão usados no processo eleitoral uma compilação própria do "GCC". Alguém da equipe do TSE baixa os fontes do GCC direto do repositório do projeto, prepara o ambiente de compilação em uma distribuição Linux e compila o executável do GCC que será utilizado pelo TSE. Em seguida, os códigos fontes das aplicações do processo eleitoral são levados também a este ambiente e compilados. Esse processo se apoia em duas premissas que não necessariamente são verdadeiras: primeiro que o compilador que acompanha a distribuição Linux utilizada e o código fonte baixado do projeto GCC são íntegros e confiáveis; segundo que o compilador baixado também estará íntegro e confiável até a sua compilação. O compilador gerado pelo TSE pode, por exemplo, ter sido alterado e incluindo em suas rotinas uma função que recebe todos os dados que são entrados na urna e verifica a presença de um "número especial". Este número esperado poderia ativar uma rotina na urna que computaria X votos para um candidato Y, e em seguida retornaria ao fluxo normal, validando como de costume aquela entrada do usuário do sistema. O número especial poderia, por exemplo, ter o seguinte padrão: MMMMCCCCVVV, onde MMMM é o número mágico que ativa a rotina oculta no sistema, CCCCCC é o número do candidato que receberá os votos e VVV o número de votos que serão computados em favor do candidato.

Para que tenhamos um processo mais seguro, sugerimos alguns procedimentos:

- Auditar o executável que será carregado nas urnas eletrônicas;
- Auditar os códigos fontes tanto do compilador como o da urna eletrônica ou
- Executar um teste de unidade no código compilado que será inseminado na urna, testando todas as entradas possíveis e checar se são obtidos apenas resultados esperados.

Auditar um código executável em linguagem de máquina, ainda que seja utilizada uma linguagem de montagem, é um processo difícil. O produto final do processo de compilação naturalmente apresenta alterações quando comparado ao que se espera da tradução direta do





código fonte em código de máquina. A finalidade destas alterações é otimizar o executável que será produzido sem alterar seu sentido, seu objetivo. A otimização consiste em alterar blocos de instruções em nível de máquina a fim de diminuir a quantidade de saltos (JMPs) presentes no código, utilização de instruções específicas do processador utilizado, entre outras. Em outras palavras, podemos dizer que, apesar de manter a mesma semântica, ou seja, o sentido do código fonte escrito em uma linguagem de alto nível, o processo de compilação não é uma tradução fiel do código que foi escrito pela equipe de desenvolvimento. Com essas alterações, a auditoria dos executáveis torna-se uma tarefa ainda mais desafiadora.

Por outro lado, a auditoria de códigos fontes também podem apresentar algumas dificuldades. O tamanho do código fonte e a sua complexidade são os primeiros obstáculos que encontramos. Mesmo assim, essa provavelmente é a alternativa que apresenta melhor relação custo benefício, tendo em vista que simplesmente confiar em um código fonte não é uma opção.

## **- Adulteração da BIOS**

### **- Cenário atual**

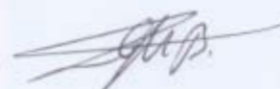
O procedimento de verificação da BIOS da urna testada ocorre de uma forma passiva, dada a indisponibilidade de barramento específico para a comunicação entre o MSD e a BIOS. Com isso, a BIOS envia informações para o MSD que faz a validação destas informações.

Uma BIOS modificada que conhece a informação que deve ser enviada para o MSD não teria problemas em enviar a mesma informação necessária para o processo de autenticação realizado pelo MSD. Após autenticada, a BIOS modificada é capaz de conter qualquer espécie de código malicioso comprometendo toda a cadeia de confiança na qual se apoia o processo de votação realizado com a urna.

### **- Cenário futuro**

O TSE propõe que, futuramente, o processo de autenticação de BIOS será realizado de forma ativa, onde o MSD lê diretamente as informações contidas na BIOS e verifica sua integridade. Porém, sem a utilização de um HSM, é possível substituir a placa mãe e reutilizar o MSD.

Uma vez que o MSD esteja presente em um ambiente malicioso, este pode ser levado a acreditar que validou a informação desejada. Uma vez que a chave privada está armazenada no MSD e ele acredita estar em um ambiente íntegro, nada o impede de validar todas as informações que lhe forem solicitadas, como por exemplo, o Boletim da Urna (BU) entre outros dados. Dessa maneira, a cadeia de confiança na qual se apoia o processo de votação com a urna é quebrada e informações produzidas maliciosamente podem ganhar caráter legítimo.



## - Segurança da Chave Privada

Durante os testes realizados, observamos que a chave privada utilizada pela urna para assinaturas das informações geradas está disponível tanto na Flash de Carga (FC) quanto na Flash Interna (FI). Pelo que nos foi informado, isso se deve ao fato de nem todas as urnas contarem ainda com MSD. Mesmo sendo um o objetivo do TSE o armazenamento da chave privada dentro do MSD, o fato é que o ambiente que nos foi disponibilizado para teste ainda não conta com essa proteção. Inclusive, pelo que tivemos de informação, a meta é que isso seja implementado apenas nas eleições de 2016.

A chave privada da urna é utilizada para autenticar e garantir sigilo às informações que são produzidas numa seção e que devem chegar até os sistemas de apuração de votos. Então, proteger a chave privada da urna é essencial para toda a segurança do processo eleitoral, porque uma vez que a chave tenha sido comprometida, dados podem ser produzidos de forma conveniente e assinados para que se tornem legítimos.

Armazenar a chave privada na FI e na FC, contando como única medida de proteção para ela o uso de criptografia, aumenta consideravelmente o nível de exposição da chave. Pelo que foi descrito, a senha para acesso a chave está espalhada pelas partições, no kernel e no Loader. Isso quer dizer que embora o esforço para recuperar essa senha e ter acesso à chave privada seja grande, é perfeitamente viável, principalmente se pudermos contar com o apoio de pessoas que conheçam os detalhes técnicos relacionados.

Mesmo com o armazenamento da chave privada na MSD, que hoje é um processador ARM programável e que conta com uma flash interna para o armazenamento das chaves, o nível de segurança provavelmente ainda não alcança o nível desejável. A solução do MSD, embora tenha sido elaborada tendo em mente requisitos de segurança, não conta com todas as garantias oferecidas por um HSM. Assim, não foram encontradas justificativas para a não utilização de, por exemplo, um Smart Card para proteger a chave privada e iniciar a cadeia de verificação da carga da urna. Tentar desenvolver um dispositivo, usando componentes que não foram concebidos para essa finalidade, como é o caso de processadores da família ARM7, ao invés de usar uma solução que a indústria já reconhece como um padrão, foi uma que realmente surpreendeu nossa equipe.

