



## Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012  
Brasília, março de 2012

### Relatório dos resultados da realização dos Testes Públicos

#### Grupo 03

Representando o Instituto Sapientia

Marcelo Achar – Especialista graduado em Ciência da Computação

Facundo Larrosa – Graduado em Gestão da Tecnologia da Informação

Pedro Ivo Pereira Gomes – Bacharel em Ciência da Computação

#### Plano de Teste G3PT3

Teste C - Clonagem de memória flash de votação

#### 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



Tribunal Superior Eleitoral

PROTOCOLO

4.301/2012

13/03/2012 - 16:37

ses pe  

## Plano de Teste do Sistema Eletrônico de Votação

## 1 Informações gerais

Título do plano de teste	Teste do Instituto Sapientia
Instituição proponente (se aplicável)	Instituto Sapientia – Grupo 3
Responsável	nome: Marcelo Achar e-mail: mce@sapientia.org.br telefone (do autor ou responsável): (61) 3326-0111 / 8401-1966
Sistemas afetados	<b>Software:</b> <i>Software</i> de votação usado nas seções eleitorais.  <b>Hardware:</b> <input type="checkbox"/> Microterminal <input checked="" type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacs <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)	540 minutos (9 horas)
Extensão do ataque	<input checked="" type="checkbox"/> Urna ou seção eleitoral <input type="checkbox"/> Local de votação <input type="checkbox"/> Zona eleitoral <input type="checkbox"/> Município <input type="checkbox"/> Unidade da Federação <input type="checkbox"/> País
Conhecimentos necessários	Conhecimentos gerais em virtualização de máquina e avançado dos comandos do Linux.

## 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



### 3 Detalhamento do teste

#### 3.1 Resumo do teste

O teste proposto é dividido em três testes menores que podem ser executados independentemente, os quais serão identificados no documento como teste A, B e C.

Teste A) Tentar inicializar a urna eletrônica usando uma memória CompactFlash na entrada externa com um loader não assinado pelo TSE.

Teste B) Conectar um adaptador USB-Ethernet na interface USB da urna eletrônica para checar se o mesmo é reconhecido e então usar um scanner de portas para verificar se existe alguma vulnerabilidade.

Teste C) Verificar se é possível clonar uma memória flash de votação antes do início da votação. Inserir a memória clonada na urna e manipular os votos de forma fraudulenta. Disponibilizar para os eleitores da seção uma urna de contingência com o flash de votação original. No final da votação, usar a urna que teve os votos manipulados para publicar o boletim de urna e transferir os dados da memória de votação.

#### 3.2 Fundamentação

Teste A) Consiste na validação do correto funcionamento de um dos sistemas de segurança que a UE (Urna Eletrônica) possui, chamado Boot Seguro. Será feita uma tentativa de execução de software não autorizado pelo TSE na UE. Para isto será usado um CF (CompactFlash) como disco de boot criado com um loader e um SO (Sistema Operacional) não autorizado pelo TSE. O resultado esperado é que a UE não reconheça o loader do CF devido a validação que a BIOS da UE faz na assinatura do loader, conforme consta na especificação do processo de Cadeia de Confiança da UE. Caso a UE reconheça o CF como um disco de boot válido e inicie o SO será considerado uma falha de segurança, pois possibilita o uso de softwares fraudulentos na UE.

Teste B) Conforme informado na palestra técnica, um dos requisitos da UE é não possuir nenhuma interface de rede Ethernet com fio ou wireless. O teste consiste em conectar em uma das interfaces USB da UE um adaptador USB-Ethernet de baixo custo para verificar se o SO também foi preparado para ignorar este tipo de adaptador. Com um cabo crossover, o adaptador será ligado ao PC, que terá um servidor DHCP instalado. Caso a UE reconheça o adaptador e adquira um IP da rede, iremos executar um scanner de portas no IP da UE para verificar se a mesma possui alguma porta aberta rodando algum serviço que a torne vulnerável a ataques.

Teste C) Neste teste de fraude uma UE seria clonada para manipular os seus votos. O teste avalia se é tecnicamente possível a fraude sem considerar as dificuldades que o fraudador enfrentaria para ter acesso físico a UE. Antes do início da votação retira-se o FV (Flash de Votação) da UE e, usando um PC com um leitor de CF, copiamos o seu conteúdo para outro CF. Coloca-se FV original na UE





de contingência e a libera para a votação pelos eleitores como é feito sempre que a UE da seção apresenta falhas. Em outro ambiente isolado pelos fraudadores é colocado o FV clonado na UE substituída e é feita a votação de forma manipulada. Ao final do processo, o mesário recebe os BUs (Boletins de Urna) da UE fraudada para publicação e distribuição, e usa a MR (Memória de Resultado) da UE fraudada para transferir os dados para a consolidação.

### 3.3 Precondições para o teste

Os recursos listados abaixo, que se repetem para testes diferentes, podem ser compartilhados. No entanto, se houver risco de um determinado teste inutilizar a urna, este deverá ter uma urna própria.

#### Recursos materiais para o teste A:

1. Uma urna eletrônica (fornecido pelo TSE);
2. O micro-computador lacrado na fase de preparação (fornecido pelo TSE);
3. Um cartão extra CompactFlash da Apacer de 512Mb sem dados (fornecido pelo TSE);
4. O leitor de CompactFlash utilizado na fase de preparação (fornecido pelo TSE);
5. Uma chave philips que possibilite a abertura da tampa do CF externo e das portas USB da urna (fornecido pelo TSE);

#### Recursos materiais para o teste B:

1. Uma urna eletrônica pronta para o início da votação (fornecido pelo TSE);
2. O micro-computador lacrado na fase de preparação (fornecido pelo TSE);
3. Um adaptador USB-Ethernet compatível com o módulo "usbnet" do Linux (fornecido pelo proponente);
4. Um cabo de rede padrão crossover de pelo menos um metro de comprimento (fornecido pelo proponente);

#### Recursos materiais para o teste C:

1. Uma urna eletrônica pronta para o início da votação (fornecido pelo TSE);
2. O micro-computador lacrado na fase de preparação (fornecido pelo TSE);
3. Um cartão extra CompactFlash da Apacer de 512Mb sem dados (fornecido pelo TSE);
4. O leitor de CompactFlash utilizado na fase de preparação (fornecido pelo TSE);
5. Uma chave philips que possibilite a abertura da tampa do CF externo da urna (fornecido pelo TSE);
6. Uma UE de contingência. Como não tem muita relevância para o teste o seu uso é opcional (fornecido pelo TSE);

#### Recursos de software para o teste A:

1. O SO Windows XP já instalado no micro-computador lacrado na fase de preparação (fornecido pelo TSE);
2. LinuxLive USB Creator Versão 2.8.10 (fornecido pelo proponente);
3. Imagem ISO do Ubuntu 10.04 Minimal i386 (fornecido pelo proponente);

#### Recursos de software para o teste B:

1. O SO Windows XP já instalado no micro-computador lacrado na fase de preparação (fornecido pelo TSE);
2. VirtualBox 4.1.8 para Windons (fornecido pelo proponente);
3. VirtualBox Extension Pack 4.1.8 (fornecido pelo proponente);



4. Arquivo OVA (Open Virtualization Format Archive) com a máquina virtual do Xubuntu 10.04.2 Desktop i386 (fornecido pelo proponente);
5. Servidor DHCP instalado no Xubuntu;
6. Aplicativo scanner de portas instalado no Xubuntu;
7. Cliente Telnet instalado no Xubuntu;

**Recursos de software para o teste C:**

1. O SO Windows XP já instalado no micro-computador lacrado na fase de preparação (fornecido pelo TSE);
2. VirtualBox 4.1.8 para Windons (fornecido pelo proponente);
3. VirtualBox Extension Pack 4.1.8 (fornecido pelo proponente);
4. Arquivo OVA (Open Virtualization Format Archive) com a máquina virtual do Xubuntu 10.04.2 Desktop i386 (fornecido pelo proponente);

**Recursos humano para os testes:**

1. Dois recursos com conhecimentos gerais de virtualização e com conhecimento avançado dos comandos do Linux;

**Considerações para os testes:**

1. Os lacres da urna eletrônica são dispensáveis, pois não estão sendo considerados nos testes;
2. Os testes avaliam apenas tecnicamente se é possível ou viável executar o ataque ao sistema da UE. Não estão sendo considerados os dispositivos de segurança que poderiam impedir o atacante de ter acesso físico a UE;

### **3.4 Escopo – Superfície de Ataque**

**Teste A)**

1. A urna eletrônica;

**Teste B)**

1. A urna eletrônica;

**Teste C)**

1. A urna eletrônica;
2. O flash de votação;

### **3.5 Janela de atuação simulada do atacante**

**Teste A)**

1. Acesso a urna eletrônica;

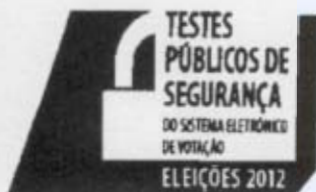
**Teste B)**

1. Acesso a urna eletrônica;

**Teste C)**

1. Acesso a urna eletrônica antes e durante o período de votação;
2. Acesso ao flash de votação antes do período de votação;





### 3.6 Pontos de intervenção

Teste A)

1. Validação pela BIOS do loader e SO autorizados pelo TSE;

Teste B)

1. Rejeição de um dispositivo ethernet pelo SO da UE;
2. Ausência de serviços acessíveis pela ethernet na UE;

Teste C)

1. A possibilidade de clonar uma urna eletrônica copiando uma memória flash de votação para um outro cartão CompactFlash não autorizado pelo TSE;
2. A validação dos votos de uma UE que usava uma memória flash de votação clonada;

### 3.7 Passos a serem realizados e material necessário

Teste A) Tempo total: 2 horas

1. O atacante adquire um CompactFlash com a mesma especificação dos usados pela urna. Para o teste este CompactFlash será fornecido pelo TSE. (10 minutos)
2. O atacante insere o CompactFlash em um leitor ligado em um computador com Windows XP. (10 minutos)
3. No Windows, o atacante abre o software LinuxLive USB Creator, seleciona o ISO do Ubuntu 10.04 Minimal i386 e cria o disco de boot no CompactFlash. (30 minutos)
4. O atacante insere o teclado do PC na entrada USB da urna. (10 minutos)
4. O atacante insere o CompactFlash na entrada externa da urna. (10 minutos)
5. O atacante liga a urna e aguarda o início do boot. (30 minutos)
6. O atacante verifica se o SO Ubuntu foi carregado com sucesso na urna. (20 minutos)
7. Se o SO Ubuntu for inicializado o ataque será considerado bem sucedido.

Teste B) 3 horas

1. O atacante adquire um adaptador USB-Ethernet de baixo custo. Para o teste este adaptador será fornecido pelo proponente. (10 minutos)
2. O atacante insere o adaptador em uma entrada USB da urna. (10 minutos)
3. O atacante conecta o adaptador a um PC usando um cabo de rede crossover. Para o teste este cabo será fornecido pelo proponente. (10 minutos)
4. O atacante liga o PC e inicia a VM (Máquina Virtual) do Xunbutu preparada com um servidor DHCP. (30 minutos)
5. O atacante liga a urna e aguarda que a mesma inicialize. (20 minutos)
6. O atacante verifica no servidor DHCP se o mesmo atribuiu um IP para a urna. (20 minutos)
7. Se não foi atribuído nenhum IP o teste é então interrompido sem sucesso.
8. Se foi atribuído um IP, usando o Xunbutu executamos um scanner de portas no IP para verificar a existência de algum serviço. (30 minutos)
9. Para os serviços existentes faremos um teste de conexão ao mesmo usando o comando telnet e se for o caso usando o cliente específico para o serviço. (50 minutos)
10. Se for encontrado algum serviço que permita acesso ao sistema da urna o ataque será considerado bem sucedido.



#### Teste C) 4 horas

1. O atacante tem acesso a urna de uma seção antes do início das votações. (10 minutos)
2. O atacante retira o flash de votação da urna. (20 minutos)
3. O atacante insere o flash em um leitor conectado a um PC com Linux. Para o teste o Linux será o Xubuntu e estará em uma VM instalada na máquina fornecida pelo TSE. (10 minutos)
4. O atacante faz uma cópia do flash de votação em um arquivo no PC usando o comando dd. (40 minutos)
5. O atacante retira o flash do leitor e o insere em uma urna de contingência (este passo é dispensável, pois se trata de um procedimento normal quando se usa a urna de contingência).
6. O atacante substitui a urna da seção pela urna de contingência (este passo é dispensável, pois se trata de um procedimento normal quando se usa a urna de contingência).
7. O atacante adquire um CompactFlash com a mesma especificação dos usados pela urna. Para o teste, este CompactFlash será fornecido pelo TSE podendo ser o mesmo usado no teste A. (10 minutos)
8. O atacante insere o novo flash no leitor conectado ao PC com a cópia do flash original. (10 minutos)
9. O atacante copia todos os dados do arquivo para o novo flash que será um clone do flash de votação. (60 minutos)
10. O atacante retira o flash clonado e o insere na urna substituída. (10 minutos)
11. O atacante liga a urna clonada e com a lista dos números dos títulos de eleitores da seção faz os votos dos mesmos manipulando as escolhas dos candidatos. (30 minutos)
12. O atacante emite na urna clonada os BUs para a publicação na seção. (30 minutos)
13. O atacante usa a MR para transferir os dados para a consolidação do resultado das eleições. (10 minutos)
14. O MR e BU da urna de contingência são ignorados pelo atacante.
15. Se todos os passos forem tecnicamente executáveis e se a memória de resultado da urna clonada for aceita como válida pelo sistema de consolidação então o ataque será bem sucedido.

### 3.8 Possíveis resultados e impacto

#### Tipo de resultado esperado:

Teste A) Uso de software não autorizado na UE.

Teste B) Possibilidade de conectividade ethernet da urna com uso de adaptador.

Teste C) Possibilidade de clonagem da urna para manipulação de votos.

#### Extensão do ataque:

Teste A) Qualquer urna.

Teste B) Qualquer urna.

Teste C) Uma urna de uma seção eleitoral.

#### Probabilidade esperada de sucesso:

Teste A) Baixa.

Teste B) Baixa.

Teste C) Alta.



### 3.9 Rastreabilidade

Todos os ataques do documento são rastreáveis desde que seja analisada individualmente cada urna atacada.

### 3.10 Solução proposta

Teste A) No caso de sucesso neste ataque, a urna deverá ser corrigida para ficar de acordo com suas especificações da Cadeia de Confiança.

Teste B) No caso de sucesso deste ataque, o kernel da urna deverá ser alterado para desabilitar o módulo "usbnet" que possibilita o uso de adaptadores USB-Ethernet.

Teste C) No caso de sucesso do ataque, poderia estudar a viabilidade de se adicionar aos dados do flash de votação o número serial do CF físico para checagem pelo software da UE.

*Paulo Silva*  
13-3-2012

*[Signature]*





## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G3PT3</b>	Coordenador:	Marcelo Achar	
	Investigador 1:	Facundo Larrosa	
	Investigador 2:	Pedro Ivo Perreira Gomes	

Informações do Acompanhamento					
Data:	22/03/2012	Hora de Início:	14:30	Hora de Término:	18:15
Resp. Acomp.:	Fernando Amatte			Rubrica:	

Dados do Teste			
Titulo do teste:	Teste do Instituto Sapiencia: Teste C		
Início do teste (Data/Hora):	22/03/2012	14:30	
Termino do teste (Data/Hora):	22/03/2012	17:40	
Critério de Parada:	Fim da votação		

Relaxamento nos mecanismos e procedimentos de segurança	
Retirada do lacre traseiro para acesso a flash de carga e memória de votação.	
Pessoas corrompidas no processo.	

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Retirada dos lacres da urna;	
2	Retirada da memória de resultado e flash de votação;	
3	Criação de um dump (imagem) das duas ;	
4	Clonagem das memórias;	
5	Início da urna ;	
6	Mesário solicita a troca da urna, simulando ou não uma falha ;	
7	Urnas seria substituída pela urna de contingência;	
8	Votação REAL se inicia na urna de contingência, com os MR e FV originais;	
9	Urnas original é levada para local, onde a fraude irá ocorrer. A mesma será iniciada com os clones da MR e FV;	
10	Boletins de urna e memória de resultado da urna "fraudada" seriam entregues ao presidente da sessão/mesário para serem substituídos pelos oficiais oriundos da urna de contingência.	

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
14:35	Retirada dos lacres da urna.
14:35	Retirada a memória de resultado e flash de votação.
14:38	Criação de um dump (imagem) com o dd da memória de resultado.
14:40	Criação de um dump (imagem) com o dd da flash de votação.
14:43	Imagem da flash de votação original é colocada em uma memória flash igual ou compatível com a original (aprox: 22 minutos ).
15:05	Imagem da memória de resultado original é colocada em uma memória USB igual ou compatível com a original
15:14	Início da urna como em dia de votação.
15:32	Urnas foi desligada, simulando um problema. Para fins do teste, usaremos a mesma urna e não a urna de contingência.
15:37	Urnas ligada para início da votação.
15:43	Zerezeira impressa.
15:44	Simular uma votação – foram inseridos 10 votos a título de teste.
16:00	Fechamento da urna com sucesso em todas as mensagens, incluindo remoção da memória de resultado conforme procedimento de finalização.

Conclusões sobre o teste
<p>É difícil um tipo de fraude dessa maneira devido ao número de controles de segurança e pessoas envolvidas no processo, no entanto, a mesma é tecnicamente possível e viável de ser feita.</p> <p>Dependendo do planejamento e execução do ataque, os rastros poderiam ser mais ou menos evidentes, mas completado com sucesso um ataque desses sem gerar nenhum alarme, a detecção de uma anomalia poderia ser bem posterior a apuração dos resultados.</p>

Considerações do grupo investigador
<p>Sugerimos um controle melhor entre as mídias e a urna, visando que trocas de mídias não ocorram.</p> <p>Existem métodos, como o Physical Unclonable Function (PUF), que podem impedir a cópia/ clone de uma memória/mídia. Caso essa cópia ocorra, ela deixaria algum tipo de rastro, não permitindo a inicialização da mesma.</p> <p>Outra opção talvez mais viável seria adicionar o serial único das compact flashs, nos arquivos finais da memória de resultado, para que seja feito uma correspondência entre as compact flashs utilizadas nas urnas.</p> <p>Neste caso, os seriais dos CF seriam previamente cadastrados pelo TSE para se fazer o controle de correspondência entre as mídias geradas e as seções onde as mesmas serão ou foram executadas.</p>

Considerações do grupo de apoio

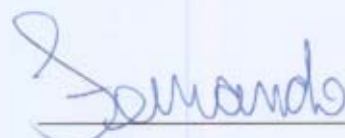


Futuras Possibilidades
Testes devem ser feitos com mídias comerciais compradas em locais públicos/comerciais normais.

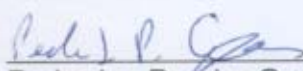
Alinhamento do PT
Foi incluída a cópia da memória de resultado também.

Informações Adicionais
Para o ataque ter sucesso seria necessário a cumplicidade de algumas pessoas que participam do processo de votação.

\_\_\_\_\_  
Marcelo Achar

  
\_\_\_\_\_  
Resp. Acompanhamento

  
\_\_\_\_\_  
Facundo Larrosa

  
\_\_\_\_\_  
Pedro Ivo Pereira Gomes



