



## Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

### Relatório dos resultados da realização dos Testes Públicos

#### Grupo 05

Representando a Universidade Federal de Uberlândia - UFU

Marcelo Rodrigues de Sousa – Doutor em Engenharia Elétrica e Computação – UFU

Kil Jin Brandini Park – Pós-doutorado em Ciência da Computação – CTI Renato Archer

Otávio Augusto Araújo da Silva – Graduado em Ciência da Computação - UFU

#### Plano de Teste G5PT3

UFO-FACOM-TEFSEV: Tentativa de comprometimento do MSD através da interface JTAG

#### 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



## Plano de Teste do Sistema Eletrônico de Votação

### 1 Informações gerais

Título do plano de teste	UFU-FACOM-TEPSEV
Instituição proponente (se aplicável)	UNIVERSIDADE FEDERAL DE UBERLÂNDIA/FACULDADE DE COMPUTAÇÃO
Responsável	nome: MARCELO RODRIGUES DE SOUSA e-mail: marcelo@facom.ufu.br ou marcelo@ufu.br telefone (do autor ou responsável): (34)9958-5050 (Celular) ou (34)3239-4478 (UFU)
Sistemas afetados	<b>Software:</b> <input checked="" type="checkbox"/> Software de votação usado nas seções eleitorais.  <b>Hardware:</b> <input type="checkbox"/> Microterminal <input checked="" type="checkbox"/> Terminal do eleitor <input checked="" type="checkbox"/> Lances <input checked="" type="checkbox"/> Mithras  <b>Procedimentos:</b> <input checked="" type="checkbox"/> Carga da urna <input checked="" type="checkbox"/> Votação
Duração estimada do teste (em minutos)	3 horas e 50 minutos (todos os 4 ataques)
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 checked="" type="checkbox"/> País
Conhecimentos necessários	Conhecimentos profundos de sistemas operacionais, microeletrônica, sistemas digitais, programação de computadores.

#### 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
	Resultado <input type="checkbox"/> Aprovado <input type="checkbox"/> Aprovado com ressalvas <input type="checkbox"/> Reprovado



### 3 Detalhamento do teste

#### 3.1 Resumo do teste

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

Serão realizados 4 (quatro) testes:

##### **A. Modificação do boot da urna**

*Descrição:*

Tentativa de alterar parâmetros de boot da urna eletrônica de maneira a comprometer seu funcionamento.

Esse teste será constituído de duas metodologias distintas. Na primeira, teste de modificação dos parâmetros de boot da urna para que esta não funcione conforme o previsto. Na segunda, teste de alteração dos parâmetros de boot da urna para que esta force o boot a partir de uma mídia distinta da mídia de carga, com o intuito de sobrepôr o sistema de renificação e forçar a carga de um sistema operacional não assinado.

*Tipo de Ataque:* Falha

*Duração do teste:* 50 minutos.

*Pontos de intervenção:* rompimento dos lacres e alteração da mídia de carga.

*Extensão do ataque:* Urna Eletrônica.

##### **B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Descrição:*

Teste de recuperação de dados da memória volátil da urna, tanto para modificação de dados relativos a votação quanto para tentativa de recuperação de chaves utilizadas para cifragem do sistema operacional e assinatura dos programas internos.

*Tipo de Ataque:* Falha

*Duração do teste:* 50 minutos.

*Pontos de intervenção:* rompimento dos lacres e alteração da mídia de carga.

*Extensão do ataque:* Urna Eletrônica.

##### **C. Tentativa de comprometimento do MSD através da interface JTAG**

*Descrição:*

Tentativa de conectar equipamento na interface JTAG da placa da urna, para comprometimento do MSD.

*Tipo de Ataque:* Falha

*Duração do teste:* 4 horas.

*Pontos de intervenção:* rompimento dos lacres.

*Extensão do ataque:* Urna Eletrônica.

##### **D. Quebra do sigilo do voto eletrônico**

*Descrição:*

Demonstração da possibilidade de uma pessoa determinar se um eleitor votou ou não em um determinado candidato usando a urna eletrônica, fazendo uma comparação com o processo de votação manual.

*Tipo de Ataque:* Fraude.

*Duração do teste:* 10 minutos.

*Pontos de intervenção:* 1 ponto (risco da urna).

*Extensão do ataque:* Brasil.



### 3.2 Fundamentação

O proponente deverá explicar, 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.

*A fundamentação dar-se-á para cada teste separadamente:*

#### **A. Modificação do boot da urna**

*Tentativa de alterar parâmetros de boot da urna eletrônica de maneira a comprometer seu funcionamento.*

Esse teste será constituído de duas metodologias distintas. Na primeira, efetuiremos tentativas de modificação dos parâmetros de boot da urna para que esta não funcione conforme o previsto. Na segunda, tentaremos alterar os parâmetros de boot da bios para que esta force o boot a partir de uma mídia distinta da mídia de carga, com o intuito de sobrepôr o sistema de verificação e forçar a carga de um sistema operacional não assinado. Considera-se que o atacante teve acesso hipotético a uma urna eletrônica, que pode ter sido subtraída em qualquer ponto da cadeia de logística de distribuição das mesmas no dia da votação. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso nesse teste.

#### **B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Tentativa de recuperação de dados da memória volátil da urna, tanto para modificação de dados relativos a votação quanto para tentativa de recuperação de chaves utilizadas para cifragem do sistema operacional e assinatura dos programas internos.*

Para tanto, a metodologia consiste em abrir a urna eletrônica, desligá-la durante sua operação, rapidamente barrifar sobre o pente de memória uma solução resfriante, retirar o pente, conectá-lo a um outro equipamento preparado para bootar com um software que copie o conteúdo da memória para uma mídia externa (USB). É necessário o acesso físico a uma urna eletrônica, considera-se que o atacante teve acesso hipotético a uma urna eletrônica, que pode ter sido subtraída em qualquer ponto da cadeia de logística de distribuição das mesmas no dia da votação. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso nesse teste.

#### **C. Tentativa de comprometimento do MSD através da interface JTAG**

*Tentativa de conectar equipamento na interface JTAG da placa da urna, para comprometimento do MSD. Considera-se que o atacante teve acesso hipotético a uma urna eletrônica, que pode ter sido subtraída em qualquer ponto da cadeia de logística de distribuição das mesmas no dia da votação. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso nesse teste. Durante a fase inicial de instrução da urna eletrônica constatou-se a possibilidade de sucesso nesse teste.*

#### **D. Quebra do sigilo do voto eletrônico**

*Demonstração da possibilidade de uma pessoa determinar se um eleitor votou ou não em um determinado candidato usando a urna eletrônica, fazendo uma comparação com o processo de votação manual. Será feita uma análise de todo processo de votação desde a carga da urna até a sua apuração. Esse teste usa a criptografia como principal arma de ataque ao sistema de votação.*





### 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 do 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 tribunais regionais eleitorais (TREs) que sejam necessários para o sucesso do teste proposto.

*Para cada teste proposto são necessários:*

#### A. Modificação do boot da urna

*Acesso à urna eletrônica. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB. Alteração da mídia de carga.*

*Equipamentos necessários:*

*Teclado externo via USB.*

*Memória USB (pendrive).*

*Cartão de memória de carga da urna.*

*Dois conversores USB/RJ232 e um adaptador de 9 pinos.*

*Conhecimentos de sistemas operacionais, microeletrônica, sistemas digitais, programação de computadores.*

#### B. Tentativa de recuperação de dados da memória volátil do equipamento

*Acesso à urna eletrônica. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB.*

*Equipamentos necessários:*

*Spray de elemento refrigerante/congelante (nitrogênio) não dermatológico, como:*

*"Multi-Purpose Freeze Spray"*

*"Spray CONGELANTE IMPLASTEC"*

*"ALIX Professional 7777 Blow Off Freeze Spray Electronic Component Cooler"*

*"SPRAY CONGELANTE GELO DUE-GI"*

*"Spray Congelante Ice"*

*"Spray Congelante de Ação Rápida CS68"*

*Memória USB (pendrive) de 8Gb para configuração do software de extração.*

*Notação: compatível com memória de mesma tipo utilizado na urna eletrônica (DDR2), capaz de boot pela interface USB.*

*Conhecimentos de sistemas operacionais, microeletrônica, sistemas digitais, programação de computadores.*

#### C. Tentativa de comprometimento do MSD através da interface JTAG

*Acesso à urna eletrônica. O ataque implica o rompimento dos lacres das interfaces de mídia e portas USB.*

*Equipamentos necessários:*

*Interface JTAG macho a ser colada nos conectores JTAG existentes na placa da urna, e fita isolante, a fim de evitar qualquer solda.*

*Cabo JTAG - USB a ser utilizado para conexão entre um computador e a urna, dentre os seguintes: ULINK-ME, ULINK2, ULINKPro, J-Link Lite, J-Link LPC Edition, J-Link ARM.*

*Mídia R.O. com Keil ARM Evaluation Kit disponível em: <http://www.keil.com/demo/eval/arm.htm>*





**D. Quebra do sigilo do voto eletrônico**

*Não há pré-condições.*

### 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 aqueles relacionados aos:

- Material (e.g. urna, mídias, lacres, etc.),
- Ambiente (e.g. condições de operação, sala, alimentação, etc.),
- Procedimento (e.g. verificação, emissão de zerésima, etc.)

*Para cada teste:*

**A. Modificação do boot da urna**

*Rompimento dos lacres da urna eletrônica.*

*Alteração da mídia de carga.*

**B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Rompimento dos lacres da urna eletrônica.*

**C. Tentativa de comprometimento do MSD através da interface JTAG**

*Rompimento dos lacres da urna eletrônica.*

**D. Quebra do sigilo do voto eletrônico**

*Não há modificações nas urnas eletrônicas.*

### 3.5 Janela de atuação simulada do atacante

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

Alguns exemplos de janelas de atuação são: (a) acesso a mídias para armazenamento fora do período eleitoral; (b) acesso ao *software* da urna eletrônica no período posterior à votação, no local de votação; (c) acesso à urna eletrônica; (d) acesso à memória *flash* de carga gerada.

*Para cada teste:*

**A. Modificação do boot da urna**

*Acesso às mídias de carga das urnas anteriormente ao período de votação.*

**B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Acesso à urna eletrônica antes ou após o pleito.*

**C. Tentativa de comprometimento do MSD através da interface JTAG**

*Acesso à urna eletrônica antes do pleito.*

**D. Quebra do sigilo do voto eletrônico**

*A atuação se dá durante o processo eleitoral (dia de votação).*



### 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 proprietária de BIOS), procedimentos (e.g. armazenamento de urnas), mídias (e.g. assinatura e criptografia do boletim de urna) e lacres.

Para cada teste:

**A. Modificação do boot da urna**

*rompimento dos lacres e alteração da mídia de carga*

**B. Tentativa de recuperação de dados da memória volátil do equipamento**

*rompimento dos lacres*

**C. Tentativa de comprometimento do MSD através da interface JTAG**

*rompimento dos lacres e alteração da mídia de carga*

**D. Quebra do sigilo do voto eletrônico**

*Uso do display da urna eletrônica.*

### 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, um exemplo de uma lista de passos:

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. Os passos devem obrigatoriamente conter critérios de parada do teste, que devem ser claros e facilmente identificáveis.

Deverá também ser informada a duração, em minutos, estimada para cada passo do teste, bem como o tempo total estimado.

O proponente deverá listar também o material necessário à realização dos testes, especificando qual material será de responsabilidade do TSE e qual será trazido pelo investigador.

Para cada teste:

**A. Modificação do boot da urna**

*Lista de passos:*

1. Atacante tem acesso físico à urna e à mídia de carga.
2. Atacante, utilizando um computador portátil, lê e altera a mídia de carga.



3. Com a mídia alterada dá-se carga à urna com o processo de boot modificado.
4. Fim

**B. Tentativa de recuperação de dados da memória volátil do equipamento**

*Lista de passos:*

1. Atacante tem acesso físico à urna eletrônica.
2. Atacante desmonta a urna, retirando seus lacres.
3. Atacante inicializa a urna e usa o spray em momento oportuno.
4. Atacante retira a memória RAM da urna e a conecta em um computador portátil.
5. Atacante faz dump da memória e busca dados valiosos.
6. Fim

**C. Tentativa de comprometimento do MSD através da interface JTAG**

*Lista de passos:*

1. Atacante tem acesso físico à urna eletrônica.
2. Atacante desmonta a urna, retirando seus lacres.
3. Atacante conecta o JTAG ou o cabo serial na placa-mãe da urna.
4. Atacante executa um software para debug ou reprogramação da urna usando um computador portátil.
5. Atacante inicializa a urna.
6. Atacante aguarda a urna entrar em processo de debug ou reprograma a própria urna.
7. Fim

**D. Quebra do sigilo do voto eletrônico**

*O processo se dá no dia da votação através de ações criminais eleitorais.*

### 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.

*Resultados esperados dos testes:*

**Modificação do boot da urna**

*Possibilidade de conteúdo do kernel da urna eletrônica, fazendo-a comporta-se maliciosamente.*

*Tipo de Ataque: Falha*

*Extensão do ataque: Urna Eletrônica.*







*Taxa de sucesso esperada: 99%*

***Tentativa de recuperação de dados da memória volátil do equipamento***

*Possibilidade de extração das chaves criptográficas da urna para uso posterior.*

*Tipo de Ataque: Falha*

*Extensão do ataque: Urna Eletrônica*

*Taxa de sucesso esperada: 70%*

***Tentativa de comprometimento do MSD através da interface JTAG***

*Possibilidade de extração das chaves criptográficas da urna para uso posterior ou reprogramação da urna eletrônica.*

*Tipo de Ataque: Falha*

*Extensão do ataque: Urna Eletrônica*

*Taxa de sucesso esperada: 40%*

***Quebra do sigilo do voto eletrônico***

*Possibilidade de quebra do sigilo do voto de um eleitor, dessa forma pode-se verificar se um eleitor votou ou não em um determinado candidato.*

*Tipo de Ataque: Fraude*

*Extensão do ataque: Brasil*

*Taxa de sucesso esperada: 99%*

### **3.9 Rastreabilidade**

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

- Não detectar o ataque;
- Detectar o ataque.

*Resultados esperados de rastreabilidade:*

***Modificação do boot da urna***

*Probabilidade de rastreamento: é possível detectar o ataque através de pontos de segurança, basta auditar a mídia de carga. Há rompimento dos lares.*

***Tentativa de recuperação de dados da memória volátil do equipamento***

*Probabilidade de rastreamento: é possível verificar o rompimento dos lares, mas não é possível detectar se as chaves foram descobertas.*

***Tentativa de comprometimento do MSD através da interface JTAG***

*Probabilidade de rastreamento: é possível verificar o rompimento dos lares, mas não é possível detectar se as chaves foram descobertas. No caso de reprogramação da urna, esta modificação é detectável através de auditoria.*

***Quebra do sigilo do voto eletrônico***

*Não é possível detectar o ataque, a menos de denúncia prévia.*



#### ***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.

*Nos testes abaixo são anulações:*

#### ***Modificação do boot da urna***

*Todas as parâmetros do boot serão built-in no kernel, e o kernel não aceitar parâmetros de boot.*

#### ***Tentativa de comprometimento do MSD através da interface JTAG***

*Tanto a porta serial e JTAG serão resistentes.*

*As outras soluções quanto possíveis serão apresentadas após o sucesso dos testes.*

Vds, 13/03/2012





## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G5PT3</b>	Coordenador:	Marcelo Rodrigues de souza	
	Investigador 1:	Kil Jin Brandini Park	
	Investigador 2:	Otávio Augusto Araújo Silva	

Informações do Acompanhamento					
Data:	22/03/2012	Hora de Início:	12:00	Hora de Término:	12:10
Resp. Acomp.:	Fernando Amatte			Rubrica:	

Dados do Teste		
Titulo do teste:	Tentativa de comprometimento do MSD através da interface JTAG	
Início do teste (Data/Hora):	22/ 03/ 2012	12:00
Termino do teste (Data/Hora):	22/ 03/ 2012	12:10
Criterio de Parada:	Não houve como o teste ser realizado em razão da ausência do hardware necessário para sua efetivação.	

Relaxamento nos mecanismos e procedimentos de segurança
Inicialmente, para o ataque, será necessário o acesso à urna eletrônica.
É necessário romper os lacres da Urna Eletrônica.

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Acesso à urna eletrônica através de furto.	
2	Abertura da urna eletrônica.	
3	Acesso à placa-mãe da urna eletrônica.	
4	Conexão do cabo JTag na placa-mãe da urna eletrônica e no computador do atacante.	
5	Início do debug do LPC2368 pelo Arm Devtool-kit via JTAG. Caso possível o debug, leitura da programação do controlador, e possivelmente o conjunto de chaves usado no boot.	
6	Caso o debug não for possível, sobrescrita da programação da urna via Flash-Utility, que funcionam tanto via JTAG quanto qualquer interface serial com o controlador LPC2368.	

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
12:00	Não houve possibilidade da realização dos procedimentos.

Conclusões sobre o teste
Embora o teste não tenha se efetivado, mostrou-se uma possibilidade de ação contra a urna eletrônica brasileira.

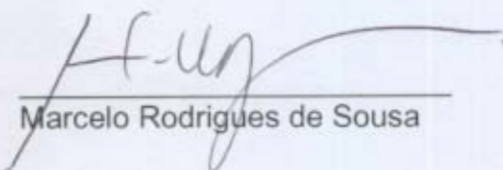
Considerações do grupo investigador
Não há como afirmar o que exatamente seria possível realizar contra a urna eletrônica, sem a execução do teste. Sugerimos que seja feita uma verificação para determinar se há ou não essa possibilidade. Posteriormente, devem ser resinados os conectores JTag da placa-mãe das urnas, o que inviabiliza esse tipo de ataque.

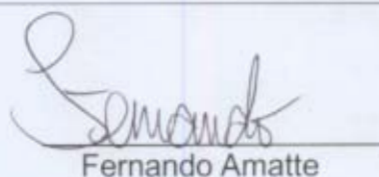
Considerações do grupo de apoio
Não há.

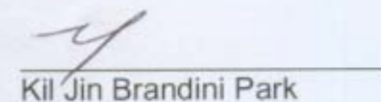
Futuras Possibilidades
Não há.

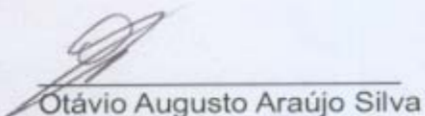
Alinhamento do PT
Não há.

Informações Adicionais
Não há.

  
 Marcelo Rodrigues de Sousa

  
 Fernando Amatte

  
 Kil Jin Brandini Park

  
 Otávio Augusto Araújo Silva

