

## 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 G5PT2

UFO-FACOM-TEFSEV: Tentativa de recuperação de dados da memória volátil do equipamento

#### 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"/> Mídias  <b>Procedimentos:</b> <input checked="" type="checkbox"/> Carga da urna <input checked="" type="checkbox"/> Votação
Duração estimada do teste (em minutos)	5 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 sobrepor o sistema de verificação e forçar a carga de um sistema operacional não assinado.

*Tipo de Ataque:* Falha.

*Duração do teste:* 30 minutos.

*Pontos de intervenção:* rompimento das 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:* 30 minutos.

*Pontos de intervenção:* rompimento das 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 das 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 (visor 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, efetuar-se-á tentativas de modificação dos parâmetros de boot da urna para que esta não funcione conforme o previsto. Na segunda, tentaremos alterar os parâmetros do boot da urna para que esta force o boot a partir de uma mídia distinta da mídia de carga, com o intuito de sobrepujar o sistema de verificação e forçar a carga de um sistema operacional não assinado. Considera-se que o atacante tem 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 laços 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 criptagem do sistema operacional e assinatura dos programas internos.

Para tanto, a metodologia consiste em abrir a urna eletrônica, desligá-la durante uma operação, rapidamente borrifar sobre o pente de memória uma solução refrigerante, 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, considerando-se que o atacante tem 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 JTAC

Tentativa de conectar equipamento na interface JTAC da placa da urna, para comprometimento do MSD. Considera-se que o atacante tem 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 realidade 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 das 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/RJ252 e um adaptador do 9 pines.*

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

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

*Acesso à urna urna eletrônica. O ataque implica o rompimento das 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"*

*"MAX Profissional 7777 Blow Off Freeze Spray Electronic Component Cooler"*

*"SPRAY CONGELANTE GELO DUE-CL"*

*"Spray Congelante Ice"*

*"Spray Congelante de Ação Rápida CS68"*

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

*Notebook 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 urna eletrônica. O ataque implica o rompimento das 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 ruído.*

*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 LDX, Edinor, J-Link ARM.*

*Mídia R.O. com Keil ARM Evaluation Kit disponível em: <https://www.keil.com/demos/eval/urn.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 ao:

- 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 pré-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 no 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 criminosas 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 controle 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, discutir 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 do processo de segurança, basta monitorar a mídia de carga. Há rompimento dos lacres.*

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

*Probabilidade de rastreamento: é possível verificar o rompimento dos lacres, 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 lacres, 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 soluções:*

**Modificação do boot da urna**

*Todos os 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 reiniciadas.*

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

*H. Vdi*  
Vdi, 13/03/2012







## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G5PT2</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:	10:20	Hora de Término:	17:00
Resp. Acomp.:	Fernando Amatte			Rubrica:	

Dados do Teste			
Titulo do teste:	UFU-FACOM-TEFSEV: Tentativa de recuperação de dados da memória volátil do equipamento		
Início do teste (Data/Hora):	22/03/2012	10:20	
Termino do teste (Data/Hora):	22/03/2012	17:00	
Critério de Parada:	Obtenção dos dados da memória RAM, término dos componentes químicos responsáveis pelo congelamento do pente de memória ou provada inviabilidade dos métodos empregados.		

Relaxamento nos mecanismos e procedimentos de segurança
Inicialmente, foi disponibilizada uma urna eletrônica UE2009. Foram removidos todos os lacres presentes na UE2009, inclusive os que lacram o gabinete externo. A urna foi desmontada, e sua placa mãe removida do gabinete. De posse da placa mãe, o Investigador foi capaz de realizar os procedimentos necessários para manipular os componentes de hardware do equipamento.

Etapas Propostas para o Teste			
Etapas	Descrição		Status
1	Desmontagem da UE2009 e remoção de sua placa mãe.		
2	Inicialização da UE2009		
3	Aguardar o momento mais oportuno para iniciar o congelamento da memória: a) carregamento do <i>init</i> b) anteriormente ao carregamento da interface gráfica e c) urna no estado de prontidão para a votação.		
4	Borrifa-se o produto congelante nos dois lados da memória, a fim de congelá-la.		
5	Com um notebook previamente preparado, retira-se a memória da urna ainda ligada e conecta-a no notebook desligado.		
6	Liga-se o notebook, que inicia um software que copia os dados da memória para um dispositivo de armazenamento USB previamente configurado.		
7	Ao término da cópia, conecta-se o dispositivo USB na máquina do investigador.		
8	Abre a ferramenta forense de <i>dump</i> fornecendo o arquivo cópia da memória.		
9	Faz-se a leitura dos dados obtidos e analisa-se a validade dos mesmos, visando a obtenção de informações importantes da urna como por exemplo chaves criptográficas.		
10			

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
10:20	Copia-se de um dispositivo USB do investigador os aplicativos forenses previamente configurados.
10:40	A urna é desmontada, e a placa mãe é exposta para que se possa usar o spray congelante.
10:55	Os primeiros testes com o químico congelante são feitos, a memória é retirada da urna e colocada no notebook, primeiramente como uma simulação do teste.
11:26	A urna é aprontada para o teste, assim como o dispositivo USB e o notebook. É feita a inicialização da urna e espera-se o momento em que o <b>kernel</b> executa o <b>init</b> , e então congelar a memória com o spray congelante (durante 40 segundos) e retirá-la da urna.
11:28	A memória congelada é retirada da urna e inserida no notebook, e assim que a mesma é conectada, o notebook é ligado com o dispositivo USB conectado.
11:29	O aplicativo de cópia inicia a cópia para o dispositivo USB
11:59	A cópia está pronta e começa a auditoria da mesma, e em paralelo, um novo teste começa a ser preparado.
12:02	O novo teste segue os mesmos parâmetros do teste anterior, alterando apenas o momento em que a memória será retirada, neste teste ela será retirada logo antes da interface gráfica ser carregada (opções a, b e c supracitadas).
12:12	A memória congelada é retirada e colocado no notebook para a cópia da mesma.
12:40	A cópia do segundo <b>dump</b> termina, e esta é copiada para a máquina dos investigadores para auditoria.
12:53	O primeiro <b>dump</b> não retorna nada que possa ser relacionado com a urna.
13:00	Pausa para almoço
14:05	O segundo <b>dump</b> é analisado e um terceiro tem seu preparo iniciado.
14:58	São extraídas do Segundo <b>dump</b> algumas <i>strings</i> referentes a BIOS da urna, e alguns termos referente a um "ARM Device", provavelmente referente ao MSD
15:07	Um dos aplicativos de forense, o <b>foremost</b> , extrai diversos dados, os quais ele assinala como PGP Encrypted Data e PGP Key Ring. Não houve tempo de analisar a consistência dessas assinaturas assim como a potencialidade do uso das mesmas.
15:23	O terceiro <b>dump</b> é inicializado, porém com o carregamento total do software de votação, entretanto o produto congelante acaba, e não é possível congelar a memória totalmente.
16:05	Observou-se que o segundo <b>dump</b> também contém dados referente ao SYSLINUX porém em versões diferentes, provavelmente um era o carregador do software de auditoria e a outra versão do carregador do <b>kernel</b> da urna.
16:27:	Não se consegue nenhuma informação relevante do terceiro <b>dump</b> .
16:28	O teste é encerrado pela ausência de material congelante.
:	

Conclusões sobre o teste
<p>Ao término dos testes conclui-se que é possível obter dados da memória da urna, e que os mesmos poderiam ser comprometedores para a segurança do sistema, a dificuldade trata-se mais de uma questão de número de tentativas-e-erros e dos recursos disponíveis do que da segurança da urna em si. Desta forma, apesar de ser trabalhoso ser complexo, é completamente viável que com o tempo e recursos certos obter toda uma cópia da memória da urna dado o momento em que a memória da mesma é desconectada.</p>



#### Considerações do grupo investigador

Dadas as circunstâncias do teste, não foi possível obter dados de alto valor, ou mesmo testar os dados obtidos já que havia uma limitação de tempo e o teste com prováveis chaves obtidas levaria muito mais tempo que o disponibilizado no teste, tendo em vista os vários mecanismos que hora são cifrados hora assinados.

Todavia, talvez seja possível dificultar a extração de dados valiosos, desde que eles sejam colocados na memória de forma divididas, ou seja, um dado valioso é colocado em várias variáveis, e que são somente juntas para a leitura e utilização, reduzindo e muito a janela de oportunidade para que esta informação seja extraída.

Também é possível que a memória seja cifrada, pelo S.O ou pelo hardware, inviabilizando totalmente a extração de qualquer informação valiosa, sendo esse método mais trabalhoso e complexo.

#### Considerações do grupo de apoio

Teste seguiu conforme o esperado, porem sem obtenção de resultado positivo.

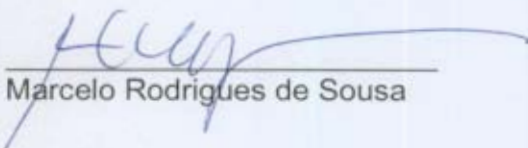
#### Futuras Possibilidades

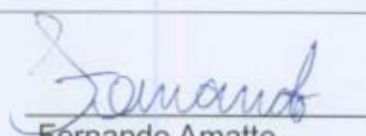
Se a urna permanecer da maneira como é hoje, em um futuro próximo será possível construir ferramentas bem mais eficazes e mais simples, para que toda a memória da urna seja copiada, e com o tempo e dedicação certos, é possível elaborar um sistema "chupa-cabra" ou replicante, capaz de obter os dados da memória em tempo real.

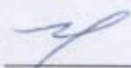
Considera-se essa possibilidade extremamente danosa à segurança total do sistema.


#### Alinhamento do PT

#### Informações Adicionais

  
Marcelo Rodrigues de Sousa

  
Fernando Amatte

  
Kil Jin Brandini Park

  
Otávio Augusto Araújo Silva

