



## Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

### Relatório dos resultados da realização dos Testes Públicos

#### Grupo 04

##### Representando a Universidade de Taubaté - UNITAU

Luís Fernando de Almeida – Doutor em Metodologia e Técnicas da Computação – UNESP

Bárbara Maximino da Fonseca Reis – Graduada em Engenharia da Computação – UNITAU

João Cristiano Monteiro Silva – Graduação em Engenharia da Computação – UNITAU

Luís Felipe Feres Santos – Graduação em Engenharia da Computação

Rafael Kudaka de Oliveira – Graduação em Sistemas de Informação – UNITAU

#### Plano de Teste G4PT2

Invalidação do FlashCard

#### 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	Invalidação do Flash Card
Instituição proponente (se aplicável)	Universidade de Taubaté
Responsável	nome: Luis Fernando de Almeida e-mail: luis.almeida@unitau.br telefone (do autor ou responsável): (12) 3625-4256, (12) 3629-5982, (12) 8113-5754
Sistemas afetados	<b>Software:</b> Sistema operacional utilizado nas urnas eletrônicas.  <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 type="checkbox"/> Votação
Duração estimada do teste (em minutos)	120
Extensão do ataque	<input checked="" type="checkbox"/> Urna ou seção eleitoral <input type="checkbox"/> Local de votação <input type="checkbox"/> Zona eleitoral <input checked="" type="checkbox"/> Município <input type="checkbox"/> Unidade da Federação <input checked="" type="checkbox"/> País
Conhecimentos necessários	Linux e shell script.

#### 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



### 3 Detalhamento do teste

#### 3.1 Resumo do teste

O teste visa desabilitar o *flash card*, possibilitando a inutilização da memória de programa e a gravação dos dados da votação, baseando-se no princípio de privilégio da arquitetura Linux.

#### 3.2 Fundamentação

A arquitetura Linux utiliza os privilégios para determinar as restrições de manipulação do usuário sobre o sistema operacional (acessar arquivos, configurações do sistema, execuções de *scripts*) e sobre hardware (controlar partição e dispositivos de entrada e saída).

#### 3.3 Precondições para o teste

Recursos materiais: para o teste é necessário um computador com editor de texto para a criação do script a ser implantado na urna.

Recursos humanos: especialistas na arquitetura Linux.

Relaxamento: como não pode alterar o sistema operacional da urna (não incluso no escopo do teste), solicita-se o acesso ao *flash card* externo e interno.

#### 3.4 Escopo – Superfície de Ataque

O ataque visa utilizar o Linux para inutilizar as mídias eletrônicas (*flash card*) utilizadas nas urnas. Ao inutilizar o *flash card*, os seguintes procedimentos serão inviabilizados:

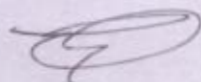
- registro de contagem de votos;
- boletins indicando o resultado da urna;
- log contendo os registros da votação.

#### 3.5 Janela de atuação simulada do atacante

O script contendo os comandos para inutilizar o *flash card* será implantado após a carga do sistema, isto é, antes das urnas serem transportadas para os locais de votação. Porém os comandos do script só serão inicializados durante o processo de votação (em um horário determinado pelo invasor).

#### 3.6 Pontos de intervenção

O laque e o sistema operacional serão os pontos de intervenção do teste.





### 3.7 Passos a serem realizados e material necessário

Lista de passos:

1. Antes da carga da urna, o atacante tem acesso físico ao *flash card*; (5 minutos)
2. Atacante insere o script no *flash card*; (15 minutos)
3. A urna recebe a primeira carga, mesmo utilizando o *flash card* alterado; (não acontecerá no dia do teste, pois a urna já está pronta)
4. As urnas são transportadas para os locais de votação; (não acontecerá no dia do teste, pois a urna já encontra em seu local de votação)
5. Em um determinado período da votação, o script é executado automaticamente (baseado no horário do sistema); (100 minutos)
6. Fim

O material de responsabilidade do TSE será um computador (para gerar o script), o leitor de flash card (possibilitar a comunicação do computador com o cartão) e o flash card (para armazenar o script).

### 3.8 Possíveis resultados e impacto

Resultado esperado:

- inutilização do *flash card*;
- alteração do resultado da votação (pois somente os votos anteriores ao bloqueio da *flash* serão computados).

Extensão do ataque:

- urna ou seção eleitoral;
- município;
- país.

Probabilidade de sucesso: 70% devido à padronização da arquitetura Linux.

### 3.9 Rastreabilidade

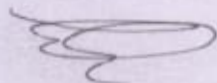
Não detectar o ataque: 85%

Detectar o ataque: 15%, pois só pode ser descoberto ao final da votação, quando emitir a contagem dos votos.



### 3.10 Solução proposta

Atribuir restrições a partir dos privilégios do usuário, impossibilitando que scripts sejam executados no sistema durante o horário de votação. Desta forma tem-se mais controle sobre o sistema operacional e assim garantir maior segurança.





## Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
<b>G4PT2</b>	Coordenador:	Luís Fernando de Almeida	
	Investigador 1:	Barbara Maximino F. Reis	
	Investigador 2:	João Cristiano Monteiro Silva	
	Investigador 3:	Luís Felipe Féres Santos	
	Investigador 4:	Rafael Kudaka de Oliveira	

Informações do Acompanhamento					
Data:	22/03/2012	Hora de Início:	10:00	Hora de Término:	11:00
Resp. Acomp.:	Fernando Amatte			Rubrica:	

Dados do Teste			
Titulo do teste:	Invalidação do FlashCard		
Início do teste (Data/Hora):	22/03/2012	10:00	
Termino do teste (Data/Hora):	22/03/2012	11:00	
Criterio de Parada:	Sucesso ou fracasso na invalidação do FlashCard.		

Relaxamento nos mecanismos e procedimentos de segurança	
Acesso à mídia de carga, antes da carga inicial das urnas (se possível acesso a mídia "mestre" que serviria como base para a geração de todas as outras mídias de carga).	

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Para execução desse teste o grupo necessitaria de acesso ao Kernel ( sistema operacional ) de urna sem que o mesmo estivesse cifrado. Ou: a) acesso ao algoritmo criptográfico + chaves b) acesso somente ao algoritmo criptográfico, e tentativa de obtenção das chaves por força bruta.	
2	Os arquivos de inicialização do sistema seriam alterados, para desmontar os dispositivos de entrada (mídias). Com acesso ao sistema, a ideia seria alterar arquivos como o "rc.local". Seria colocado	



	um "timer" (sleep), para que no momento determinado o sistema executasse um "umount" forçando a desmontagem de todos os dispositivos	
3	Sendo assim o sistema (software) da urna, não seria capaz de utilizar essas mídias após as mídias desmontadas.	
4	Em sistemas Linux normais existe um arquivo chamado "/etc/mod.probe/blacklist-usb-storage.conf". * Caso um dispositivo seja inserido nesse arquivo, o sistema ignora esse dispositivo, não permitindo que o mesmo seja montado/utilizado. * (nome do arquivo deve ser verificado, pois pode mudar entre as distribuições disponíveis)	
5	Os testes foram executados nas seguintes distribuições: Debian, Fedora e Ubuntu mais recentes. Em todas as versões testadas os testes foram bem sucedidos.	
6	Essa proposta, deveria ser efetuada, antes da carga das urnas, corrompendo a mídia matriz que seria base para a gravação de novas mídias.	

Hora	Procedimentos realizados durante o teste
:	Não foram executados, devido ao kernel da urna ser cifrado.
:	
:	
:	

Conclusões sobre o teste
Devido ao kernel ( núcleo do sistema operacional) da urna ser cifrado, não conseguimos acesso ao sistema, impossibilitando o teste.

Considerações do grupo investigador
Como sugestão de melhoria, caso existam links simbólicos no sistema operacional da urna, os mesmos devem ter o menor privilégio possível, evitando-se links com acesso total de gravação/escrita (principalmente).

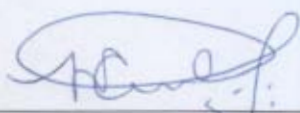
Considerações do grupo de apoio
O Teste transcorreu sem problemas e ou dificuldades.



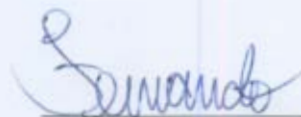
Futuras Possibilidades
Não há.

Alinhamento do PT

Informações Adicionais



Luís Fernando de Almeida



Resp. Acompanhamento



Barbara Maximino F. Reis



João Cristiano Monteiro Silva



Luís Felipe Feres Santos



Rafael Kudaka de Oliveira

