



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 G5PT4

UFO-FACOM-TEFSEV: Quebra do sigilo do voto eletrônico

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-TEFSEV
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	Software: <input type="checkbox"/> Software de votação usado nas seções eleitorais. Hardware: <input type="checkbox"/> Microterminal <input checked="" type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacres <input type="checkbox"/> Mídias Procedimentos: <input type="checkbox"/> Carga da urna <input checked="" type="checkbox"/> Votação
Duração estimada do teste (em minutos)	5 minutos
Extensão do ataque	<input 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	Para efetuar o teste basta conhecer o processo de votação através da Urna Eletrônica.

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.

O teste consiste na verificação da possibilidade de uma pessoa determinar se um eleitor votou ou não em um determinado candidato em uma eleição onde há uso da urna eletrônica brasileira. Objetiva-se demonstrar que através da utilização da urna eletrônica brasileira é possível verificar se um eleitor não votou em um candidato específico (com certeza absoluta) ou se votou no candidato com um grau de incerteza.

Tipo de Ataque: fraude (quebra de sigilo do voto eletrônico)

Extensão do Ataque: Brasil

Ponto de intervenção: O foco do ataque é a fotografia do candidato que é apresentada no visor da urna eletrônica durante a votação.

3.2 Fundamentação

O proponente deverá explanar, 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.

São Premissas do teste:

- 1. Um eleitor não deve ter o sigilo do seu voto quebrado, o voto é inviolável. Assim, não deve ser possível a qualquer pessoa determinar se um eleitor votou ou não votou em um candidato. O voto secreto é instituído no Artigo 14º da Constituição Federal do Brasil.*
- 2. A urna eletrônica possibilita a identificação do candidato pelo eleitor através da foto do candidato. O Artigo 27, inciso III, da Resolução nº 23.373 define a forma da fotografia do candidato: recente, digitalizada, preferencialmente em preto-e-branco, com dimensões 5x7cm, cor de fundo clara (preferencialmente branca), trajes adequados para fotografia oficial e sem adornos etc.*
- 3. Apesar da foto do candidato que será apresentada na urna ser pública (para conhecê-la basta o eleitor fazer acesso ao sítio do Tribunal Superior Eleitoral), o procedimento não é comum aos eleitores no Brasil. Assim, na eleição de 2010, para um eleitor tomar ciência da foto de seu candidato ele deveria entrar no sítio do TSE www.tse.jus.br, clicar no link Eleições 2010, então clicar no link Divulgação dos Candidatos, daí é aberta uma janela TSE Divulgação de Registro de Candidatos, onde o eleitor deve escolher o estado da federação desejado, daí escreve o Cargo e a Situação do seu candidato, realiza a pesquisa e finalmente basta clicar no nome apresentado para visualizar a foto do mesmo, que será apresentada na urna eletrônica no dia da votação.*
- 4. O voto no papel é uma manifestação escrita pelo eleitor. Nesse sistema não é possível ao eleitor identificar o candidato por uma foto pré-estabelecida, pois simplesmente não há fotos no sistema.*

5. O teste é possível em decorrência do uso de um sistema de Urna Eletrônica onde o candidato apresenta uma foto.

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.

*Não há necessidade de nenhum relaxamento por parte do TSE e dos TREs para a efetivação e sucesso desse teste. A fraude se dá por conta da forma que as fotos dos candidatos são definidas. O candidato (partido do candidato) informa ao Tribunal Eleitoral quem são os seus candidatos aprovados e ainda envia uma foto de cada candidato para ser divulgada pelo TSE e utilizada na eleição. O artigo 27, inciso III, da Resolução nº 23.373 do TSE determina como deve ser a foto, no entanto, há uma indeterminação no termo **traje adequado**, o que possibilita o ataque aqui proposto.*

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.)

Nesse teste, não haverá alteração de nenhum componente da urna eletrônica, físico ou lógico. O ataque é possibilitado na ocasião da eleição, no horário de votação oficial. Podemos realizar um ataque similar em todo território nacional, ou mesmo no exterior, nas embaixadas. Trata-se de um ataque à vulnerabilidade provocada pelo fato da urna eletrônica mostrar a foto do candidato quando seu número ou nome foram selecionados pelo eleitor.

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 precondições 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.

A janela de atuação do atacante se dá no dia da eleição, em local próximo à zona eleitoral e na própria zona eleitoral.

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.

O foco do ataque é a fotografia do candidato que é apresentada no visor da urna eletrônica durante a votação.

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.

O teste é totalmente descrito abaixo e para tal foram considerados 3 personagens que de forma indutiva definem um modelo do ataque.

Para a efetivação do ataque serão necessários 3 personagens com papéis bem definidos: Bob, Alice e Marcos.

- ✓ *Bob é o candidato à eleição. Bob usa normalmente roupas de baixo custo como camisetas e calça jeans. Na foto apresentada à Justiça Eleitoral, Bob encontra-se de terno e gravata, bem penteado.*
- ✓ *Marcos trabalha na campanha de Bob, é responsável por uma rede de pessoas que estão aliciando votos para Bob. O voto deve ser conseguido através de um pagamento de uma quantia em reais, sempre que o eleitor demonstrar que certamente votou em Bob.*
- ✓ *Alice é a eleitora, conhece Marcos e aceitou receber a quantia em reais para votar em Bob. Ela será acompanhada por Marcos no processo de votação, onde após a comprovação do voto em Bob receberá a quantia combinada.*

A fraude se dá no momento em que Alice sai da seção eleitoral e reencontra Marcos. Marcos pergunta então à Alice se ela votou em Bob. Ela diz que sim, demonstrando querer receber imediatamente o valor monetário. Nesse momento, Marcos faz a pergunta: - "Como Bob estava vestido?"

Sem perda de generalidade, aqui há duas possibilidades:

1ª) Alice diz que Bob estava com uma camisa branca. Marcos deduz imediatamente que Alice não votou em Bob. Há uma quebra no sigilo do voto de Alice, pois Marcos pode afirmar taxativamente que Alice não votou no candidato Bob.

2ª) Alice diz que Bob estava com terno e gravata, todo bonito. Marcos deduz que há uma grande probabilidade de Alice ter votado em Bob. Marcos diz a Alice que fará o pagamento quando a urna for apurada e Bob apresentar voto na urna. Nessa possibilidade, não há uma verdadeira quebra no sigilo do voto de Alice, todavia Marcos tem uma grande certeza no voto de Alice, que será ainda maior quando na urna forem totalizados votos para Bob.

O roteiro acima apenas descreve um *modus operandi* de compra de votos possibilitado pelo uso de urnas eletrônicas. Podemos criar outros cenários, onde diversas perguntas podem ser feitas para verificar se um eleitor votou ou não em um candidato, como por exemplo: "A gravata de Bob era de bolinhas?".

Para o teste ser realizado, basta votar em algum candidato e verificar a possibilidade de visualização da foto. Essa é a vulnerabilidade a ser atacada. Para a realização desse teste são necessários no máximo 5 (cinco) minutos.

Não há necessidade de equipamentos ou materiais para a realização desse teste, apenas o uso da urna eletrônica possibilita-o.

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.

O resultado esperado é a *quebra do sigilo do voto*, conforme demonstrado no item 3.7. Notadamente, a extensão do ataque é todo o País, visto que pode ser reproduzido em qualquer local de votação, mais ainda, em escala.

A probabilidade de efetividade desse ataque é de 100%, considerando o processo de seleção de fotos realizado nas eleições de 2010 e a legislação para a eleição de 2012.

3.9 Rastreabilidade

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

- Não detectar o ataque;
- Detectar o ataque.

Sem denúncias, o processo acima descrito é impossível de ser rastreado ou haver um flagrante da compra do voto. O "ataque" não é detectável pela Justiça Eleitoral.

3.10 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.

Fazer com que todos os candidatos se apresentem com o mesmo padrão. Sugerimos que todas as fotografias dos candidatos sejam apresentadas sem adereços e com uma vestimenta padrão, como por exemplo: terno escuro, camisa branca e gravata lisa para candidatos homens e, para candidatas mulheres, um terno escuro com camisa clara, foto em preto-e-branco.

JUSTIFICATIVA PARA O INDEFERIMENTO
DO

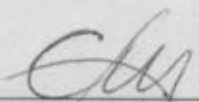
"Plano de Teste G5PT4"

"UFO-FACOM-TEFSEV: Quebra do sigilo do voto eletrônico"

Segundo ensina Walter Costa Porto em sua obra "Dicionário do Voto", na definição de "Voto Secreto", entende-se que "... a finalidade do sigilo é precaver o eleitor contra pressões que afetem a liberdade de sua escolha." O autor ainda cita o artigo 21 das Declarações dos Direitos do Homem, proclamada pelas Nações Unidas em 1948, o qual diz que a vontade do povo deverá se expressar "mediante eleições autênticas que haverão de celebrar-se periodicamente, por sufrágio universal e igual e por voto secreto ou outro procedimento equivalente que garanta a liberdade do voto."

Portanto, se o eleitor decidir, por sua livre escolha, pronunciar ou manifestar o seu voto, ainda assim o eleitor exerce sua liberdade, não comprometendo o sigilo do seu voto, conforme os conceitos expostos acima.

Cabe ainda lembrar que o eleitor pode verificar a aparência do eleitor, durante a votação, na urna eletrônica, e para votar em outro candidato simplesmente pode pressionar a tecla "CORRIGE" e votar em outro candidato, de acordo com sua própria consciência.



Comissão Disciplinadora
CELSO CASTRO

Marcelo Rodrigues de Souza
Investigador Responsável

JUSTIFICATIVA PARA O INDEFERIMENTO

DO

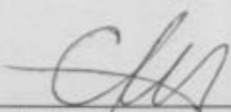
"Plano de Teste G5PT4"

"UFO-FACOM-TEFSEV: Quebra do sigilo do voto eletrônico"

Segundo ensina Walter Costa Porto em sua obra "Dicionário do Voto", na definição de "Voto Secreto", entende-se que "... a finalidade do sigilo é precaver o eleitor contra pressões que afetem a liberdade de sua escolha." O autor ainda cita o artigo 21 das Declarações dos Direitos do Homem, proclamada pelas Nações Unidas em 1948, o qual diz que a vontade do povo deverá se expressar "mediante eleições autênticas que haverão de celebrar-se periodicamente, por sufrágio universal e igual e por voto secreto ou outro procedimento equivalente que garanta a liberdade do voto."

Portanto, se o eleitor decidir, por sua livre escolha, pronunciar ou manifestar o seu voto, ainda assim o eleitor exerce sua liberdade, não comprometendo o sigilo do seu voto, conforme os conceitos expostos acima.

Cabe ainda lembrar que o eleitor pode verificar a aparência do eleitor, durante a votação, na urna eletrônica, e para votar em outro candidato simplesmente pode pressionar a tecla "CORRIGE" e votar em outro candidato, de acordo com sua própria consciência.



Comissão Disciplinadora
CELLO CASTRO

Marcelo Rodrigues de Souza
Investigador Responsável