



Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012
Brasília, março de 2012

Relatório dos resultados da realização dos Testes Públicos

Grupo 02

Representando a UnB – Universidade de Brasília

Lauro Cesar Araújo – Mestre em Arquitetura da Informação – UnB

Sérgio Freitas da Silva – Pós-graduado em Ciência da Computação - ESAB

Plano de Teste G2PT1

Quebra de sigilo do voto utilizando um aparelho celular

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

A handwritten signature in blue ink, appearing to be 'R', is located in the bottom left corner of the page.



61422

Tribunal Superior Eleitoral

PROTOCOLO

4.336/2012

13/03/2012 - 18:54



BF

Plano de Teste do Sistema Eletrônico de Votação

1 Informações gerais

Título do Plano de Teste	Quebra de sigilo do voto utilizando um aparelho celular
Instituição Proponente	Universidade de Brasília
Responsável (nome, e-mail e telefone do autor ou responsável)	Lauro César Araújo - laurocesar@gmail.com Sérgio Freitas da Silva - sergio.freitas.silva@gmail.com
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"/> Geração de mídias <input type="checkbox"/> Etapas de preparação da urna <input checked="" type="checkbox"/> Votação
Duração Estimada do Teste (em minutos)	30 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	Utilização de um celular

Observações:

- O teste a ser realizado deve ser, obrigatoriamente, reproduzível.
- Este plano deverá ter no máximo 10 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*

Conforme esquematizado na Figura 1, o teste consiste na quebra do sigilo do voto. Ao votar na urna eletrônica (1), o eleitor pode utilizar um celular (2) para registrar o processo de votação. Os dados do processo de votação podem ser armazenados (3) no próprio celular ou disponibilizados na Internet (4).

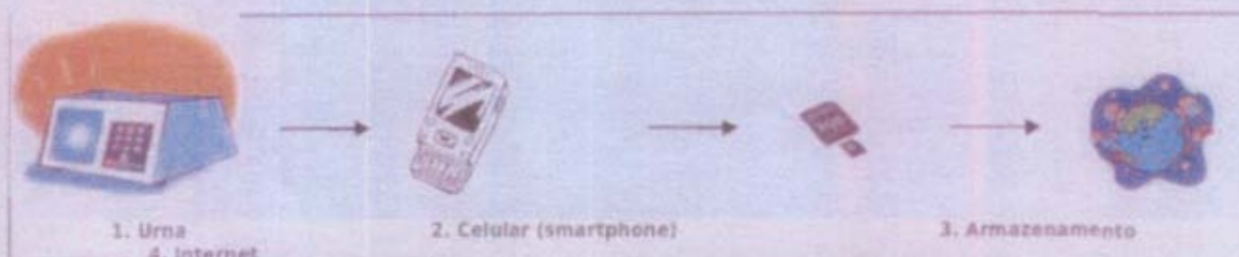


Figura 1 - Processo de teste da urna eletrônica

O objetivo do teste é demonstrar a vulnerabilidade do sigilo do voto diante da utilização de dispositivos eletrônicos (tais como celulares, câmeras e outros) durante o processo de votação.

A interceptação do processo de votação, ocorrido dentro da cabine de votação, pode ocorrer basicamente das seguintes formas:

1. Direta: a imagem da interface da urna eletrônica é gravada diretamente pelo dispositivo utilizado pelo eleitor (exemplo: câmera embutida em celular ou escondida em dispositivos de espionagem);
2. Indireta: o processo de digitação do voto no teclado da urna, ou a imagem apresentada no monitor LCD, pode causar uma interferência eletromagnética que pode ser detectada por receptores próximos à urna;

A exploração direta, citada acima no item um, publica indevidamente o conteúdo do voto e deixa o eleitor desprotegido já que, tecnicamente, é possível comprovar o conteúdo do seu voto.

A exploração indireta, citada acima no item dois, atinge o processo de votação (entrada de dados) e também coloca em risco o sigilo do voto, pois os sinais detectados podem ser armazenados e decodificados posteriormente (por exemplo, utilizando uma técnica de comparação dos ruídos).

Destarte, a finalidade principal do teste é demonstrar a possibilidade de quebra do sigilo do voto utilizando tanto a exploração direta quanto a indireta. Ressalte-se, porém, que não é escopo desse plano de teste a decodificação dos dados capturados com a exploração indireta. Tal experimento exigiria a utilização de recursos não empregados nesse plano de teste.

3.2 Fundamentação

A instituição do voto secreto, previsto no art. 14 da Carta Magna e art. 61 da Lei 9.504, deve resguardar tanto o conteúdo do voto (os dados) quanto o processo de votação (entrada de dados). Desse modo, é responsabilidade do Tribunal Superior Eleitoral não só o uso adequado e correto dos recursos técnicos disponíveis para cumprimento da Constituição, como também a própria proteção do eleitor quanto à inviolabilidade do voto.

A utilização de dispositivos eletrônicos na cabine de votação possibilita o registro, direto ou indireto, do voto implicando na quebra do sigilo, senão vejamos:

1. O eleitor que voluntariamente registra e publica seu voto interfere no sigilo do voto dos demais eleitores viabilizando a dedução lógica dos votos dos demais;
2. O eleitor que pretende negociar seu voto passa a ter uma prova material do mesmo;
3. O eleitor que é coagido a votar pode tornar-se refém do aparato tecnológico capaz de rastrear sua votação;

Referente à interceptação das radiações eletromagnéticas, durante a Segunda Guerra Mundial, o exército americano usou um dispositivo de comunicação telegráfica chamado Bell 131-B2. Ao testar este equipamento, um pesquisador do laboratório Bell observou, por acaso, que o funcionamento deste dispositivo causava interferência num osciloscópio localizado remotamente no laboratório. Para testar a vulnerabilidade do dispositivo, os engenheiros instalaram o dispositivo à cerca de 25 metros de distância e capturaram as radiações comprometedoras, sendo capazes de recuperar 75% do texto original emitido pelo dispositivo. Este problema de radiação comprometedora tem sido denominado de TEMPEST [1]. O termo TEMPEST também se refere à investigação e estudo destas radiações comprometedoras [2], ou seja, dessas radiações que comprometem a segurança da informação.

Desde então, diversos fenômenos desse tipo têm sido relatados e estudados pelos cientistas. Recentemente, dois pesquisadores suíços (Vuagnoux e Pasini) publicaram seu estudo sobre TEMPEST relacionado especificamente aos teclados. Os pesquisadores concluíram que a maioria dos teclados modernos gera radiações comprometedoras e que estes teclados não são seguros para transmitir informações confidenciais. [3]

Nesse estudo, os pesquisadores relatam vulnerabilidades em todos os tipos de teclados testados e registram a recuperação de 95% da digitação em teclados do tipo PS/2 (numa distância de até 20 metros). Um vídeo demonstra a decodificação dos sinais capturados e a reconstituição da digitação interceptada através de filtros específicos [4].

Referências:

- [1] NATIONAL SECURITY AGENCY. TEMPEST: A Signal Problem, 2007.
Disponível em: http://www.nsa.gov/css/inf/inf_files/cryptologic_spectrum/tempest.pdf.
Último acesso em: 13/03/2012.





[2] NATIONAL COMMUNICATIONS SECURITY COMMITTEE (NCSC). TEMPEST GLOSSARY, 2001.

Disponível em: <http://cryptome.info/0001.ncsc-3.htm>

Último acesso em: 13/03/2012.

[3] VUAGNOUX, Martin & PASINI, Sylvain. *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*. LASEC/EPFL, 2009.

Disponível em: http://www.usenix.org/events/sec09/technical_papers/vuagnoux.pdf

Último acesso em: 13/03/2012.

[4] VUAGNOUX, Martin & PASINI, Sylvain. Vídeo do experimento.

Disponível em: <http://lasec.epfl.ch/keyboard/>

Último acesso em: 13/03/2012.

3.3 Precondições para o teste

Para realização dos testes será necessária a utilização dos seguintes recursos:

Recursos materiais:

- a. Urna eletrônica (terminal do eleitor), escolhida aleatoriamente, com programas carregados, configurada e disponível para votação;
- b. 1 (um) Aparelho Celular com as seguintes especificações:
 - i. Câmera embutida;
 - ii. Conexão com a Internet (2G ou 3G);
 - iii. Chip GSM habilitado;
 - iv. Aplicativos instalados (gravador de som, e-mail ou browser);
- c. 1 (um) Receptor de rádio, com as seguintes especificações:
 - i. Pelo menos 2 bandas (AM/FM)
 - ii. Amplo espectro de AM (pelo menos de 530 a 1700 KHZ)
 - iii. Sintonia manual com ajuste fino;
 - iv. Conector de saída fêmea P2 ("Phone" ou "line out");
 - v. Antena telescópica (retrátil);
- d. 1 Cabo com 2 (dois) conectores macho do tipo P2 ("TRS Connector") com no mínimo 2(dois) metros de comprimento;
- e. 1 Fone de ouvido com um conector do tipo P2 com no mínimo 2 (dois) metros de comprimento;
- f. 2 pontos de energia disponíveis (110/220 Volts)
- g. Papel e caneta

2. Recursos humanos:

Nome	Qualificação
Lauro César Araújo	Mestre em Ciência da Informação
Sérgio Freitas da Silva	Especialista em Tecnologia da Informação

3. Informações adicionais:

- i. O celular e o receptor de rádio devem ser instalados o mais próximo possível da urna eletrônica (terminal do eleitor)

- ii. O receptor de rádio poderá ser conectado ao celular via cabo com conectores macho do tipo P2;

3.4 Escopo - Superfície de Ataque

O ataque consiste na quebra do sigilo o voto através da exploração direta ou indireta (supracitada). Os seguintes componentes do sistema de votação eletrônica sofrerão atuação durante o teste:

- Material: urna eletrônica (o terminal do eleitor deve estar disponível para votação);
- Ambiental: o ambiente deve possuir, preferencialmente, uma única urna eletrônica e devem-se evitar ruídos e interferências eletromagnéticas para facilitar a execução do experimento;
- Procedural: simulação de votação do eleitor;

3.5 Janela de atuação simulada do atacante

A atuação do atacante deve ocorrer nos seguintes instantes:

- a) Acesso à urna eletrônica, escolhida aleatoriamente e disponível para votação;
- b) Simulação de votação na urna eletrônica;
- c) Acesso ao celular e/ou ao receptor de rádio para rastreamento e detecção da radiação eletromagnética emitida pelos componentes eletrônicos da urna e/ou gravação do processo de votação;
- d) Gravação no celular do sinal detectado pelo receptor de rádio e/ou das imagens do processo de votação;

3.6 Pontos de intervenção

O único ponto de intervenção é a captação pelo celular e/ou receptor de rádio da radiação eletromagnética emitida pelos componentes eletrônicos da urna. Durante o teste, o celular ou receptor devem estar localizado o mais próximo possível da urna para simplificar o teste e dispensar a utilização de equipamentos especiais tais como osciloscópios e antenas especiais.

3.7 Passos a serem realizados e Material Necessário

O processo é detalhado abaixo:

- a) O atacante posiciona o celular e/ou o receptor de rádio o mais próximo possível da urna eletrônica (o celular e o receptor de rádio podem ser movimentados livremente para melhorar a recepção);
 - Duração estimada: 1 minuto
- b) O atacante simula um processo de votação e filma todo o processo através do celular;
 - Duração estimada: 4 minutos
- c) O atacante digita repetidamente qualquer tecla da urna eletrônica;





- d) O atacante sintoniza o receptor de rádio em diversas frequências até detectar *uma possível interferência eletromagnética emitida pelo teclado ou pelo monitor LCD da urna eletrônica*;
- Observação: nessa etapa pode ser útil a utilização do fone de ouvido;
- e) Se a interferência foi detectada então vá para o próximo passo (f), senão volte ao passo (c)
- Duração estimada (c+d): 15 minutos
- f) O atacante registra a frequência obtida e conecta a saída do receptor de rádio (ex: "phone" ou "line out") ao celular via cabo com 2 (dois) conectores macho do tipo P2 ("TRS Connector");
- Duração estimada: 2 minutos
- g) Iniciar o aplicativo de gravação do celular e configurá-lo para captura dos sinais;
- Duração estimada: 1 minuto
- h) Iniciar a gravação dos sinais digitalizados no aplicativo do celular;
- Duração estimada: 1 minuto
- i) Digitar repetida e pausadamente uma sequência padrão na urna eletrônica (ex: 1,2,3,4,5,6,7,8,9,0, Branco, Corrige, Confirma)
- j) Se a gravação de toda a sequência foi concluída com sucesso Então vá para o próximo passo (j) Senão volte ao passo anterior (h)
- Duração estimada (h+i): 2 minutos
- k) Reproduzir o arquivo gravado;
- Duração estimada: 3 minutos;
- l) Simular o envio e/ou entrega do arquivo à terceiro;
- Duração estimada: 1 minuto;
- m) Fim;

Critério de parada:

- Gravação, direta e indireta, do processo de votação;

Tempo total estimado:

- 30 minutos;

Materiais necessários:

1. Urna eletrônica (terminal do eleitor), escolhida aleatoriamente, com programas carregados, configurada e disponível para votação;
2. 1 (um) Receptor de rádio (conforme especificado anteriormente);
3. 1 Aparelho Celular (conforme especificado anteriormente);
4. 1 Cabo com 2 (dois) conectores macho do tipo P2 ("TRS Connector") com no mínimo 2 metros de comprimento;
5. 1 Fone de ouvido com um conector macho do tipo P2 ("TRS Connector") com no mínimo 2 metros de comprimento;
6. 2 pontos de energia disponíveis (110/220 Volts)
7. Papel e caneta

3.8 Possíveis resultados e impacto

Os resultados esperados são os seguintes:

- Tipo do resultado esperado:
 - o Registro, direto e indireto, do processo de votação na urna eletrônica;
- Impacto:
 - o Risco de quebra do sigilo do voto;
- Extensão do ataque:
 - o Todo o País

Segundo pesquisa citada no item 3.2 (Vuagnoux & Pasini), em condições ideais, a probabilidade esperada de sucesso do ataque é de 100% de detecção de radiação comprometidora. Nas condições do teste, sem a utilização de equipamentos especiais, estimamos a probabilidade de sucesso do ataque em 50%.

3.9 Rastreabilidade

A princípio, o ataque não seria detectado diretamente já que não há intervenção no sistema de votação eletrônica. Outro dificultador é que o recurso utilizado no ataque trata-se de um celular e/ou receptor de rádio que se encontram amplamente disponíveis como equipamento de uso pessoal. Por fim, dependendo da configuração e sensibilidade, o receptor com uma boa antena pode ser utilizado à distância dificultando em muito a rastreabilidade do ataque.

3.10 Solução proposta

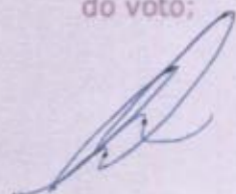
Para solucionar o problema identificado no plano de teste sugerem-se as seguintes alternativas:

Solução 1) Revista manual em busca de equipamentos eletrônicos ou uso de equipamento detectores de metais;

- A revista manual de todos os cidadãos deveria ser realizada no momento anterior à entrada na cabine de votação;

Solução 2) Redesenho da interface de votação para dificultar a gravação direta das imagens via câmeras embutidas em dispositivos móveis;

Solução 2) Emissão de ruídos aleatórios para confundir o inimigo e proteger o sigilo do voto;





- Esta solução poderia ser desenvolvida na própria urna para emular a radiação eletromagnética emitida pelos componentes eletrônicos da urna;

Solução 3) Blindagem da urna eletrônica;

- Esta solução evitaria a interceptação da radiação eletromagnética emitida pelos componentes eletrônicos da urna;

Solução 4) Mudança da interface para tela sensível ao toque ("touch screen");

- Esta solução permitiria a geração de teclados virtuais dinâmicos que aumentariam a segurança do processo de votação;
- Nesse caso o monitor LCD também deveria ser blindado;

Notas finais:

Este plano de testes contém informações sensíveis de segurança da informação. Recomendamos a gestão adequada destas informações para evitar prejuízos materiais e institucionais relacionados à sua má utilização.

A partir da análise do código-fonte do Sistema de Apuração realizada por estes investigadores, registramos que temos sugestões há serem realizadas fora do escopo deste teste. Caso haja interesse, as sugestões poderão ser realizadas diretamente a representantes da Instituição TSE.

JUSTIFICATIVA PARA O INDEFERIMENTO

DO

"Plano de Teste G2PT1"

"Quebra de sigilo do voto utilizando um aparelho celular"

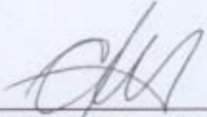
Segundo ensina Walter Costa Porto em sua obra "Dicionário do Voto", na definição de "Voto Secreto", entende-se que "... a finalidade do sigilo é precaver o eleitor contra pressões que afetem a liberdade de sua escolha." O autor ainda cita o artigo 21 das Declarações dos Direitos do Homem, proclamada 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."

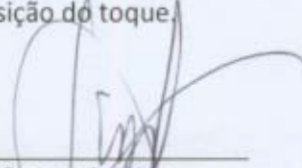
Portanto, se o eleitor decidir, por sua livre escolha, pronunciar ou manifestar o seu voto, ainda assim o eleitor exerce sua liberdade, não comprometendo o sigilo do seu voto, conforme os conceitos expostos acima.

Convém ainda mencionar o Artigo 54 da Resolução TSE Nº 23.372/2011, a qual "Dispõe sobre os atos preparatórios, a recepção dos votos, as garantias eleitorais, a justificativa eleitoral, a totalização, a divulgação, a proclamação dos resultados e a diplomação para as eleições 2012". O referido artigo diz: "na cabina de votação é vedado ao eleitor portar aparelho de telefonia celular, máquinas fotográficas, filmadoras, equipamento de radiocomunicação, ou qualquer instrumento que possa comprometer o sigilo do voto, devendo ficar retidos na Mesa Receptora enquanto o eleitor estiver votando (Lei nº 9.504/97, art. 91-A, parágrafo único)".

Portanto, o TSE tem conhecimento da possibilidade apontada no Plano de Testes em questão, tendo para isso envidado ações no sentido de mitigar os efeitos deste tipo de ataque.

Sobre as sugestões emitidas pelo proponente do Plano de Testes, elas são valiosas e serão analisadas. Particularmente, sobre as sugestões 2 e 3 (sic), as urnas atuais já contam com teclado protegido a emissões de radiações eletromagnéticas. Esta ação foi consequência dos resultados dos Testes Públicos de Segurança de 2009. A solução 4 reconhecidamente inseriria vulnerabilidades indesejadas por exigir um processo de calibração da posição do toque.



Comissão Disciplinadora

Lauro Cesar Araújo
Investigador Responsável