



Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012
Brasília, março de 2012

Relatório dos resultados da realização dos Testes Públicos

Investigador Individual 2

Representando o CERTI - Fundação Centros de Referência em Tecnologias Inovadoras

Ricardo Antonio Pralon Santos – Mestre em Engenharia Mecânica - UFSC

Plano de Teste I2PT1

Teste de exploração dos Mecanismos de proteção de carga da Urna

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



JRV-02

Plano de Teste do Sistema Eletrônico de Votação

1 Informações gerais

Título do plano de teste	Teste de exploração dos <i>Mecanismos de proteção de carga da Urna</i>
Instituição proponente (se aplicável)	Fundação CERTI
Responsável	nome: <u>Ricardo Antonio Pralon Santos</u> e-mail: <u>rap@certi.org.br</u> telefone (do autor ou responsável): <u>(48) 32392164/(48)91117813</u>
Sistemas afetados	Software: <i>Software de votação usado nas seções eleitorais.</i> Hardware: <input type="checkbox"/> Microterminal <input checked="" type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacres <input checked="" type="checkbox"/> Mídias Procedimentos: <input checked="" type="checkbox"/> Carga da urna <input type="checkbox"/> Votação
Duração estimada do teste (em minutos)	30 Minutos (Não incluído o tempo necessário a preparação)
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 type="checkbox"/> País
Conhecimentos necessários	[Mínimos conhecimentos técnicos necessários para a realização do teste] <i>Operação de Micro Informática.</i>

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 terá o objetivo de examinar os mecanismos de proteção de carga de programas da urna eletrônica; em sua fase de carga via exploração do loader, ataque a BIOS e extensão da mesma. Em uma segunda etapa será explorado o conceito de ataque ao conteúdo da Flash de Carga via virtualização de hardware.

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.

É sabido que o ponto crítico para a carga de programas maliciosos na urna é necessário burlar os mecanismos de proteção embutidos no hardware. Sabemos que em situação real que um "atacante" de posse da urna poderá incluir pequenas modificações do hardware (de forma dissimulada) incluindo corte de trilhas e uso de ligações wire-up no sentido de desabilitar momentaneamente as proteções por hardware durante o boot. Tais modificações são usadas em ataques a produtos de mercados com proteção intrínseca como consoles de jogos (ex: PS/2), e sabemos que uma vez aberto caminho e documentado qualquer técnica eletrônica competente pode replicá-lo sem nenhum problema.

Uma vez que um loader malicioso consiga rodar na Urna, teoricamente poderá reutilizar o loader original para carregar o SO encriptado, fazê-lo rodar e introduzir código malicioso no sistema operacional permitindo interceptar chamadas do SO e atacar os programas originais em tempo de execução sem ao menos ser necessário modificá-los a nível de arquivo. Para isto pode usar dos recursos atuais de virtualização máquinas de arquitetura Intel 32 bits dentro de máquinas Intel 32 bits (bochs, Vmware, etc) incluindo permitir o acesso controlado aos recursos de hardware original (incluindo imagem da BIOS original, da extensão da BIOS original, número identificação da urna, micro terminal, acesso teclado criptografado, e ao hardware de segurança) existentes na urna. Este conceito já foi exposto pelo projeto "Blue Pill" (<http://www.esweek.com/c/a/Windows/Blue-Pill-Prototype-Creates-100-Undetectable-Malware/>) e conceitualmente pode ser considerado de difícil detecção pelo próprio software. O software original da urna rodando em uma máquina virtual dentro da própria urna seria alvo ataques de fraudes ou perda de sigilo através do acesso as áreas de memórias por um programa "supervisor" malicioso rodando no host da máquina virtual, no caso a própria urna. Muitos destes softwares de virtualização X86 tem recursos de "debugger" facilitando esta tarefa de ataque. Desde já entendemos que o trabalho de virtualização completo não será possível de implementação no curto prazo disponível dos testes, mas como pré requisito deve-se conseguir burlar os mecanismo de proteção de carga de programas da urna, uma vez feito isto a segunda parte teoricamente é viável sendo apresentado como uma prova de conceito.



3.3 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.

Recursos necessários: Acesso ao hardware da Urna, Flash de Carga.

Software (Para preparação do ataque): Leitores/Editores de Disco/Arquivo(WinHex) , Utilitário de Leitura/Gravacao de BIOS(do fabricante da BIOS), Dissassembler (IDA Pro), Software de Virtualizacao(Boschs, VMware) , Debuggers(GDB), SO (Linux)

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.)

Urna Eletrônica Completa , Flash de Carga, Flash de Votação

3.5 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.

Acesso à urna eletrônica antes do período eleitoral; Acesso à memória flash de carga gerada antes do momento da carga da urna comprometida.



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.

Flash de Carga, Bios, Extensão de Bios. Pode ser necessário desabilitar o Hardware de segurança.

3.7 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.

- 1) O Atacante tem acesso uma urna antes do período eleitoral e executa as alterações de hardware pertinentes (incluído se necessário uma Flash interna de maior capacidade ou um "pendrive" auxiliar na usb interna, mais memória RAM pra permitir virtualização etc.)
- 2) Atacante tem acesso físico à Flash de Carga
- 3) Atacante, utilizando um computador portátil, lê Flash de Carga e copia seu conteúdo.
- 4) O atacante inclui a flash de carga original em sua versão de flash com loader comprometido, so embarcado com recursos de virtualização e programa supervisor malicioso.
- 5) Previamente a eleição em algum momento o atacante carrega sua versão de flash na memória da urna
- 6) Esta urna pode ser usada na eleição, ou mesmo gerar resultados de forma paralela a própria eleição gerando uma flash de votação adulterada para aquela seção.



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:
 - uma 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 do ataque caso tenha sucesso poderá ser a alteração do destino do voto ou a quebra do sigilo do voto conforme recursos do software supervisor rodando na urna hospedeira, a extensão do ataque será proporcional ao número de urnas impactadas, embora através de virtualização de urnas seja possível imaginar de que aproveitando dos recursos das flashes de cargas originais possa "fabricar" resultados (flash de votações) de várias urnas tendo uma única urna uma vez que nos foi informado que a assinatura assimétrica destes arquivos de votação pelo hardware de segurança (único de cada urna) ainda não será implementada nesta eleição sendo usada uma chave única por unidade de federação.

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.

Um ataque como este se bem sucedido pode não ser detectado de forma automática, porque teoricamente usa o próprio software gerado pelo TSE apenas rodando de forma virtualizada na própria máquina. Se for usado de forma paralela para gerar fraude na Flash de Votação via eleição paralela simulada pode ser detectado via confrontação dos resultados do boletim de urna da real e da flash de votação fraudada.

A Urna usada certamente fica comprometida, mas exigiria inspeção por técnico minimamente especializado.

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.

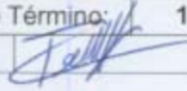
O problema tem solução, desde que a leitura do loader e decifração seja feita diretamente pelo hardware de segurança que "a princípio" não poderia ser substituído física ou virtualmente. Um loader em aberto embutindo informações e chaves da criptografia carregado pelo processo padrão do PC para leitura do SO teoricamente pode ser atacado usando as técnicas descritas. A implementação da assinatura digital da mídia de votação pela chave privada da urna evitaria também o caso da clonagem de resultados de urnas caso uma fosse comprometida.





Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores		
I2PT1	Investigador	Ricardo Antonio Pralon Santos
	Coordenador:	

Informações do Acompanhamento			
Data:	21/03/2012	Hora de Início:	17:20
		Hora de Término:	11:00
Resp. Acomp.:	Pedro Henrique Matheus da Costa Ferreira		Rubrica: 

Dados do Teste		
Titulo do teste:	Teste de exploração dos Mecanismos de proteção de carga da Urna	
Início do teste (Data/Hora):	21/03/2012	17:20
Termino do teste (Data/Hora):	22/03/2012	11:00
Critério de Parada:	Falha e ou sucesso em burlar o BIOS da Urna Eletrônica	
	Falha e ou sucesso na carga de arquivos alterados na mídia de carga da Urna Eletrônica	
	Falha e ou sucesso em carregar o sistema operacional da Urna Eletrônica em um hypervisor de maquina virtual, tal como o VMWare, ESXi, Bosch, etc.	

Relaxamento nos mecanismos e procedimentos de segurança	
Rompimento do lacre da flash de votação, após a cerimônia de lacração.	

Etapas Propostas para o Teste		
Etapa	Descrição	Status
1	O teste ocorreu de acordo com o plano de teste.	



Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
17:20	O Lacre foi rompido e a mídia de votação removida.
17:22	A Mídia de carga adquirida foi testada.
17:30	O Investigador conecta a mídia de carga ao micro-computador para efetuar um DUMP (Cópia de todo conteúdo da mídia de carga para o computador)
17:35	O Investigador inicia os procedimento de alteração em uma cópia do DUMP obtido através da flash de carga.
17:36	O Investigador abre o aplicativo Frhed e carrega o DUMP nesse aplicativo.
17:37	O Investigador altera 0xd8 onde consta Justiça Eleitoral, é alterado para Justiça Brasileira., essa imagem é salva.
17:40	O Investigador grava a imagem na flash de carga, e tenta efetuar o BOOT na urna eletrônica.
17:41	A Urna eletrônica, ao validar o boot loader acusa que o mesmo não é valido, devido à assinatura do mesmo não bater.
17:43	O Investigador tenta alterar um novo endereço da Flash de carga 0x69c, alterando novamente Justiça Eleitoral, para Justiça Brasileira.
17:45	É gravado o DUMP alterado na flash de carga e é feito um novo teste, obtendo-se o mesmo resultado do teste anterior.
17:50	Em um novo teste, dessa vez alterando o endereço 0x21e, onde consta parâmetros de inicialização do kernel do uenux, o Investigador modificou o parâmetro que contem a partição de inicialização do kernel, com o objetivo de carregar outro init.
17:52	O Investigador obteve sucesso em parte, pois o processo de boot do BIOS e validação da mídia ocorreram corretamente, mas durante a carga do kernel original da urna, ocorreu um erro e não foi possível prosseguir, tendo a Urna eletrônica reiniciado.
17:57	Em um novo teste, o investigador tentou carregar um kernel padrão do Linux, mas não houve sucesso na validação, pois foi acusado um erro na assinatura eletrônica do kernel.
18:00	Em um novo teste o investigador tentou remover o parâmetro de inicialização vga=769, o uenux carregou corretamente não acusando nenhum erro de validação da assinatura. Porém a urna eletrônica veio a travar na tentativa de carregar os softwares eleitorais. Nesse teste a urna eletrônica não desligou e nem reiniciou, ficando apenas congelada.
18:10	O Teste é suspenso até o dia seguinte devido ao encerramento dos trabalhos no local de testes da Urna Eletrônica.

10:00	O teste é reiniciado com a volta dos trabalhos no local de teste da urna eletrônica.
10:05	<p>Em análise ao sistema de boot o Investigado verificou que o MSD apresenta o Finger Print do boot loader, e ao procurar por esse finger print dentro da mídia de carga, o mesmo foi encontrado no endereço 0x3e0b, o investigador alterou o finger print para o que o MSD apresentava na tela, e obteve sucesso ao colidir 4 bytes do hash.</p> <p>Mesmo o MSD apresentando os finger print idênticos, o MSD não prosseguiu, vindo a travar e reiniciar a urna.</p>
10:10	<p>O Investigador tentou utilizar o DUMP da flash de carga como um disco em uma máquina virtual do Bochs.</p> <p>Ao inicializar a máquina virtual aparece a mensagem que essa mídia pertence à urna eletrônica e a justiça eleitoral, não prosseguindo o Boot.</p>
10:15	O investigador utilizou-se da ferramenta de depuração do bochs para tentar identificar e modificar os parâmetros de boot. Não vindo a obter sucesso.
10:30	O Investigador encerra seus testes.

Conclusões sobre o teste

Após algum estudo o investigador chegou a conclusão de que sem uma intervenção no Hardware torna-se infactível a modificação dos sistemas de carga e boot da Urna Eletrônica.

Seria necessário um estudo aprofundado dos métodos de carga e boot da urna, assim como o estudo dos meios criptográficos e de assinatura do boot loader. Para tal seria necessário se obter uma cópia do BIOS e sua extensão MSD, que executa todos os passos de autenticação deste processo.

O Investigador acredita que se for possível alterar fisicamente o hardware da urna eletrônica seria possível rodar o software do TSE de uma forma emulado em uma máquina virtual, sem que o software venha a detectar que esteja rodando em um ambiente comprometido. Para tal os passos resumidamente seriam os seguintes:

- 1- Cópia da ROM original;
- 2- Corte físico da linha de comunicação entre o MSD e o PIC, utilizado para reset da urna eletrônica;
- 3- Configuração da máquina virtual para utilizar os endereços específicos dos componentes de Hardware da Urna tais como Portas de IO, Portas USB, e junto

a isso a imagem do BIOS Original;

Considerações do grupo investigador

- O kernel da UE não veria aceitar parâmetros exceto os necessários, e uma vez ajustados os parâmetros, os mesmos deveriam ser cifrados, e assinados.
- Após o teste das 10:05h o investigador relata que não deveria conter o finger print na tela para que possa ser procurado dentro da flash de carga.
- Se atentando a este detalhe ele recomenda que o MSD não apresente informações relativas ao hash valido e invalido para comparação.
- Para minimizar as possibilidades deste tipo de ataque via virtualização, seria necessário se habilitar os mecanismos de assinatura disponíveis no MSD.
- Ao visualizar o esquema elétrico da urna, visualizou-se que poderia ser melhorado a forma como foi implementada a comunicação do MSD com o restante do hardware. Inclusive a validação da ROM (BIOS).

Considerações do grupo de apoio

O Teste transcorreu sem problemas e ou dificuldades.

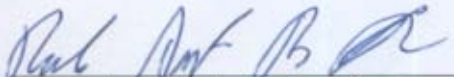
Futuras Possibilidades

O investigador pondera que ao possuir uma placa mãe da Urna Eletrônica, e um tempo maior, junto com equipamentos laboratoriais de microeletrônica, seria possível ler o conteúdo do BIOS e adaptá-lo a um ambiente de depuração de maquinas virtuais. Para investigar seu funcionamento.



Alinhamento do PT
O Teste seguiu corretamente o plano de trabalho, tendo poucos passos fora do descrito no plano original que foram detalhados na execução do plano.

Informações Adicionais
No plano de trabalho consta um passo anterior ao descrito neste plano, que seria atacar a parte física da Urna Eletrônica, e que devido à falta de equipamento necessário e ambiente especializado não foi possível de ser executado.


Ricardo Antonio Pralon Santos


Resp. Acompanhamento
Pedro H. Matheus

