Testes Públicos de Segurança do Sistema Eletrônico de Votação

Eleições 2012

Brasília, março de 2012

Relatório dos resultados da realização dos Testes Públicos

Grupo 03

Representando o Instituto Sapientia

Marcelo Achar – Especialista graduado em Ciência da Computação

Facundo Larrosa – Graduado em Gestão da Tecnologia da Informação

Pedro Ivo Pereira Gomes – Bacharel em Ciência da Computação

Plano de Teste G3PT1

Teste A - Boot com loader não assinado

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

TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

Plano de Teste do Sistema Eletrônico de Votação

1 Informações gerais

Título do plano de teste	Teste do Instituto Sapientia
Instituição proponente (se aplicável)	Instituto Sapientia – Grupo 3
Responsável	nome: Marcelo Achar e-mail: mce@sapientia.org.br telefone (do autor ou responsável): (61) 3326-0111 / 8401-1966
Sistemas afetados	**Software**: *Software* de votação usado nas seções eleitorais. **Hardware**: ☐ Microterminal ☒ Terminal do eleitor ☐ Lacres ☒ Mídias **Procedimentos**: ☐ Carga da urna ☒ Votação
Duração estimada do teste (em minutos)	540 minutos (9 horas)
Extensão do ataque	☒ Urna ou seção eleitoral ☐ Local de votação ☐ Zona eleitoral ☐ Município ☐ Unidade da Federação ☐ País
Conhecimentos necessários	Conhecimentos gerais em virtualização de máquina e avançado dos comandos do Linux.

2 Reservado ao Tribunal Superior Eleitoral (TSE)

Protocolo	**Data**
	Resultado ☐ Aprovado ☐ Aprovado com ressalvas ☐ Reprovado

3 Detalhamento do teste

3.1 Resumo do teste

O teste proposto é dividido em três testes menores que podem ser executados independentemente, os quais serão identificados no documento como teste A, B e C.

Teste A) Tentar inicializar a urna eletrônica usando uma memória CompactFlash na entrada externa com um loader não assinado pelo TSE.

Teste B) Conectar um adaptador USB-Ethernet na interface USB da urna eletrônica para checar se o mesmo é reconhecido e então usar um scanner de portas para verificar se existe alguma vulnerabilidade.

Teste C) Verificar se é possível clonar uma memória flash de votação antes do início da votação. Inserir a memória clonada na urna e manipular os votos de forma fraudulenta. Disponibilizar para os eleitores da seção uma urna de contingência com o flash de votação original. No final da votação, usar a urna que teve os votos manipulados para publicar o boletim de urna e transferir os dados da memória de votação.

3.2 Fundamentação

Teste A) Consiste na validação do correto funcionamento de um dos sistemas se segurança que a UE (Urna Eletrônica) possui, chamado Boot Seguro. Será feita uma tentativa de execução de software não autorizado pelo TSE na UE. Para isto será usado um CF (CompactFlash) como disco de boot criado com um loader e um SO (Sistema Operacional) não autorizado pelo TSE. O resultado esperado é que a UE não reconheça o loader do CF devido a validação que a BIOS da UE faz na assinatura do loader, conforme consta na especificação do processo de Cadeia de Confiança da UE. Caso a UE reconheça o CF como um disco de boot válido e inicie o SO será considerado uma falha de segurança, pois possibilita o uso de softwares fraudulentos na UE.

Teste B) Conforme informado na palestra técnica, um dos requisitos da UE é não possuir nenhuma interface de rede Ethernet com fio ou wireless. O teste consiste em conectar em uma das interfaces USB da UE um adaptador USB-Ethernet de baixo custo para verificar se o SO também foi preparado para ignorar este tipo de adaptador. Com um cabo crossover, o adaptador será ligado ao PC, que terá um servidor DHCP instalado. Caso a UE reconheça o adaptador e adquira um IP da rede, iremos executar um scanner de portas no IP da UE para verificar se a mesma possui alguma porta aberta rodando algum serviço que a torne vulnerável a ataques.

Teste C) Neste teste de fraude uma UE seria clonada para manipular os seus votos. O teste avalia se é tecnicamente possível a fraude sem considerar as dificuldades que o fraudador enfrentaria para ter acesso físico a UE. Antes do início da votação retira-se o FV (Flash de Votação) da UE e, usando um PC com um leitor de CF, copiamos o seu conteúdo para outro CF. Coloca-se FV original na UE

de contingência e a libera para a votação pelos eleitores como é feito sempre que a UE da seção apresenta falhas. Em outro ambiente isolado pelos fraudadores é colocado o FV clonado na UE substituída e é feita a votação de forma manipulada. Ao final do processo, o mesário recebe os BUs (Boletins de Urna) da UE fraudada para publicação e distribuição, e usa a MR (Memória de Resultado) da UE fraudada para transferir os dados para a consolidação.

3.3 Precondições para o teste

Os recursos listados abaixo, que se repetem para testes diferentes, podem ser compartilhados. No entanto, se houver risco de um determinado teste inutilizar a urna, este deverá ter uma urna própria.

Recursos materiais para o teste A:
1. Uma urna eletrônica (fornecido pelo TSE);
2. O micro-computador lacrado na fase de preparação (fornecido pelo TSE);
3. Um cartão extra CompactFlash da Apacer de 512Mb sem dados (fornecido pelo TSE);
4. O leitor de CompactFlash utilizado na fase de preparação (fornecido pelo TSE);
5. Uma chave philips que possibilite a abertura da tampa do CF externo e das portas USB da urna (fornecido pelo TSE);

Recursos materiais para o teste B:
1. Uma urna eletrônica pronta para o inicio da votação (fornecido pelo TSE);
2. O micro-computador lacrado na fase de preparação (fornecido pelo TSE);
3. Um adaptador USB-Ethernet compatível com o módulo "usbnet" do Linux (fornecido pelo proponente);
4. Um cabo de rede padrão crossover de pelo menos um metro de comprimento (fornecido pelo proponente);

Recursos materiais para o teste C:
1. Uma urna eletrônica pronta para o inicio da votação (fornecido pelo TSE);
2. O micro-computador lacrado na fase de preparação (fornecido pelo TSE);
3. Um cartão extra CompactFlash da Apacer de 512Mb sem dados (fornecido pelo TSE);
4. O leitor de CompactFlash utilizado na fase de preparação (fornecido pelo TSE);
5. Uma chave philips que possibilite a abertura da tampa do CF externo da urna (fornecido pelo TSE);
6. Uma UE de contingência. Como não tem muita relevância para o teste o seu uso é opcional (fornecido pelo TSE);

Recursos de software para o teste A:
1. O SO Windows XP já instalado no micro-computador lacrado na fase de preparação (fornecido pelo TSE);
2. LinuxLive USB Creator Versão 2.8.10 (fornecido pelo proponente);
3. Imagem ISO do Ubuntu 10.04 Minimal i386 (fornecido pelo proponente);

Recursos de software para o teste B:
1. O SO Windows XP já instalado no micro-computador lacrado na fase de preparação (fornecido pelo TSE);
2. VirtualBox 4.1.8 para Windons (fornecido pelo proponente);
3. VirtualBox Extension Pack 4.1.8 (fornecido pelo proponente);

4. Arquivo OVA (Open Virtualization Format Archive) com a máquina virtual do Xubuntu 10.04.2 Desktop i386 (fornecido pelo proponente);
5. Servidor DHCP instalado no Xubuntu;
6. Aplicativo scanner de portas instalado no Xubuntu;
7. Cliente Telnet instalado no Xubuntu;

Recursos de software para o teste C:
1. O SO Windows XP já instalado no micro-computador lacrado na fase de preparação (fornecido pelo TSE);
2. VirtualBox 4.1.8 para Windons (fornecido pelo proponente);
3. VirtualBox Extension Pack 4.1.8 (fornecido pelo proponente);
4. Arquivo OVA (Open Virtualization Format Archive) com a máquina virtual do Xubuntu 10.04.2 Desktop i386 (fornecido pelo proponente);

Recursos humano para os testes:
1. Dois recursos com conhecimentos gerais de virtualização e com conhecimento avançado dos comandos do Linux;

Considerações para os testes:
1. Os lacres da urna eletrônica são dispensáveis, pois não estão sendo considerados nos testes;
2. Os testes avaliam apenas tecnicamente se é possível ou viável executar o ataque ao sistema da UE. Não estão sendo considerados os dispositivos de segurança que poderiam impedir o atacante de ter acesso físico a UE;

3.4 Escopo – Superfície de Ataque

Teste A)
1. A urna eletrônica;

Teste B)
1. A urna eletrônica;

Teste C)
1. A urna eletrônica;
2. O flash de votação;

3.5 Janela de atuação simulada do atacante

Teste A)
1. Acesso a urna eletrônica;

Teste B)
1. Acesso a urna eletrônica;

Teste C)
1. Acesso a urna eletrônica antes e durante o período de votação;
2. Acesso ao flash de votação antes do período de votação;

3.6 Pontos de intervenção

Teste A)
1. Validação pela BIOS do loader e SO autorizados pelo TSE;

Teste B)
1. Rejeição de um dispositivo ethernet pelo SO da UE;
2. Ausência de serviços acessíveis pela ethernet na UE;

Teste C)
1. A possibilidade de clonar uma urna eletrônica copiando uma memória flash de votação para um outro cartão CompactFlash não autorizado pelo TSE;
2. A validação dos votos de uma UE que usava uma memória flash de votação clonada;

3.7 Passos a serem realizados e material necessário

Teste A) Tempo total: 2 horas
1. O atacante adquire um CompactFlash com a mesma especificação dos usados pela urna. Para o teste este CompactFlash será fornecido pelo TSE. (10 minutos)
2. O atacante insere o CompactFlash em um leitor ligado em um computador com Windows XP. (10 minutos)
3. No Windows, o atacante abre o software LinuxLive USB Creator, seleciona o ISO do Ubuntu 10.04 Minimal i386 e cria o disco de boot no CompactFlash. (30 minutos)
4. O atacante insere o teclado do PC na entrada USB da urna. (10 minutos)
4. O atacante insere o CompactFlash na entrada externa da urna. (10 minutos)
5. O atacante liga a urna e aguarda o inicio do boot. (30 minutos)
6. O atacante verifica se o SO Ubuntu foi carregado com sucesso na urna. (20 minutos)
7. Se o SO Ubuntu for inicializado o ataque será considerado bem sucedido.

Teste B) 3 horas
1. O atacante adquire um adaptador USB-Ethernet de baixo custo. Para o teste este adaptador será fornecido pelo proponente. (10 minutos)
2. O atacante insere o adaptador em uma entrada USB da urna. (10 minutos)
3. O atacante conecta o adaptador a um PC usando um cabo de rede crossover. Para o teste este cabo será fornecido pelo proponente. (10 minutos)
4. O atacante liga o PC e inicia a VM (Máquina Virtual) do Xunbutu preparada com um servidor DHCP. (30 minutos)
5. O atacante liga a urna e aguarda que a mesma inicialize. (20 minutos)
6. O atacante verifica no servidor DHCP se o mesmo atribuiu um IP para a urna. (20 minutos)
7. Se não foi atribuído nenhum IP o teste é então interrompido sem sucesso.
8. Se foi atribuído um IP, usando o Xunbutu executamos um scanner de portas no IP para verificar a existência de algum serviço. (30 minutos)
9. Para os serviços existentes faremos um teste de conexão ao mesmo usando o comando telnet e se for o caso usando o cliente especifico para o serviço. (50 minutos)
10. Se for encontrado algum serviço que permita acesso ao sistema da urna o ataque será considerado bem sucedido.

Teste C) 4 horas

1. O atacante tem acesso a urna de uma seção antes do inicio das votações. (10 minutos)
2. O atacante retira o flash de votação da urna. (20 minutos)
3. O atacante insere o flash em um leitor conectado a um PC com Linux. Para o teste o Linux será o Xubuntu e estará em uma VM instalada na máquina fornecida pelo TSE. (10 minutos)
4. O atacante faz uma copia do flash de votação em um arquivo no PC usando o comando dd. (40 minutos)
5. O atacante retira o flash do leitor e o insere em uma urna de contingência (este passo é dispensável, pois se trata de um procedimento normal quando se usa a urna de contingência).
6. O atacante substitui a urna da seção pela urna de contingência (este passo é dispensável, pois se trata de um procedimento normal quando se usa a urna de contingência).
7. O atacante adquire um CompactFlash com a mesma especificação dos usados pela urna. Para o teste, este CompactFlash será fornecido pelo TSE podendo ser o mesmo usado no teste A. (10 minutos)
8. O atacante insere o novo flash no leitor conectado ao PC com a copia do flash original. (10 minutos)
9. O atacante copia todos os dados do arquivo para o novo flash que será um clone do flash de votação. (60 minutos)
10. O atacante retira o flash clonado e o insere na urna substituída . (10 minutos)
11. O atacante liga a urna clonada e com a lista dos números dos títulos de eleitores da seção faz os votos dos mesmos manipulando as escolhas dos candidatos. (30 minutos)
12. O atacante emite na urna clonada os BUs para a publicação na seção. (30 minutos)
13. O atacante usa a MR para transferir os dados para a consolidação do resultado das eleições. (10 minutos)
14. O MR e BU da urna de contingência são ignorados pelo atacante.
15. Se todos os passos forem tecnicamente executáveis e se a memória de resultado da urna clonada for aceita como válida pelo sistema de consolidação então o ataque será bem sucedido.

3.8 Possíveis resultados e impacto

Tipo de resultado esperado:

Teste A) Uso de software não autorizado na UE.
Teste B) Possibilidade de conectividade ethernet da urna com uso de adaptador.
Teste C) Possibilidade de clonagem da urna para manipulação de votos.

Extensão do ataque:

Teste A) Qualquer urna.
Teste B) Qualquer urna.
Teste C) Uma urna de uma seção eleitoral.

Probabilidade esperada de sucesso:

Teste A) Baixa.
Teste B) Baixa.
Teste C) Alta.

3.9 Rastreabilidade

Todos os ataques do documento são rastreáveis desde que seja analisada individualmente cada urna atacada.

3.10 Solução proposta

Teste A) No caso de sucesso neste ataque, a urna deverá ser corrigida para ficar de acordo com suas especificações da Cadeia de Confiança.

Teste B) No caso de sucesso deste ataque, o kernel da urna deverá ser alterado para desabilitar o módulo "usbnet" que possibilita o uso de adaptadores USB-Ethernet.

Teste C) No caso de sucesso do ataque, poderia estudar a viabilidade de se adicionar aos dados do flash de votação o número serial do CF físico para checagem pelo software da UE.

13-3-2012

Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
G3PT1	Coordenador:	Marcelo Achar	
	Investigador 1:	Facundo Larrosa	
	Investigador 2:	Pedro Ivo Perreira Gomes	

Informações do Acompanhamento					
Data:	21/03/2012	Hora de Início:	10:27	Hora de Término:	11:03
Resp. Acomp.:	Marco Constantino			Rubrica:	

Dados do Teste		
Titulo do teste:	Teste do Instituto Sapientia: Teste A	
Inicio do teste (Data/Hora):	21/03/2012	10:27
Termino do teste (Data/Hora):	21/03/2012	11:03
Criterio de Parada:		

Relaxamento nos mecanismos e procedimentos de segurança
Foram necessários os relaxamentos referentes aos lacres, lacre do slot da flash de carga rompido.

Etapas Propostas para o Teste		
Etapa	Descrição	Status
1	Os passos foram executados conforme proposta.	
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
10:27	Foi solicitado o rompimento do lacre do slot da Flash de carga para acesso ao mesmo Teclado inserido na USB traseira da urna para caso de sucesso no teste haver interface para input de informações.
10:32	Mídia de carga modificada inserida na urna para tentativa de boot de Sistema Operacional (SO) não assinado. Urna ligada e iniciado a tentativa de boot da urna com SO não assinado. Devido a urna já estar carregada com o SO de votação ela não acessou a mídia externa com o SO modificado. Sendo assim, não houve sucesso nessa etapa do teste. Portanto, foi solicitado a abertura da urna para inserção da mídia modificado no slot interno da urna, lacres rompidos acesso facilitado e inserção da flash modificado no slot interno para tentativa de boot. Novamente não houve sucesso pois não reconheceu o loader do SO modificado.
11:00	Efetuado pedido de uma FC para que essa fosse zerada e se passasse por uma FI limpa, sem nenhum dado. Novamente foi feita a tentativa de boot com o SO modificado através do slot externo com a FI limpa. Após essa etapa não foi possível ser reconhecido no slot externo o SO modificado e a urna não terminou seu loader do FI, pois este estava zerado.
11:03	Dessa maneira o teste de boot com loader não assinado não obteve sucesso, pois a BIOS da urna não reconheceu como válido o loader do SO modificado. Na contextualização do investigador sobre seu acesso a urna, houve um extravio de uma urna onde posteriormente ele conseguiu acesso a ela. Dessa maneira foi possível todo procedimento de tentativa de modificação do SO. No que tange a sua devolução ela seria entregue no próprio depósito onde anteriormente estava armazenada através de ajuda de algum funcionário interno da segurança.

Conclusões sobre o teste
Não foi possível a inicialização de Sistema Operacional modificado uma vez que o BIOS verifica a assinatura do Sistema Operacional.

Considerações do grupo investigador

Considerações do grupo de apoio
Foram feitas algumas tentativas com os 3 tipos de Flash: Votação, Carga e Interna.
A urna foi aberta para que uma flash com Sistema Operacional modificado fosse
inserido no slot da flash interna para uma última tentativa. Sendo assim foram
esgotadas as possibilidades para o grupo nesse teste.

Futuras Possibilidades
O grupo não enxergou futuras possibilidades neste ataque.

Alinhamento do PT
O teste ocorreu de acordo com o que o plano de teste contemplava, não houve
nenhuma demanda distinta ao que o plano indicava que seria feito.

Informações Adicionais

Marcelo Achar

Marco Constantino

Facundo Larrosa

Pedro Ivo Perreira Gomes