



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 – Graduado em Engenharia da Computação – UNITAU

Luís Felipe Feres Santos – Graduado em Engenharia da Computação

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

Plano de Teste G4PT4

Mapeamento de voto com o eleitor

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	Mapeamento de voto com o eleitor
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	Software: 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)	300
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	Arquitetura do Sistema Operacional, Compilador Utilizado para geração do Sistema da Urna, Linguagem de Programação.

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

Este teste visa identificar o voto do eleitor, quebrando o seu sigilo por meio do mapeamento das sementes utilizadas em cada chamada da rotina aleatória utilizada para gravação destes votos. Este teste trata de uma variação do teste G4PT3 intitulado “Injeção de código e mapeamento da rotina de aleatoriedade”.

3.2 Fundamentação

Considerando a abordagem realizada pelo NIST SP800-90A, para realização e determinação de números randômicos, o teste procura mapear a função aleatória para inserção de votos e confrontá-la com a norma citada.

Para tal o procedimento a ser adotado seria a utilização dos dados contidos no arquivo de log na tentativa de identificação da semente da rotina aleatória e para gerar um mapa de localização do local de gravação do voto dentro do arquivo rdv. Desse modo, o atacante poderia associar o voto ao eleitor, comprometendo o sigilo do voto.

3.3 Precondições para o teste

Recursos Humanos:

- Especialista na Arquitetura do registro dos arquivos gerados pela urna.
- Domínio da Estrutura do Sistema Operacional.
- Especialista em Desenvolvimento.

Recursos Materiais:

- Ambiente da urna eletrônica.
- Mídias utilizadas para gravação de dados.
- Compilador C, C++ e Java.
- Mídia de resultados contendo todos os arquivos gerados pela urna eletrônica.

3.4 Escopo – Superfície de Ataque

Atingir o programa da Urna, propriamente o módulo “Vota”, e assim possibilitar a quebra do sigilo do voto. Para que isso seja possível, deve-se considerar um agente externo presente na seção eleitoral durante toda a votação identificando a sequência cronológica de votantes.



3.5 Janela de atuação simulada do atacante

O teste proposto considera a utilização do arquivo de log gerado pela urna disponibilizado eletronicamente, e o arquivo rdv com os votos de todos os eleitores de uma determinada seção eleitoral, que pode ser requisitado por um partido após as eleições.

Para a efetividade desse mapeamento torna-se necessário a atuação de um agente presente na seção eleitoral em questão identificando a ordem de votação dos eleitores, para em seguida associar os votos realizados.

3.6 Pontos de intervenção

Não percepção da ação do agente externo, presente no dia da votação, de identificação cronológica dos votantes. Leitura e interpretação dos dados constante no arquivo contendo os votos dos eleitores.

3.7 Passos a serem realizados e material necessário

1. Simulação de processo de votação (40 minutos).
2. Desenvolvimento e execução de rotina para leitura dos dados do arquivo com os votos dos eleitores (90 minutos).
3. Desenvolvimento e execução de rotina para leitura dos dados do arquivo de log da urna eletrônica (90 minutos).
4. Análise dos dados do arquivo de log (30 minutos).
5. Desenvolvimento e execução de rotina para identificar semente utilizada na rotina aleatória.
6. Mapeamento da rotina de aleatoriedade, possibilitando a associação de votos.
7. Fim.

Material necessário:

- Distribuição Linux, compatível a utilizada durante a etapa final de compilação;
- Ferramentas de compilação e depuradores;
- Ambiente de desenvolvimento (Eclipse ou NetBeans), com suporte a desenvolvimento em linguagem C/C++;

3.8 Possíveis resultados e impacto

Resultado Esperado:

- Rompimento do sigilo do voto.

Extensão do Ataque:

- País.





3.9 Rastreabilidade

Para estimar as chances de sucesso, o atacante deve considerar como é realizado o controle dos fiscais de votação em uma dada seção eleitoral e o grau de confiabilidade de seu representante responsável pela coleta destas informações durante o processo de votação.

Chances de sucesso: 40%

Detectar o ataque: 60%

3.10 Solução proposta

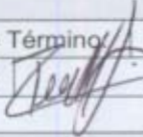
Para mitigar o ataque proposto, deve-se adotar um plano de controle dos representantes de partidos, inibindo a utilização de celulares, material para possíveis anotações, abordagens a eleitores após o processo eleitoral.

A handwritten signature in blue ink, consisting of a stylized 'R' followed by a flourish.



Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
G4PT4	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:	16:00
		Hora de Término:	17:00
Resp. Acomp.:	Pedro Henrique Matheus da Costa Ferreira		Rubrica: 

Dados do Teste			
Titulo do teste:	Mapeamento de voto com o eleitor		
Início do teste (Data/Hora):	22/03/2012	16:00	
Termino do teste (Data/Hora):	22/03/2012	17:00	
Critério de Parada:	Sucesso no mapeamento do eleitor com o voto.		
	Falha ao mapear as estruturas dos arquivos de LOG e RDV.		
	Mudança na rotina de captura da semente ou da rotina pseudo aleatória.		

Relaxamento nos mecanismos e procedimentos de segurança	
Não foram necessários nenhum tipo de relaxamento para realização do teste.	

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Simulação do processo de votação	
2	Desenvolvimento e execução de rotina para leitura dos dados do arquivo com os votos dos eleitores	



3	Desenvolvimento e execução de rotina para leitura dos dados do arquivo de log da urna eletrônica	
4	Análise dos dados do arquivo de log	
5	Desenvolvimento e execução de rotina para identificar semente utilizada na rotina aleatória.	
6	Mapeamento da rotina de aleatoriedade, possibilitando a associação de votos.	
7	Fim.	

Acompanhamento dos Procedimentos

Hora	Procedimentos realizados durante o teste
16:00	Devido ao plano de teste ser submetido a comissão avaliadora durante o período de teste, não houve por parte da comissão uma aprovação com tempo hábil para execução e desenvolvimento satisfatório do teste, uma vez que foi aventada a hipótese de que o teste fosse realizado em uma nova versão do sistema eleitoral.

Conclusões sobre o teste

Devido ao teste não poder ser colocado em prática, não foi possível se obter uma conclusão definitiva e acertada sobre a eficácia do ataque.

Considerações do grupo investigador

Parecer em tempo útil sobre o indeferimento ou deferimento dos planos de teste submetidos, frente ao fato de que a equipe aguardou em vão durante um dia a apresentação da negação de um de seus planos, sendo que a equipe havia dispensa cerca de oito horas de trabalho em um plano que a princípio já se encontrava negado. Deste modo, houve um mau aproveitamento do tempo disponível.

Maior facilidade para obtenção das informações que seriam comuns a um atacante externo, frente ao fato de que por diversas vezes a Equipe da UniTau não obteve sucesso ao utilizar as ferramentas disponibilizadas, tal como o LogViewer do TSE, qual não era compatível com a versão disponibilizada do UENUX. Um atacante externo teria em mãos o log oficial da sessão, disponível pela web e também contaria com respaldo legal para obter o arquivo RDV com os votos sufragados.

Tanto as informações apresentadas durante a palestra introdutória quanto as informações

fornecidas durante o primeiro dia do evento, pareciam não ser complacentes com o cenário encontrado pelos investigadores da UniTau quando da análise do código-fonte. Exemplificando: Durante a palestra de abertura, informou-se que os dados eram gravados aleatoriamente durante o processamento da UE, ocorrendo à possibilidade de ao final do processo existirem espaços em branco na matriz final com os votos. No processo de geração do RDV, tais espaços eram então suprimidos e somente os votos sufragados eram armazenados. Porém, durante o segundo dia dos testes públicos de segurança, um dos funcionários do TSE envolvidos com o processo de visualização do código-fonte, retificou a informação para o grupo, informando que os espaços eram mantidos para efeito de auditoria.

Considerações do grupo de apoio

Não há considerações a serem relatadas.

Futuras Possibilidades

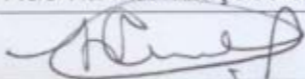
Análise da nova rotina de aleatoriedade para possível interpretação e detecção de sua entropia.

Alinhamento do PT

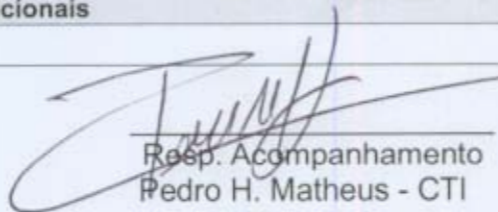
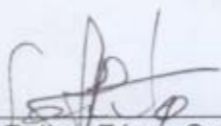
O teste transcorreu de acordo com o plano de trabalho.

Informações Adicionais

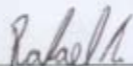
Não há informações adicionais



Luís Fernando de Almeida


Resp. Acompanhamento
Pedro H. Matheus - CTI

Luís Felipe Féres Santos



Rafael Kudaka de Oliveira

Barbara Maximino F. Reis

João Cristiano Monteiro Silva

