



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 – Graduação em Engenharia da Computação – UNITAU
Luís Felipe Feres Santos – Graduação em Engenharia da Computação
Rafael Kudaka de Oliveira – Graduação em Sistemas de Informação – UNITAU

Plano de Teste G4PT3

Proposta de Execução de Shellcode

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	Proposta de Execução de <i>Shellcode</i>
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: <i>Software</i> de votação usado nas seções eleitorais. Hardware: <input checked="" type="checkbox"/> Microterminal <input checked="" type="checkbox"/> Terminal do eleitor <input type="checkbox"/> Lacres <input type="checkbox"/> Mídias Procedimentos: <input checked="" type="checkbox"/> Carga da urna <input checked="" type="checkbox"/> Votação
Duração estimada do teste (em minutos)	180
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	Funcionamento de compiladores (modos de compilação, parâmetros, opções, etc), arquitetura de hardware, características de sistemas operacionais (versão, <i>kernel</i> , serviços e aplicações disponíveis, etc), lógica de programação para computadores (destaque para linguagem c/c++) e fundamentos de segurança de sistemas e aplicações com ênfase em programação e execução de <i>shellcodes</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

Este teste tem como objetivo realizar tentativas de execução de *shellcode* via injeção de código malicioso através do compilador, campos de entrada de dados e quaisquer outros meios possíveis de entrada de dados que os programas e/ou sistema operacional utilizados pelos aparelhos disponíveis para testes fazem uso.

3.2 Fundamentação

O ataque denominado inserção de *shellcode* tem o objetivo de executar instruções indesejadas no alvo por meio da exploração de vulnerabilidades que podem ser encontradas em aplicações (*softwares*) ou sistemas operacionais que permitem que essas instruções tomem conta do fluxo de execução da aplicação e/ou sistema vulnerável. Na maioria das vezes, eles são utilizados para permitir o controle remoto do alvo.

As vulnerabilidades exploradas via *shellcode* são fruto da falta de cuidados no momento em que uma aplicação ou sistema é desenvolvido. Esta falta de cuidado muitas vezes acaba deixando falhas em relação ao tratamento da memória que as aplicações utilizam, o que acaba, por fim, sendo o ponto de entrada das falhas exploradas via *shellcode*.

Atualmente, os *shellcodes* são chamados de *payloads*, pois eles são utilizados para os mais diversos tipos de ataques, não se limitando apenas a permissão de controle remoto do alvo desejado.

Em relação ao sistema eleitoral brasileiro, o objetivo deste teste é a tentativa de inserção de *shellcode* no compilador que será utilizado para compilar as aplicações que serão utilizadas para votação com a pretensão de se alterar alguma função utilizada por esses programas. Por fim, uma segunda frente de ataque esta relacionada com os campos de entrada de dados que as aplicações oferecem para que então possamos validar se estes campos estão ou não seguros de *input* indesejado de dados.

Considerando que o ataque está limitado as aplicações e sistemas utilizados nos aparelhos da eleição, os componentes afetados pelos ataques são todos aqueles que utilizam essas aplicações, destacando-se o terminal do eleitor e o microterminal.





3.3 Precondições para o teste

Recursos Humanos:

- Grupo de aproximadamente 4 ou 5 pessoas capacitadas para programar em c/c++ com noções de segurança de sistemas, memória de computadores, bases de conversão de dados (e.g. hexadecimal, ASCII, binário) e compiladores.

Recursos Materiais:

- Compiladores gcc e g++ (incluindo gdb);
- nasm (Compilador Assembly);
- ld (Linker);
- objdump;
- Um Computador para execução dos testes;
- Um editor de código fonte (preferencialmente notepad++ ou dev-c++);
- Livros, artigos e sites de programação, segurança da informação e compiladores;
- Sistema Operacional Linux BackTrack Versão 5r2 (podendo ser necessário alterar a versão).

Relaxamento:

- Não será necessário relaxamentos para este teste.

3.4 Escopo – Superfície de Ataque

Os componentes do sistema de votação que sofrerão atuação por parte da equipe executora são as aplicações e sistemas que são utilizados pelos microterminais e terminais dos eleitores.

3.5 Janela de atuação simulada do atacante

O atacante, em caso de alteração do compilador (inserção de *shellcode*), deverá ser alguém que consiga realizar a modificação no compilador que irá gerar os executáveis das aplicações que serão utilizadas na eleição antes que os programas sejam compilados.

No caso de entrada de dados via campos disponibilizados pela aplicação, o atacante poderá ser qualquer pessoa que tenha contato com os aparelhos da eleição após a carga das aplicações nos aparelhos.

3.6 Pontos de intervenção

Os pontos de intervenção identificados até o momento são:

- Software: Programas assinados;
- Segurança dos compiladores e do processo de compilação das aplicações;
- Hardware: Conhecimento da arquitetura interna para efeitos de mapeamento de endereços de memória e identificação de instruções adequadas para o sucesso do ataque.

3.7 Passos a serem realizados e material necessário

1º - Considerando que o atacante alterou o compilador dos programas da eleição:

1. Atacante altera o compilador que será utilizado para gerar os executáveis dos *softwares* da eleição, inserindo *shellcode* no mesmo;
2. Dependendo do objetivo do atacante, no momento da eleição podem ocorrer situações de dois tipos:
 - Aparelhos ficam indisponíveis para votação;
 - Comportamento dos softwares da votação podem ser alterados viabilizando que o *shellcode* execute instruções indesejadas utilizando o fluxo de execução da aplicação;
3. Fim

2º - Considerando que o atacante inseriu *shellcode* via algum campo de entrada de dados disponibilizado pelas aplicações:

1. Atacante pode atuar a qualquer momento depois que foi realizada a carga das aplicações nos aparelhos da eleição;
2. Atacante insere *shellcode* em algum campo de entrada de dados disponibilizado pela aplicação;
3. Se o código for executado com sucesso, o atacante obtém êxito no ataque que pode ter diversos objetivos como: indisponibilizar os aparelhos da votação, copiar os dados da votação, apagar os dados da eleição, entre outros;
4. Caso o atacante não obtenha sucesso na execução do ataque, nada acontece;
5. Fim

3.8 Possíveis resultados e impacto

Resultado Operado:





- Alterar o fluxo de execução das aplicações/sistemas de modo a forçar a execução de instruções indesejadas que podem ter objetivos como:
 1. Inutilizar os aparelhos de votação;
 2. Copiar os dados da votação;
 3. Apagar os dados da votação;
 4. Etc.

Extensão do ataque:

- Levando em consideração ataque ao compilador, a extensão acontece em âmbito nacional, pois afetaria as aplicações antes de serem carregadas nos aparelhos;
- Em relação ao ataque via campo de entrada de dados das aplicações, a extensão se limita a disponibilidade do atacante em comparecer a seção eleitoral para votar com a ressalva que existe somente um atacante. Em caso de mais atacantes, a extensão do ataque pode aumentar chegando em nível de país.

Probabilidade de sucesso:

Inserção de shellcode via compilador: 70% devido ao processo de compilação das aplicações que serão carregadas nos aparelhos da eleição;

Inserção de shellcode via campo de dados das aplicações: 50%, pois depende da segurança que já existe implementada nas aplicações da eleição;

3.9 Rastreabilidade

Não Detectar o Ataque: 70%

A chance de não detectar o ataque é alta considerando que não é verificado o *checksum* (ou assinatura) do compilador no qual são compiladas as aplicações e também considerando que não existe um meio de verificação eficiente das entradas de dados das aplicações.

Detectar o Ataque: 30%

A chance de detectar o ataque pode ser elevada se for levado em consideração a comparação do *checksum* (ou assinatura) do compilador utilizado para desenvolvimento e o compilador utilizado para compilação de modo a garantir que são idênticos e não existem alterações entre eles. Por fim, essa probabilidade também pode ser elevada com o desenvolvimento de um mecanismo eficiente de verificação de todos os campos de entrada de dados que as aplicações fornecem.



3.10 Solução proposta

Como soluções propostas:

- Comparação do *checksum* (ou assinatura) do compilador utilizado para desenvolvimento com o *checksum* (ou assinatura) compilador utilizado para compilação final das aplicações de modo a garantir que o mesmo não tenha sido alterado;
- Desenvolvimento de um mecanismo eficiente para verificar as entradas de dados nas aplicações de forma a garantir que nenhuma entrada fora do normal seja interpretada incorretamente e altere o comportamento do programa em execução.



Formulário de Acompanhamento dos Testes Públicos

Dados do Grupo de Investigadores			
G4PT3	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:	11:40	Hora de Término:	12:00
Resp. Acomp.:	Fernando Amatte			Rubrica:	

Dados do Teste			
Título do teste:	Proposta de execução de ShellCode		
Início do teste (Data/Hora):	22/03/2012		11:40
Termino do teste (Data/Hora):	22/03/2012		12:00
Critério de Parada:	Execução ou falha do shellcode		

Relaxamento nos mecanismos e procedimentos de segurança	
Para a execução dos testes, seria necessário:	
A) Acesso ao código fonte de urna	
B) Retirada de lacres	
C) Acesso a Flash de carga	

Etapas Propostas para o Teste		
Etapas	Descrição	Status
1	Esse teste pressupõe a) conseguir acesso ao código fonte da urna, ou b) alteração da Flash de carga, ou c) acesso direto ao sistema da urna, durante execução da mesma visando inserir um shellcode malicioso.	
2	O item A está fora do escopo do teste, pois não existe a possibilidade de acesso ao código para alteração e compilação mesmo nessa situação de prova de conceito.	
3	No item B, devido a cifragem do sistema de arquivo, não haveria tempo hábil para reproduzir o teste, visto que o grupo não tem acesso aos algoritmos e chaves.	
4	No caso do item C o acesso se daria, via interface USB presente na urna e um teclado com a interface USB.	
5	Caso com a interferência do teclado conseguíssemos um Shell (interface onde poderíamos digitar códigos/comandos) enviaríamos uma sequência de bytes para o sistema operacional, possibilitado a execução de comandos ou códigos a fim de controlar a urna.	

Acompanhamento dos Procedimentos	
Hora	Procedimentos realizados durante o teste
:	<p>Não realizado devido a:</p> <p>a) impossibilidade de acesso ao processo de compilação (compilador + parâmetros), onde com a alteração de parâmetros poderia permitir a execução de instruções maliciosas.</p> <p>b) sistema de arquivos cifrado</p> <p>c) impossibilidade de abertura de Shell e desativação do teclado (mecanismo de segurança) após a inicialização do Kernel.</p>

Conclusões sobre o teste
Devido aos mecanismos de segurança existentes na urna, os itens b e c não foram possíveis de serem reproduzidos.

Considerações do grupo investigador
Não há.

Considerações do grupo de apoio
Não há.

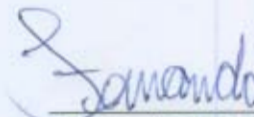
Futuras Possibilidades
Não há.

Alinhamento do PT
Não há.

Informações Adicionais
Não há.



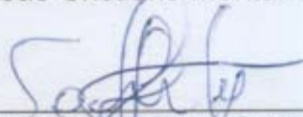
Luís Fernando de Almeida



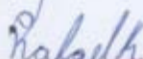
Resp. Acompanhamento

Barbara Maximino F. Reis

João Cristiano Monteiro Silva



Luís Felipe Féres Santos



Rafael Kudaka de Oliveira

