

As urnas eletrônicas e o sistema de votação no Brasil são seguros?



Debate “**Polêmicas Contemporâneas**” - FACED/UFBA

Maria Aparecida R. Cortiz

Advogada Eleitoral (PDT, etc.), CMInd

pt.wikipedia.org/wiki/Comitê_Multidisciplinar_Independente

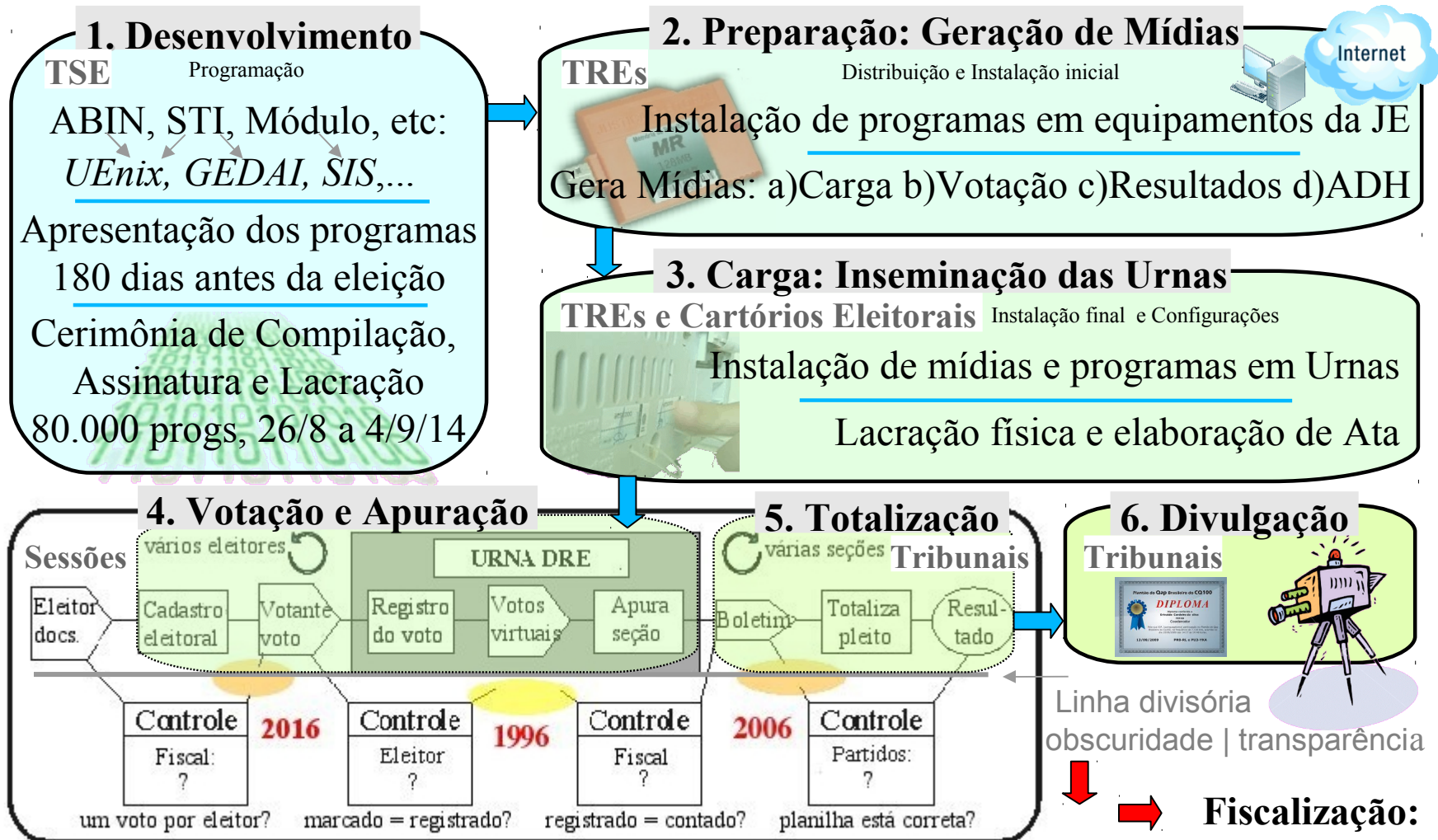
Roteiro

- O Processo de Votação no Brasil**
- Análise de código-fonte em 2014**
- Sobre prévias irregularidades**

O Processo de Votação

Organizado em 6 fases

Votação no Brasil: fases do processo



Lisura do pleito depende *totalmente* da honestidade dos programas que rodam *na* eleição

Conforme a Lei 9.504/97 e Resoluções TSE 23.397/13 e TSE 23.399/13

Análise de código-fonte

Relatada na Petição TSE 29.891/2014

Perguntas e Respostas

1- P: Sobre ADH: Em que momento, no processo, os arquivos gravados na mídia ADH são acessados/usados? Para quê as informações neles contidas são usadas?

TSE: É importante esclarecer que o ajuste de data e hora da urna – ADH – é regulado pela Resolução TSE nº 23.399/2013, conforme trecho transcrito a seguir:

“Art. 69. Eventual ajuste de horário ou calendário interno da urna, após a lacração a que se refere o artigo 65 desta resolução, será feito por meio da utilização de programa específico desenvolvido pelo Tribunal Superior Eleitoral, por técnico autorizado pelo Juiz Eleitoral, notificados os partidos políticos, coligações, Ministério Público e Ordem dos Advogados do Brasil, lavrando-se ata.

§ 1º A ata a que se refere o caput deverá ser assinada pelos presentes e conter os seguintes dados: I – data, horário e local de início e término das atividades; II – nome e qualificação dos presentes; III – quantidade e identificação das urnas que tiveram calendário ou horário alterado.”

A mídia do ADH contém apenas três arquivos de dados que permitem ativar o software de ajuste de data e hora previamente instalado na urna durante a preparação do equipamento para a eleição. A data ou hora da urna precisam ser ajustadas em função de defeito no relógio interno após a preparação e lacração do equipamento para a eleição. É possível usar o ADH antes da impressão da zéresima e depois do encerramento da urna. Não é possível usar ADH durante a votação dos eleitores.

Perguntas e Respostas

3- P: Inerator: No projeto SIS, o programa de nome “programaInerator.cpp” gera um *script* com base em *paths* para pares de chaves públicas/privadas. Qual a finalidade de tal *script*, e qual o propósito dessas chaves públicas/privadas em tal contexto?

TSE: Essa Classe MiniCA era utilizada para criação de uma Mini Certification Authority, utilizada até as eleições de 2004 como geradora de certificados para o TSE. Em 2006 já começou a utilização de certificados ICP. A referida classe apesar de estar em desuso desde 2004 se encontra ainda na sala de lacração pela necessidade de utilização dos **leitores binários em diversos outros projetos**. Não é mais utilizada para manipulação de certificados.

II- P: Internet acessível durante a geração de mídia: Solicito que na demonstração que será feita em 02/09/2014, sejam geradas mídias em computador com e sem conexão com a Internet..

TSE: Em 2/9/2014, foi realizada a apresentação do GEDAI-UE e software da urna. No GEDAI-UE houve geração de mídias (flashes e MRs) com e sem conexão com a Internet, visualização dos candidatos e visualização do log.

Também foram apresentados os seguintes procedimentos na urna: carga, autoteste, votação com e sem biometria, contingência, apuração da seção, ajuste de data e hora, impressão dos hashes, visualização do log.

Vulnerabilidades encontradas



PARTIDO DEMOCRÁTICO TRABALHISTA
PDT – DIRETÓRIO NACIONAL

CÓPIA

EXCELENTÍSSIMO SENHOR MINISTRO DIAS TOFFOLI – RELATOR DAS ELEIÇÕES
DE 2014 NO COLENDO TRIBUNAL SUPERIOR ELEITORAL

Tribunal Superior Eleitoral
PROTOCOLO JUDICIARIO
23.891/2014 Cópia.
04/09/2014-16:16



PARTIDO DEMOCRÁTICO TRABALHISTA – PDT – por sua advogada e representante credenciada para analisar os códigos-fonte e participar da Cerimônia de Homologação e Lacração dos programas a serem usados nas eleições 2014 vem, com todo respeito e acato, informar que:

Nos exames de código fonte dos programas apresentados para auditoria do sistema de votação informatizada no TSE, realizado conforme preve a Resolução TSE nº 23.397, artigo 1º, fatos relevantes foram encontrados a seguir articulados.

I – VULNERABILIDADES

- 1 - Vulnerabilidade no gerador de mídias de ajuste de data e hora:

No projeto GEDAI, o programa geradoradh.cpp tem sua inicialização feita com uma chamada de função srand(time(null)), fato que constitui vulnerabilidade, por redução drástica de entropia ao efeito protetor pretendido pelo desenho deste programa, que seria o de impedir a geração indiscriminada de mídias de ajuste de data e hora para as Urnas Eletrônicas.

Exatamente a mesma vulnerabilidade encontrada pela equipe vencedora nos Testes Públicos de segurança de 2012 com respeito ao embaralhamento do RDV, permanece, portanto, também para a geração de mídias de ajuste de data e hora.

Vulnerabilidades encontradas

2- Vulnerabilidade no driver de partições minix no kernel Linux das Urnas Eletrônicas.

No projeto UEnux, no arquivo ueminixkey.h, há um vetor de ofuscamento e uma chave criptográfica às claras, fixas e acessíveis por leitura direta. Tal chave se destina a cifrar partições minix, conforme invocada a partir do código em ueminix.c, como por exemplo nas mídias capazes de inicializar as Urnas Eletrônicas de modelo 2009 ou posterior, tais como os flashes de carga oficiais.

Tal arquitetura para inicialização criptográfica torna inócuos os mecanismos de controle e proteção a esses novos modelos, pois, mediante simples acesso a uma mídia de inicialização oficial, será possível gerar outras de diferente teor.

3 - Vulnerabilidade na classe MiniCA.cpp.

Essa classe do projeto SIS foi desenvolvida contendo um - único método - obterChaveSimetricaCA() - cuja única funcionalidade é retornar uma chave criptográfica simétrica ofuscada, porém fixa e embutida, o que anula qualquer efeito pretendível com o ofuscamento.

O programa programalInserator.cpp é o único local do código do projeto SIS que invoca tal classe, de forma tal que sua existência não revela propósito claro, pois não é literalmente chamado por nenhum outro programa desse projeto.

Trata-se de um programa independente e separado, que só pode ser diretamente invocado através de digitação no teclado - linha de comando - por um operador do SIS que conheça sua existência, seja no TSE ou nos TREs. Ele gera um script SQL (executável por banco de dados) capaz de inserir chaves de assinatura e verificação digitais em bancos de dados indeterminados.

Consultados por volta das 15h do dia 3 de setembro, representantes do fornecedor do sistema SIS, presentes à cerimônia de apresentação no TSE, não souberam explicar nem a origem do programa nem a finalidade da classe programalInserator - cujo formato e contexto significam que só pode ser acionado pelo operador no teclado -, de potencial impacto na higidez da verificação automática de programas.

Vulnerabilidades encontradas

II – Conexão Internet

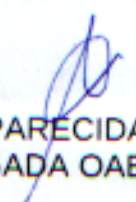
1 - Noutro ponto, a signatária solicitou que fossem demonstrados os procedimentos de geração de mídias, usando um computador conectado à Internet. A demonstração foi realizada na sala de apresentação dos programas em 02.09.2014. Foram realizados todos os atos dos procedimentos, desde a geração de mídias até o final da votação.

Constatou-se, nessa oportunidade, que o computador que gera mídias para eleições oficiais pode estar conectado à rede mundial Internet. Essa conexão não é bloqueada, nem o sistema emite qualquer aviso da conseqüente exposição a riscos, o que a torna imperceptível a potencialização agravada por acesso externo das vulnerabilidades descritas nos itens 1 e 3 acima, com possibilidade de instalação, validação e uso de programas não oficiais.

Por todo o exposto, tem a presente o objetivo de noticiar a essa Colenda Corte as vulnerabilidades encontradas, para as providencias que o caso requer.

Brasília, 05 de setembro de 2014.

Pp


MARIA APARECIDA ROCHA CORTIZ
ADVOGADA OAB.SP 147.214

Praça Joao Mendes, 42 – Conjunto 155
Centro – SP – CEP 01501-000

Comunicado institucional



Um Partido Socialista

PARTIDO DEMOCRÁTICO TRABALHISTA
PDT - DIRETÓRIO NACIONAL

CÓPIA

CÓPIA

EXCELENTÍSSIMO SENHOR PRESIDENTE DO CONSELHO FEDERAL DA ORDEM
DOS ADVOGADOS DO BRASIL



PARTIDO DEMOCRÁTICO TRABALHISTA PDT - por sua advogada e representante credenciada junto ao Colendo Tribunal Superior Eleitoral, vem respeitosamente perante Vossa Excelência noticiar fatos detectados durante a análise dos códigos fontes dos programas a serem utilizados nas eleições de 2014.

Dada a relevância do assunto, serve a presente para reiterar a essa Magna Instituição que dê implementação a criação de uma Comissão que tenha por objetivo analisar institucionalmente o processo eletrônico de votação brasileiro, sendo indicada como membro representante do requerente, a signatária da presente petição.

Nestes termos;
Pede deferimento

Brasília, 05 de setembro de 2014

PP
MARIA APARECIDA ROCHA CORTIZ
ADVOGADA OAB/SP 147.214

Sobre Prévias Irregularidades

O Caso Londrina 2012

Excertos do Processo 163.24.2012.6.160157

RESUMO

Uma versão adulterada do programa *hotswap* teve testes iniciados na 157ª Zona Eleitoral de Londrina em 27/08/2012, conforme dados do arquivo de fiscalização (log) do sistema GEDAI gerados no respectivo cartório:

27/08/2012 13:31:51 info Abertura do GEDAI-UE

27/08/2012 13:31:51 info Usuario: 091874830612 | Perfil: 0 | UF: PR

27/08/2012 13:31:51 info Verificação de Assinatura | Envelope:

M:/Aplic/Ele2012/GEDAIUE/gedai-ue.vst

27/08/2012 13:31:51 info Arquivo de URIs atualizado a partir de 'http://uri-ele.tse.jus.br:80/URLs/producao/uris-sistemas-eleitorais-pr-oficial.properties'.

27/08/2012 13:31:53 info Verificação de Assinatura | Envelope:

M:/Aplic/Ele2012/GEDAIUE/app.ini.vsc

27/08/2012 13:31:53 info Início da verificação do serviço HotSwapFlash

27/08/2012 13:31:53 info Serviço HotSwapFlash, versão 1.9.9.0, em execução

27/08/2012 13:31:53 alerta Versão incompatível do HotSwapFlash.

Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].

27/08/2012 13:32:17 info Fechamento do GEDAI-UE

28/08/2012 14:47:29 info Abertura do GEDAI-EU

Excertos do Processo 163.24.2012.6.160157

RESUMO

No dia 28/08/2012, no mesmo computador do cartório eleitoral da 157ª Zona, nova tentativa de inserção do programa adulterado – como se fosse uma versão oficial – foi tentada. Novamente sem êxito:

28/08/2012 14:47:31 info Verificação de Assinatura | Envelope:
M:/Aplic/Ele2012/GEDAIUE/uenux/avpart.vst

28/08/2012 14:47:31 info Início da verificação do serviço HotSwapFlash

28/08/2012 14:47:31 info ServiçoHotSwapFlash, versão 1.9.9.0,
em execução.

28/08/2012 14:47:31 alerta Versão incompatível do HotSwapFlash.
Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].

28/08/2012 14:47:36 info Fechamento do GEDAI-UE

28/08/2012 14:47:57 info Abertura do GEDAI-EU

Excertos do Processo 163.24.2012.6.160157

RESUMO

Já no dia 21/09/2012, o programa adulterado estava funcionalmente adaptado ao sistema oficial das eleições. Embora ainda gerando alertas sobre a adulteração, conseguiu, enfim, ser verificado como um programa oficial, ...

21/09/2012 15:15:02 info Início da verificação do serviço HotSwapFlash

21/09/2012 15:15:02 info Serviço HotSwapFlash, versão 1.9.9.0, em execução.

21/09/2012 15:15:02 alerta Versão incompatível do HotSwapFlash. Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].

21/09/2012 15:15:53 info Processo eleitoral registrado: 00001 - Eleições Municipais 2012

21/09/2012 15:15:53 info Pacote 'o00001pr-cp.jez' (versão '201208271452') importado.

Excertos do Processo 163.24.2012.6.160157

RESUMO

... e na cerimônia de Geração de Mídias para a 157ª Zona Eleitoral na Eleição Municipal de 2012 em Londrina, o programa adulterado passou pela verificação e entrou normalmente, como se fosse oficial:

24/09/2012 08:51:20 info Início da verificação do serviço HotSwapFlash

24/09/2012 08:51:20 info Serviço HotSwapFlash, versão 1.9.9.0,
em execução.

24/09/2012 08:51:20 alerta Versão incompatível do HotSwapFlash.
Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].

24/09/2012 08:54:03 info Pacote 'o00047pr76678-ca.jez'
(versão '201209211536') importado.

Concluindo

Para que serve mesmo a assinatura digital e lacração de programas?



Concluindo

Precisamos mudar de atitude na relação entre democracia e eleição?

