

01010010100110110101010011

FCSL
20 out 2006



Confiança no Sistema Informatizado de Eleições - SIE - em uso no Brasil

Prof. Pedro A. D. Rezende

Ciência da Computação – Universidade de Brasília

Colaboração: Amilcar Brunazo Filho

Forum do Voto Seguro - CIVILIS

Evolução do mal(ware)



Ano	Tipo	Conhecido por	Característica
1961	Jogo	Darwin, Code war	Controle de memória
1971	Verme	Creeper, Reaper	1o. "anti-virus" (BBS Arpanet)
1982	Verme	Elk Cloner	1a. epidemia (via disquete)
1986	Vírus	Brain	1o. vírus de PC-DOS
1988	Verme	Morris	1o. (único?) de Unix (Internet)
1991	Vírus	Tequila	1o. polimórfico (falsos -/+)
1994	Hoax	Good Times	1o. falso vírus
1995	Vírus	Concept	1o. vírus de macro (aplicativo)
1998	Troiano	Back Oriffice	Rootkit administrativo (windows)
1999	Vírus	Melissa	1o. de email, web (MS Vbasic)
2000	Vírus	IloveYou	1a. epidemia de zero dias (")
2001	Vírus	Anna Kournikova	1o. kit para virus
2002	Vírus	Klez	1o. vírus de anti-virus
2003	Hackers	Johansen, Sklyarov	Dissecar é crime? (Lei DMCA)
2004	Vírus	MyDoom	Meta-vírus (SCO, FOSS?)
2005	Troiano	Aries.sys - SONY	Rootkit via DRM (CD musical)

Malware 2006: WMF



A partir do NT 4.0, TODA versão de sistema Windows vem de fábrica com mecanismo que permite a arquivos de imagem, ao ser visualizada, executar código privilegiado:

- “Recurso” não documentado por 15 anos;
- Descoberto quando utilizado por quadrilhas;
- Abafado pelo fabricante como “falha”;
- *Backdoor* e/ou reparos desconhecidos em/para algumas versões (WinNT, WinCE)

SIE



A informatização das eleições no Brasil **NÃO** se resume na implementação de máquinas de votar eletrônicas. Inclui:

- Proconsult – *totalização RJ** (1982)
- Recadastramento eleitoral - *sem foto* (1985)
- Modelo DRE de Urna Eletrônica - *UE* (1996)
- Completa informatização (2000, 2004)

Desmaterializou-se o voto, mas a necessidade do sigilo deste **E** da auditabilidade do processo se manteve.

SIE

Eleição Informatizada

NÃO se resume em UEs

- Inicia-se na licitação de equipamentos (*hardware*), programas (*software*) e suporte;
- Deveria passar por **homologação** independente de equipamentos e sistemas;
- Deveria incluir meios independentes de **verificação** dos resultados divulgados.



SIE



Atores envolvidos, com

interesses potencialmente conflitantes:

- **Eleitores** (via de regra, que desejam lisura)
- **Candidatos a cargo** (via de regra, mais de um)
- **Administradores** do processo (Juízes eleitorais)
- **Técnicos Internos** (do TSE e TREs)
- **Auxiliares Externos** (fornecedores, técnicos terc.)
- **Mesários** (eleitores com função operativa)
- **Fiscais** (de partidos ou candidatos)

SIE



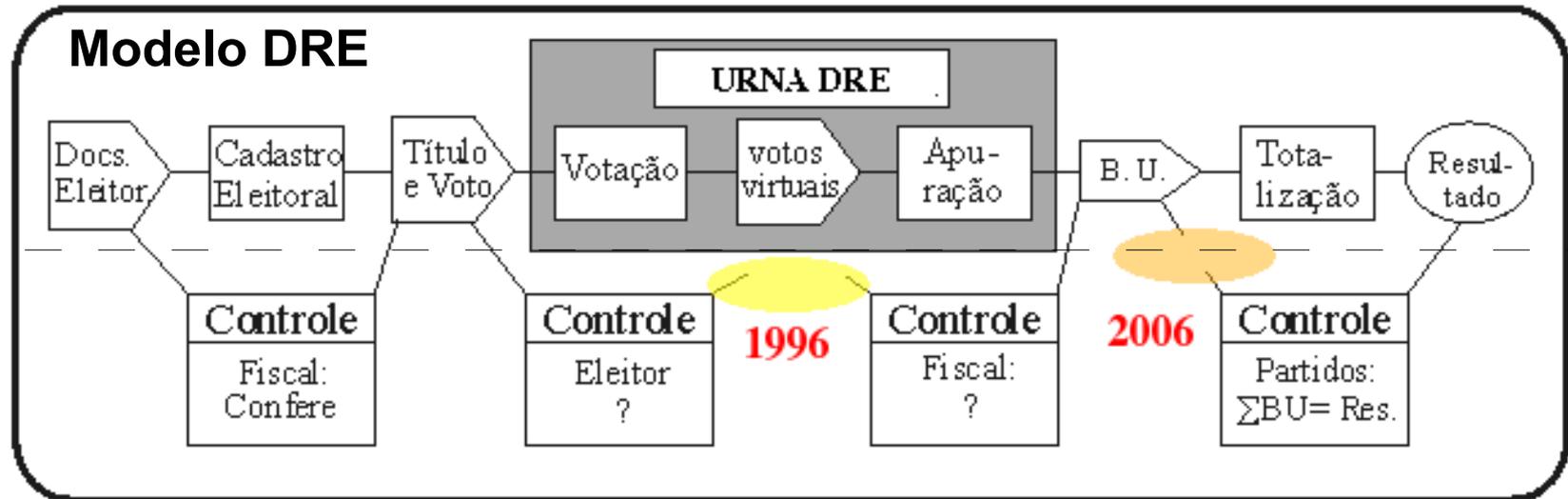
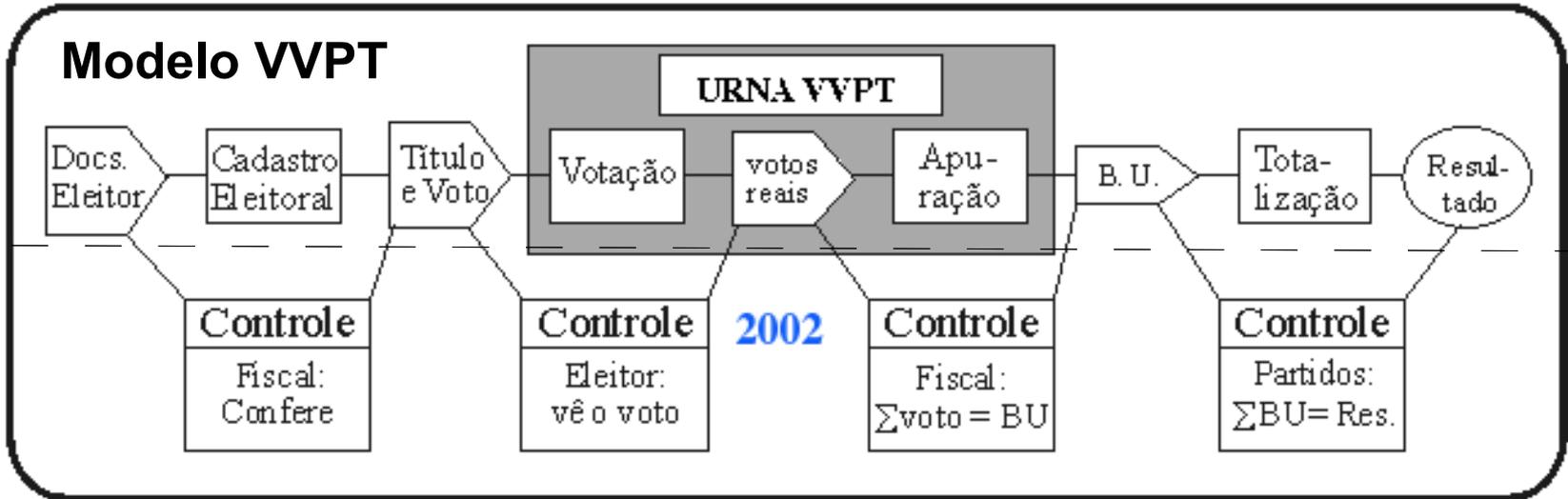
Onde interesses podem conflitar:

(pontos de ataque e defesa)

- Tribunais (Regionais e Superior)
- Zonas / Comarcas Eleitorais
- Seções Eleitorais / Locais de Votação
- Locais de Armazenamento das UE
- Estações de Transmissão Digital (sw e dados)
- Meios de Disponibilização (sw, UEs, BUs, logs, tabelas de correspondência, resultados).



Etapas do processo



“Segurança”



Conceito Técnico:

- **Segurança** = Controle da **proteção**

Proteger **NÃO** é verbo intransitivo
nem transitivo: é bi-transitivo

- Protege-se **ALGUÉM** (com algum interesse)
DE ALGO (algum risco), e **NÃO** “o sistema”
- Mais de 2 interesses em jogo introduzem riscos de **CONLUIO**: Neste caso, segurança é **equilíbrio** de riscos e responsabilidades (sigilo vs. transparência)

Segurança digital



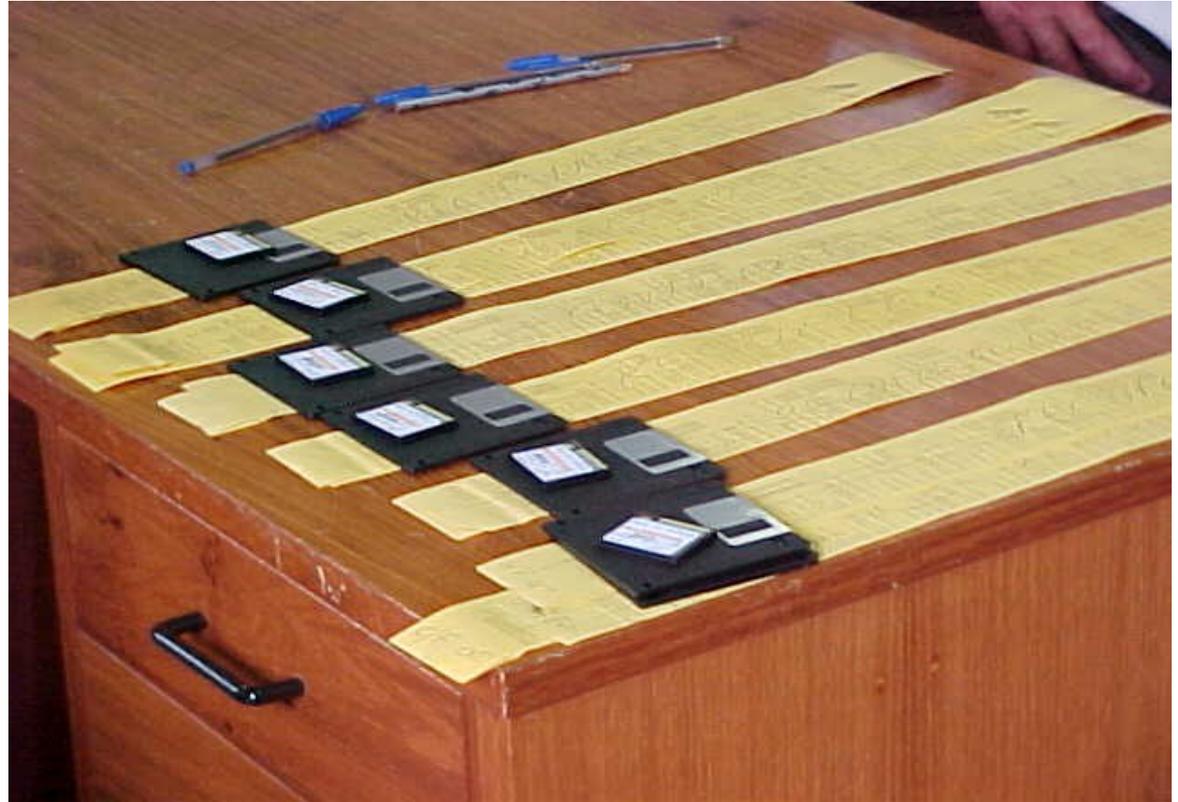
Em processo (eletrônico) com mais de dois interesses em jogo, segurança **pressupõe**:

- Mapas de risco
- Auditorias independentes
- Fiscalização externa em pontos de conflito
- *Software* (todos) em código-fonte auditável sem restrições (negociais, de compilação, de Propriedade Intelectual, etc.)
- Simulação de ataques (teste de penetração)

Vulnerabilidades ?



"Se ventila que pode haver deficiências no sistema, mas não se indica com precisão que deficiências são estas."



Presidente do TSE, citado em matéria da Agência Brasil, 1º de setembro de 2006

Ventilações precisas



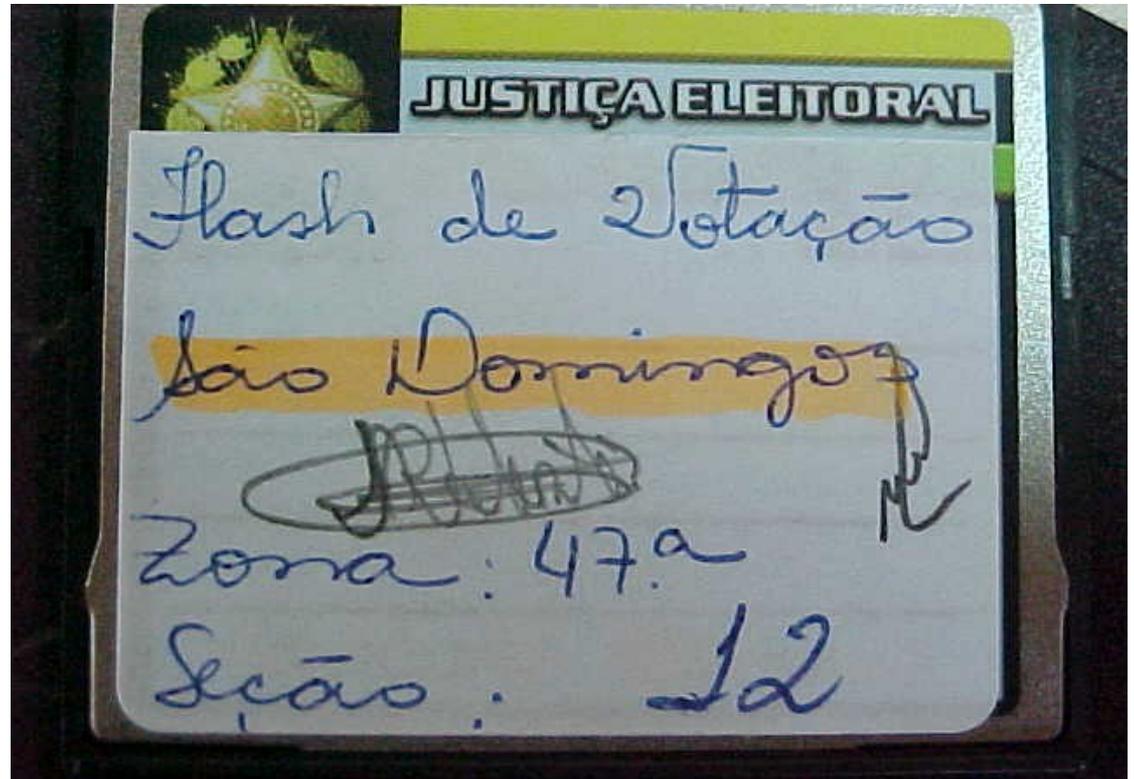
Vulnerabilidades envolvendo participação externa incluem:

- Voto de falecidos / ausentes (fraude cadastral)
- Transmissão de disquete clonado
- Clones a partir de *Flash* de Carga extraviados
- Vazamento da chave de assinatura da UE
- Código malicioso ofuscado em software externo
- Código malicioso em fotos digitais (wmf + winCE)
- Extravio de BUs impressos (totalização)

Vulnerabilidades ?



"Desde 1996 nunca houve uma impugnação eleitoral séria. O sistema está sob auditoria permanente."



Presidente do TSE, em entrevista no programa Roda Viva, TVE, 28 de agosto de 2006

Ventilações precisas



Vulnerabilidades internas incluem: (1)

Inserção de cavalos de tróia

- Para fraudes **por atacado** (num estado ou país):
 - antes da compilação dos programas das UE
 - antes da distribuição para TREs
- **Semi-atacado** (zonas): antes da carga das UE
- **De varejo** (sessões): depois da carga das UE
 - via rootkit na BIOS (plugável e programável)
 - via *flashcard* externo
 - via disquete de atualização das UE

Ventilações precisas



Vulnerabilidades internas incluem: (2)

Ataques na totalização

- Sonegação de BUs impressos na sessão eleitoral [art. 42 da Resolução TSE 22.154, maio de 2006] com troca do BU digital
 - via urna inseminada por flash de carga clonado
 - via falsificação do BU digital por chave vazada
 - via alteração do Banco de Dados da totalização
- Sonegação do relatório de votos por sessão com alteração do Banco de Dados da totalização

Ventilações precisas



Roteiro básico para cavalos de tróia na UE

- **Desarme** (imperceptível) da auto-verificação de integridade (assinatura digital, hash etc.) no arquivo de controle de inicialização [setup.bat ou equiv.]
- Instalação de rotina para **desvio** de votos pós-votação e pré-gravação do BU (baseado em porcentagens, limiares, etc.), em sw da UE
- **Auto-deleção** (da rotina de desvio e do gatilho de desarme) após a gravação do BU.

Ventilações precisas



Ex: Desarme da auto-verificação nas UE 2000

[cinza: arquivo setup.bat; azul: Cavalo de tróia]

....

```
diskfix c: /vs > nul
```

```
REM if errorlevel 1 goto
```

```
TentaRecuperar
```

```
ckpack c:\raiz.crc c:\ > nul
```

```
REM if errorlevel 1 goto ebatger
```

....

Análise publicada no Observatório da Imprensa
em 7 de setembro de 2004

Ventilações precisas



Ex: Modelo de rotina p/ desvio de um em cada 40 votos (5%) de A (ex: "13") para B (ex: "45")

[código em linguagem C, nomes de variáveis hipotéticos]

```
int fator = 40;  
int x = bu.prefeito.votos["13"] / fator;  
bu.prefeito.votos["45"] += x;  
bu.prefeito.votos["13"] -= x;
```

Análise apresentada no Seminário de Votação Eletrônica, Camara Federal, em 28 de maio de 2002

SIE



foto de divulgação
destinada a mostrar
como é a votação
oficial.

Por que se deve
confiar no que
esta foto hoje
representa??

WMF no SIE?



www.microsoft.com/technet/security/advisory/912840.mspx

MS bulletin confirms that this vulnerability applies to all the main versions of Windows (Windows ME, Windows 2000, Windows XP and Windows 2003...)

Workaround: Un-register Shimgvw.dll

“This workaround is better than just trying to filter files with a WMF extension... There are methods where files with other image extensions (such as BMP, GIF, PNG, **JPG, JPEG**, JPE, JFIF, DIB, RLE, EMF, TIF, TIFF or ICO) **could be used to exploit a vulnerable machine.**”

WMF no SIE?



TRIBUNAL SUPERIOR ELEITORAL SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

PEDIDO DE ESCLARECIMENTO Nº03

Diante do não-atendimento do Pedido nº 05, de 7.6.2006, do Pedido nº 09, de 4.7.2006, e do Pedido nº 12, de 3.8.2006, para apresentação do código-fonte dos sistemas WIN CE em tempo hábil a fim de desenvolver análise de tal complexidade, a análise foi restringida à seguinte consulta:

- 1) Que testes foram realizados nos Sistemas Windows versões CE, NT, e XP a serem utilizados durante o processo eleitoral para determinar se estão vulneráveis a falha WMF?
- 2) Que remendos (patches) da Microsoft foram implantados em cada sistema vulnerável?
- 3) Diante da não distribuição de remendos oficiais da Microsoft para versão NT, pergunta-se que outras medidas de segurança foram tomadas para assegurar que fotos fornecidas por candidatos não possam explorar a falha de segurança WMF?

WMF no SIE?

RESPOSTA

1. Quanto aos testes realizados nos Sistemas Windows versões CE, NT, e XP a serem utilizados durante o processo eleitoral para determinar se estão vulneráveis a falha WMF, é importante esclarecer que esse formato de arquivo não é utilizado por nenhum sistema eleitoral.

As fotos dos candidatos são do tipo JPG. Os candidatos não fornecem fotos em meio magnético. Todas as fotos dos candidatos são digitalizadas diretamente, sob a responsabilidade dos próprios Tribunais Regionais Eleitorais, formatadas e gravadas no formato JPG.

2. As atualizações (*patch*) da plataforma Microsoft implantadas em cada sistema foram:

Windows NT:

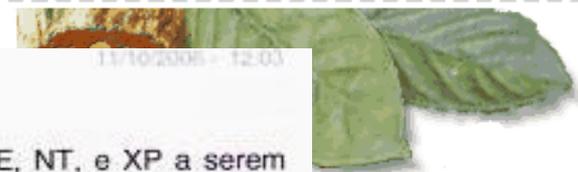
- Foi instalado o último *patch* **versão 6A**, disponibilizados pela Microsoft. É importante esclarecer que os computadores com Windows NT serão utilizados somente para transmissão de Boletins de Urna. A plataforma para uso dos sistemas, inclusive o Sistema de Candidaturas, em toda a Justiça Eleitoral é o Windows XP.

Windows CE:

- Não foi encontrada qualquer relação da vulnerabilidade relatada (arquivo em formato WMF) com o Windows CE. Ressalte-se que nas urnas eletrônicas com Windows CE, a biblioteca responsável pela exibição da foto é a **jpgue2k2.dll**, proprietária, desenvolvida em 2002 especificamente para as fotos da urna eletrônica.

3. As outras medidas de segurança tomadas para assegurar que fotos fornecidas por candidatos não possam explorar a falha de segurança WMF são:

- c) As fotos são digitalizadas e formatadas nos padrões da justiça eleitoral, pela sua própria equipe técnica.



A seita do Santo Byte



Descrita em artigo homônimo, sobre a atabalhoada votação da Lei eleitoral 10.740 (de 1/10/03):

- No sacrário eletrônico (TV, etc.), adeptos ingerem uma beberagem marqueteira *pelos ouvidos*;
- Põem-se a bailar com a mídia o mantra “*Nosso sistema é confiável, nunca ninguém provou o contrário, nós dominamos a tecnologia!*”;
- Passam a ter visões, de seres angelicais programando urnas e apurando eleições. Vêm infiéis como retrógrados, paranóicos, impatriotas.

Santo Byte, circa 1987



e-Jagube + e-Chacrona :

**Sem ele a
vida seria
um inferno.**

Propaganda da Microtec



Referências

Portal de artigos do autor:

www.cic.unb.br/docentes/pedro/sd.htm

Fórum do voto eletrônico:

www.votoseguro.org

CIVILIS

