

(In)segurança da urna eletrônica brasileira: 5 anos depois

Diego F. Aranha / UNICAMP & Aarhus Universiteit

MAIS UM EVENTO:



REALIZAÇÃO:



mindthesec[↑]
SÃO PAULO 2018





(In)segurança da *torradeira elétrica* brasileira: 5 anos depois

Diego F. Aranha / UNICAMP & Aarhus Universiteit

MAIS UM EVENTO:



REALIZAÇÃO:



mindthesecon[↑]
SÃO PAULO 2018



Contexto

Propriedades de segurança

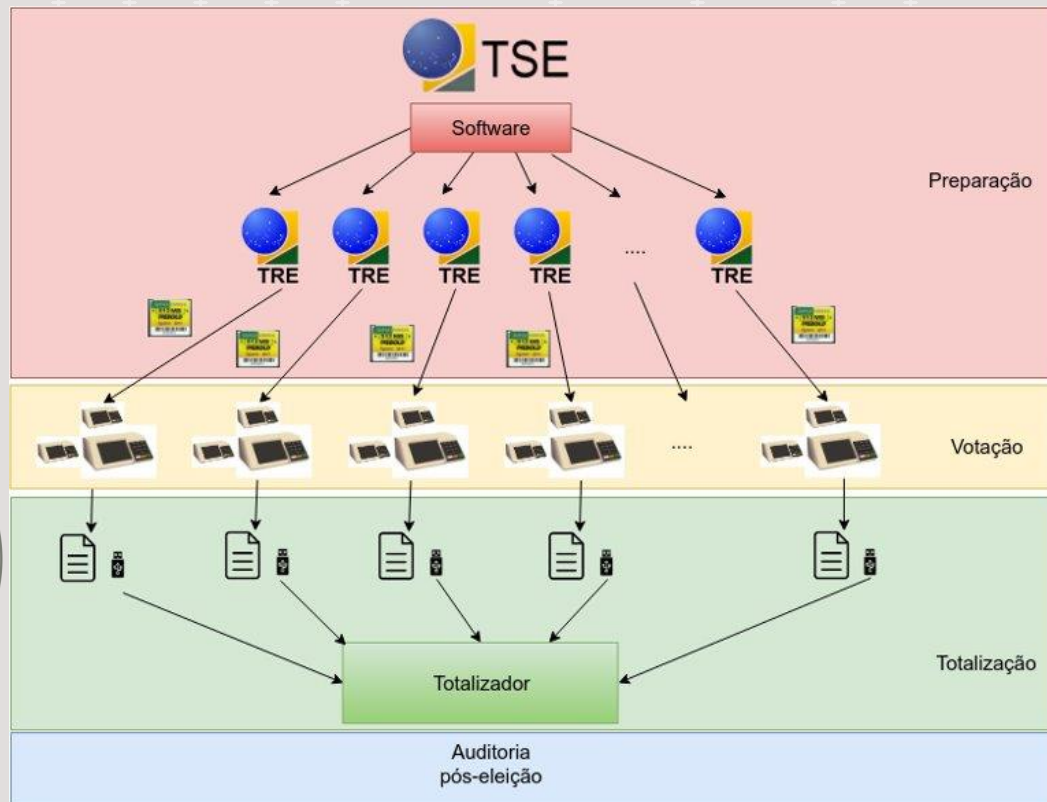
1. Autenticação dos eleitores
2. Sigilo do voto
3. Integridade dos resultados
4. Possibilidade de auditoria (especialização?)

Importante: em sistema exclusivamente eletrônico propriedades são responsabilidade da tecnologia!

Cronologia

- 1996-2000: **Implantação das urnas**
- 2002: Primeira experiência com **voto impresso**
- 2004-2008: **Migração de tecnologia**
- 2009-2017: Testes Públicos de Segurança (**TPS**)
- 2018: STF suspende voto impresso novamente
- Nunca? Implantação do voto impresso?

Organização do sistema



Recursos de transparência:

- TPS
- Inspeção de código
- Zerésima e RDV
- Votação Paralela
- Conferência de BUs
- Totalização paralela
- Pedido de auditoria

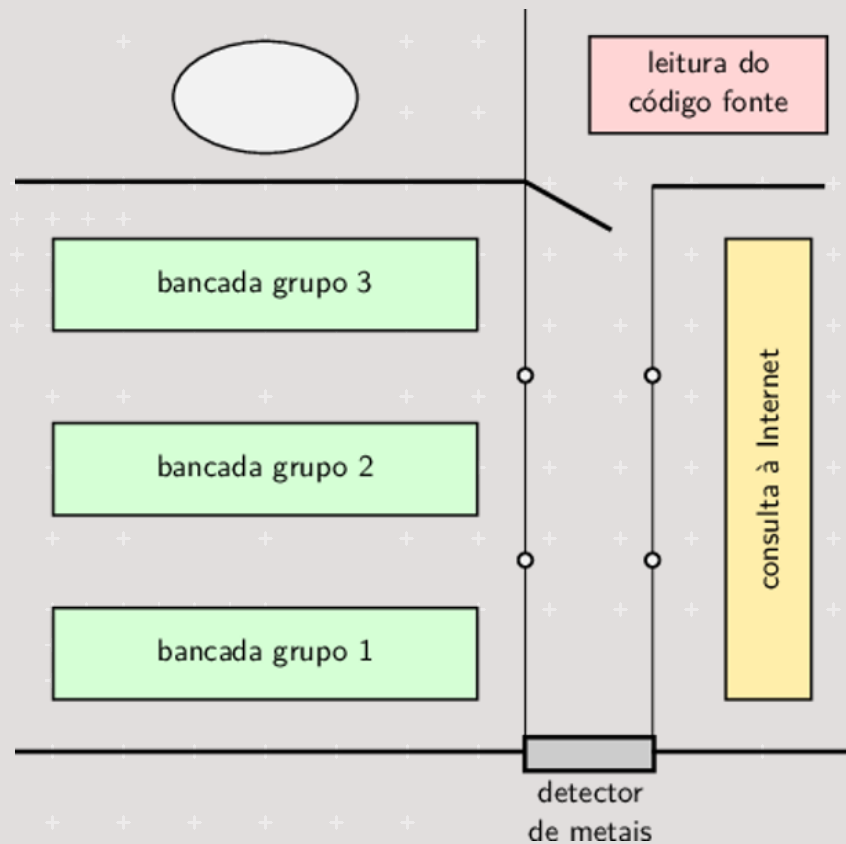
Limitações

Testes Públicos de Segurança (TPS)

mindthesec[®]
SÃO PAULO 2018

- Formato **burocrático** (8 tipos de formulário)
- **Limitações** de escopo (biometria?) e tempo
- Condições de trabalho **pouco realistas**
- Modelo adversarial **inadequado**
- **Conflito de interesse** intrínseco
- Termo de Confidencialidade (em 2016)

Testes Públicos de Segurança (TPS)



Zerésima, RDV, votação paralela

- Não previnem software **desonesto** nem permitem **recontagem**
- Simulação × Realidade (caso da **Volkswagen**)
- Tamanho e qualidade da **amostra**

Exemplo de comportamento malicioso **indetectável**:

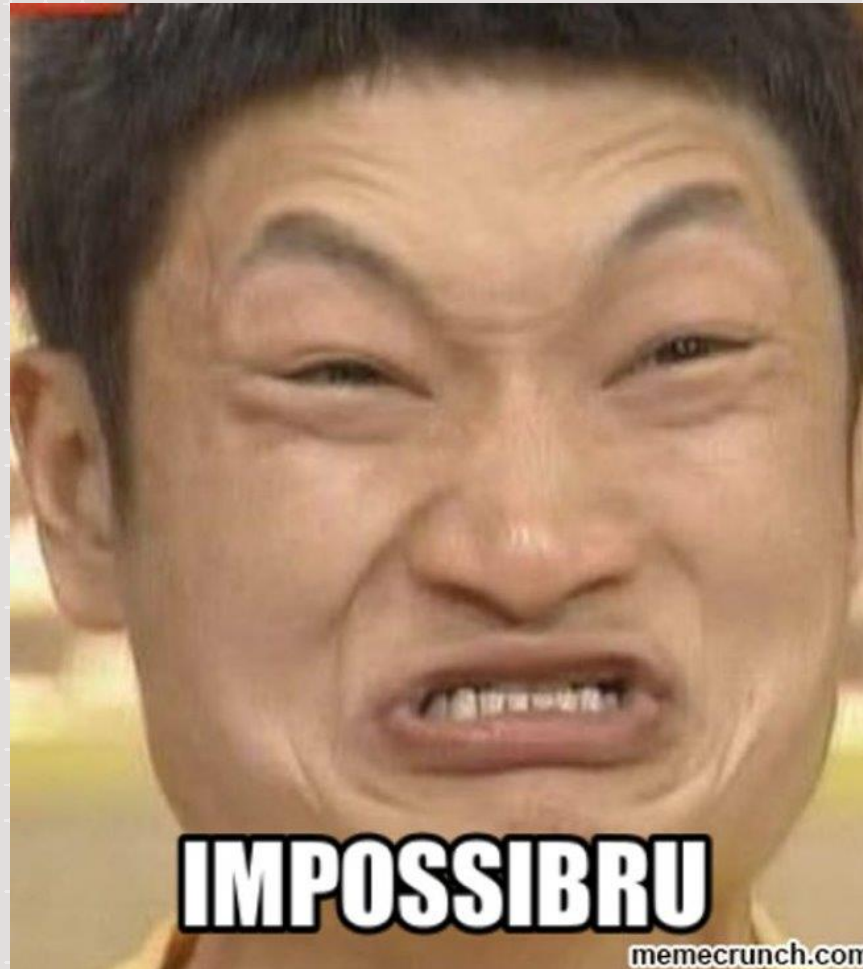
```
if (voto == 99999)
    ativar_comportamento_malicioso();
```

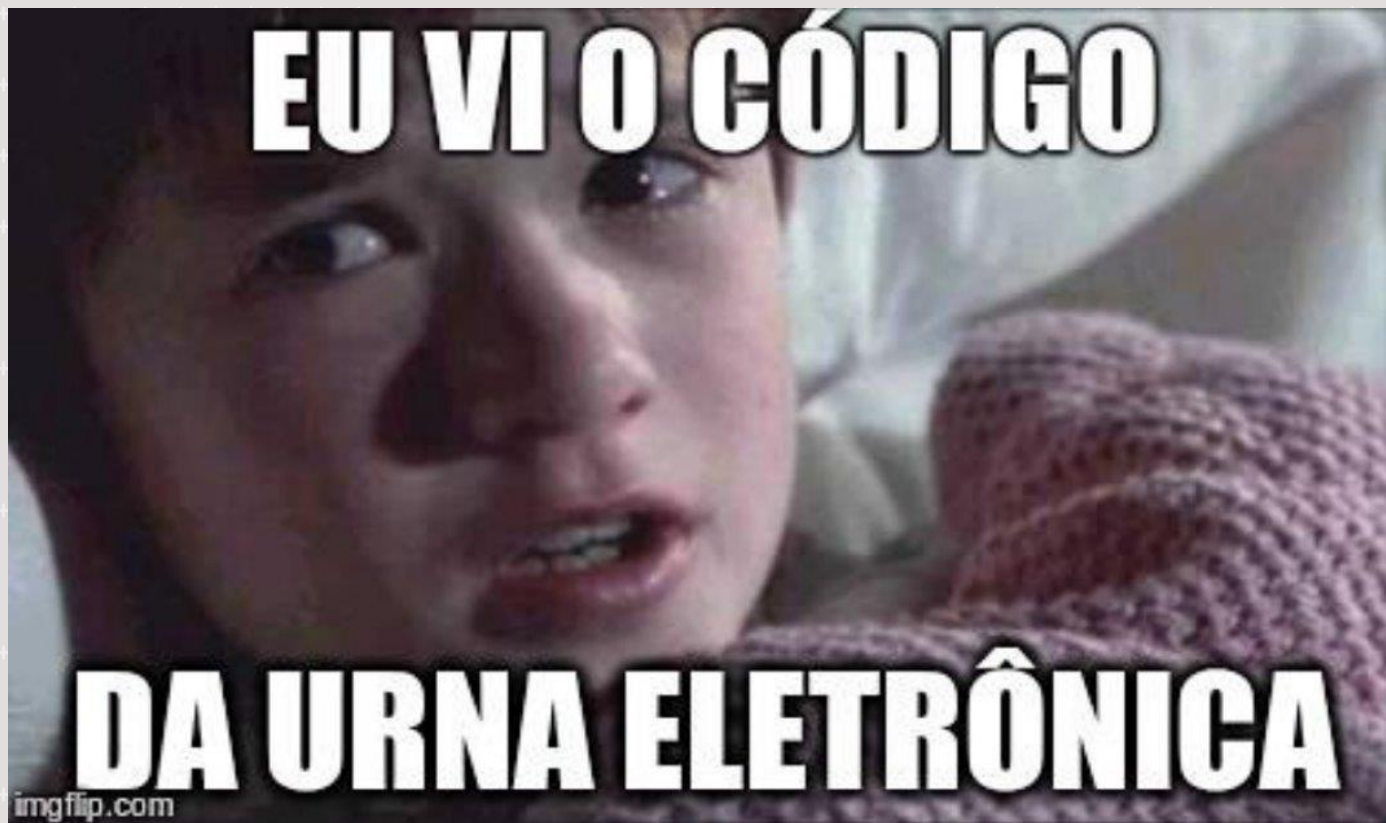
Auditoria pós-eleição

- Primeira realizada em 2014, relatório **inconclusivo** (*“não permite a plena auditoragem”*)
- **Conflito de interesse** com TSE e partido político
- Influência da situação **política**
- Imprensa e TSE divulgam que *“Auditoria conclui que não houve fraude na eleição de 2014”*

Conclusão: sistema de votação não é auditável!

Mas o software é 100% seguro!





TPS 2012 - Resultados

- Vulnerabilidade **trivial** no sigilo do voto
- Compartilhamento e armazenamento **inseguro** de segredos criptográficos
- Verificação **insuficiente** de integridade
- Processo de desenvolvimento **inseguro**
- Modelo adversarial **inadequado**
- Cultura interna **sem transparência**

TPS 2012 - Sigilo do voto

Governador Senador Presidente

71	31	37
	BRANCO	
13		
71	NULO	
		BRANCO
		37

TPS 2012 - Resultados

Semente secreta
e aleatória para
embaralhar RDV

```
rand(time(NULL))
```

Inst. Federal de Educação Ciência
e Tecnologia do Rio Grande do Sul
Campus Bento Gonçalves

Zerésima

Eleição do IFRS
(28/06/2011)

Município	88888
Bento Gonçalves	
Zona Eleitoral	0008
Seção Eleitoral	0021
Eleitores aptos	0083
Código identificação UE	01105161
Data	28/06/2011
Hora	08:32:08

RESUMO DA CORRESPONDÊNCIA
588.653

TPS 2012 - Sigilo do voto

File 1/1: lew.jpg

File name: lew.jpg

File size: 47009 Bytes

MIME type: image/jpeg

Image size: 276 x 360

Camera make: Canon

Camera model: Canon EOS-1Ds Mark III

Image timestamp: 2010:10:03 11:20:37



TPS 2016 - Integridade

Código verificador
do Boletim de Urna
para **digitação**
manual:

-----PRESIDENTE-----		
Nome do candidato	Nro cand	Votos
DILMA	13	0124
AECIO NEVES	45	0037
Total de votos Nominais		0161
Branços		0004
Nulos		0021
Total Apurado		0186
Código Verificador: 94316		
=====		
Código de identificação da carga 856.562.403.165.702.654.890.929		
Ver: 4.12.0.0 - Rio São Francisco		
ASSINATURAS:		

TPS 2017 - Equipe

Membros do ELT com habilidades **diversas**:

- **Pedro Yossis**: Assembly e criptografia
- **Thiago Cardoso**: Web e exploração
- **Caio Lüders**: Tecnologias Web
- **Paulo Matias**: Engenharia Reversa e exploração
- **Diego Aranha**: ecossistema da urna, criptografia

Importante: cada membro contribuiu com uma idéia fundamental em algum ponto.

TPS 2017 - Inspeção de código

mindthesec[®]
SÃO PAULO 2018

Edital de abertura especificava que investigadores **não teriam acesso** a chaves criptográficas.

Interpretação do TSE: apagar as chaves do código,
"para aumentar o desafio"!

Esqueceram de apagar uma chave do *kernel* ;-)

TPS 2017 - Dias 1,2,3

- Preenchimento de formulários
- Montagem do ambiente
- Decifração da mídia de instalação :-)
- Detecção de dois módulos **sem assinatura** :-)

Progresso: injeção de código para imprimir FRAUDE no terminal, o que aconteceu. :-)



TPS 2017 - Dia 5

Controle do software nos módulos para alterar aplicativo de votação em tempo real permitiu:

- Alterar versão do *software* de votação
- Alterar conteúdo da tela apresentada para eleitor
- Interferir com armazenamento de votos

Progresso: Ataque de desvio de votos estava pronto, mas não houve tempo para fazer carga. Peritos da PF encontram outro caminho para chave sem código-fonte.

TPS 2017 - Resultado principal

mindthecsec[®]
SÃO PAULO 2018

SEU VOTO PARA


Presidente

Número:


Nome:

Partido:


Aperte a tecla:
VERDE para CONFIRMAR este voto
LARANJA para REINICIAR este voto



Presidente



Vice-Presidente



**JUSTIÇA
ELEITORAL**

1

2

3

4

5

6

7

8

9

0

BRANCO

CORRIGE

CONFIRMA

TPS 2017 - Resultado principal

mindthesec[®]
SÃO PAULO 2018

VOTE 99


Presidente

Número:


Nome: Darth Vader

Partido: Dark Side

Aperte a tecla:
VERDE para CONFIRMAR este voto
LARANJA para REINICIAR este voto



Presidente



Vice-Presidente

JUSTIÇA ELEITORAL

1	2	3
4	5	6
7	8	9
0		
BRANCO	CORRIGE	CONFIRMA

TPS 2017 - Resultado principal

mindthesec[™]
SÃO PAULO 2018

Testes de confirmação apresentaram **contramedidas**:

- **Correção** da verificação de integridade
- **Automatização** das assinaturas
- Camadas adicionais de **ofuscação**
- **Derivação** de chaves dinâmica utilizando BIOS

Conclusão: procedimento de carga ficou mais **robusto**, mas sistema continua vulnerável contra **ataques internos**

TPS 2017 - Alegações oficiais

"O registro digital do voto garante o seu sigilo."

"Não é possível executar aplicativos não autorizados na urna eletrônica. Da mesma forma, também não é possível modificar nenhum aplicativo da urna."

"A urna eletrônica não é vulnerável a ataques externos."

Problemas que persistem

1. *Software* **secreto** por mais de 20 anos
2. *Software* demonstravelmente **inseguro**
3. Ausência de **recontagem**
4. Ausência de auditoria **efetiva**
5. **Conflitos de interesse** em todo lugar
6. Ataques internos completamente ignorados

O que fazer?

1. Implementação de registro físico anônimo para auditoria/recontagem
2. Publicação do *software* (desejável, mas insuficiente)
3. Aprimoramento de mecanismos de controle social

Obrigado! Perguntas?

dfaranha@eng.au.dk
@dfaranha

mindthesec[®]
SÃO PAULO 2018

[1] Software vulnerabilities in the Brazilian voting machine.

In: Design, Development, and Use of Secure Electronic Voting Systems (2014)

[2] Crowdsourced integrity verification of election results. (2016)

[3] The Return of Software Vulnerabilities in the Brazilian voting machine. (2018)

[4] Execução de código arbitrário na urna eletrônica brasileira. (2018)

MAIS UM EVENTO:

REALIZAÇÃO:

