As fragilidades das urnas eletrônicas sem o voto impresso - a visão dos peritos criminais federais e as falhas encontradas nos testes públicos de segurança do TSE

Marcos Camargo
Presidente da APCF

Introdução

Urnas Eletrônicas

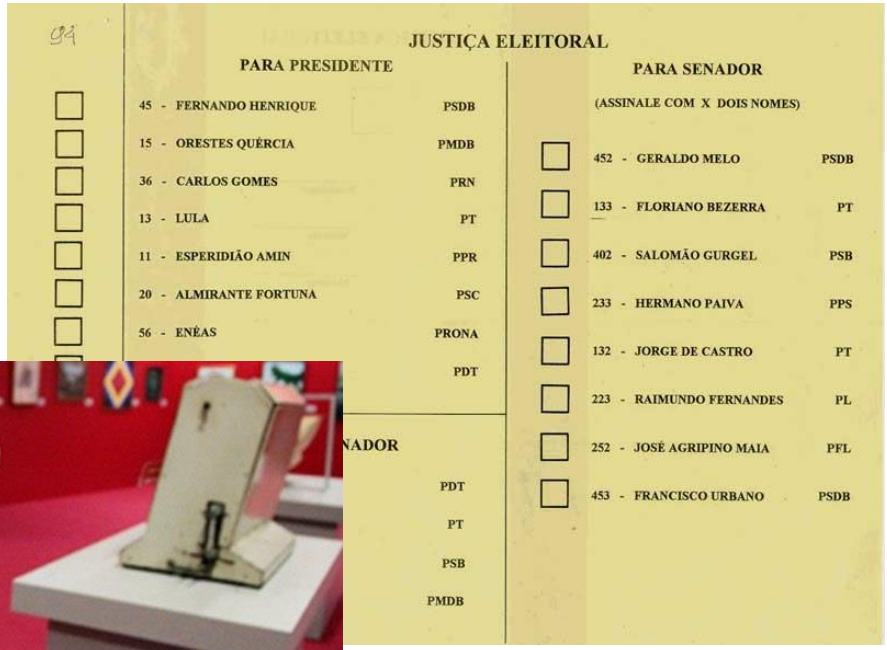
1. As urnas eletrônicas são seguras?

2. Por que as urnas eletrônicas têm tanta desconfiança por parte da população?

3. O voto impresso pode ajudar a melhorar essa questão?

Histórico

Como era antes...



JUSTIÇA ELEITORAL

PARA PRESIDENTE

45	FERNANDO HENRIQUE	PSDB
15	ORESTES QUÉRCIA	PMDB
36	CARLOS GOMES	PRN
13	LULA	PT
11	ESPERIDIÃO AMIN	PPR
20	ALMIRANTE FORTUNA	PSC
56	ENÉAS	PRONA
		PDT

NADOR

PDT
PT
PSB
PMDB

PARA SENADOR

(ASSINALE COM X DOIS NOMES)

452	GERALDO MELO	PSDB
133	FLORIANO BEZERRA	PT
402	SALOMÃO GURGEL	PSB
233	HERMANO PAIVA	PPS
132	JORGE DE CASTRO	PT
223	RAIMUNDO FERNANDES	PL
252	JOSÉ AGRIPINO MAIA	PFL
453	FRANCISCO URBANO	PSDB

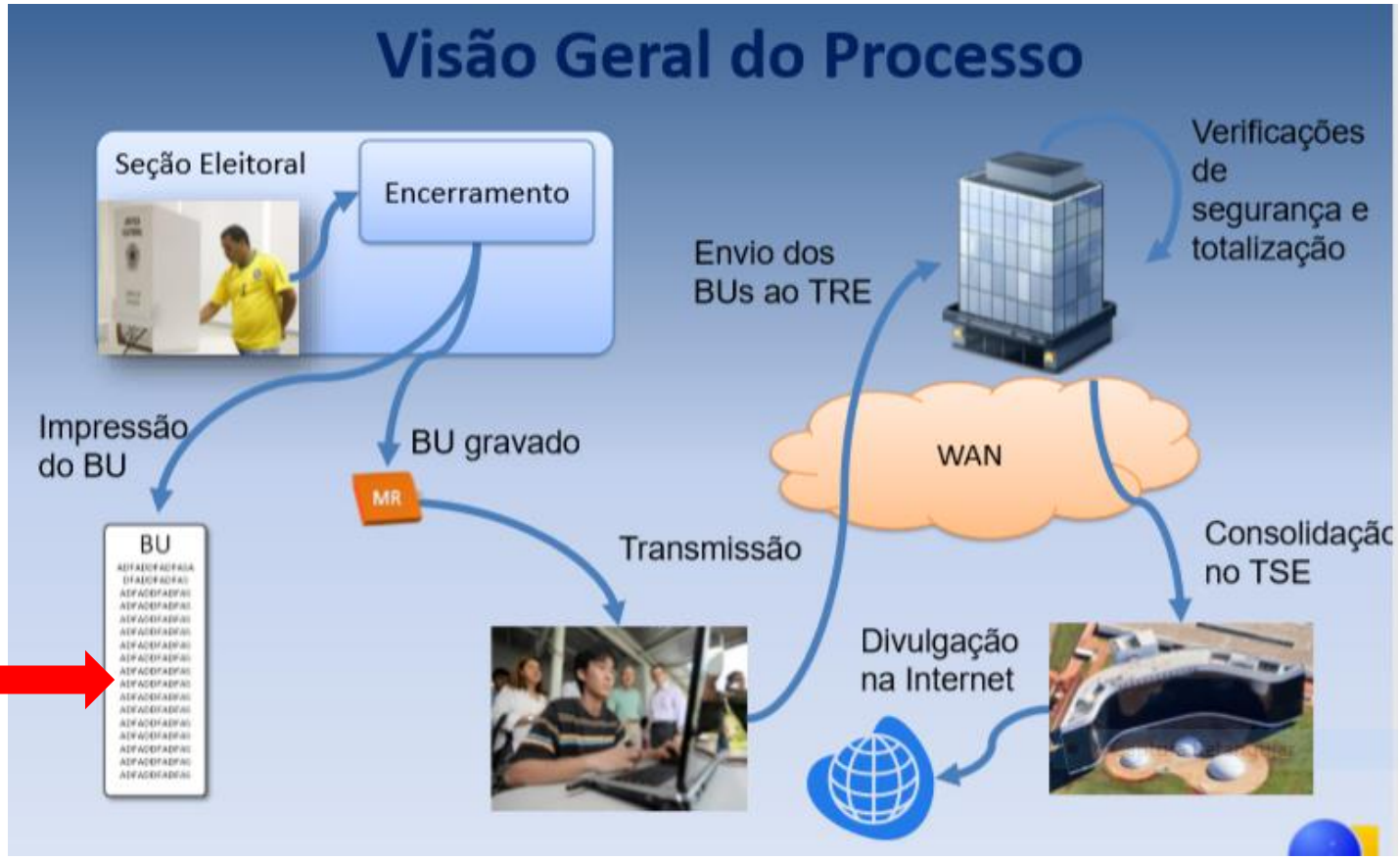
Histórico

Como era antes...

- Voto em papel
  - Contagem e totalização lentos e sujeitos a erro
  - Fraudes
    - Inserção de votos antes do fechamento
    - “Sumiço” de urnas
    - Fraude documental
  - Fraude sistêmica difícil
  - Eleitor tem “confiança” no processo
    - Compreensão do funcionamento

Urnas eletrônicas

Processo de votação



Urnas eletrônicas

Características

- Voto eletrônico
  - Contagem rápida e precisa (depende do software)
  - Fraudes
    - Inserção de votos antes do fechamento (log)
    - “Sumiço” de urnas
    - Fraude documental
  - **Fraude sistêmica facilitada**
    - Software adulterado compromete todas as urnas
    - Consenso científico - todo sistema eletrônico / computacional possui vulnerabilidades.
  - **Eleitor não tem confiança no processo**
    - Requer conhecimentos técnicos e acesso

Urnas eletrônicas

Segurança da Urna

- Ações do TSE
  - Análise dos códigos fonte 180 dias antes da eleição
  - Cerimônia de lacração e assinatura dos códigos
  - Cadeia de confiança e criptografia na urna
  - Elemento físico para verificação de integridade (MSD)
  - Zerésima
  - Votação paralela nos TRE's
  - Boletim de Urna impresso
  - RDV – Registro Digital do Voto
  - **Testes públicos de segurança**

Urnas eletrônicas

Testes públicos

- Criados em 2009 para que especialistas analisem a urna
  - Requer plano de ataque prévio autorizado pelo TSE
  - Prazo reduzido (4 dias em 2017)
  - Uso de novas ferramentas durante o teste necessita autorização
  - Computadores sem acesso à Internet

- Quatro edições:
  - 2009, 2012, 2016, 2017

Urnas eletrônicas

Testes públicos

- Teste público 2009
  - Vencedor (Sergio Freitas da Silva) usou um receptor de rádio para captar emanações eletromagnéticas do teclado
    - TSE passou a blindar o teclado e suas conexões

- Teste público 2012
  - Vencedor (Equipe Diego Aranha) conseguiu recuperar a ordem dos votos no RDV
    - TSE corrigiu a rotina de embaralhamento dos votos no RDV

Urnas eletrônicas

Testes públicos

- Teste público 2016
  - Vencedor (Sergio Freitas da Silva) descobriu o calculo do código verificador do boletim de urna e gerou um boletim falso.
    - TSE mudou a forma de calculo e aumentou o tamanho do campo verificador

- Teste público 2017
  - Equipe Diego Aranha encontrou a chave de criptografia do sistema de arquivos
  - Equipe Diego Aranha encontrou bibliotecas não assinadas e fez alterações não autorizadas no *software* da urna
    - TSE alterou o procedimento para assinar todas as bibliotecas e retirar de forma automática as chaves de criptografia do código

Urnas eletrônicas

Testes públicos

- Teste público 2017
  - Equipe PF contornou a proteção de inicialização do cartão em computadores PC, por meio da cópia de um setor de inicialização padrão no cartão. *(possibilidade teórica de construção de programa que altere a votação da urna e modifique o BU).*
  - Equipe PF conseguiu inicializar o cartão de carga num PC virtual e encontrou a chave de criptografia do sistema de arquivos por meio de extração da memória volátil (RAM)
    - TSE incluiu proteções para alterar o setor de inicialização e passou a derivar a chave de criptografia de parâmetros presente em componente físico da urna (BIOS).

Urnas eletrônicas

Outros riscos

- Possibilidades de falhas / vulnerabilidades
  - Vazamento de chaves da cadeia de confiança
    - Assinatura de código malicioso ou produtos da urna
  - Inserção de código malicioso durante o desenvolvimento
    - Invasão da rede do TSE
    - Desenvolvedor malicioso
  - Vazamento de chaves de manutenção (MSD)
    - Inserção de certificado malicioso

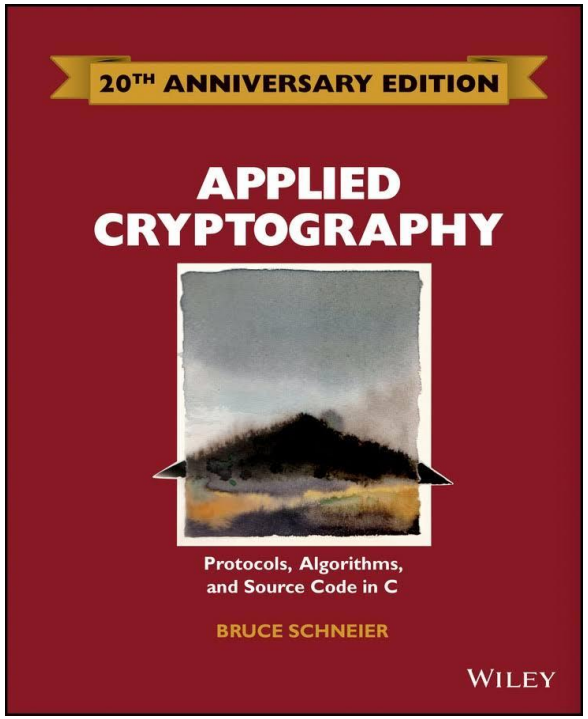
Referencial bibliográfico

- Princípio da independência do software
  - http://people.csail.mit.edu/rivest/pubs/RW06.pdf
  - cunhado em 2006, pelo Ph.D. do MIT Ronald Rivest e pelo pesquisador do NIST Jonh Wack
  - *Um **sistema eleitoral é independente do software** se uma modificação ou erro não-detectado no seu software não pode causar uma modificação ou erro indetectável no resultado da apuração*.
  - Adotado em 2007 pelo *Voluntary Voting System Guidelines,* proposta de norma técnica do NIST

Urnas eletrônicas

Referencial bibliográfico

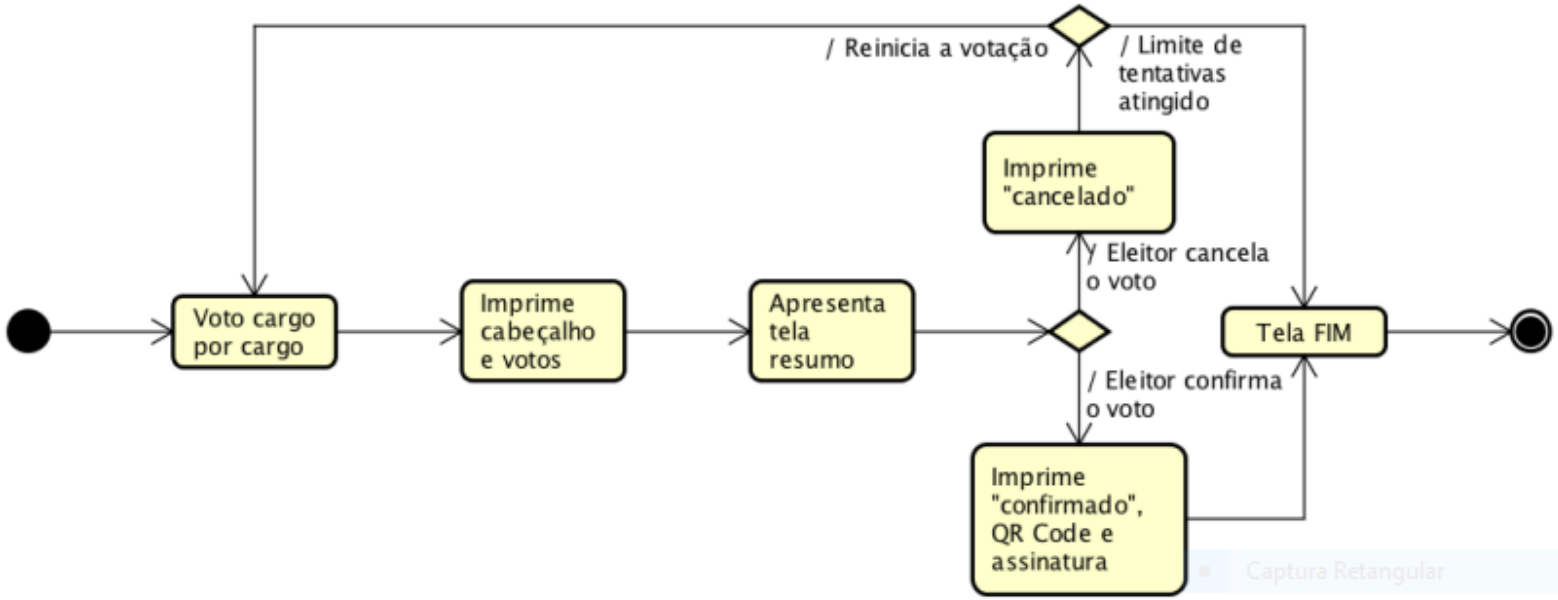
- **The Problem with Electronic Voting Machines** (Bruce Schneier)
  - https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html
    1. DRE machines **must** have a voter-verifiable paper audit trails
    2. Software used on DRE machines must be open to public scrutiny.



Urnas eletrônicas

Voto impresso

- Como funciona (artigo TSE SBSEG 2017)



Urnas eletrônicas

Voto impresso

- Como funciona (artigo TSE SBSEG 2017)

Conclusões

- Urna eletrônica: projeto de *hardware* e *software* nacional de sucesso
  - Ser crítico e propor melhorias
  - Não desmerecer o projeto
- Voto impresso é importante para ter uma trilha de auditoria não eletrônica
  - Recomendado pela academia e NIST
  - Não existe solução computacional 100% segura
  - Eleitor não leva comprovante para casa (sigilo do voto)
- Testes públicos são importantes para melhorar o projeto
  - Participação dos PCF's

Conclusões

- A adoção do registro impresso de voto - de forma secreta e protegida, não tem o condão de substituir a urna eletrônica ou de desqualificá-la, mas sim de complementá-la, a fim de que o processo eleitoral seja cada vez mais íntegro e seguro, evitando diversos tipos de suspeitas, ainda que infundadas.

- Uso de ferramentas estatísticas para auditorias específicas e com alto grau de confiança.

- Aumento da segurança do processo eleitoral e de confiança dos eleitores (auditoria inicial realizada pelo próprio eleitor - sem qualquer contato manual).

- Valor intangível e sem comparação e nenhuma outra atividade cotidiana que envolva processos eletrônicos.

Contato

Obrigado

apcf@apcf.org.br