Votação Eletrônica: Desafios no Brasil e no mundo

(ou: porque falar de insegurança da urna brasileira é "pura paranoia")

Prof. Dr. Marcos A. Simplicio Jr.

Escola Politécnica da USP

Depto. Engenharia de Computação e Sistemas Digitais

(mjunior@larc.usp.br)

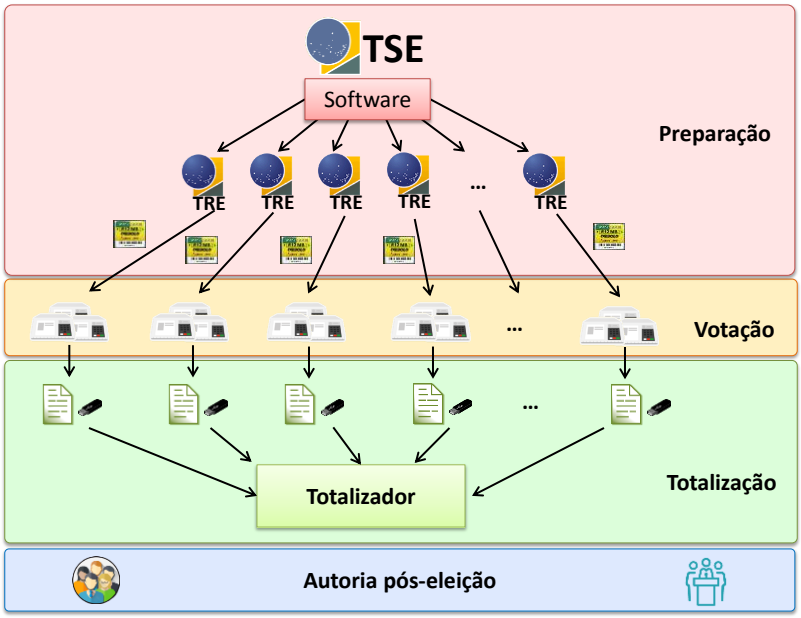
(Apresentação em parte baseada em slides do Prof. Dr. Diego Aranha)

Votação: Requisitos de segurança

- Qualquer que seja a tecnologia usada, requer-se:
  1. **Autenticação dos eleitores**: apenas eleitores autorizados podem votar, apenas uma vez
  2. **Sigilo do voto**: voto deve ser secreto
  3. **Integridade dos resultados**: resultado é justo
  4. **Possibilidade de auditoria**: idealmente, por qualquer cidadão
- **Importante**: em um sistema puramente eletrônico de votação, todas as propriedades são responsabilidade da tecnologia.

2

Visão geral



3

PREPARAÇÃO

4

Preparação

1. Confecção do *software* de votação e assinatura no TSE
2. Transmissão do *software* de votação para TREs
3. Gravação do *software* em cartões de memória *flash* e instalação nas urnas (carga)

O lado bom: verificação

- Exame do software por fiscais de partido, OAB, MPU, SBC
- Assinatura do software: verificação pela urna e versão lacrada para posterior conferência
- Testes Públicos de Segurança

5

Preparação

O lado ruim: erros propositais?

- Processo como um todo requer **confiança em diversas partes internas**
  - **TSE como instituição**: código examinado é o de fato carregado na urna?
  - **Desenvolvedores do software** (TSE, SEPIN): portas dos fundos?
  - **Hardware/firmware** (Diebold): "chave extra de verificação"? Ignorar algum processo de segurança?
  - **Compilador/SO** (gcc, Linux modificado por TSE): não insere nem ignora partes do código?

6

Preparação


O lado ruim: erros acidentais?

- Testes públicos
  - **Limitados**: ~5 dias para avaliar >10^6 linhas de código
  - E ainda assim revelam **falhas graves**:


OMG

    - (2012) Geração de aleatoriedade revela desconhecimento de **princípios extremamente básicos** de segurança
    - (2017) **Execução de código arbitrário** na urna
  - **Documentação do código** não é animadora:

    - O que dizer ao encontrar "Uhuuuuuuuuu!!!!" ou "Isso causa erro no processo X. Corrigir e testar" nos comentários de um software de missão crítica **em produção**...?
  - Conclusão: **processo de desenvolvimento falho...**

Preparação: isso tudo é paranoia...

- **Não há atacantes internos** em ambientes seguros
  - Edward Snowden? Bradley Manning[1]? Tudo fake news...

- **Ataques internos são raros** em sistemas reais
  - Apenas 60% dos ataques no mundo em 2016[2]... Irrelevante!

- A Diebold, que fabrica o **hardware**, é "obrigada a seguir o **projeto brasileiro**" [3]
  - Por que? Porque o TSE manda ser assim[3]

- "**Jamais conseguiram desviar votos na urna**" (2017) [4]

  - Não, "código *arbitrário*" não significa "código *arbitrário*"
- Erros são **rapidamente corrigidos**
  - Falha explorada em 2017 foi apontada em 2012 (e antes...)[4]

- **Erros não são tão básicos** assim...
  - Por exemplo...

1. https://www.linux.com/news/top-five-insider-attacks-decade (Wikileaks – DoD)
2. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company
3. http://www.tse.jus.br/imprensa/noticias-tse/2017/Agosto/nota-em-resposta-a-materia-divulgada-pela-folha-de-s-paulo-nesta-segunda-7
4. https://noticias.r7.com/tecnologia-e-ciencia/testes-mostram-falhas-mas-tse-diz-que-urna-eletronica-e-confiavel-13052018

Preparação: Falha de 2012

- **Sigilo do voto**: protegido por número "**secreto e aleatório**"… até ser publicado na documentação oficial gerada pela urna

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

Preparação: Falha de 2017

- **Integridade do software**: chaves criptográficas no código… nenhum problema com isso conforme certa cartilha…

Page Discussion Read View source View history Search

HOW TO WRITE INSECURE CODE

Introduction

In the interest of ensuring that there will be a future for hackers, criminals, and others who want to destroy the digital future, this paper captures tips from the masters on how to create insecure code. With a little creative use of these tips, you can also ensure your own financial future. Be careful, you don't want to make your code look hopelessly insecure, or your insecurity may be uncovered and fixed.

The idea for this article comes from Roedy Green's How to write unmaintainable code. You may find the one page version more readable. Actually, making your code unmaintainable is a great first step towards making it insecure and there are some great ideas in this article, particularly the section on camouflage. Also many thanks to Steven Christey from MITRE who contributed a bunch of particularly insecure items.

*Special note for the slow to pick up on irony set. This essay is a **joke**! Developers and architects are often bored with lectures about how to write **secure** code. Perhaps this is another way to get the point across.*

Always use default deny

Apply the principle of "Default Deny" when building your application. Deny that your code can ever be broken, deny vulnerabilities until there's a proven exploit, deny to your customers that there was ever anything wrong, and above all - deny responsibility for flaws. Blame the dirty cache buffers.

Trust insiders

Malicious input only comes from the Internet, and you can trust that all the data in your databases is perfectly validated, encoded, and sanitized for your purposes.

Hard-code your keys

Hard-coding is the best way to retain control. This way those pesky operations folks won't be able to monkey with (they say "rotate") the keys, and they'll be locked into the source code where only smart people can understand them. This will also make it easier to move from environment to environment as the hard-coded key will be the same everywhere. This in turn means your code is secure everywhere.

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
Presentations
Press

Fonte: https://www.owasp.org/index.php/How_to_write_insecure_code

VOTAÇÃO

11

Votação

1. Impressão da zerésima
2. Sessão de votação (autenticação, interação com urna)
3. Impressão e gravação dos resultados. Ex.:
   - Totais: Boletim de Urna (BU)
   - Votos embaralhados: Registro Digital do Voto (RDV)

O lado bom:

- Zerésima: “nenhum voto registrado”
- RDV: permite conferência do BU (?)
- Assinatura digital dos resultados
- Votação paralela: amostra de urnas é testada “ao vivo”
- Autenticação dos votantes (docs e biometria)

12

Votação

O lado ruim: se software é desonesto...

- Zerésima, RDV, assinatura: inúteis (dados forjados)
- Votação paralela: inútil se porta dos fundos esperta

Exemplos: limitações da votação paralela

```
If (voto == 99999) { //voto "ativador"
    ativar_comportamento_malicioso();
}

If (biometria == true AND liberacao_por_mesario < 50%){
    //não estou sob teste![1]
    ativar_comportamento_malicioso();
}
```

Importante: Assumir versão ofuscada escondida na base de código!

1. http://siaiap34.univali.br/sbseg2015/anais/WTE/artigoWTE01.pdf

13

Votação

O lado ruim: (in)utilidade da biometria

- Biometria: para impedir que A vote por B
  - Ex.: identidade falsa ou de pessoa semelhante[1]
- Medidas de segurança:
  - **Fiscais**: risco de serem enganados
  - **Biometria é solução**: falha na leitura impede voto...
    - Só que não: fiscal libera em caso de falha repetida[2]...
    - Análise simples:
      - **Custo**[3]: R$6.90/eleitor * 147 mi eleitores ≅ R$1 bi
      - **Benefício**: zero na eleição (talvez útil em outros cenários não muito nobres[4]... Felizmente proibidos[5]...)

1. https://veja.abril.com.br/politica/morto-irmao-de-pizzolato-votou-em-2008/
2. http://g1.globo.com/politica/eleicoes/2014/noticia/2014/07/video-do-g1-explica-como-e-o-voto-por-identificacao-biometrica.html
3. https://oglobo.globo.com/brasil/eleitores-de-765-cidades-votarao-nas-eleicoes-de-outubro-em-urna-biometrica-12382789
4. https://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255
5. http://www.tse.jus.br/imprensa/noticias-tse/2013/Agosto/corregedoria-geral-eleitoral-suspende-acordo-entre-tse-e-serasa

14

Votação: isso tudo é paranoia…

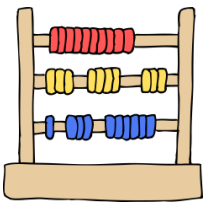
- Na prática, **não existe** software que muda seu comportamento quando está sob testes
  - Caso da Volkswagen[1]? Fake news…
- Testes na votação paralela **simulam eleição perfeitamente**

  - Impressão dos logs em 2014 em todo o estado de MG[2]? É normal fazer um procedimento no teste completamente diferente do normal na eleição…
- Biometria é uma **tecnologia da moda**!

  - Nossa urna é "cool". Isso é o que importa…

1. https://exame.abril.com.br/negocios/volkswagen-e-multada-por-fraude-em-testes-de-emissao-de-poluentes/
2. http://siaiap34.univali.br/sbseg2015/anais/WTE/artigoWTE01.pdf

15



TOTALIZAÇÃO

16

Totalização

1. Transmissão dos resultados parciais
2. Combinação dos resultados parciais
3. Divulgação do resultado final
4. Publicação dos BUs eletrônicos

O lado bom:

- Verificação de assinaturas da urna
- Conferência entre BUs físico e eletrônico
- Totalização por terceiros (QR Code)

17

Totalização

O lado ruim:

- **Logística e custos** para verificação por terceiros
  - Ex.: Você Fiscal , Auditoria de 2014

- **Importante**: provavelmente a **fase mais transparente** do processo eleitoral eletrônico

18

Totalização: isso tudo é paran…

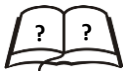
- ... Ops.... Não! Nesse caso, só li verdades...

19

AUDITORIA PÓS-ELEIÇÃO

20

Auditoria Pós-Eleição



- ... não é previsto...

O lado ruim: não é previsto...

- Tentativa feita em 2014 (PSDB)[1] ...
- ... Mas **"auditoria"** permitida por TSE exige usar o **software da própria urna** para verificar integridade
  - **Não** se pode analisar o código interno à urna
  - Similar a: "pergunte ao suspeito se ele é honesto e confie na resposta que ele der"

1. http://siaiap34.univali.br/sbseg2015/anais/WTE/artigoWTE01.pdf

21

Auditoria Pós-Eleição

- **"Auditoria"** permitida pelo TSE: uma [analogia]
  - Você precisa **comprar um carro** [urna] do TSE
  - Você quer avaliar o **estado do veículo** [fraude?]
    - Mas não pode **sequer abrir o capô** para isso [verificar programa e dados na memória das urnas]
  - Seus mecânicos conseguem identificar o estado do carro apenas pelo **ronco do motor** [auditores com experiência]
    - Mas só lhe é fornecida uma **gravação do ronco**, feita pelo próprio vendedor [**um** código fonte é fornecido]
  - Você pede o **manual** do carro [documentos com requisitos de segurança]
    - Mas não tem acesso a ele por "razões de segurança"

Auditoria Pós-Eleição: Paranoia…

- Algumas conclusões do relatório de 2014[1]:
  - A **<u>urna é inauditável</u>**
  - Votação paralela não replica votação normal
    - Ex.: biometria invalida premissas da votação paralela
  - Biometria operando fora dos parâmetros normais
    - Falsos positivos e negativos chega a 10x do especificado
- O que o TSE entendeu:
  - **"Não foram detectadas fraudes na urna"**
  - Analogia (parece episódio de "The Simpsons"[2]):
    - Médico (Auditores): sem testes adicionais, não consigo avaliar sua saúde
    - Paciente (TSE): nenhum problema encontrado? Então estou em ótima condições de saúde!!!

1. http://siaiap34.univali.br/sbseg2015/anais/WTE/artigoWTE01.pdf
2. https://www.youtube.com/watch?v=aI0euMFAWF8

23

CONCLUSÕES

24

O que fazer? (v1)

1. Voto impresso
Implementar registro físico e anônimo do voto, conferível pelo eleitor, para auditoria/recontagem.

2. Código aberto
Publicar código-fonte do software *é desejável para ampliar a capacidade de auditoria, mas insuficiente.*

3. Controle social
Ampliar mecanismos de transparência para que sociedade possa exercer maior controle social sobre o sistema, financiado por recursos públicos.

25

O que fazer (v2): nada... paranoia!

- Como mostra a campanha do TSE, a urna:
  - Tem mais de 30 camadas de segurança

"Insira seu voto aqui para 50 camadas de segurança (?)"

  - Não está ligada à Internet

"O que impede totalmente as fraudes! Pergunte ao jamais fraudado (?) bilhete único..."[1]

  - Garante o sigilo das suas escolhas como eleitor

"Garantia = confiança cega no TSE... Afinal, em caso de disputa o TSE pode simplesmente se julgar inocente..."[2,3]

1. https://sao-paulo.estadao.com.br/noticias/geral,fraude-no-bilhete-unico-aumenta-820-com-esquema-tipico-do-crime-organizado,70001725502
2. https://www1.folha.uol.com.br/fsp/brasil/fc2301200713.htm
3. https://tse.jusbrasil.com.br/noticias/2146730/tse-rejeita-recurso-de-joao-lyra-contra-governador-de-alagoas

26

Sobre voto impresso: Tostines?

- Grande discussão entre 2014-2017.
  - Congresso aprovou em 2015[1]; STF derrubou em 2018[2]
- Razões:
  - **Técnica** (risco a sigilo): falha na impressora pode revelar voto a técnico/mesário que acessar urna

    - Possível solução (usada no mundo): voto **feito** em papel, posteriormente **escaneado pela urna**
  - **Filosófica**: raciocínio circular no STF...

    - "Não há provas de fraude na urna eletrônica"[2], "porque não é possível auditar" [3]
    - Logo: "não se criam mecanismos de auditoria porque não há provas de fraude" [2]

1. https://www12.senado.leg.br/noticias/materias/2015/12/28/eleicoes-terao-voto-impresso-a-partir-de-2018
2. https://noticias.uol.com.br/politica/eleicoes/2018/noticias/2018/06/06/stf-voto-impresso.htm
3. http://siaiap34.univali.br/sbseg2015/anais/WTE/artigoWTE01.pdf

27

Perguntas?

EUA

México

India

Argentina:
(sim, estamos atrás...)

Auditoria em papel no mundo...

28

Leitura recomendada

- Livro “O mito da urna”
  - www.o-mito-da-urna.org

29

Auditoria Pós-Eleição

- **“Auditoria”** permitida pelo TSE: outra analogia
  - Suponha que o sistema de detecção de fraudes da urna seja tão avançado que pareça mágica:
    - Existe uma **fita branca** interna à urna
    - Quando há fraude, essa fita fica **preta**.

  - **Forma óbvia de auditoria**:
    - Abra a urna e veja a cor da fita.
    - Como fraudar: ???
  - **Forma permitida pelo TSE**:

    - Aperte um botão na urna, que irá imprimir um papel com a cor da fita em seu interior
    - Como fraudar: programe o botão para sempre imprimir “branco”...