Hackeando a urna eletrônica brasileira com o Python

Caipyra 2018

Diego Aranha (Unicamp), Pedro Barbosa (UFCG),
Thiago Cardoso (Hekima), Caio Lüders (UFPE),
Paulo Matias (UFSCar)

09 de Junho, 2018

Propriedades de segurança

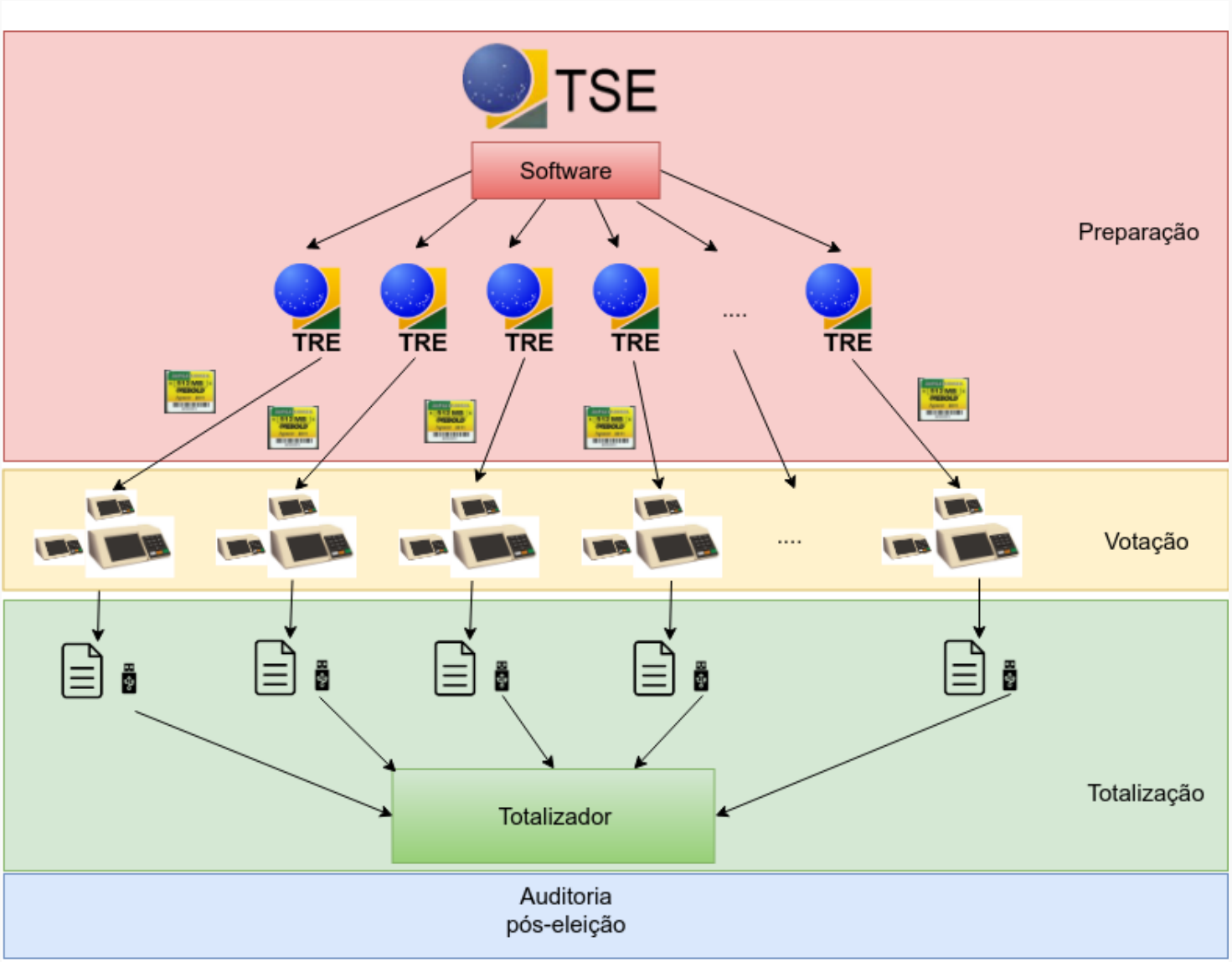
Não importando a tecnologia empregada, um sistema de votação precisa satisfazer algumas propriedades:

1. *Autenticação dos eleitores*: apenas eleitores autorizados podem votar
2. *Sigilo do voto*: voto deve ser secreto
3. *Integridade dos resultados*: resultado é justo
4. *Possibilidade de auditoria*: idealmente, sem especialização

Um breve histórico

1996 : Urnas eletrônicas em 30% das seções eleitorais
2000 : Primeiras eleições inteiramente eletrônicas
2002 : Primeira experiência com voto impresso
2006 : TSE passa a ser responsável pelo *software*
2008 : Migração para GNU/Linux
2009 : I Testes Públicos de Segurança (quebra de sigilo do voto)
2012 : II TPS (quebra de sigilo do voto)
2016 : III TPS (quebra na integridade de resultados)
2017 : IV TPS (quebra na integridade de *software*)

Organização do sistema



Preparação

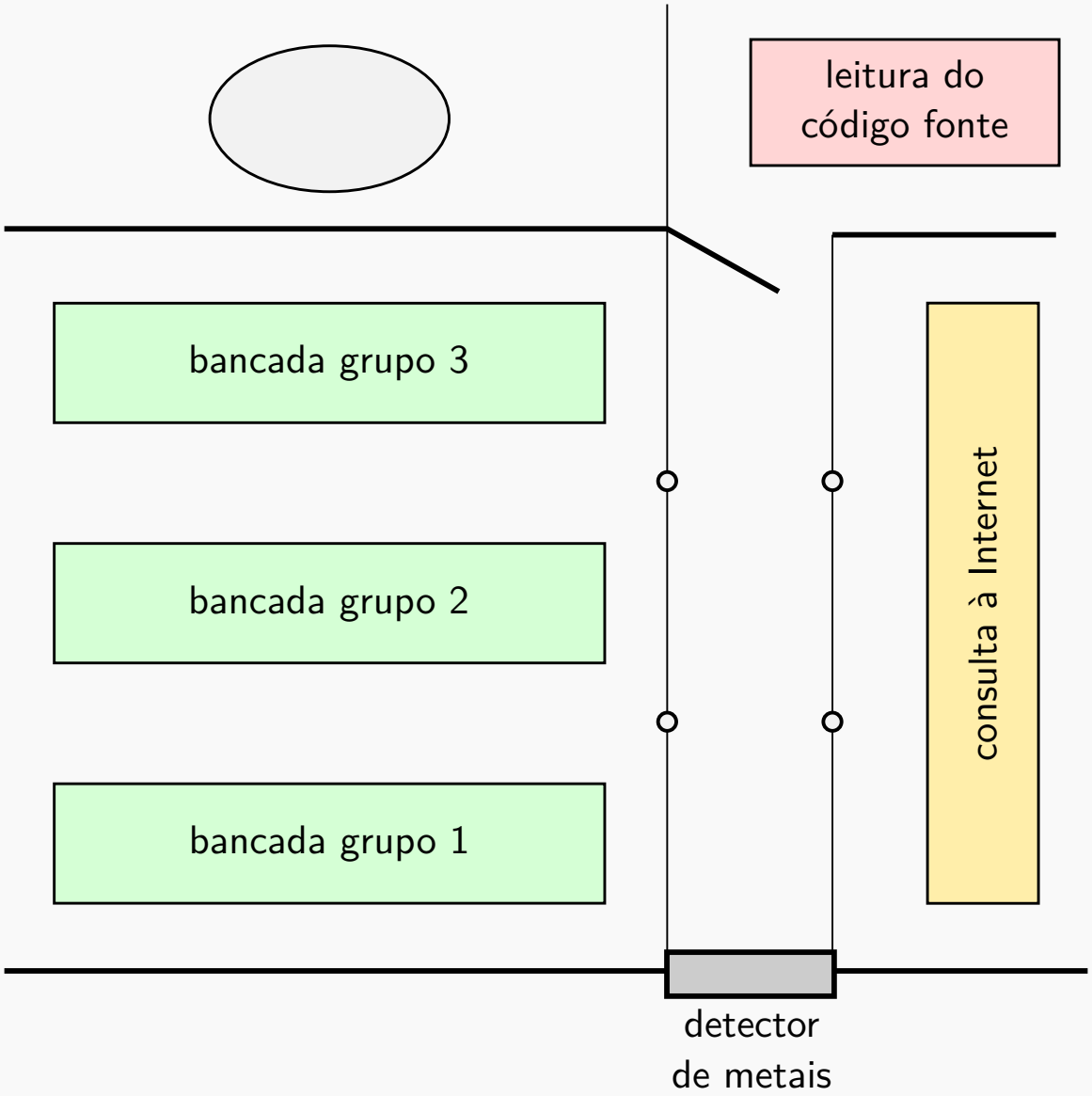
1. Confecção do *software* de votação no TSE
2. Transmissão do *software* de votação para TREs
3. Gravação do *software* de votação em cartões de memória *flash*
4. Distribuição dos cartões de memória
5. Instalação nas urnas eletrônicas (carga)

Instalação (carga) nas urnas

Como funciona o TPS?

- Fase de inspeção dos códigos fonte
- Submetemos **planos de teste**
- Os planos de teste são analisados e aprovados pelo TSE
- Executamos os planos de teste em uma bancada com computador e urna eletrônica

Planta do ambiente

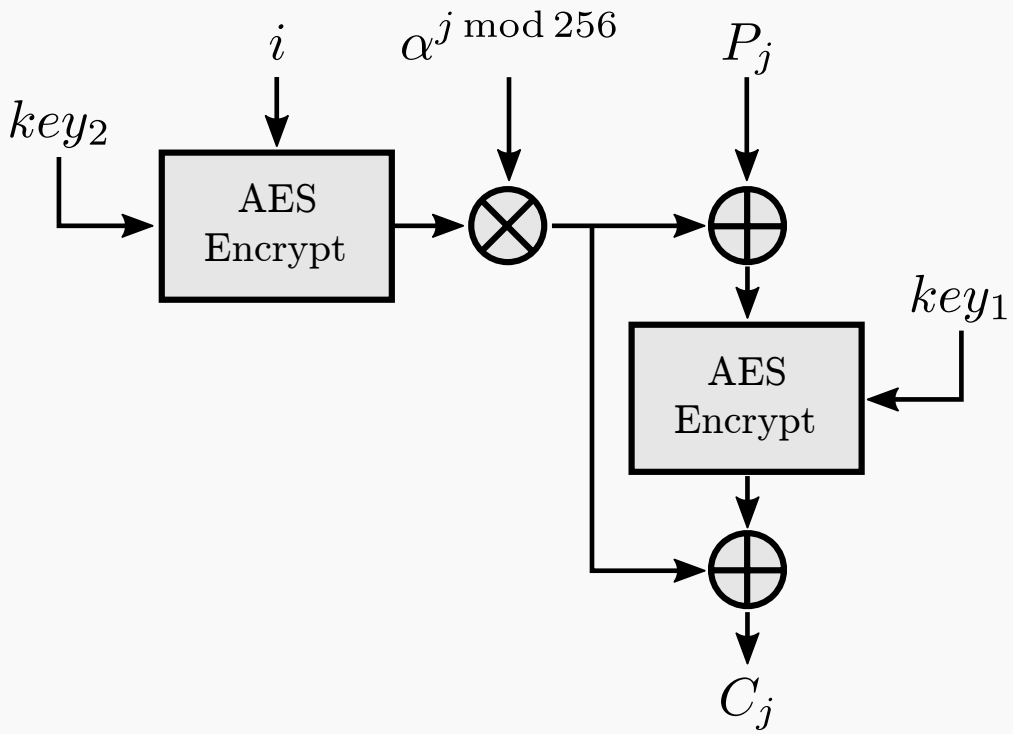


Dificuldades

- Formato burocrático (8 tipos de formulários)
- Escopo e duração dos testes
- Entrada de software (em DVD-ROM) ou material impresso apenas após análise e aprovação de *solicitação de material*
- Regras aplicam-se mesmo para material discriminado nos planos de teste previamente aprovados
- Proibido transitar com anotações entre ambiente de leitura de código fonte e bancada de testes
- Problemas para habilitar virtualização nos computadores fornecidos
- Necessidade de realizar apresentações de resultados parciais

Inspeção de código

- Encontramos chave da mídia de instalação em claro no código fonte do kernel 3.18



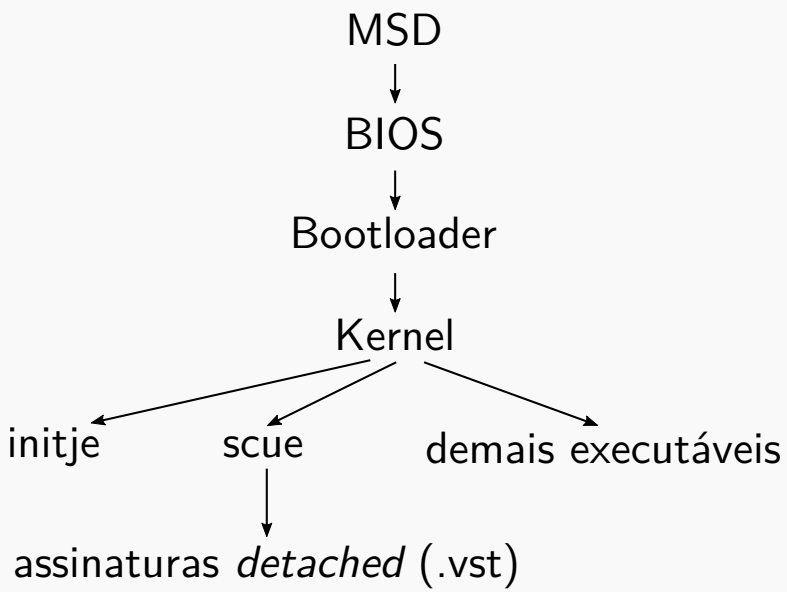
Primeiro dia

- Preencher formulários, solicitar computadores, inspeção de código, configuração do ambiente. . .

- Fizemos script Python+OpenSSL em uma máquina de inspeção de código e conseguimos decifrar um stub da partição cifrada que encontramos por lá

Segundo dia

- Reimplementamos o script de decifrar o cartão de memória com pycrypto nas máquinas de teste
- Estudamos a verificação de integridade do software:



Terceiro dia

- Encontramos duas bibliotecas (libapilog.so e libhkdf.so) sem assinaturas digitais.
- Alteramos todas as funções de uma das bibliotecas para imprimir FRAUDE! no terminal, o que aconteceu :-)

Terceiro dia

- Encontramos duas bibliotecas (libapilog.so e libhkdf.so) sem assinaturas digitais.
- Alteramos todas as funções de uma das bibliotecas para imprimir FRAUDE! no terminal, o que aconteceu :-)

- *Onde está o VOTA?*

Quarto dia

- libapilog.so: adulteramos o registro de log, substituindo INFO por XXXX
- libhkdf.so: adulteramos a biblioteca para zerar a chave criptográfica derivada para cifrar o RDV e violar o sigilo de um voto específico
- Programa para interagir com um teclado USB conectado à urna

Quarto dia

- libapilog.so: adulteramos o registro de log, substituindo INFO por XXXX
- libhkdf.so: adulteramos a biblioteca para zerar a chave criptográfica derivada para cifrar o RDV e violar o sigilo de um voto específico
- Programa para interagir com um teclado USB conectado à urna
- *Onde está o VOTA?*

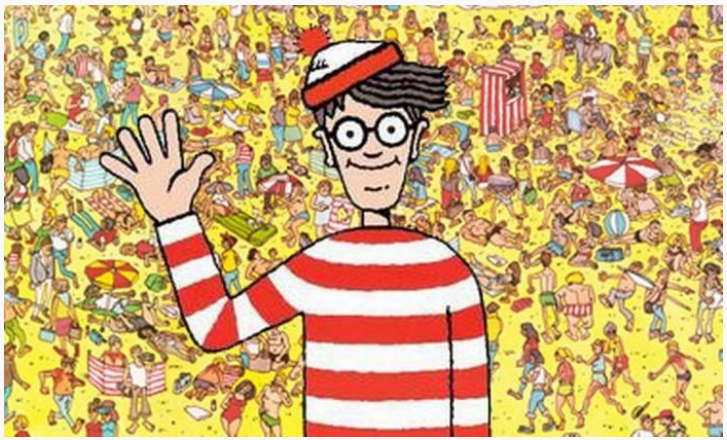
Quinto e último dia

- Peritos da Polícia Federal inicializam carga da urna em uma máquina virtual e recuperam a chave da mídia de instalação
  $\Rightarrow$ basta acesso a um cartão para montar nosso ataque!

Quinto e último dia

- Peritos da Polícia Federal inicializam carga da urna em uma máquina virtual e recuperam a chave da mídia de instalação
  $\Rightarrow$ basta acesso a um cartão para montar nosso ataque!

- *Achamos o VOTA!*

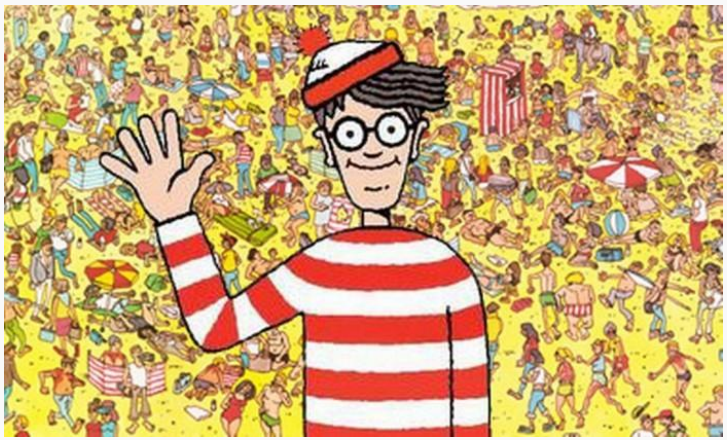


- Estava na terceira partição, e ninguém do time prestou atenção :-(

Quinto e último dia

- Peritos da Polícia Federal inicializam carga da urna em uma máquina virtual e recuperam a chave da mídia de instalação
  $\Rightarrow$ basta acesso a um cartão para montar nosso ataque!

- *Achamos o VOTA!*

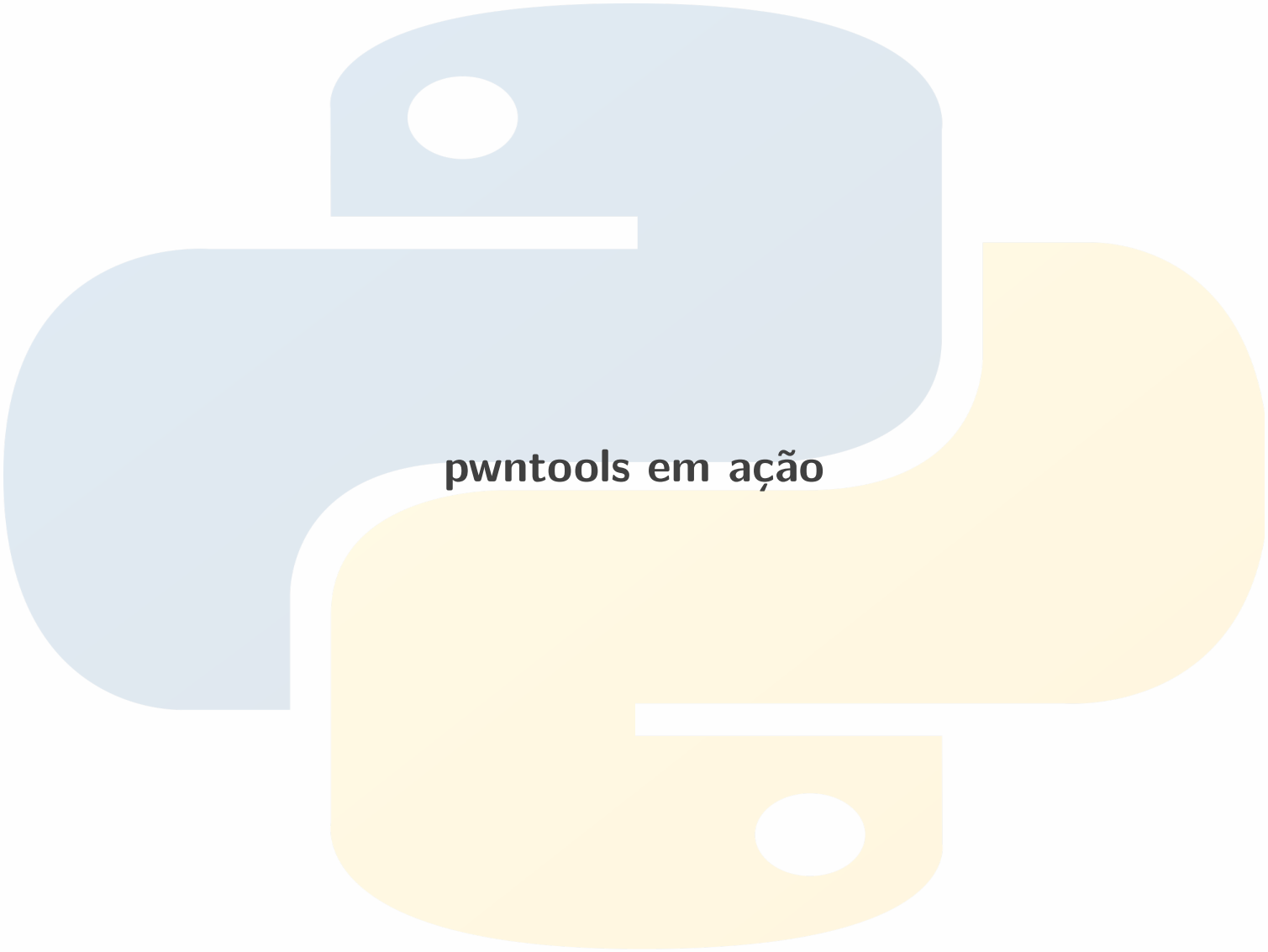


- Estava na terceira partição, e ninguém do time prestou atenção :-(

- Mas corre que dá tempo!

Quinto e último dia

- Desempacotamos o VOTA (UPX)
- Percebemos que o VOTA estava ligado com as duas bibliotecas sem assinaturas
- **Agora tínhamos total controle sobre o software de votação**
- Era suficiente? Não para os leigos...



pwntools em ação

Conclusão

- Outras vulnerabilidades devem existir...

- A independência do software é importante!
- Definição de Ronald Rivest: "*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*"

- Voto impresso: Registro físico e anônimo do voto, conferível pelo eleitor e que serve para auditoria/recontagem

Sou brasileiro e não desisto nunca

ars TECHNICA SUBSCRIPTIONS SIGN IN

NO AUDIT TRAIL FOR YOU —

In a blow to e-voting critics, Brazil suspends use of all paper ballots

Country's top court equates e-voting critics with conspiracy theorists.

DAN GOODIN - 6/8/2018, 5:35 PM