The Return of Insecure Brazilian Voting Machines

Diego F. Aranha, Aarhus University
dfaranha@eng.au.dk
@dfaranha

Joint work with Pedro Barbosa, Thiago Cardoso, Caio Lüders, Paulo Matias

Context

Brazilian elections are special:

- Massive (140M voters, 81% turnout)
- Held every 2 years
- Became electronic in 1996 (fully in 2000)
- Controlled/executed/judged by TSE (SEC – Superior Electoral Court)

Context

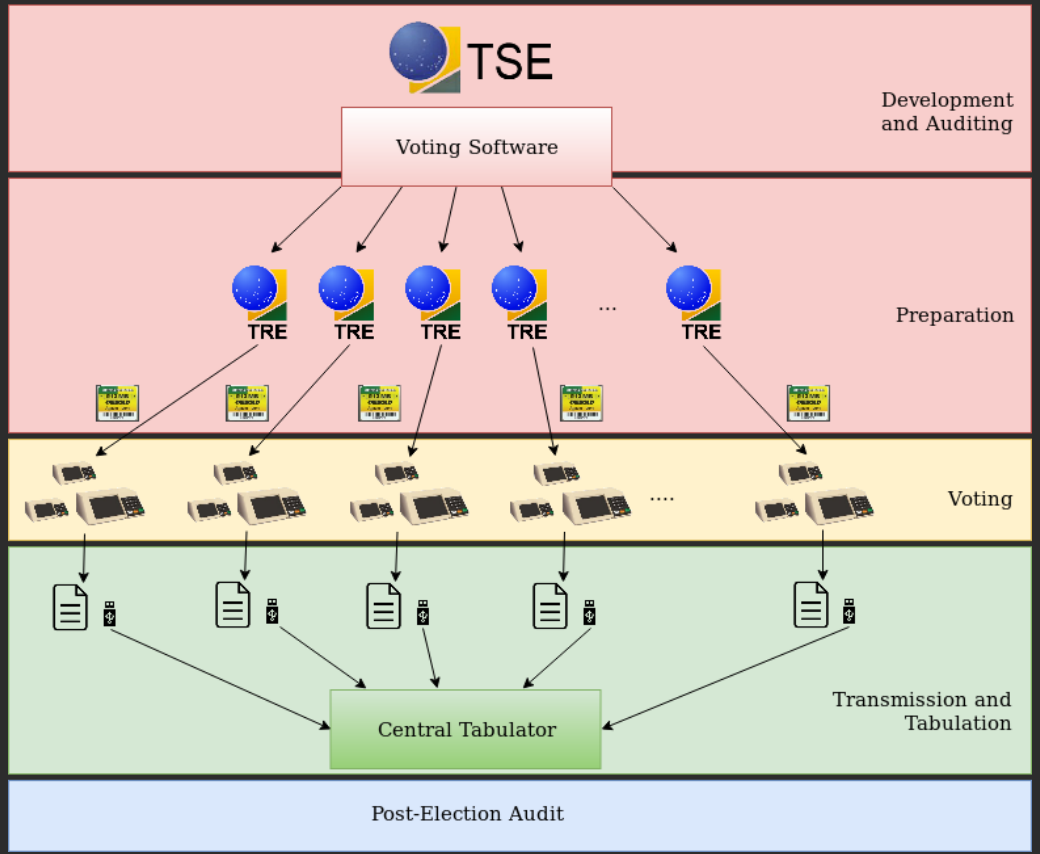
Source: Diebold

Quick facts

Brazilian paperless DRE voting machines:
- Claimed **100% secure** (but only tested in 2012...)
- Hardware by **Diebold** (> 0.5M)
- Software by SEC since 2006 (> 24M LOCs)
- Adopted GNU/Linux in 2008 (after **Windows CE**...)
- Experimented with **paper records** in 2002
- **Fingerprint** identification since 2011 (> 50%)

- Highly vulnerable against **insiders**

Election workflow



Election workflow

1. Software **installation** (a card installs 50 machines)
2. Zero tape **printed** (7-8 AM)
3. Voting session **opened**
4. Votes **cast**
5. Voting session **closed (5PM)** and poll tape **printed**
6. Media **written** with public files (PT, DRV, LOG)
7. Public products **transmitted** to central tabulator

Public Security Tests

Objective: Untraceable violation of **ballot integrity/privacy**

Extremely restricted tests:

1. No **pen/paper** for source code
2. **3 days** to inspect code, **4 days** to mount attacks
3. Participants **pre-approved** by SEC
4. Attacks **pre-approved** by SEC
5. No **guarantees** about software (correct or recent?)
6. Intrinsic **conflict of interests**

Vulnerabilities from 2012

- Serious vulnerability in **vote shuffling mechanism**
- Massive **sharing** and insecure **storage** of keys
- Voting software checks **itself** through signatures
- No **ballot secrecy** or **integrity** of software/results
- **Insecure** development process
- **Inadequate** threat model
- Internal culture lacks **transparency**

Digital Record of the Votes (DRV)

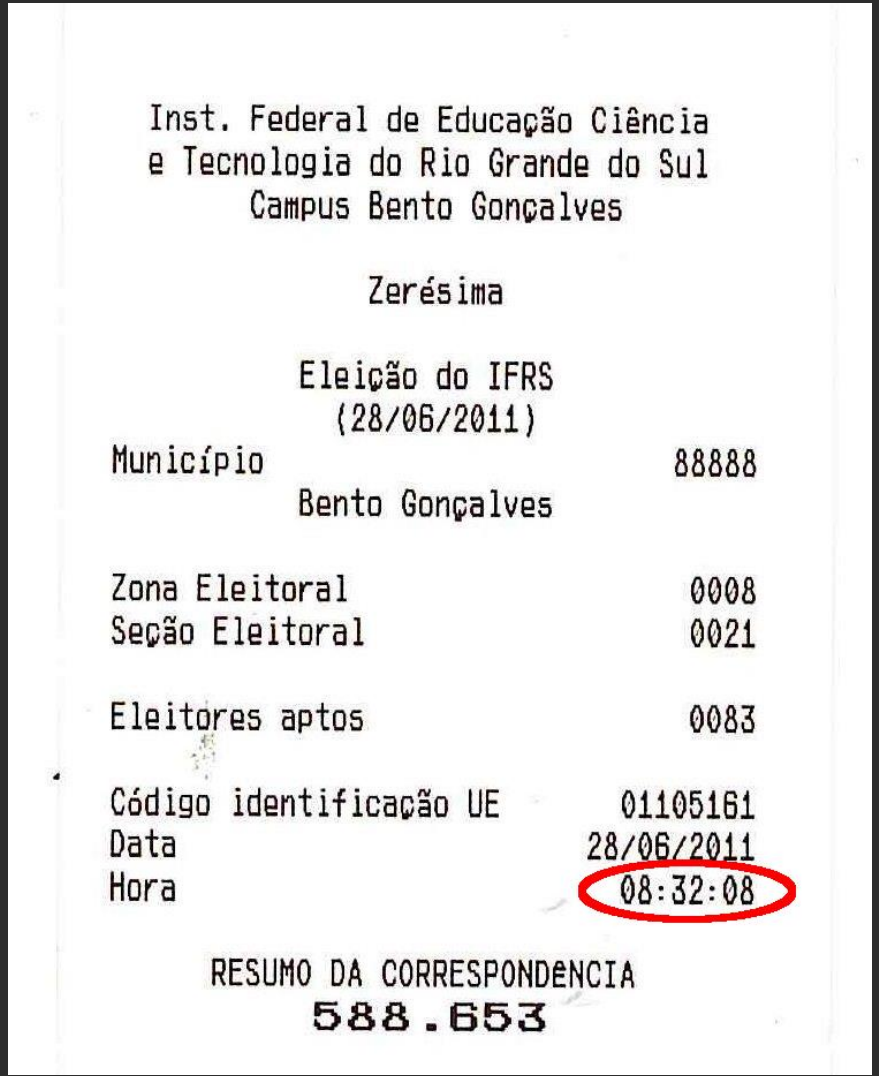
Governor	Senator	President
71	31	37
	BLANK	
13		
71	NULL	
		BLANK
		37

Warning: Advanced Cryptanalysis

grep -r rand *

Match in DRV.cpp! Seed?

```
srand(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

Defense in depth?

```
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
```

Conclusions from 2012

- Trivial to recover votes in order
- Trivial to recover vote cast at specific time

Eliminate the DRV and do not store metadata!

"Fixed" by **custom** algorithm seeded with system entropy, although voting machine has **two hardware RNGs**

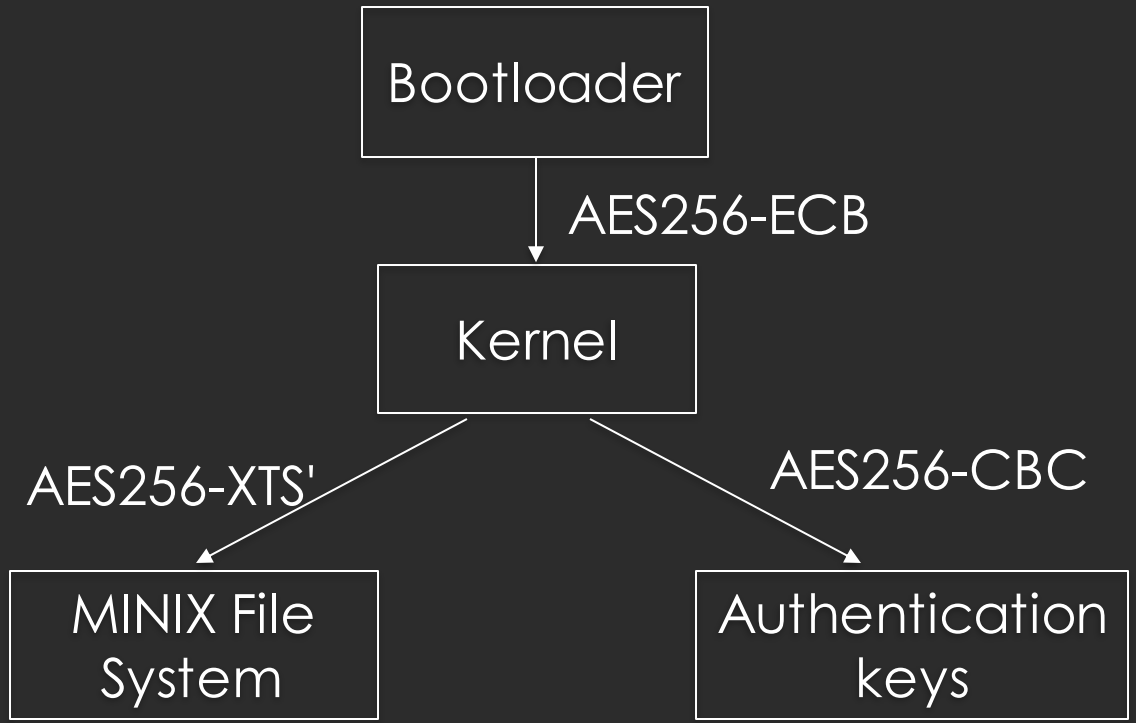
Installation as attack vector

Lots of cryptography...

- Install cards encrypted with AES-XTS-256', key embedded in the kernel.
- Digital signatures for integrity checking, both in userland and kernel mode.

Keys for signing **results** stored in install cards, encrypted under another embedded key.

Encryption chain



2017: Researchers would not have access to cryptographic keys...

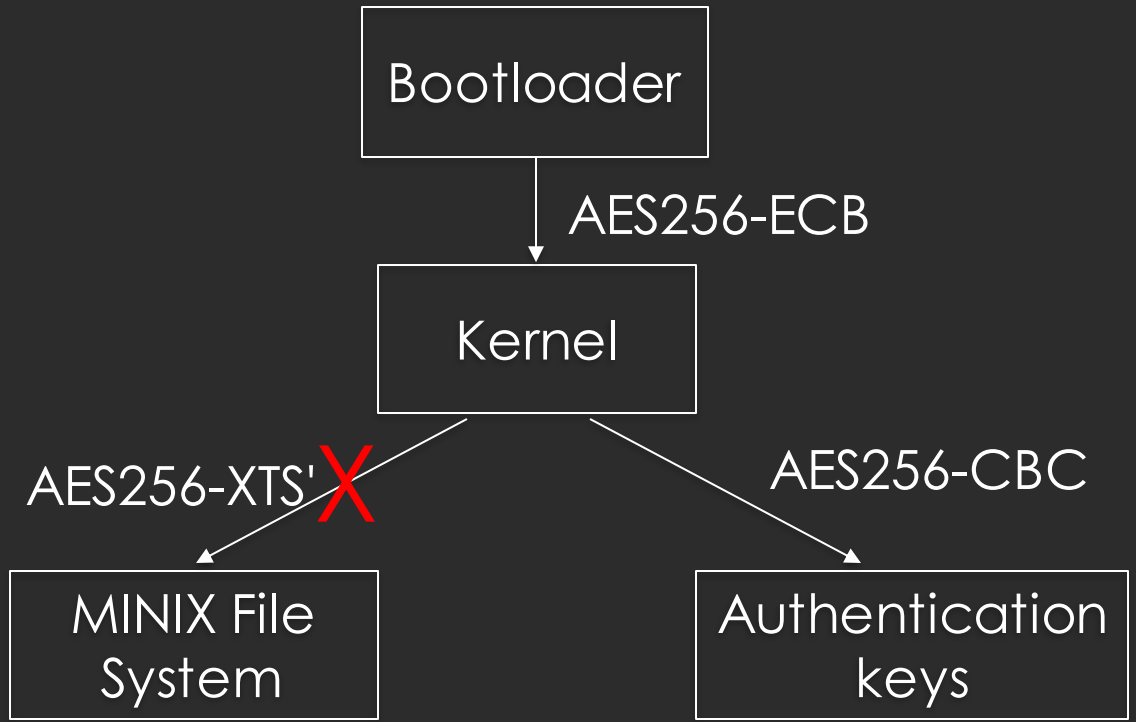
...but only because they erased them!

grep -r KEY *

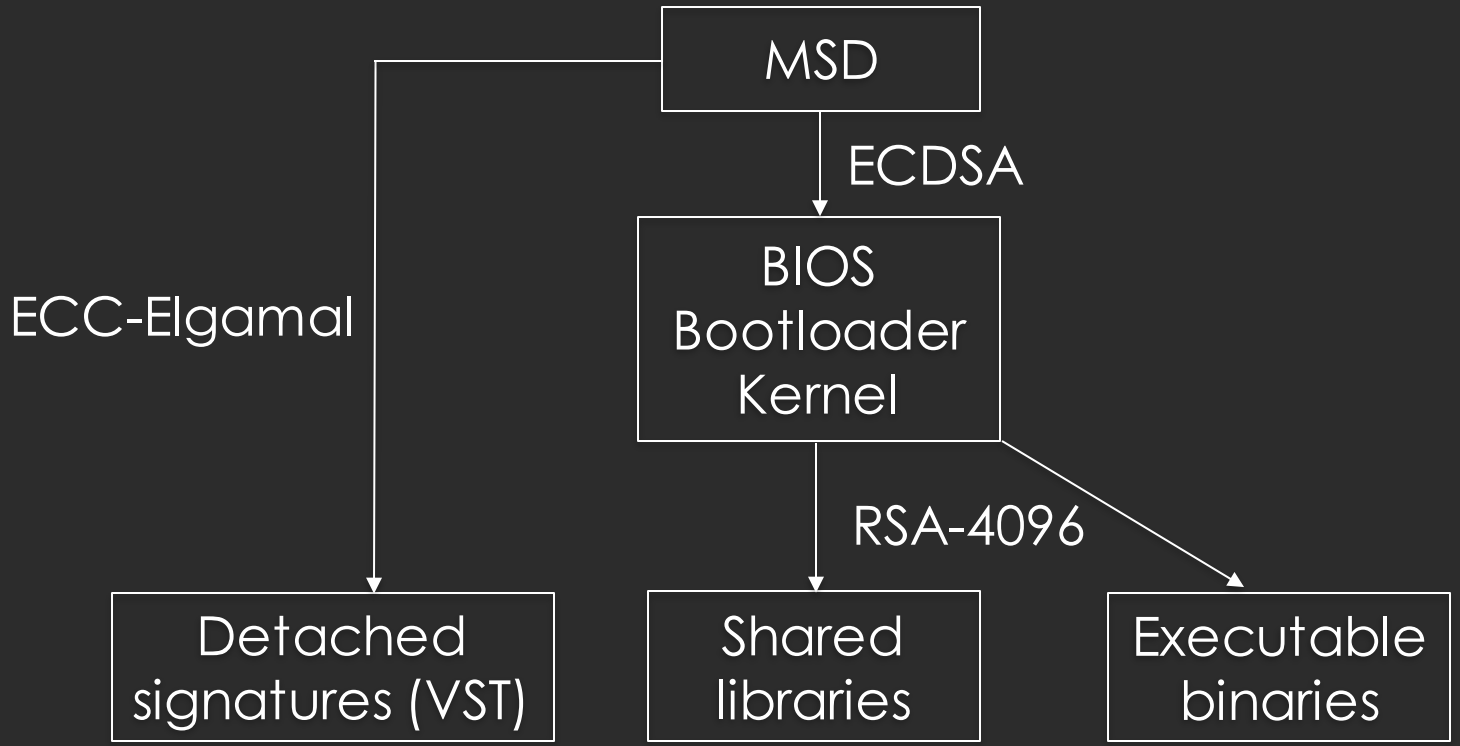
Match in ueminix.c!

#define UEMINIX_BLOCK_KEY {0x34, ...}

Encryption chain



Authentication chain



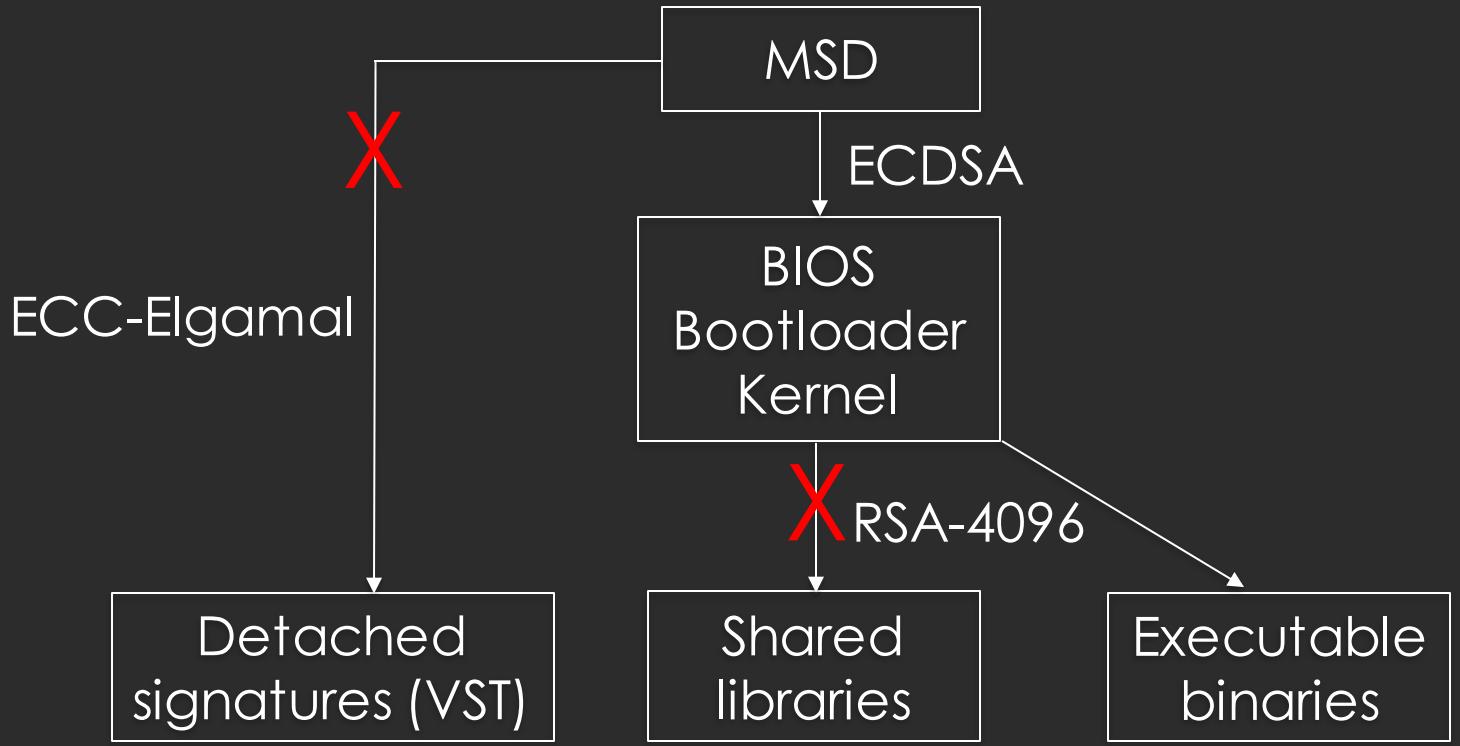
Issues with authentication

- Found two shared libraries **without detached** signatures (`libapilog.so` and `libhkdf.so`)
- Problem with kernel-side verification too:

```
uint32_t check = loader_sig_verify(...);
If (check >= 0) looks_good();
```

Voting software was linked against both!

Authentication chain



Arbitrary injection/execution

- Manipulated **LOG contents**
- Tampered with key generation for **DRV**
- USB keyboard to **issue commands**
- Changed software version/**screen contents**
- Manipulated how votes were **stored**

Manipulating vote counting follows directly!

SEU VOTO PARA

Presidente

Número: 6 1

Nome: Natação

Partido: PEsp

Presidente

Vice-Presidente

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

JUSTIÇA ELEITORAL

1 2 3
4 5 6
7 8 9
0

BRANCO CORRIGE CONFIRMA

VOTE 99

Presidente

Número: 9 9

Nome: Darth Vader

Partido: Dark Side

Presidente

Vice-Presidente

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

JUSTIÇA ELEITORAL

1 2 3
4 5 6
7 8 9
0

BRANCO CORRIGE CONFIRMA

Conclusions from 2017

- **Insecure** encryption of install cards
- **Insecure** integrity checking
- Another team found the encryption key without source (**fully external attack**)

Automate signing, deploy proper key management!

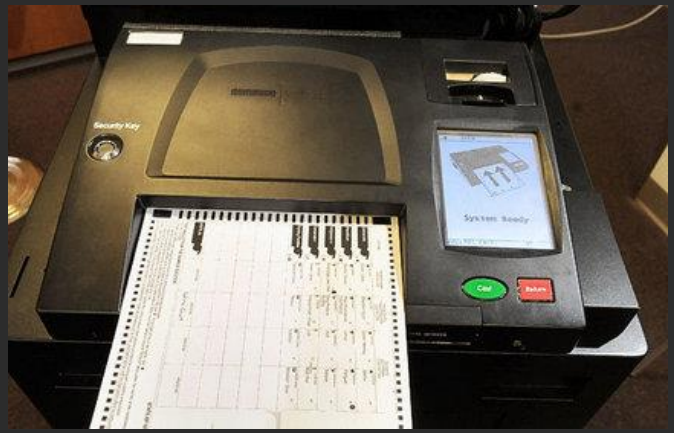
"Fixed" by deriving keys from BIOS, still shared by all voting machines and vulnerable to **insiders**.

Current problems

1. Software is **secret** for > 20 years
2. Software is demonstrably **insecure**
3. No paper record for **recount**
4. No effective means to **audit** the system
5. **Conflicts of interest** everywhere
6. **Insider attacks** completely disregarded

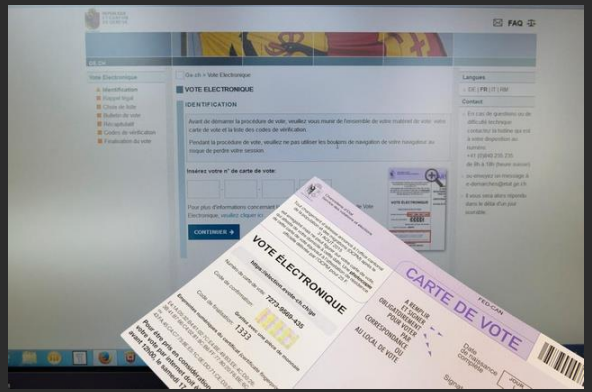
How to solve problems

1. Deploy software-**independent** systems
2. **Risk-limiting audits** on physical record
3. **Engage** society/technical community



How not to solve them

- **Internet** voting



- **Blockchain** voting

Future

1. Voter-Verified Paper Audit Trail for **security**
2. Auditable software for **transparency**
3. Social control mechanisms for **participation**

With increasing political polarization, it is critical that elections can be **independently verified.**

Thanks! Questions?

Diego F. Aranha, Aarhus University
dfaranha@eng.au.dk
@dfaranha

References:

[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 Good, the Bad and the Ugly: Two Decades of E-Voting in Brazil (2018)
[4] The Return of Software Vulnerabilities in the Brazilian voting machine. (2018)

Bonus round from 2016

Poll tapes could be changed after the fact by forging checksum.

Use a MAC instead!