Software vulnerabilities in the Brazilian voting machine

Diego F. Aranha, UNICAMP
dfaranha@ic.unicamp.br
@dfaranha
http://www.ic.unicamp.br/~dfaranha
Context

Brazilian elections:
- Massive (140M voters, 81% turnout)
- Held every 2 years
- Became electronic in 1996 (fully in 2000)
- Controlled/executed/judged by a single entity (SEC - Superior Electoral Court)
Context

Brazilian DRE voting machines:
- **Claimed** 100% secure (but only tested in 2012...)
- Hardware manufactured by **Diebold** (> 0.5M)
- Software written by SEC since 2006 (> 13M LOCs)
- Adopted GNU/Linux in 2008 (after **Windows CE**...)
- Experimented with **paper records** in 2002
- Identify 16% of the voters with **fingerprints** since 2011

Source: Diebold
Context

Source: Diebold
Algorithm

1. Voting machines loaded with software
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 products (PT, DRV, LOG)
7. Public products transmitted to central tabulator
Vulnerabilities from 2012

II Public Security Tests of Brazilian Voting System:
- **Restricted** security tests (no pen/paper)
- Limited to voting machines
- Serious vulnerability in vote shuffling mechanism
- Massive **sharing** and insecure **storage** of keys
- Voting software checks **itself**
- No **ballot secrecy** or **integrity** of software/results.
# Digital Record of the Votes (DRV)

<table>
<thead>
<tr>
<th>Governor</th>
<th>Senator</th>
<th>President</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>31</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>BLANK</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BLANK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>37</td>
</tr>
</tbody>
</table>
Warning: Advanced Cryptanalysis
grep  -r rand  *

9
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
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
Conclusions from 2012

- Trivial to recover votes in order
- LOG associates vote with timestamp
- Thus trivial to recover a specific vote

Eliminate the DRV and do not store metadata!

"Fixed" by using /dev/urandom, although voting machine has two hardware RNGs
Current problems

1. Software is secret for almost 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
YouInspect in 2014

Audit transmission of results by matching pictures of poll tapes taken from mobile app with electronic records.
Results from YouInspect

- Around 8,000 poll tapes in the two rounds
- Approximately 100 GB in pictures
- Image processing -> OCR -> final check
- Verified transmission for 4.1% of the votes
- Quality of the sample?
Challenge for 2016

How to **design** sampling process for large-scale elections?

Source: SEC
Future

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

Elections need not only to appear fair, but provide real means for independent verification.
Thanks! Questions?

Diego F. Aranha, UNICAMP
dfaranha@ic.unicamp.br
@dfaranha
http://www.ic.unicamp.br/~dfaranha

References: