Online voting

Quentin Rivollat

Electronic voting

- Electronic voting can be split in 2 :
- - EVM : Electronic Voting Machine
- - Online voting

E-voting around the world

Used for the first time in the USA, for a state election, in 2004

E-VOTING IN ESTONIA

First country in the world to use online voting in national elections in 2005

31.3% of Estonians voted online in the last European Parliament Elections in 2014

Saves over 11,000 working days per election through online voting

Criteria

- Authorization
- Anonymity
- Data integrity
- Privacy
- Voter authenticity
- Availability
- Verifiability

Possible attacks

Viruses or Malicious Software

Hacking

Denial of service attacks (DDOS)

Most used, because the easiest and the most powerful

Man in the Middle

In Switzerland

In december 2018, a new online voting system appears, called e-Voting, developped by two companies :

SWISS POST + Scytl Innovating Democracy =

Concours

Organized by SwissPost in February 2019

Rewards :

- Corrupting votes or rendering them unusable
  => 5000 .-
- Successful attack on voting secrecy on the servers
  => 10 000 .-
- Manipulation of votes detected by the system
  => 20 000 .-
- Undetected manipulation of votes
  => 30 000 – 50 000 .-

Results

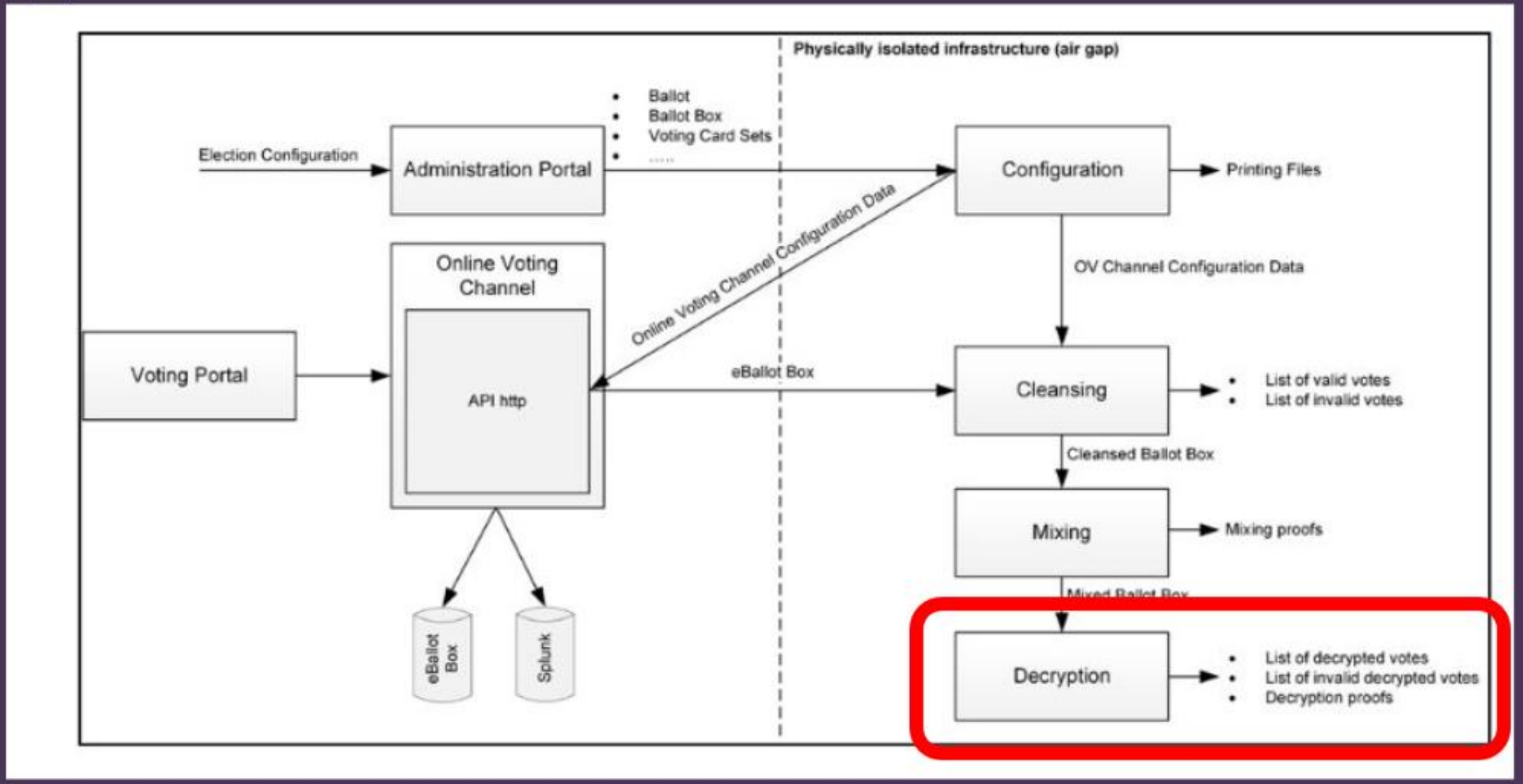
0 hack 0 penetration 0 vote modification

But…

Source code went public

Anyone could inspect it

Matthew Green and Sarah Jamie Lewis found a critical issue



https://chaosticino.ch/docs/20191017--sarah-jamie-lewis-on-e-voting-et-al_slides.pdf

Peggy has a Ciphertext & a Key to decrypt it, which she uses to get the Plaintext

Peggy

Vicky wants proof that the Plaintext came from the Ciphertext

Vicky

In theory land...Peggy constructs Proof....

The Ciphertext has the form (C_0, C_1)

Alice computes $C'_1=C_1/m$ where m is the decryption. And proves to Vicky that the decryption factor is correct.

Alice picks a random a

$B_0=g^a$

$B_1=C_0^a$

Peggy / Alice

Vicky picks a random challenge c

Alice compute..

$z=a+cx$. (x is the private key)

Vicky checks that....

$B_0 \stackrel{?}{=} g^z(pk)^{-c}$

$B_1 \stackrel{?}{=} C_0^z(C'_1)^{-c}$

Vicky

Instead of waiting for a challenge from Vicky. Peggy & Vicky agree on a way of generating challenges

Peggy

We can do this by using a cryptographic hash function,

assuming it acts totally randomly

Vicky

First, Peggy calculate the challenge, then send the result to Vicky, who will check the exactness of the result

Peggy

The transcript is given ALL public information associated with the proof and generates a hash based on that input.

Vicky

Sha256(“3”+“10”+”10
20”) ==
23648ddd3be51d04a
21d90c254cd529a7f7
0f719161e6645c5bde
72cf9d948b7

Peggy

We use the public parameters as the input, and get unpredictable “randomness” as an output

Vicky

In the Scytl code base...

Peggy

Only certain public parameters were given to the hash function. And they were not differentiated by context

Vicky

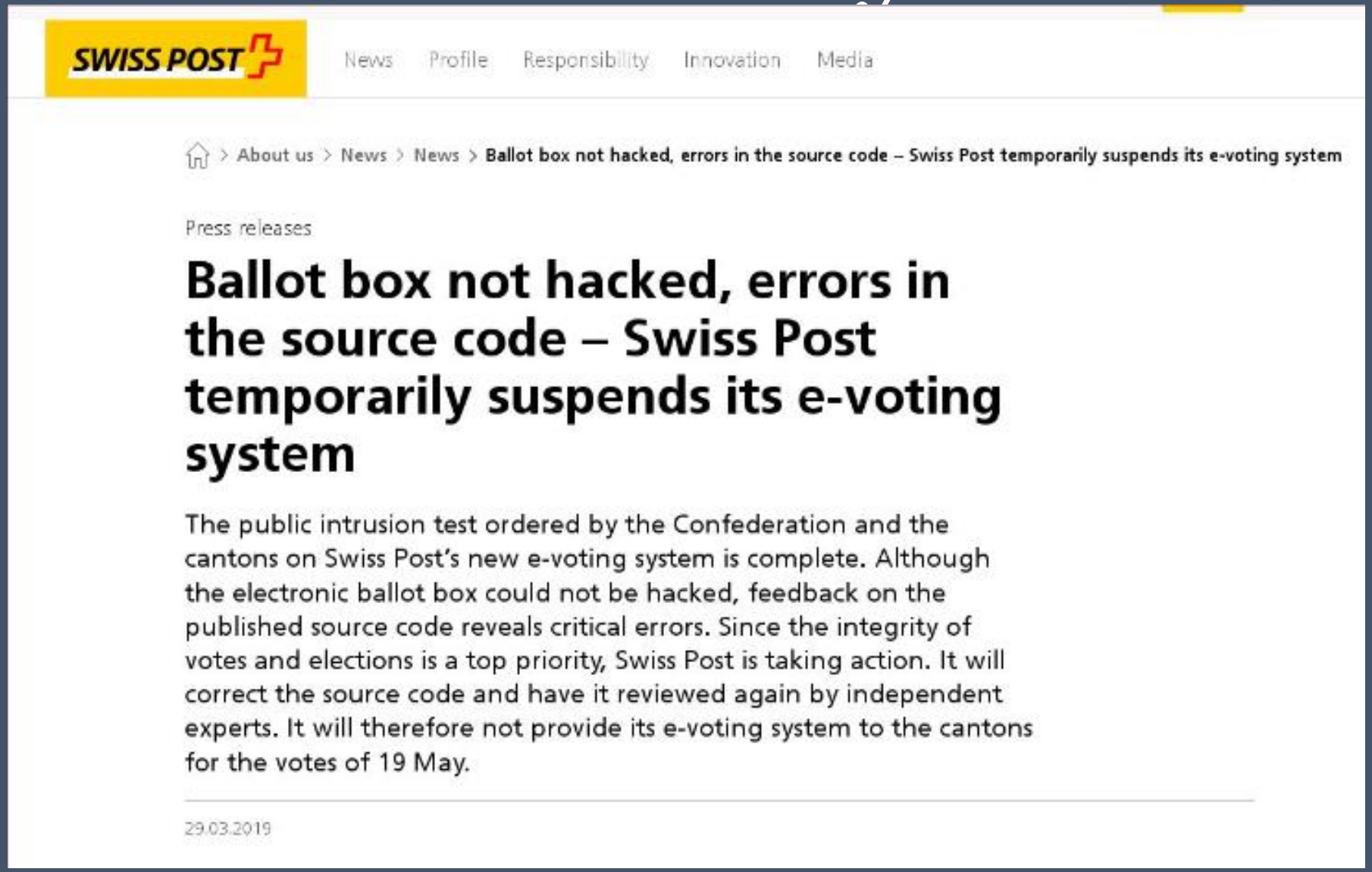
Sha256(“3”+“10”) ==
Sha256(“31” + “0”)

Peggy

This means given one valid proof we can generate other valid proofs!

Vicky

Finally



SWISS POST

News Profile Responsibility Innovation Media

About us > News > News > Ballot box not hacked, errors in the source code – Swiss Post temporarily suspends its e-voting system

Press releases

Ballot box not hacked, errors in the source code – Swiss Post temporarily suspends its e-voting system

The public intrusion test ordered by the Confederation and the cantons on Swiss Post's new e-voting system is complete. Although the electronic ballot box could not be hacked, feedback on the published source code reveals critical errors. Since the integrity of votes and elections is a top priority, Swiss Post is taking action. It will correct the source code and have it reviewed again by independent experts. It will therefore not provide its e-voting system to the cantons for the votes of 19 May.

29.03.2019

Sources

https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/sr.pdf

https://en.wikipedia.org/wiki/Electronic_voting

https://www.civiciti.info/7-benefits-of-electronic-voting/

https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html

http://juspoliticum.com/article/Vote-par-internet-failles-techniques-et-recul-democratique-74.html
https://decryptage.be/2019/03/svote/

https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/sr.pdf

https://portswigger.net/daily-swig/control-alt-delete-swiss-govt-puts-the-brakes-on-e-voting

https://resources.infosecinstitute.com/top-threats-to-online-voting-from-a-cybersecurity-perspective/
https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system

https://www.lemonde.fr/pixels/article/2019/02/25/les-hackers-invites-a-pirater-le-systeme-de-vote-electronique-suisse_5428208_4408996.html