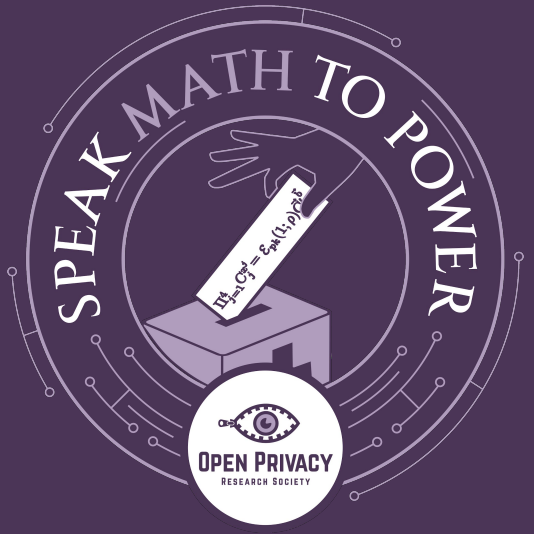
How Not To Secure An Election



Sarah's Adventures in Switzerland

This work was done in collaboration with Vanessa Teague (University of Melbourne) & Olivier Pereira (UCLouvain)

Sarah Jamie Lewis

OPEN PRIVACY
RESEARCH SOCIETY

Executive Director, Open Privacy Research Society

Before:

- Independent Privacy & Anonymity Researcher & Book Publisher (Queer Privacy)
- Automated Systems Fraud / Security @ *Amazon*
- Computer Scientist @ *<Redacted> (British Government)*

February 2019

Swiss e-voting trial offers $150,000 in bug bounties to hackers

The white hat hacking begins February 24th

Sarah Jamie Lewis
@SarahJamieLewis

So, I took a look at swiss online voting system code that someone leaked, and having written, deployed and audited large enterprise java code...that thing triggers every flag.

11:55 AM · Feb 17, 2019 · Twitter Web Client

“These criticisms are mainly based on misunderstandings related to the cryptographic mechanisms”

https://www.scytl.com/en/statement-recent-comments-regarding-source-code-publication-swiss-e-voting/

What is Universal Verifiability?

Universal Verifiability: anyone may determine that all of the ballots in the box have been correctly counted.

What is a Zero Knowledge Proof?

A Zero Knowledge Proof...

“is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x.”

Meet Alice

And Bob!

Meet ~~Alice~~ Peggy

And ~~Bob~~ Vicky!

What is an OR-Proof...?

In theory land...Peggy encrypts 1 of 2* possibilities

Vicky can verify that Peggy didn't cheat and encrypt something else...

Voter			Verifier
$v=1$	$v=0$		
$w, r_1, d_1 \in_R \mathbb{Z}_q$	$w, r_2, d_2 \in_R \mathbb{Z}_q$		
$x \leftarrow g^{x_j}$	$x \leftarrow g^{x_j}$		
$y \leftarrow h^{x_j} \cdot g$	$y \leftarrow h^{x_j}$		
$a_1 \leftarrow g^{r_1} x^{d_1}$	$a_1 \leftarrow g^{w}$		
$b_1 \leftarrow h^{r_1} y^{d_1}$	$b_1 \leftarrow h^{w}$		
$a_2 \leftarrow g^{w}$	$a_2 \leftarrow g^{r_2} x^{d_2}$		
$b_2 \leftarrow h^{w}$	$b_2 \leftarrow h^{r_2}(y/g)^{d_2}$	x, y, a_1, b_1, a_2, b_2 →	
		c ←	$c \in_R \mathbb{Z}_q$
$d_2 \leftarrow c - d_1$	$d_1 \leftarrow c - d_2$		$c \stackrel{?}{=} d_1 + d_2$
$r_2 \leftarrow w - x_j d_2$	$r_1 \leftarrow w - x_j d_1$	d_1, d_2, r_1, r_2 →	$a_1 \stackrel{?}{=} g^{r_1} x^{d_1}$
			$b_1 \stackrel{?}{=} h^{r_1} y^{d_1}$
			$a_2 \stackrel{?}{=} g^{r_2} x^{d_2}$
			$b_2 \stackrel{?}{=} h^{r_2}(y/g)^{d_2}$

*Simplified

In the Scytl Codebase*...

Voter

$v = 1$	$v = 0$
$w, r_1, d_1 \in_R \mathbb{Z}_q$	$w, r_2, d_2 \in_R \mathbb{Z}_q$
$x \leftarrow g^{x_j}$	$x \leftarrow g^{x_j}$
$y \leftarrow h^{x_j} \cdot g$	$y \leftarrow h^{x_j}$
$a_1 \leftarrow g^{r_1} x^{d_1}$	$a_1 \leftarrow g^{w}$
$b_1 \leftarrow h^{r_1} y^{d_1}$	$b_1 \leftarrow h^{w}$
$a_2 \leftarrow g^{w}$	$a_2 \leftarrow g^{r_2} x^{d_2}$
$b_2 \leftarrow h^{w}$	$b_2 \leftarrow h^{r_2} (y/g)^{d_2}$
$d_2 \leftarrow c - d_1$	$d_1 \leftarrow c - d_2$
$r_2 \leftarrow w - x_j d_2$	$r_1 \leftarrow w - x_j d_1$

Verifier

$x, y, a_1, b_1, a_2, b_2 \rightarrow$

$\leftarrow c$

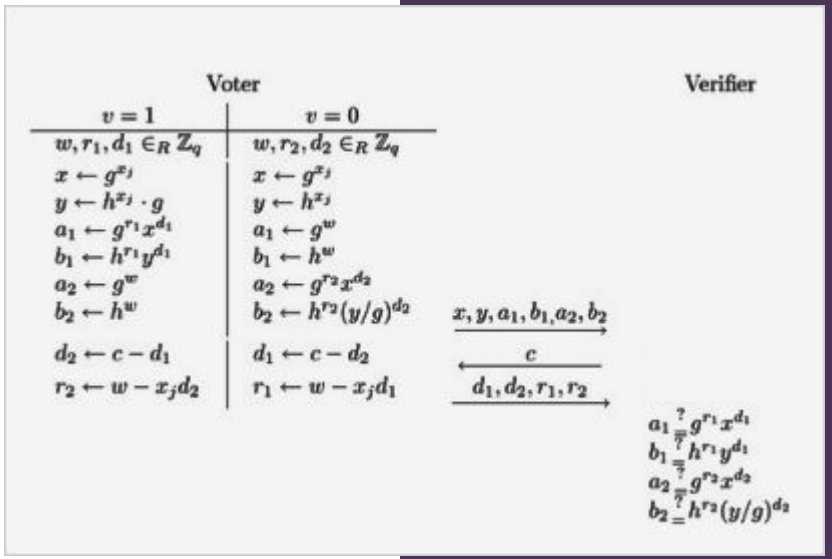
$d_1, d_2, r_1, r_2 \rightarrow$

$a_1 \stackrel{?}{=} g^{r_1} x^{d_1}$
$b_1 \stackrel{?}{=} h^{r_1} y^{d_1}$
$a_2 \stackrel{?}{=} g^{r_2} x^{d_2}$
$b_2 \stackrel{?}{=} h^{r_2} (y/g)^{d_2}$

*Simplified

In the Scytl Codebase*...

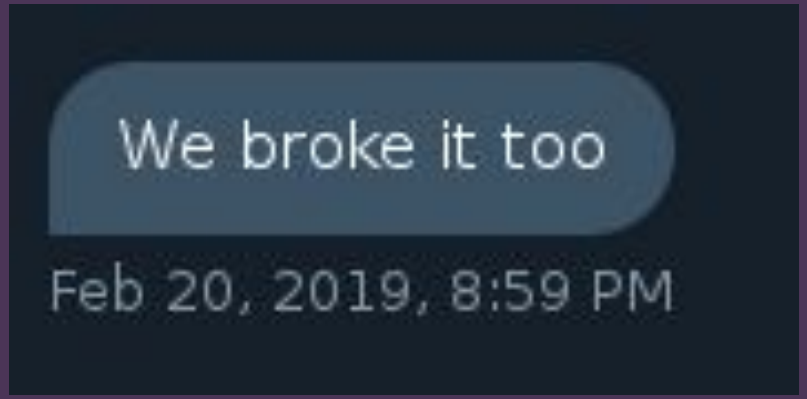
Vicky doesn't check the challenge!



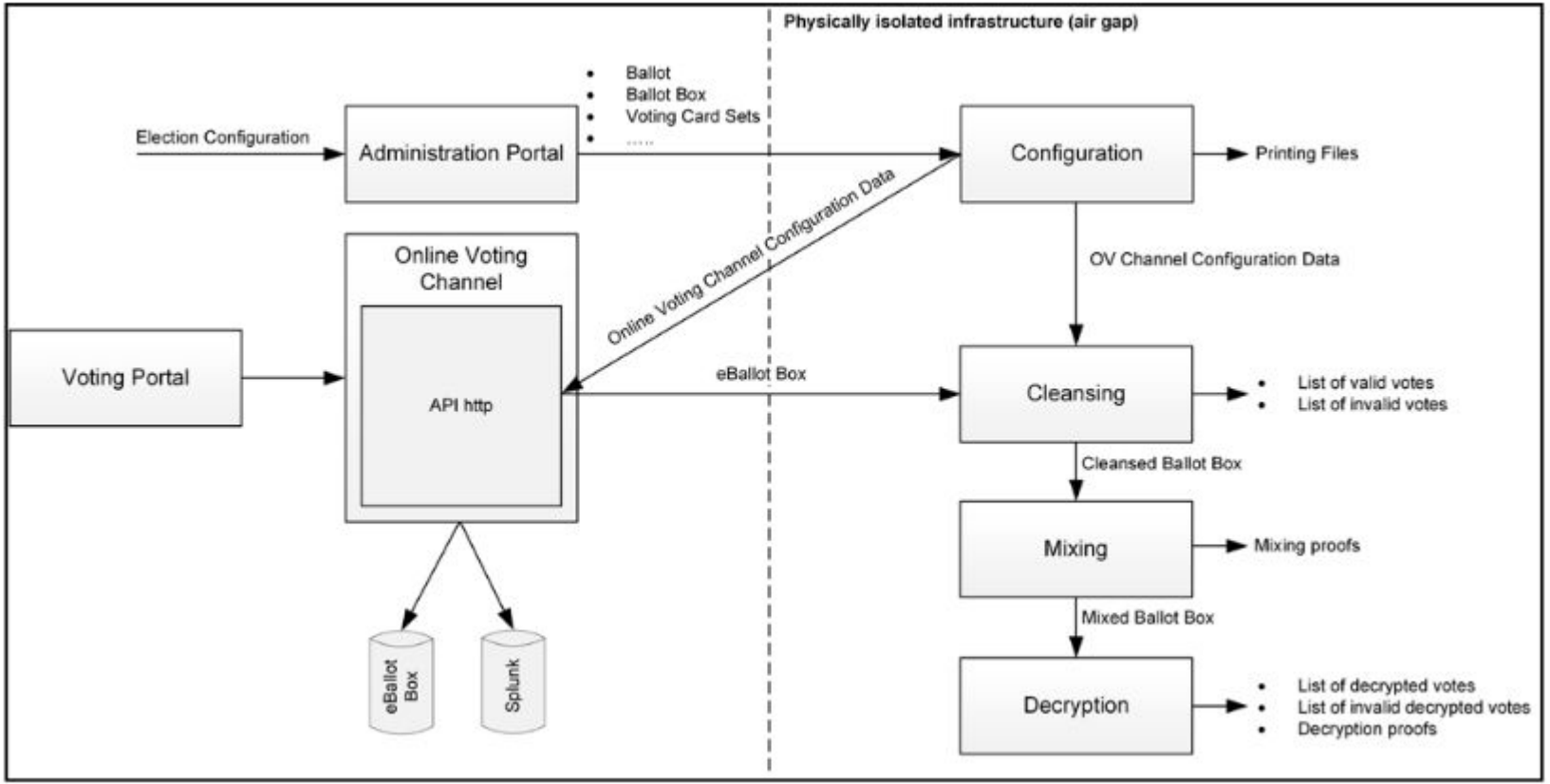
Voter			Verifier
$v = 1$	$v = 0$		
$w, r_1, d_1 \in_R \mathbb{Z}_q$	$w, r_2, d_2 \in_R \mathbb{Z}_q$		
$x \leftarrow g^{x_j}$	$x \leftarrow g^{x_j}$		
$y \leftarrow h^{x_j} \cdot g$	$y \leftarrow h^{x_j}$		
$a_1 \leftarrow g^{r_1} x^{d_1}$	$a_1 \leftarrow g^{w}$		
$b_1 \leftarrow h^{r_1} y^{d_1}$	$b_1 \leftarrow h^{w}$		
$a_2 \leftarrow g^{w}$	$a_2 \leftarrow g^{r_2} x^{d_2}$		
$b_2 \leftarrow h^{w}$	$b_2 \leftarrow h^{r_2} (y/g)^{d_2}$	$x, y, a_1, b_1, a_2, b_2 \rightarrow$	
$d_2 \leftarrow c - d_1$	$d_1 \leftarrow c - d_2$	$\leftarrow c$	
$r_2 \leftarrow w - x_j d_2$	$r_1 \leftarrow w - x_j d_1$	$\rightarrow d_1, d_2, r_1, r_2$	$a_1 \stackrel{?}{=} g^{r_1} x^{d_1}$ $b_1 \stackrel{?}{=} h^{r_1} y^{d_1}$ $a_2 \stackrel{?}{=} g^{r_2} x^{d_2}$ $b_2 \stackrel{?}{=} h^{r_2} (y/g)^{d_2}$

*Simplified

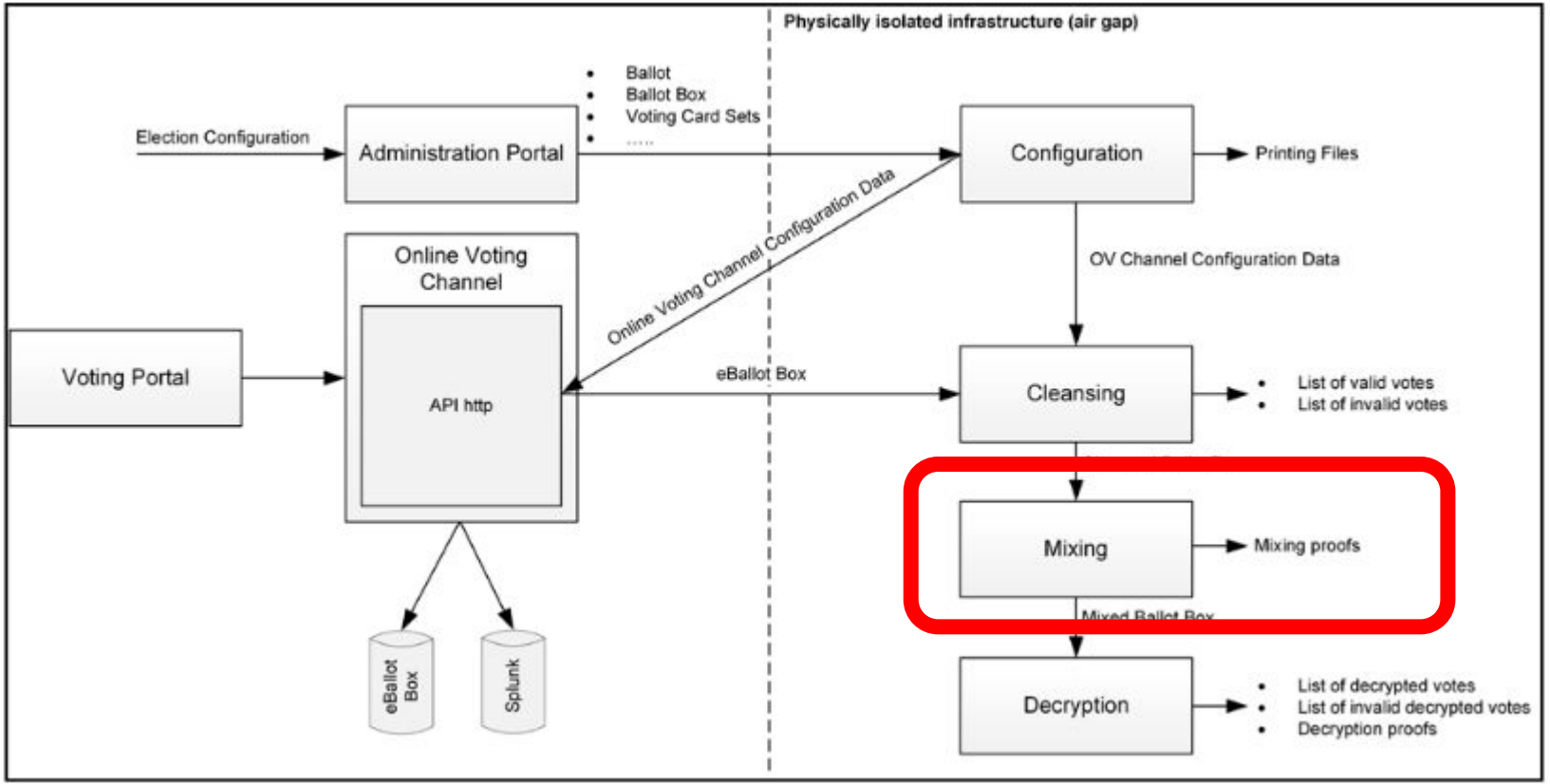

Sarah Jamie Lewis
@SarahJamieLewis
Ah f[redacted]k, I think I broke something and now I need an actual cryptographer.
8:49 PM · Feb 20, 2019 · Twitter Web Client


We broke it too
Feb 20, 2019, 8:59 PM

Turns out: we had broken two different pieces, and we decided to team up.

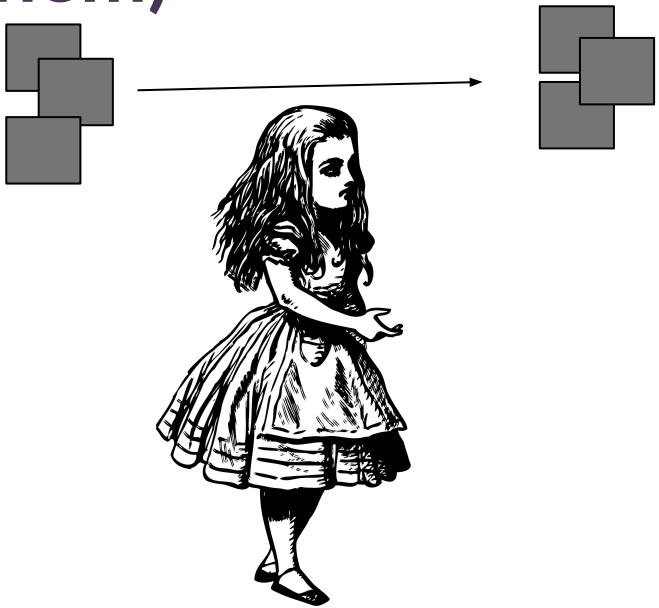

Physically isolated infrastructure (air gap)
Ballot
Ballot Box
Voting Card Sets
.....
Election Configuration
Administration Portal
Configuration
Printing Files
Online Voting Channel Configuration Data
OV Channel Configuration Data
Online Voting Channel
Voting Portal
API http
eBallot Box
Cleansing
List of valid votes
List of invalid votes
Cleansed Ballot Box
Mixing
Mixing proofs
Mixed Ballot Box
eBallot Box
Splunk
Decryption
List of decrypted votes
List of invalid decrypted votes
Decryption proofs

What is a Shuffle Proof?


Physically isolated infrastructure (air gap)
Ballot
Ballot Box
Voting Card Sets
.....
Election Configuration
Administration Portal
Configuration
Printing Files
Online Voting Channel Configuration Data
OV Channel Configuration Data
Online Voting Channel
Voting Portal
API http
eBallot Box
Cleansing
List of valid votes
List of invalid votes
Mixing
Mixing proofs
Mixed Ballot Box
eBallot Box
Splunk
Decryption
List of decrypted votes
List of invalid decrypted votes
Decryption proofs

Stephanie Bayer and Jens Groth. Efficient zero-knowledge argument for correctness of a shuffle. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 263–280. Springer, 2012

Peggy is a given a set of Ciphertexts, mixes (and re-encrypts them)



Vicky wants proof that the new Re-encrypted ciphertexts are the same as the ones Peggy was given….

Peggy & Vicky need to agree on a set of **generators…**

We need these so we can build **commitments!**

While mixing, Peggy cryptographically **commits** (sends locked boxes) to Vicky

After Peggy has finished mixing, she opens the boxes for Vicky and shows her what is inside

```
public CommitmentParams(final ZpSubgroup group, final int n) {
        group = group;
        h = GroupTools.getRandomElement(group);
        commitmentlength = n;
        g = GroupTools.getVectorRandomElement(group,
this.commitmentlength);
        }

        // from getRandomElement(group)
Exponent randomExponent = ExponentTools.getRandomExponent(group.getQ());
return group.getGenerator().exponentiate(randomExponent);
```

Using these trapdoored parameters, Peggy can open the commitments to any value she desires!

$$\begin{aligned}
\mathsf{com}_{ck}(\vec{a}; r) &= H^r \Pi_{i=1}^n G_i^{a_i} \\
&= H^r \Pi_{i=1}^n H^{a_i e_i} \\
&= H^{r+\sum_{i=1}^n (a_i - b_i) e_i} \Pi_{i=1}^n H^{b_i e_i} \\
&= H^{r'} \Pi_{i=1}^n G_i^{b_i} \\
&= \mathsf{com}_{ck}(\vec{b}; r').
\end{aligned}$$

$$r' = r + \sum_{i=1}^{n} e_i (a_i - b_i)$$

Peggy can manipulate votes by replacing them when she mixes...

$$
\begin{array}{rcccl}
C'_1 & = & \mathcal{E}_{pk}(1;\rho_1)C_1 & = & \mathcal{E}_{pk}(M_1, \rho_1 + \rho'_1) \\
\hline
C'_2 & = & \mathcal{E}_{pk}(\mathbf{1};\rho_2)\mathbf{C_3} & = & \mathcal{E}_{pk}(\mathbf{M_3}, \rho_2 + \rho'_3) \\
\hline
C'_3 & = & \mathcal{E}_{pk}(1;\rho_3)C_3 & = & \mathcal{E}_{pk}(M_3, \rho_3 + \rho'_3) \\
\text{and } C'_4 & = & \mathcal{E}_{pk}(1;\rho_4)C_4 & = & \mathcal{E}_{pk}(M_4, \rho_4 + \rho'_4)
\end{array}
$$

A. Technical detail on how to generate a fake proof transcript with known randomness

A.1. Calculating ρ

This section shows why we get the expression for ρ that we use above.
We needed to find ρ s.t.

$$\vec{C}^{\vec{x}} = \mathcal{E}_{pk}(1;\rho)\vec{C'}^{\vec{b}}$$

where $\vec{C}$ are the input ciphertexts and $\vec{C'}$ are the output ciphertexts. (Bayer-Groth p.8)

$$
\begin{array}{rcl}
LHS & = & \vec{C}^{\vec{x}} \\
 & = & \Pi_{j=1}^{4} C_j^{x^j} \\
 & = & \mathcal{E}_{pk}(q_1^{x+x^2} q_2^{x^3} q_4^{x^4}; \sum_{i=1}^{4} x^i \rho'_i) \\
 & & \\
RHS & = & \mathcal{E}_{pk}(1;\rho)\vec{C'}^{\vec{b}} \\
 & = & \mathcal{E}_{pk}(q_1^{x+x^2} q_2^{x^3} q_4^{x^4}; \rho + (\rho_1 + \rho'_1)(x + x^2) + (\rho_3 + \rho'_3)x^3 + (\rho_4 + \rho'_4)x^4). \\
\text{So } \rho & = & -\rho_1 x - (\rho_1 + \rho'_1)x^2 + x^2\rho'_2 - \rho_3 x^3 - \rho_4 x^4.
\end{array}
$$

Note ρ'_4 is unknown but $\rho'_4 x^4$ cancels out.

“How Do We Disclose This”?

We decided to not sign any Non-Disclosure Agreements, but to contact Swiss Post as a courtesy.

March 2019

—

Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. "Ceci n'est pas une preuve." (2019).

https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf

—

“This mixnet has a trapdoor—a malicious administrator or software provider for the mix could manipulate votes but produce a proof transcript that passes verification.

Thus complete verifiability fails.”

Meanwhile In Australia...

...There was an election going on

NSW Electoral Commission iVote and Swiss Post e-voting

The NSW Electoral Commission is aware of an issue relating to its iVote internet and telephone voting system, which has been raised in the context of the e-voting system operated by Swiss Post.

The identification of this issue does not affect the use of iVote for the NSW State election.

Swiss Post delivers mail, banking and an online voting platform to cantons for Swiss elections. A 'Public Intrusion Test' of the Swiss e-voting system is currently being conducted by Swiss Post and the Swiss Federal Chancellery, offering cash prizes for cryptographers, academics and hackers to identify any weaknesses in their system, either directly or from reviewing its source code. In the course of this exercise an issue has been identified that is also present in the iVote system.

—

“The identification of this issue does not affect the use of iVote for the NSW State election...because...Air Gap”

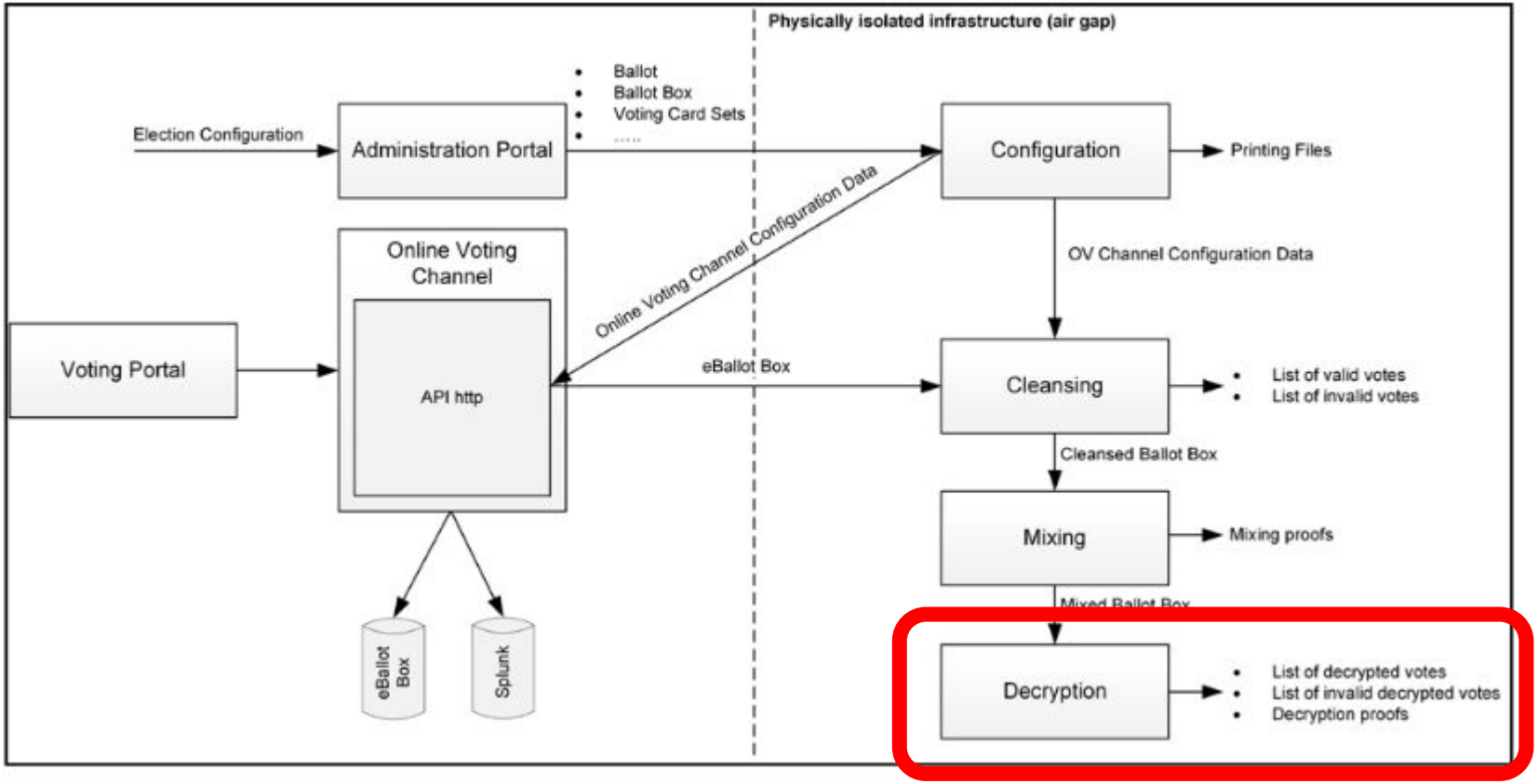
https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post-e-vo

“Scytl is delivering a patch which will be tested and implemented shortly to address this matter.”

https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post-e-vo

Back to Switzerland...

What is a Decryption Proof?


Physically isolated infrastructure (air gap)
Ballot
Ballot Box
Voting Card Sets
.....
Election Configuration
Administration Portal
Configuration
Printing Files
Online Voting Channel Configuration Data
OV Channel Configuration Data
Online Voting Channel
Voting Portal
API http
eBallot Box
Cleansing
List of valid votes
List of invalid votes
Cleansed Ballot Box
Mixing
Mixing proofs
Mixed Ballot Box
eBallot Box
Splunk
Decryption
List of decrypted votes
List of invalid decrypted votes
Decryption proofs

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

Vicky wants proof that the Plaintext came from the Ciphertext (but we cannot allow Vicky to have the key)

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 Bob that the decryption factor is correct.

Alice picks a random a

$B_0=g^a$

$B_1=C_0^{\ a}$

Vicky picks a random challenge c

Alice compute..

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

Vicky checks that....

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

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

What is Fiat-Shamir?

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

We can do this by using a cryptographic hash function, **assuming** it acts as a **random oracle**.

In secure codebases, a primitive known as a “transcript” is used.

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

Sha256(“3”+“10”+”1020”) == 23648ddd3be51d04a21d90c254cd529a7f70f719161e6645c5bde72cf9d948b7

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

What is Weak Fiat-Shamir?

David Bernhard, Olivier Pereira, and Bogdan Warinschi. "How not to prove yourself: Pitfalls of the fiat-shamir heuristic and applications to helios." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012.

In the Scytl code base...

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

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

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

Peggy constructs Proof….

The Ciphertext has the form (C_0, C_1)

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

Peggy picks a random a

$B_0=g^a$

$B_1=C_0^{\ a}$

$c = \text{Hash}(pk, C'_1, B_0, B_1)$

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

Vicky checks that….

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

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

$C \stackrel{?}{=} \text{Hash}(pk, C'_1, B_0, B_1)$

Peggy constructs a Cheating Proof….

Peggy picks a random a,s,t

$B_0 = g^a$

$B_1 = g^t$

$C'_1 = g^s$

$c = \text{Hash}(pk, C'_1, B_0, B_1)$

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

$C_0 = g^{(t+sc)/z}$

Verifier checks that….

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

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

$C \stackrel{?}{=} \text{Hash}(pk, C'_1, B_0, B_1)$

Peggy can modify her proof because the challenge only hashes parameters she has control over instead of all of the context (e.g. the ciphertext, the group etc.)

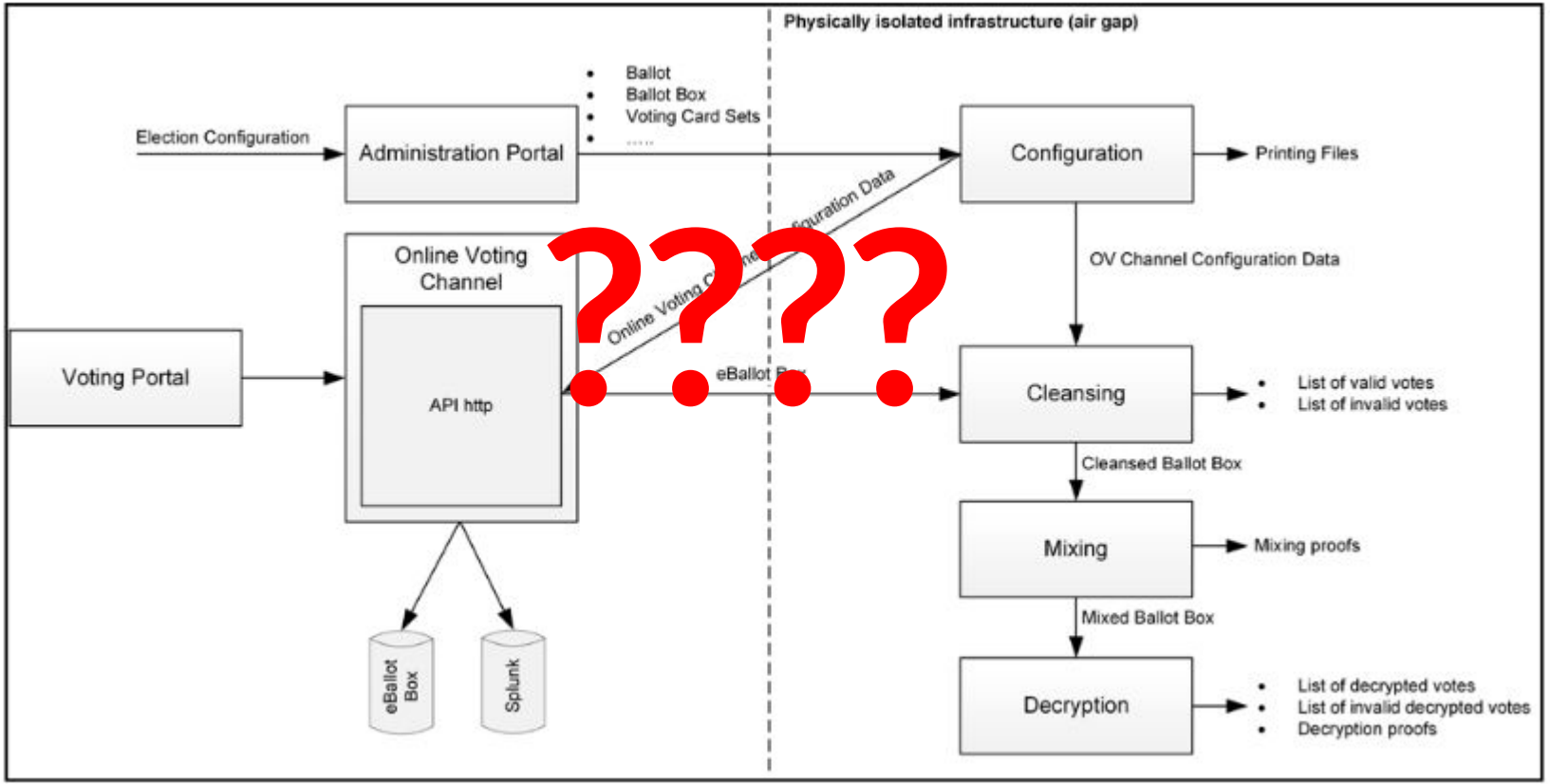
She can modify her statement based on the challenge!

Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. "How not to prove your election outcome: The use of non-adaptive zero knowledge proofs in the scytl-swisspost internet voting system, and its implications for decryption proof soundness" 2019.

https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf

Unanswered Questions...

What is an OR-Proof doing in this code base!?


Physically isolated infrastructure (air gap)
Election Configuration
Administration Portal
Ballot
Ballot Box
Voting Card Sets
.....
Configuration
Printing Files
OV Channel Configuration Data
Online Voting Channel
API http
Voting Portal
????
eBallot Box
Cleansing
List of valid votes
List of invalid votes
Cleansed Ballot Box
Mixing
Mixing proofs
Mixed Ballot Box
Decryption
List of decrypted votes
List of invalid decrypted votes
Decryption proofs
eBallot Box
Splunk

—

“Yes, you are right. The verifier was using the hash for checking the proofs but if was not checking if hash is related to the sum of c_j. Thank you for the highlight!” - Scytl Employee

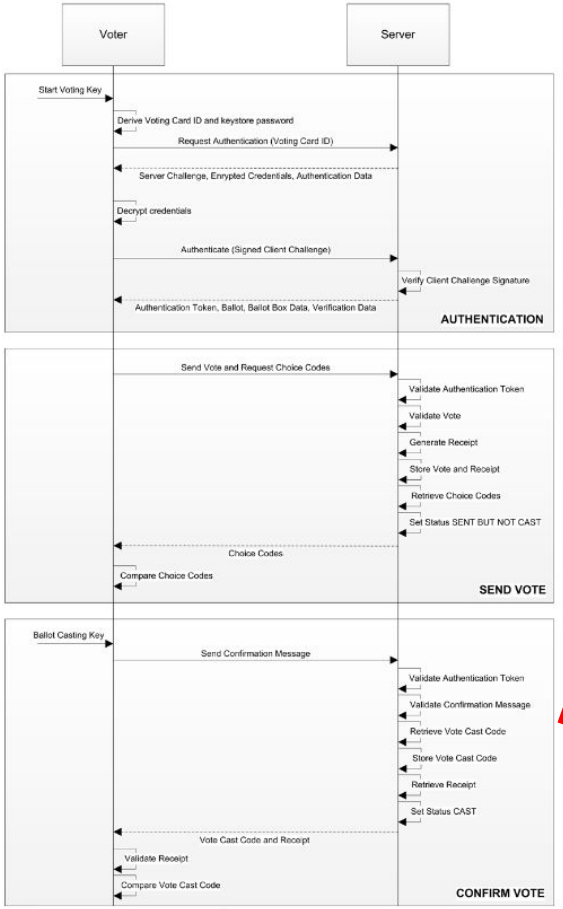
—

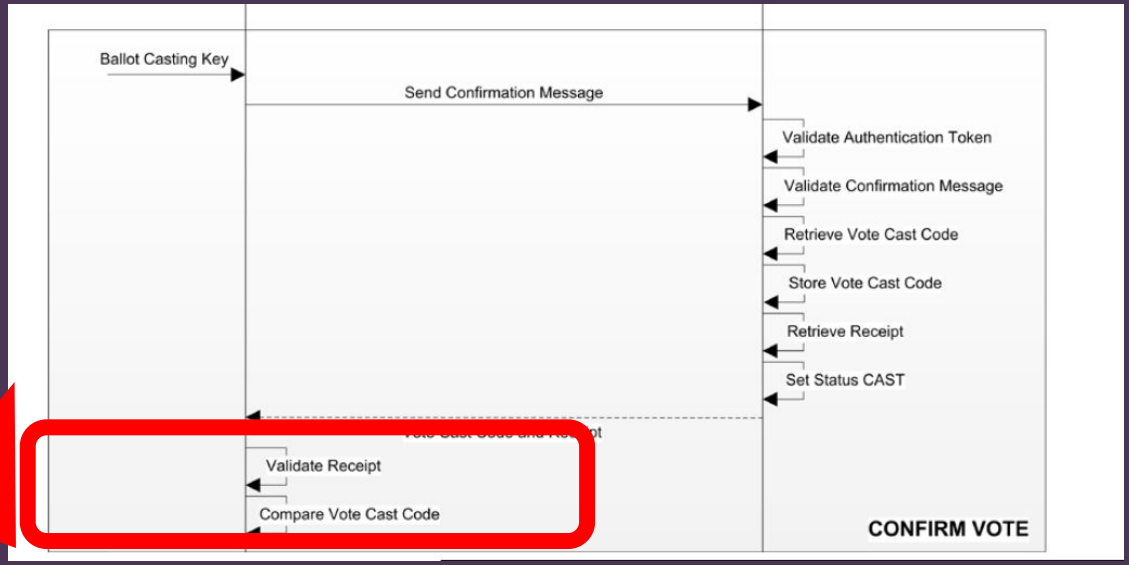
“The reason is because it is inside our cryptolib and this was initially planned as a library and therefore, it is not prepared to break it in small pieces and include only the needed parts. So while a refactor is not finished, we are still including it as a library.” - Scytl Employee

The Vulnerability That (temporarily) Stopped E-Voting

What is Individual Verifiability?

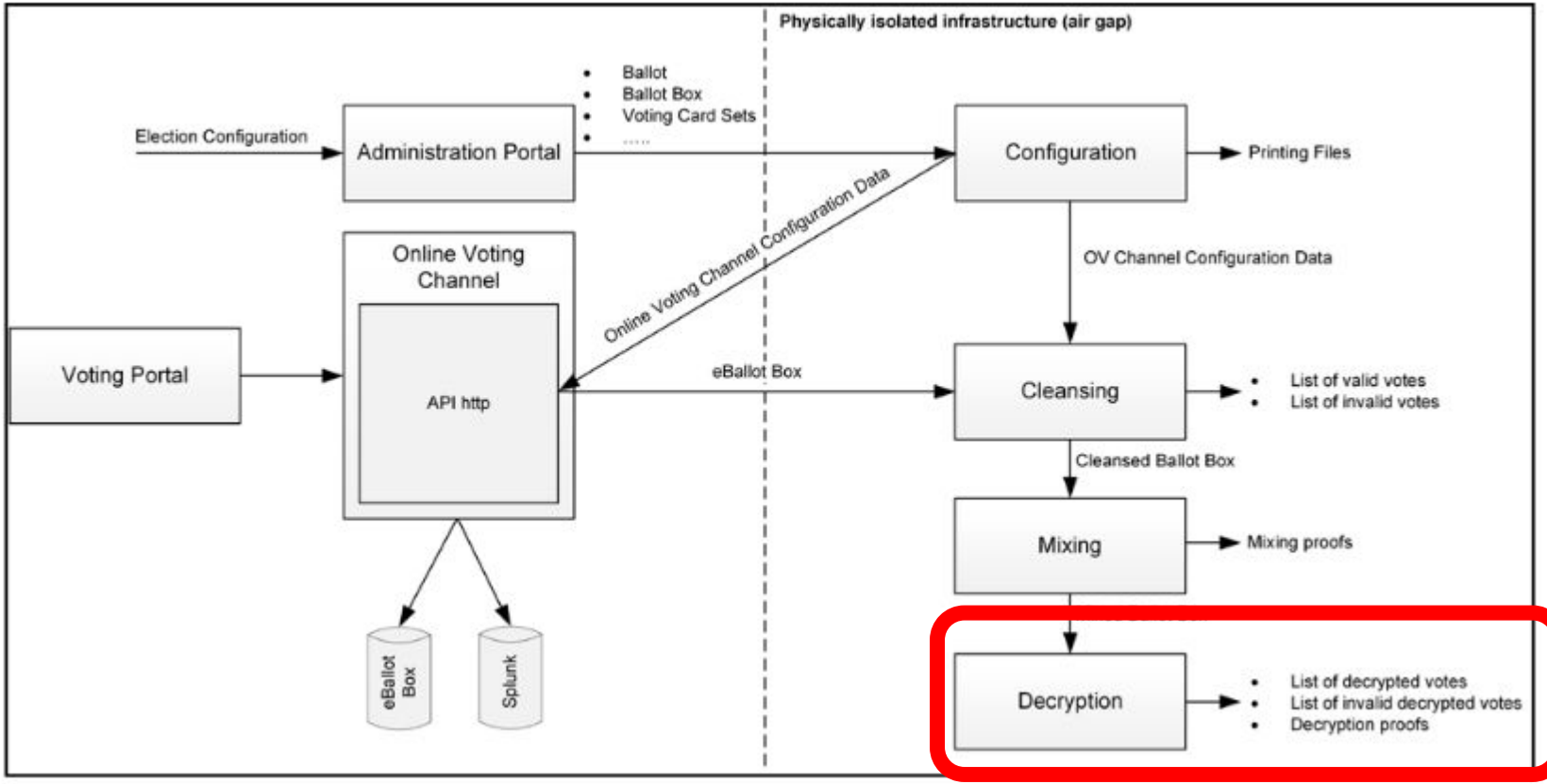
Individual Verifiability: Any voter can check that their ballot has been correctly counted.





Scytl
innovating Democracy

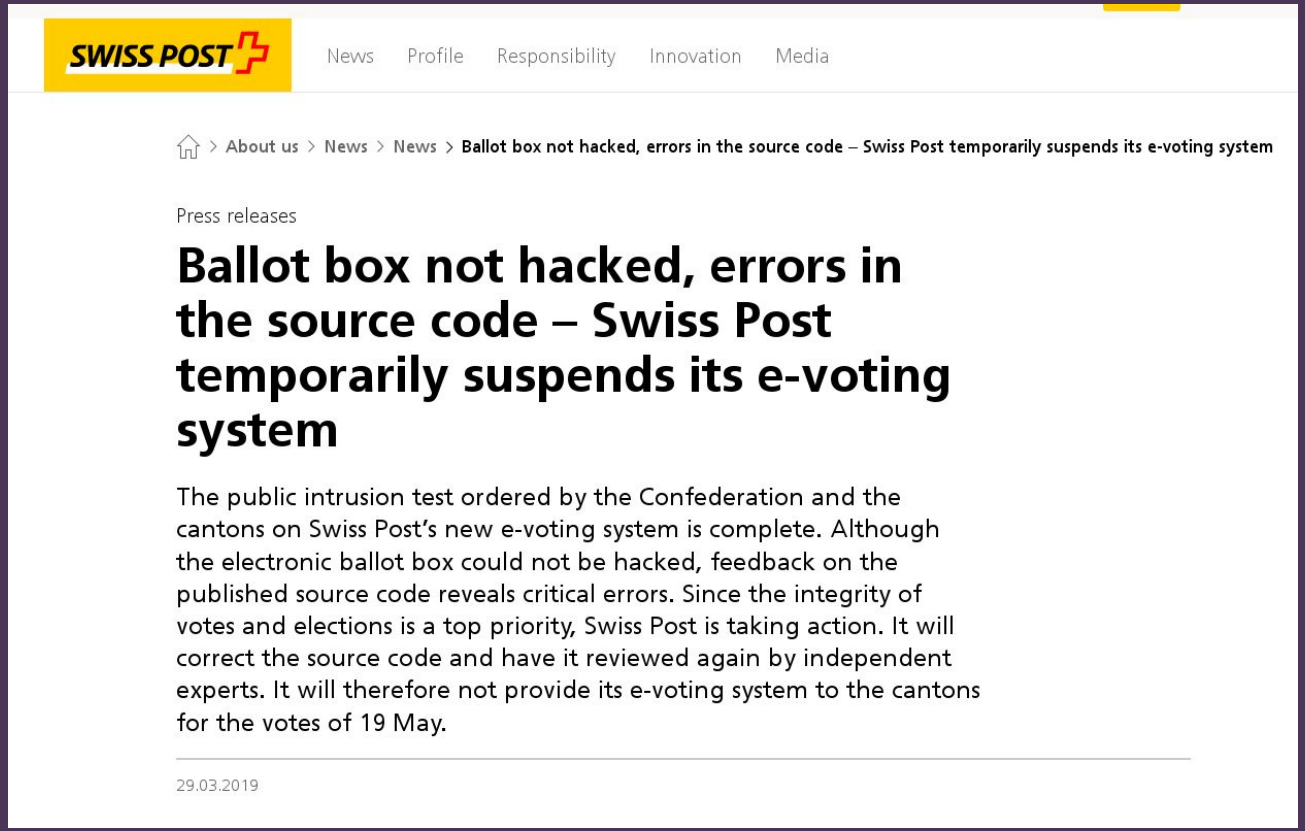
November 2017


Physically isolated infrastructure (air gap)
Ballot
Ballot Box
Voting Card Sets
.....
Election Configuration
Administration Portal
Configuration
Printing Files
Online Voting Channel Configuration Data
OV Channel Configuration Data
Online Voting Channel
Voting Portal
API http
eBallot Box
Cleansing
List of valid votes
List of invalid votes
Cleansed Ballot Box
Mixing
Mixing proofs
eBallot Box
Splunk
Decryption
List of decrypted votes
List of invalid decrypted votes
Decryption proofs

Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. "Addendum to How not to prove your election outcome: The use of non-adaptive zero knowledge proofs in the Scytl-SwissPost Internet voting system, and its implications for cast-as-intended verification" 2019.

https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcomeAddendum.pdf

All the proofs are valid, so E_2 will be used to derive the return codes corresponding to the vote intent v, which will then be accepted by an honest voter, who will have his/her vote confirmed. However, when E_1 is decrypted (after being processed through the mixnet), it will be declared invalid.


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

“It will therefore not provide its e-voting system to the cantons for the votes of 19 May.”

https://www.post.ch/en/about-us/news/news/2019/swiss-post-temporarily-suspends-its-e-voting-system

“Temporarily”

https://www.post.ch/en/about-us/news/news/2019/swiss-post-temporarily-suspends-its-e-voting-system

April 2019

“Last week, a vulnerability was found that affects the individual verifiability process used by the cantons of Thurgau, Neuchâtel, Fribourg and Basel-Stadt”

https://www.scytl.com/en/statement-related-to-the-recent-decision-to-place-evoting-temporarily-on-hold-in-switzerland/

Scytl acknowledges the valuable input provided by the researchers who have participated in this initiative and more concretely to the ones that detected the issues in the source code.

https://www.scytl.com/en/statement-related-to-the-recent-decision-to-place-evoting-temporarily-on-hold-in-switzerland/

“These criticisms are mainly based on misunderstandings related to the cryptographic mechanisms”

https://www.scytl.com/en/statement-recent-comments-regarding-source-code-publication-swiss-e-voting/

Aftermath

SwissPost awarded our research team 5000 CHf

Sarah Jamie Lewis
@SarahJamieLewis

Swiss Post will not be offering their evoting system in the October elections. The "temporary" suspension which followed disclosures of critical security vulnerabilities by @VTeagueAus, Olivier Pereira and myself, is extended.

Worst bug bounty ever?

Swiss Post to focus solely on new system with universal verifiability

Swiss Post has decided to pool its strengths in the e-voting sector and work solely on the new system with universal verifiability. It plans to make the system...

post.ch

The system that was previously in use in four cantons will therefore no longer be operated by Swiss Post... and will not be available for the National Council elections in the autumn.

What Happened In Australia?

Remember the Air-Gap?

Findings

Finding 17: [redacted] on air-gapped (offline) computers was not disabled.

Control:

14.01 The network hosting the internet voting system should be segregated based on the defined security model to achieve defence in depth.

Specified Procedure

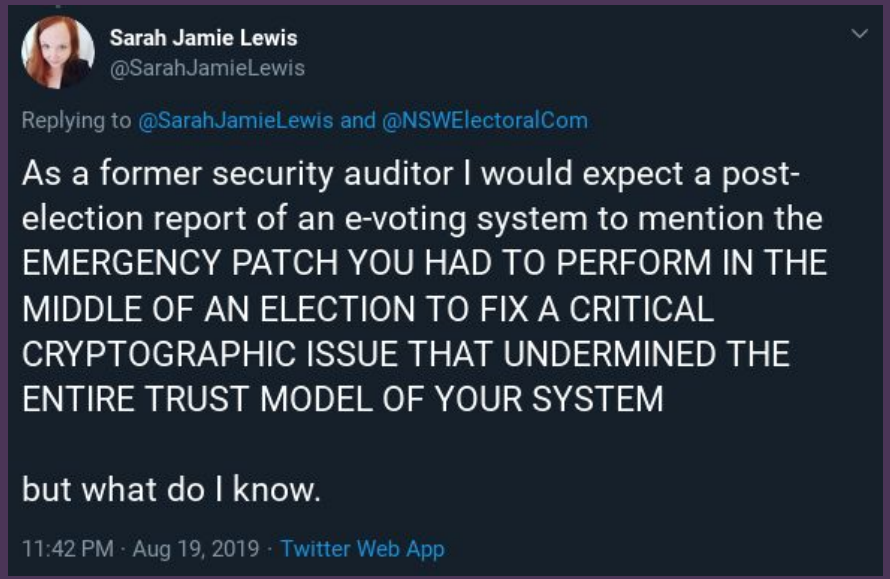
1. Verify if the network hosting the voting system are logically segregated(using VLANs etc.) in order to align with the NSWEC's security model.
2. Verify if voting system and assurance system is segregated.

Finding / Observation

During the review, PwC observed that NSW Electoral Commission used 2 computers for critical tasks such as encryption key generation, mixing of votes, cleansing process and decryption were air-gapped (not connected to any network).

[redacted]

The reports that came out after the election also make no reference to the emergency patch.



Remember....

Prime Minister claims laws of mathematics 'do not apply' in Australia

Malcolm Turnbull makes 'Orwellian' comments when challenged on problem of encryption

Takeaways

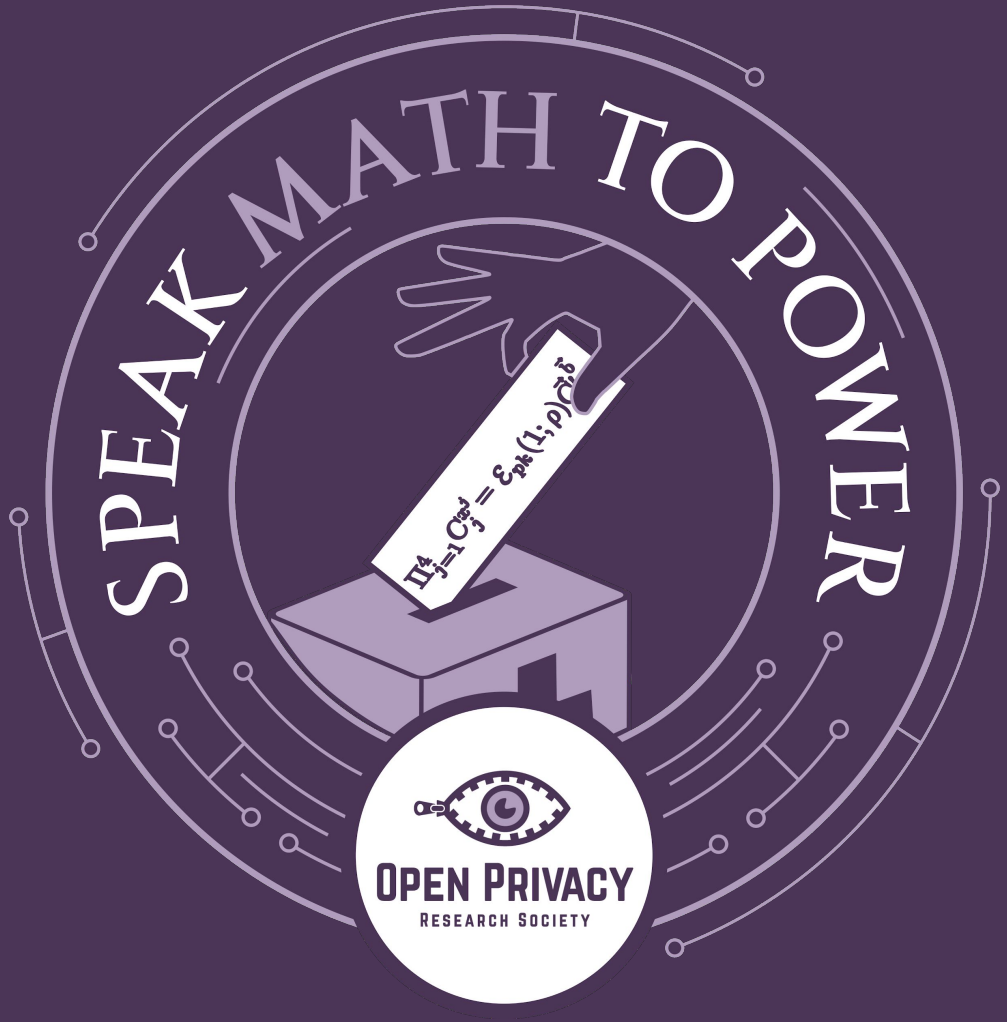
Public Infrastructure Demands Public Scrutiny

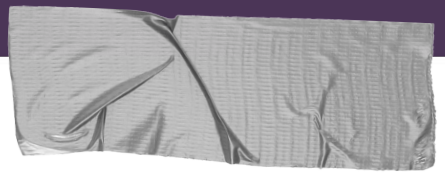
The Math and the Implementation of that Math are different

If researchers working on little to no sleep can break your system, so can actual threat actors.

Transparency is as important as Technology

Swiss Post announced it wants to offer the new system to the cantons for trial operation from 2020.


SPEAK MATH TO POWER
OPEN PRIVACY
RESEARCH SOCIETY



The End!

Open Privacy Research Society is a non-profit dedicated to researching and building privacy-enhancing technologies that benefit marginalized communities.

Please support our work:
https://openprivacy.ca/donate

OPEN PRIVACY
RESEARCH SOCIETY