(In)Security of e-voting

Pascal Lafourcade

UNIVERSITÉ Clermont Auvergne

LIMOS

FIC 2023, April 2023

E-voting a reality

Hauts-De-Seine : Neuilly-Sur-Seine Met En Place Un Système De Vote Électronique

On **Juil 5, 2021**

Le vote électronique fera son retour en 2022

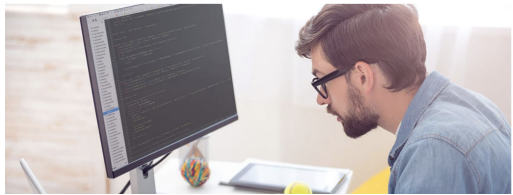
Après la découverte de failles en 2019, tous les projets de scrutin en ligne ont été suspendus. La Poste a cependant poursuivi l'aventure. Elle développe à Neuchâtel un système mieux sécurisé qu'elle soumettra à des hackers

Flaws in E-voting a reality

TECH > VIE NUMÉRIQUE

SUISSE: UNE FAILLE DE SÉCURITÉ "MAJEURE" DANS LE SYSTÈME DE VOTE EN LIGNE

Raphaël Grably Le 13/03/2019 à 11:10



NEWS

Flaw in NSW's iVote platform confirmed by researcher

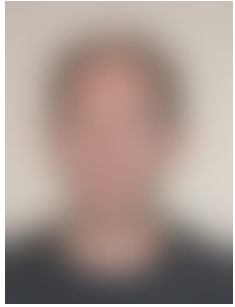
By Rohan Pearce

Editor, Computerworld | NOV 14, 2019 6:08 AM PST

A security researcher has confirmed that the version of New South Wales' online voting platform, iVote, employed during the 2019 election contained a vulnerability that potentially allowed the creation of false decryption proofs for ballots.

Livre

Le Vote électronique



De Pierrick GAUDRY, Véronique CORTIER
256 pages, Odile Jacob 18/05/2022

Outline

Cryptography

Cryptography

Primitives
RSA, Elgamal,
AES, DES, SHA-3...

Security: Cryptography

Cryptography

Primitives
RSA, Elgamal,
AES, DES, SHA-3...

Protocols
Distributed
Programs

Security: Cryptography for a Property

Cryptography

Primitives
RSA, Elgamal,
AES, DES, SHA-3...

Protocols
Distributed
Programs

Security: Cryptography for a Property in an Hostile Environment

Cryptography

Primitives
RSA, Elgamal,
AES, DES, SHA-3...

Protocols
Distributed
Programs

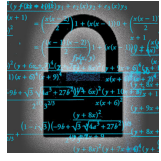
Security: Cryptography for a Property in an Hostile Environment

Cryptography

Verification

Primitives

RSA, Elgamal,
AES, DES, SHA-3...

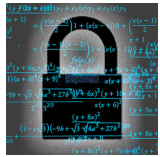


Protocols

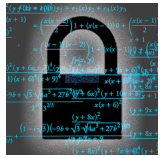
Distributed
Programs

Why Verification is Useful !

Formal Security Verification Team



Formal Security Verification Team

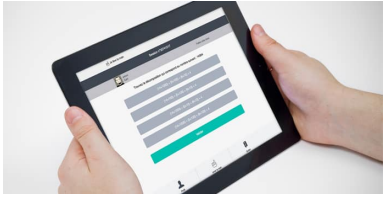


Formal Security Verification Team

Formal Security Verification Team

Outline

E-Voting *vs* Traditional Voting



Vote électronique

Vote traditionnel

+ Accessibility
+ Reducing the abstention rate
+ Automatic counting
+ Less organisation costs

Two e-voting (1/2)

Offline

+ Efficient and fast counting
+ Vote in any voting station
- Trust the machines

Two e-voting (2/2)

Online

+ Vote at home
+ Easy process
+ Less costs
- Possible influence

Voting Protocol Organisation

5 Phases

1. Registration
2. Validation
3. Vote
4. Counting
5. Verification



Security Requirements

Eligibility

Fairness

Universal Verifiability

Individual Verifiability

Secure e-voting protocol

Correctness

Coercion-Resistance

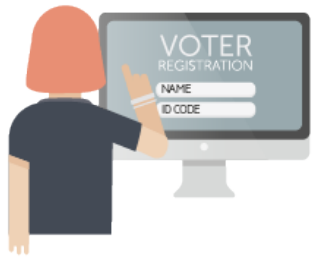
Privacy

Robustness

Receipt-Freeness

Eligibility

Only the registered voters can vote

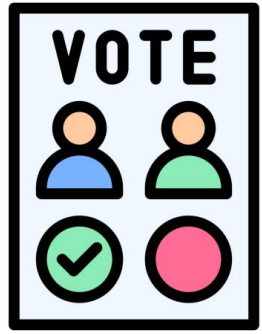


Prevent double voting

Robustness

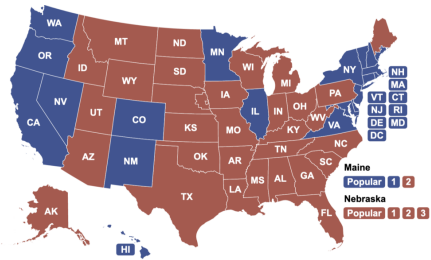
Tolerate a certain number of misbehaving voters

Correctness



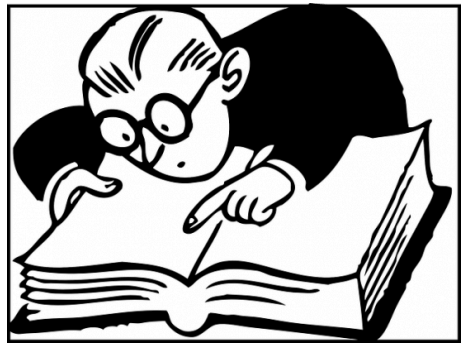
Results should be correct

Fairness



No preliminary results

Individual Verifiability



Each voter can check whether his vote was counted correctly

Universal Verifiability

Anybody can verify that the announced result corresponds to the sum of all votes

Anonymity

Privacy: unlinkability between the voter and his vote

Receipt-Freeness: A voter cannot construct a receipt

Corecion-Resistance: A coercer cannot be sure the voter followed his instructions

Privacy implies Individual Verifiability

2018 Cortier et al.



A system without Individual Verifiability cannot acheive privacy !

Reduction Results: How many agents ?

- Security properties: **two** agents are sufficient.
  2004 by Hubert Comon-Lundh, Véronique Cortier
- When Are **Three Voters** Enough for Privacy Properties?
  2016 by Myrto Arapinis, Véronique Cortier, Steve Kremer

Outline

State of the Art

Several Definitions for Privacy for e-voting protocols:

[DKR09,DKR10,MN06,BHM08,KT09,KSR10,LJP10,SC11,...]

But

- designed for a specific protocol
- often cannot be applied to other protocols

OUR GOAL

Propose fine-grain definitions
to compare security levels of protocols

4 Dimensions for Privacy [DLL'12a, DLL'11]

Modeling in Applied π-Calculus

1. Communication between the attacker and the targeted voter

Vote-Privacy (VP)

Receipt-Freeness (RF)

Coercion-Resistance (CR)

4 Dimensions for Privacy [DLL'12a, DLL'11]

Modeling in Applied π-Calculus

1. Communication between the attacker and the targeted voter

Vote-Privacy (VP)

Receipt-Freeness (RF)

Coercion-Resistance (CR)

2. Intruder is controlling another voter:

Outsider (O)

Insider (I)

4 Dimensions for Privacy [DLL'12a, DLL'11]

Modeling in Applied π-Calculus

1. Communication between the attacker and the targeted voter

Vote-Privacy (VP)

Receipt-Freeness (RF)

Coercion-Resistance (CR)

2. Intruder is controlling another voter:

Outsider (O)

Insider (I)

3. Secure against Forced-Abstention: (FA) or not (PO)

4 Dimensions for Privacy [DLL'12a, DLL'11]

Modeling in Applied π-Calculus

1. Communication between the attacker and the targeted voter

Vote-Privacy (VP) Receipt-Freeness (RF) Coercion-Resistance (CR)

2. Intruder is controlling another voter:

Outsider (O) Insider (I)

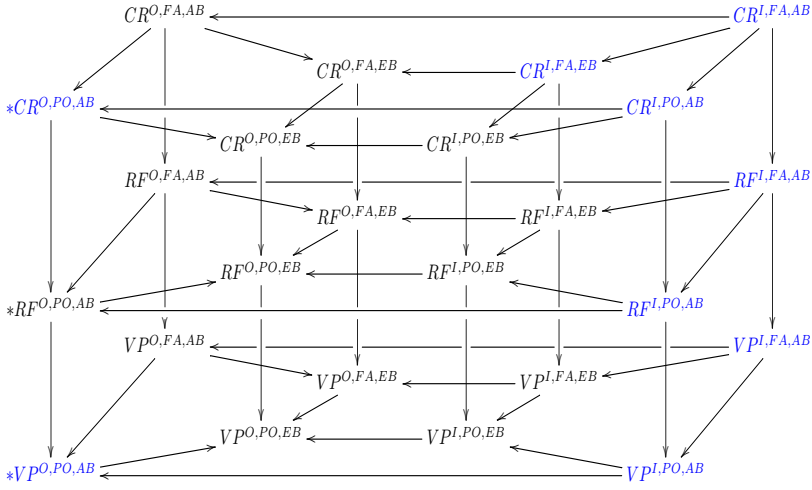
3. Secure against Forced-Abstention: (FA) or not (PO)

4. Honest voters behavior:

$\exists$

$\forall$

Relations among the notions



Outline

Sicilian Attack

Arlette
François
Emanuel
Marine
Jean-Luc
Arnaud
Ségolène
Jacques
Georges
Charles
Jean-Marie
Valérie

With 12 candidates, $>$ 479 millions possible combinations!

$> 2,000,000$ votes have been cast

`https://vote.heliosvoting.org/`

Helios code is Open Source
Based on scientific papers
Use mixnet

Attacking and fixing Helios

By V. Cortier et al in 2010

Replaying a voter's ballot

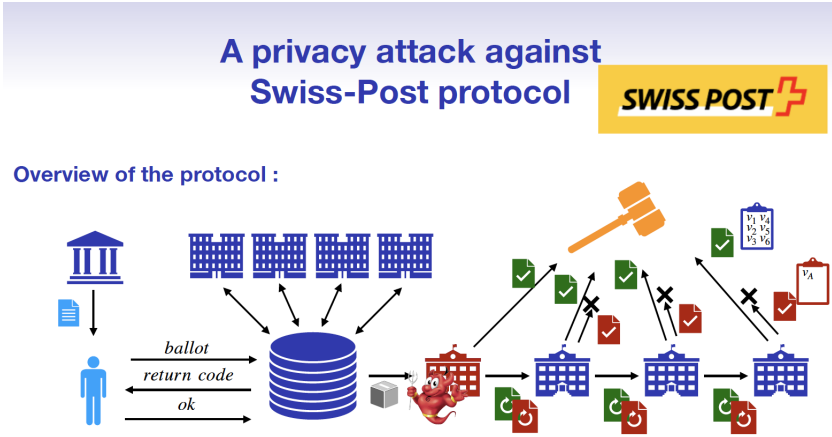
- Alice votes A
- Bob votes B
- Charlie votes like Alice

This attack works on other protocols like Lee et al and Sako et al.

Belenios

`https://www.belenios.org/`
Belenios code is Open Source

Swiss Post Attack (Bug Bounty 40Keuros)



Cortier et al. RWC'22

Russian Online Election

In 2019, Breaking the encryption scheme of the Moscow Internet voting system by P. Gaudry et al

- Elgamal key sizes are too small (CADO-NFS)
- Counting the number of votes cast for a candidate.

1994 Benaloh's Scheme

$$enc(a, pk_S) * enc(b, pk_S) = enc(a + b, pk_S)$$

Partial homomorphic are widely used in voting schemes

$$\prod enc(v_i, pk_S) = enc(\sum v_i, pk_S)$$

Original Benaloh's scheme is ambiguous

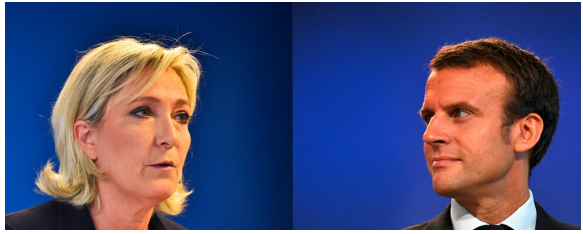
$$dec(enc(14, pk_S), sk_S) = 14 \mod 15 \text{ or } 14 \mod 5 = 4$$

Revisited Benaloh's encryption [FLA'11]

- Drawing false parameters: 33%
- Proposition of corrected version
- Proof using Kristian Gjosteen result.

Impact

Example with 15 voters



$\{0\}_{pk_S}$ $\{1\}_{pk_S}$

- $\prod enc(v_i, pk_S) = enc(\sum v_i, pk_S) = enc(14, pk_S)$
- Result can be either 14 or 4

Clash Attack on the verifiability of e-voting systems

By 2012 Kuesters et al.

Different voters with the same receipt

$\Rightarrow$ Authorities can manipulate the election without being detected

Attacks

- In 2007, Security Analysis of the Diebold AccuVote-TS Voting Machine
- In 2012, Attacking the Washington, D.C. Internet Voting System
- In 2017 Voting Machine Hacking Village by Matt Blaze et al.

Machines :

- AVS WinVote DRE
- Premier AccuVote TSx DRE
- ES&S iVotronic DRE
- PEB version 1.7c-PEB-S
- Sequoia AVC Edge DRE
- Diebold Express Poll 5000 electronic pollbook

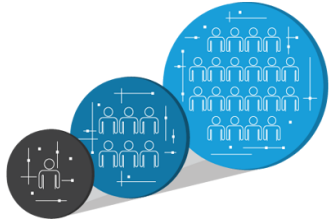
With limited resources and information, they can be hacked.

Outline

Summary

- Voting is important for democracy
- Protocols must be open
- Design of voting protocols is not easy
- Formal Verification can help
- Proving all properties togheter is difficult

Future Work



- Scalability
- Human aspect are not yet taken into account
- End-to-end verification
- All properties in one tool !

Thank you for your attention.