Introduction to SecVote 2010

Hugo Jonker

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

1. Collect individual preferences.

Elections

Elections:

a way to establish the preference of a group,
based on the preferences of the individual members.

1. Collect individual preferences.
2. Derive group preference.

Scope of SecVote 2010

Focus on

- collecting the individual preferences.
- cryptographic/computer science point of view.

Requirements

Universal Declaration of Human Rights, article 21, sub 3:

> *The will of the people shall be the basis of the authority of government;*
>
> *this will shall be expressed in periodic and **genuine** elections which shall be by universal and equal suffrage and shall be held by **secret vote** or by equivalent free voting procedures.*

Requirements

Universal Declaration of Human Rights, article 21, sub 3:

> *The will of the people shall be the basis of the authority of government;*
>
> *this will shall be expressed in periodic and* ***genuine*** *elections which shall be by universal and equal suffrage and shall be held by* ***secret vote*** *or by equivalent free voting procedures.*

- some form of assurance needed.

Requirements

Universal Declaration of Human Rights, article 21, sub 3:

> *The will of the people shall be the basis of the authority of government;*
>
> *this will shall be expressed in periodic and* ***genuine*** *elections which shall be by universal and equal suffrage and shall be held by* ***secret vote*** *or by equivalent free voting procedures.*

- some form of assurance needed.
- some form of privacy needed.

Assurance

Nedap: “our machine is not a computer.”

Assurance

Nedap: “our machine is not a computer.”

Assurance

- Claim of correctness is insufficient. . .
- . . . actual correctness is insufficient as well!

Assurance

- Claim of correctness is insufficient. . .
- . . . actual correctness is insufficient as well!

What we want: **verifiability** of result.

privacy = tricky

Italian attack

Luxembourgian central district ballot:

1. ADR	...	7. KPL
1-1. J. Henckes ☐ ☐	...	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	...	7-21. M. Tani ☐ ☐

Italian attack

Luxembourgian central district ballot:

1. ADR	...	7. KPL
1-1. J. Henckes ☐ ☐	...	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	...	7-21. M. Tani ☐ ☐

- voter marks 21 boxes.

Italian attack

Luxembourgian central district ballot:

1.	ADR			· · ·	7.	KPL	
1-1.	J. Henckes	■	■	· · ·	7-1.	P. Back	□	□
⋮				⋮	⋮		
1-21.	F. Zeutzius	□	□	· · ·	7-21.	M. Tani	□	□

- voter marks 21 boxes.

Italian attack

Luxembourgian central district ballot:

1.	ADR			···	7.	KPL	
1-1.	J. Henckes	■	■	···	7-1.	P. Back	□ □
⋮				⋮	⋮		
1-21.	F. Zeutzius	□	□	···	7-21.	M. Tani	□ □

- voter marks 21 boxes.
- pick 2. That leaves $\binom{292}{19} =$ 314,269,098,408,967,151,724,980,483,800 ways to fill in ballot.

Italian attack

Luxembourgian central district ballot:

1.	ADR		···	7.	KPL
1-1.	J. Henckes	■ ■	···	7-1.	P. Back □ □
⋮			⋮	⋮	
1-21.	F. Zeutzius	□ □	···	7-21.	M. Tani □ □

- voter marks 21 boxes.
- pick 2. That leaves $\binom{292}{19} =$ 314,269,098,408,967,151,724,980,483,800 ways to fill in ballot.

- what can the ballot reveal about who voted?

helpful voters

helpful voters

- receipt-freeness:
  Voter cannot prove how she voted *after voting*.

helpful voters

- receipt-freeness:
  Voter cannot prove how she voted *after voting*.
- coercion-resistance:
  Voter cannot prove anything on how she voted.

Summing up

Needed:

- Privacy,
- Verifiability.

Informally:

Summing up

Needed:

- Privacy,
- Verifiability.

Informally:

- Privacy: no one can learn how I voted.
- Verifiability: I can verify the process.
  e.g.: I can verify my vote counts correctly.

Summing up

Needed:

- Privacy,
- Verifiability.

Informally:

- Privacy: no one can learn how I voted.
- Verifiability: I can verify the process.
  e.g.: I can verify my vote counts correctly.

How to resolve?

Reconciling privacy and verifiability

We need:

- *(cryptographics) tools*, to create
- *voting systems*, that can be
- *verified* to be secure.

Cryptography

Vanessa Teague

University of Melbourne

Douglas Wikström

KTH Sweden

Jens Groth

University College London

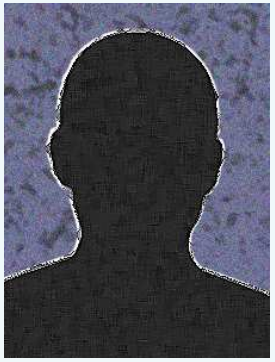
Voting Systems

James Heather

University of Surrey

Peter Ryan

University of Luxembourg

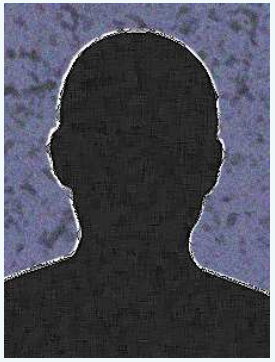


Tal Moran

Harvard University

Michael Clarkson

Cornell University



Jacques Traoré

Orange Labs

Analysis & verification

Steve Kremer

LSV & INRIA

Ralf Küsters

University of Trier

Stephanie Delaune

LSV & CNRS

Thanks!

Thank you for your attention.

Questions/comments?