A Formal Taxonomy of Privacy in Voting Protocols

Jannik Dreier, Pascal Lafourcade, Yassine Lakhnech

Université Grenoble 1, CNRS, Verimag, France

First IEEE International Workshop on Security and Forensics in Communication Systems, Ottawa, Canada
June 15, 2012

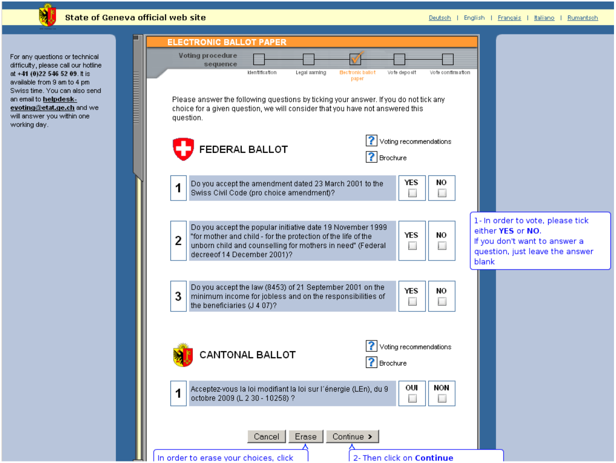
Electronic voting machines. . .

. . . are used all over the world

Internet voting

Available in

- Estonia
- France
- Switzerland
- ...



Security Requirements

Fairness

Individual Verifiability

Eligibility

Universal Verifiability

Security Requirements

Privacy

Vote-Independence

Receipt-Freeness

Robustness

Coercion-Resistance

Security Requirements

Fairness

Individual Verifiability

Eligibility

Universal Verifiability

Security Requirements

Vote-Independence

Privacy

Receipt-Freeness

Robustness

Coercion-Resistance

How to secure electronic voting?

Idea: Use formal methods to find bugs and increase confidence

- Need for formal definitions
- Lots of related work: [?, ?, ?, ?, ?, ?, ?]...

Ideally we need definitions that

- can be applied on any protocol
- are comparable
- include known threats: coercion, vote-buying, vote-copying, forced abstention
- are suitable for automation

Plan

1. Introduction
2. Definitions: Four Dimensions
   - Communication
   - Vote-Independence
   - Forced Abstention
   - Knowledge about honest voters
3. Analysis and Case Studies
4. Conclusion

Plan

Four Dimensions

- Communication: Vote-Privacy (VP), Receipt-Freeness (RF), Coercion-Resistance (CR)
- Vote-Independence: Outsider (O), Insider (I)
- Forced Abstention Attacks: Participation Only (PO), Security against Forced-Abstention-Attacks (FA)
- Knowledge about honest voters: Exists Behavior (EB), Any Behavior (AB)

Plan

Vote-Privacy (VP)

Main idea: Observational equivalence between two situations.

	Alice	Bob
Vote	$\boxed{A}$	$\boxed{B}$
	$\approx_l$	
Vote	$\boxed{B}$	$\boxed{A}$

The Applied Pi Calculus [?]

Syntax

$P, Q, R :=$	processes
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	restriction (“new”)
$\texttt{if } M = N \texttt{ then } P \texttt{ else } Q$	conditional
$\texttt{in}(u, x).P$	message input
$\texttt{out}(u, x).P$	message output
$\{^{M}/_{x}\}$	active substitution

Vote-Privacy: The formal definition

Definition (Vote-Privacy)

A voting process respects *Vote-Privacy (VP)* if for all votes σ_{v_A} and σ_{v_B} we have

$$VP'\left[V\sigma_{id_A}\sigma_{f_A}\sigma_{v_A}\middle|V\sigma_{id_B}\sigma_{f_B}\sigma_{v_B}\right] \approx_l VP'\left[\sigma_{id_A}\sigma_{f_A}\sigma_{v_B}\middle|V\sigma_{id_B}\sigma_{f_B}\sigma_{v_A}\right]$$

Receipt-Freeness (RF)

Again: Observational equivalence between two situations, but Alice tries to create a receipt or a fake.

Mallory	Alice	Bob
	$\boxed{\text{A}}$	$\boxed{\text{B}}$
	$\approx_l$	
	$\boxed{\text{B}}$	$\boxed{\text{A}}$

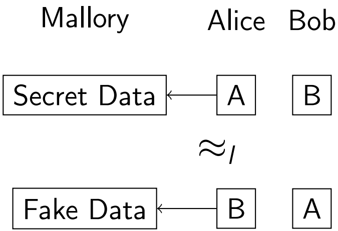
Receipt-Freeness (RF)

Again: Observational equivalence between two situations, but Alice tries to create a receipt or a fake.

$$
\begin{array}{ccc}
\text{Mallory} & \text{Alice} & \text{Bob} \\
\boxed{\text{Secret Data}} \leftarrow & \boxed{A} & \boxed{B} \\
 & \approx_l & \\
\boxed{\text{Fake Data}} \leftarrow & \boxed{B} & \boxed{A}
\end{array}
$$

Coercion-Resistance (CR)

Observational equivalence between two situations, but Alice is under control by Mallory or only pretends to be so.



Coercion-Resistance (CR)

Observational equivalence between two situations, but Alice is under control by Mallory or only pretends to be so.

$$\text{Mallory} \xrightarrow{\text{Orders}} \text{Alice} \quad \text{Bob}$$

$$\boxed{\text{Secret Data}} \longleftarrow \boxed{A} \quad \boxed{B}$$

$$\approx_l$$

$$\boxed{\text{Fake Data}} \longleftarrow \boxed{B} \quad \boxed{A}$$

Plan

Insider (I) vs. Outsider (O)

Main idea: Privacy, but with a voter under control of the attacker. If he can relate his vote to e.g. Alice's vote, Mallory can distinguish both sides.

Mallory		Alice	Bob
	Vote	A	B
			$\approx_I$
	Vote	B	A

Insider (I) vs. Outsider (O)

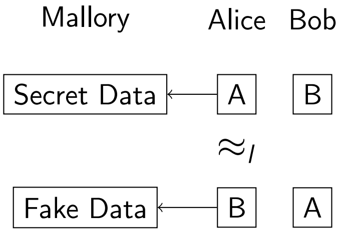
Main idea: Privacy, but with a voter under control of the attacker. If he can relate his vote to e.g. Alice's vote, Mallory can distinguish both sides.

Orders

Mallory	Alice	Bob	Chuck
Vote	$\boxed{A}$	$\boxed{B}$	$\boxed{?}$
		$\approx_I$	
Vote	$\boxed{B}$	$\boxed{A}$	$\boxed{?}$

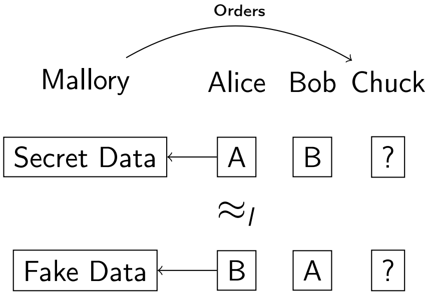
Can we combine Vote-Independence with Receipt-Freeness?

"Receipt-Freeness with Chuck":



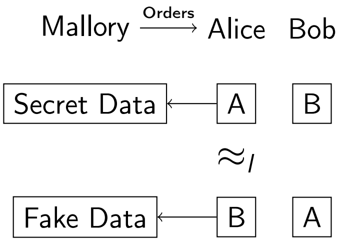
Can we combine Vote-Independence with Receipt-Freeness?

"Receipt-Freeness with Chuck":



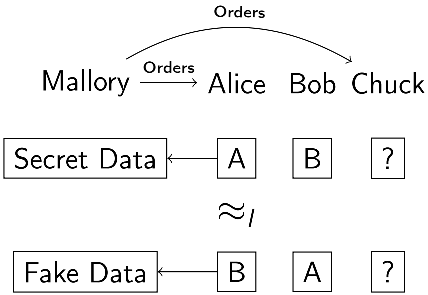
And with Coercion-Resistance?

“Coercion-Resistance with Chuck”:



And with Coercion-Resistance?

"Coercion-Resistance with Chuck":



Plan

Security against Forced Abstention Attacks (FA) vs. Participation Only (PO)

Alice abstains or votes in turn with Bob:

	Alice	Bob
Vote	$\boxed{A}$	$\boxed{B}$
	$\approx_l$	
Vote	$\boxed{B}$	$\boxed{A}$

Security against Forced Abstention Attacks (FA) vs. Participation Only (PO)

Alice abstains or votes in turn with Bob:

	Alice	Bob
Vote		$\boxed{\text{B}}$

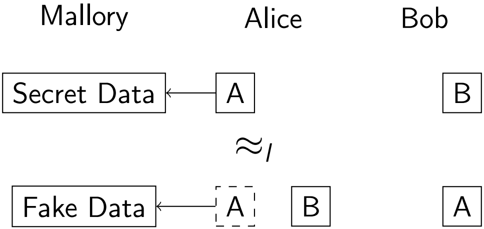
$$\approx_l$$

	Alice	Bob
Vote	$\boxed{\text{B}}$	

Plan

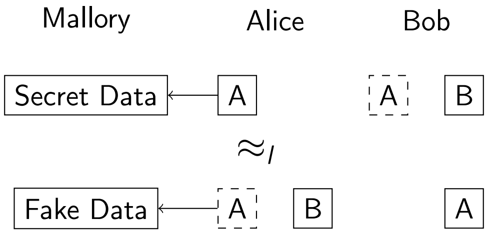
Introducing Fakes: Exists Behavior (EB) vs. Any Behavior (AB)

Some protocols use fake votes [?] to achieve Receipt-Freeness and Coercion-Restistance.



Introducing Fakes: Exists Behavior (EB) vs. Any Behavior (AB)

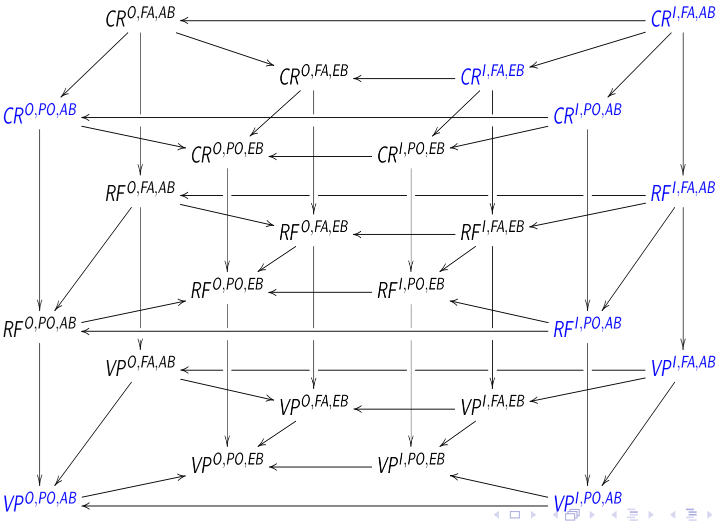
Some protocols use fake votes [?] to achieve Receipt-Freeness and Coercion-Restistance.



Plan

1. Introduction
2. Definitions: Four Dimensions
   - Communication
   - Vote-Independence
   - Forced Abstention
   - Knowledge about honest voters
3. Analysis and Case Studies
4. Conclusion

Relations among the notions



Plan

Conclusion

- Generalized model
- New modular definition
- Includes known threats
- Hierarchy of notions
- Allows fine-grained comparison of different types of protocols
- Can be automatically verified using existing tools (within certain complexity limits)

Future Work

- Automate and/or automatically verify more of the proofs
- Computational definition

Thank you for your attention!

Questions?

Existing definitions

- [?, ?]: Tailored to a specific protocol
- [?, ?]: Unsuitable for protocol by Juels/Civitas
- [?, ?]: Vote-Independence based on definitions by [?, ?]
- [?]: Coercion Resistance, very fine-grained $\rightarrow$ difficult to compare
- [?]: Privacy as unlinkability, unsuitable for automated verification
- ...

Case Studies

Protocol	Priv. Notion	Comments
Juels et al. [?]	$CR^{I,FA,EB}$	Requires fakes to achieve CR
Bingo Voting [?]	$CR^{I,PO,AB}$	Trusted voting machine
- variant	$CR^{I,FA,AB}$	Secure against forced abstention
Lee et al. [?]	$CR^{O,PO,AB}$	Vulnerable to vote-copying
Okamoto [?]	$RF^{I,PO,AB}$	Based on trap-door commitments
- variant	$RF^{I,FA,AB}$	Private channel to administrator
Fujioka et al. [?]	$VP^{I,PO,AB}$	Based on blind signatures
- variant	$VP^{I,PO,AB}$	Permits multiple votes
Simp. Voting Prot.	$VP^{O,PO,AB}$	Vulnerable to vote-copying

Modeling a voting protocol

Definition (Voting Protocol)

A voting protocol is a tuple of processes $(V, A_1, \ldots, A_m)$ where V is the process that is executed by the voter, and the A_j's are the processes executed by the election authorities.

Definition (Voting Process)

A voting process of a voting protocol $(V, A_1, \ldots, A_m)$ is a closed plain process

$$VP = \nu\tilde{n}.(V\sigma_{id_1}\sigma_{f_1}\sigma_{v_1}|\ldots|V\sigma_{id_n}\sigma_{f_n}\sigma_{v_n}|A_1|\ldots|A_l)$$

We define an evaluation context VP' which is like VP, but has a hole instead of two $V\sigma_i$.

Definition (Process P^{ch} [?])

Let P be a process and ch be a channel. We define P^{ch} as follows:

- $0^{ch} \triangleq 0$,
- $(P|Q)^{ch} \triangleq P^{ch}|Q^{ch}$,
- $(\nu n.P)^{ch} \triangleq \nu n.\mathtt{out}(ch, n).P^{ch}$ when n is a name of base type,
- $(\nu n.P)^{ch} \triangleq \nu n.P^{ch}$ otherwise,
- $(\mathtt{in}(u, x).P)^{ch} \triangleq \mathtt{in}(u, x).\mathtt{out}(ch, x).P^{ch}$ when x is a variable of base type,
- $(\mathtt{in}(u, x).P)^{ch} \triangleq \mathtt{in}(u, x).P^{ch}$ otherwise,
- $(\mathtt{out}(u, M).P)^{ch} \triangleq \mathtt{out}(u, M).P^{ch}$,
- $(!P)^{ch} \triangleq !P^{ch}$,
- $(\mathtt{if}\ M = N\ \mathtt{then}\ P\ \mathtt{else}\ Q)^{ch} \triangleq \mathtt{if}\ M = N\ \mathtt{then}\ P^{ch}\ \mathtt{else}\ Q^{ch}$.

Definition (Process P^{c_1,c_2} [?])

Let P be a process, c_1, c_2 channels. We define P^{c_1,c_2} as follows:

- $0^{c_1,c_2} \triangleq 0$,
- $(P|Q)^{c_1,c_2} \triangleq P^{c_1,c_2}|Q^{c_1,c_2}$,
- $(\nu n.P)^{c_1,c_2} \triangleq \nu n.\mathtt{out}(c_1,n).P^{c_1,c_2}$ if n is a name of base type,
- $(\nu n.P)^{c_1,c_2} \triangleq \nu n.P^{c_1,c_2}$ otherwise,
- $(\mathtt{in}(u,x).P)^{c_1,c_2} \triangleq \mathtt{in}(u,x).\mathtt{out}(c_1,x).P^{c_1,c_2}$ if x is a variable of base type & x is a fresh variable,
- $(\mathtt{in}(u,x).P)^{c_1,c_2} \triangleq \mathtt{in}(u,x).P^{c_1,c_2}$ otherwise,
- $(\mathtt{out}(u,M).P)^{c_1,c_2} \triangleq \mathtt{in}(c_2,x).\mathtt{out}(u,x).P^{c_1,c_2}$,
- $(!P)^{c_1,c_2} \triangleq !P^{c_1,c_2}$,
- $(\mathtt{if}\ M = N\ \mathtt{then}\ P\ \mathtt{else}\ Q)^{c_1,c_2} \triangleq \mathtt{in}(c_2,x).\mathtt{if}\ x = \mathrm{true}$ $\mathtt{then}\ P^{c_1,c_2}\ \mathtt{else}\ Q^{c_1,c_2}$ where x is a fresh variable and true is a constant

Definition (Process $A^{\setminus out(ch,\cdot)}$ [?])

Let A be an extended process. We define the process $A^{\setminus out(ch,\cdot)}$ as $\nu ch.(A|!\mathrm{in}(ch,x))$.

Definition (Equivalence in a Frame)

Two terms M and N are equal in the frame ϕ, written $(M = N)\phi$, if and only if $\phi \equiv \nu \tilde{n}.\sigma$, $M\sigma = N\sigma$, and $\{\tilde{n}\} \cap (fn(M) \cup fn(N)) = \emptyset$ for some names $\tilde{n}$ and some substitution σ.

Definition (Static Equivalence ($\approx_s$))

Two closed frames ϕ and ψ are statically equivalent, written $\phi \approx_s \psi$, when $\mathrm{dom}(\phi) = \mathrm{dom}(\psi)$ and when for all terms M and N $(M = N)\phi$ if and only if $(M = N)\psi$. Two extended processes A and B are statically equivalent ($A \approx_s B$) if their frames are statically equivalent.

Definition (Labelled Bisimilarity ($\approx_l$))

Labelled bisimilarity is the largest symmetric relation $\mathcal{R}$ on closed extended processes, such that $A \ \mathcal{R} \ B$ implies

1. $A \approx_s B$,
2. if $A \rightarrow A'$, then $B \rightarrow B'$ and $A' \ \mathcal{R} \ B'$ for some B',
3. if $A \xrightarrow{\alpha} A'$ and $fv(\alpha) \subseteq \mathrm{dom}(A)$ and $bn(\alpha) \cap fn(B) = \emptyset$, then $B \rightarrow^* \xrightarrow{\alpha} \rightarrow^* B'$ and $A' \ \mathcal{R} \ B'$ for some B'.