# Formal Verification of e-Reputation Protocols[1]

Ali Kassem[2], Pascal Lafourcade[1], Yassine Lakhnech[2]

[1]University d'Auvergne, LIMOS
[2]Université Grenoble Alpes, CNRS, VERIMAG

The 7th International Symposium on Foundations & Practice of Security FPS'2014, Montréal

November 4, 2014

[1]This research was conducted with the support of the "Digital trust" Chair from the Foundation of the University of Auvergne.

# Reputation Systems


**Reputation systems:** quantify the trust between different users.

**Application:**

- Electronic commerce
- Social news
- Peer-to-peer routing
- etc.

**Goal:** act in truthfulness way.

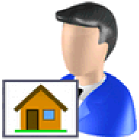
# E-Reputation Players

**Three Players:** different interest.

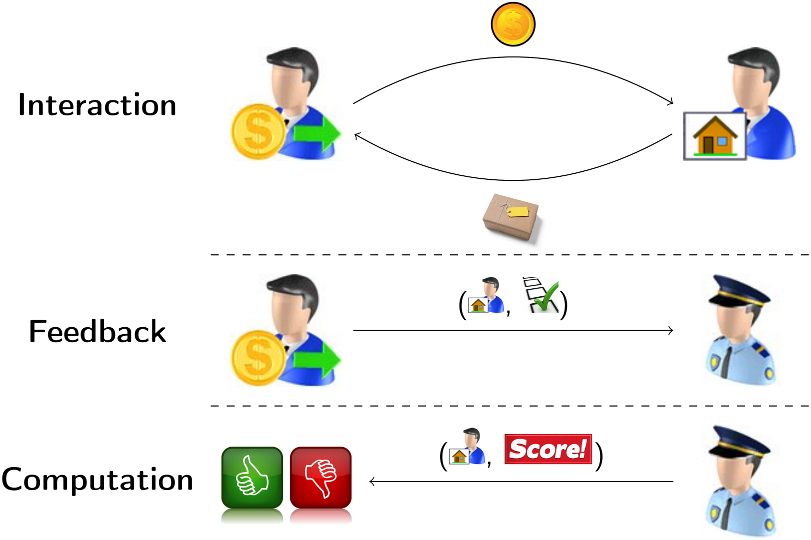
**User**

**Authority**

**Target**



# How they work?



# Requirements

**To be beneficial:** users have to provide fedbacks

↦ preserve their **privacy** and **anonymity**

**To rely on them:** compute the score correctly

↦ score **verifiability**

# Related Work

**Related Work:**

- Several **secure** e-reputation protocols:
  - Supporting Privacy in Decentralized Additive Reputation Systems [**?**]
  - Signatures of Reputation [**?**]
  - Extending Signatures of Reputation [**?**]
  - etc.
- **Definitions** of the security properties are only **informal**.
- **No tool** to check whether a reputation protocol satisfies the security properties.

# Contributions

**Contributions:**

- **Formalize** e-reputation protocols in the applied $\pi$-calculus.
- Formal definitions of **Privacy**, **Authentication** and **Verifiability** properties.
- **Automated verification in ProVerif** of Pavlov *et al.* reputation protocol [?]

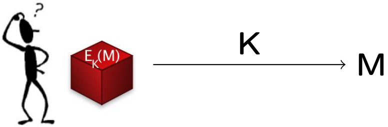
# Plan

# Plan

# Attacker

**Dolev-Yao** [?] attacker:

- controls the **public** channels
- read, block, modify and send **messages**
- under **perfect** cryptographic assumption



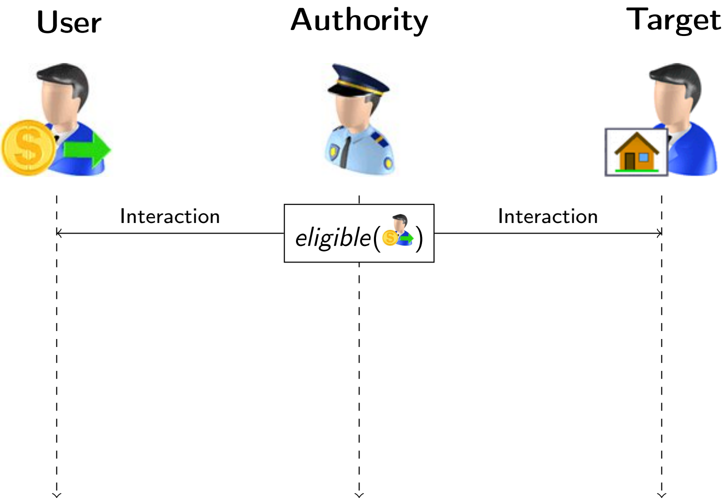
# Processes

Players as **processes** in the applied $\pi$-calculus [?]

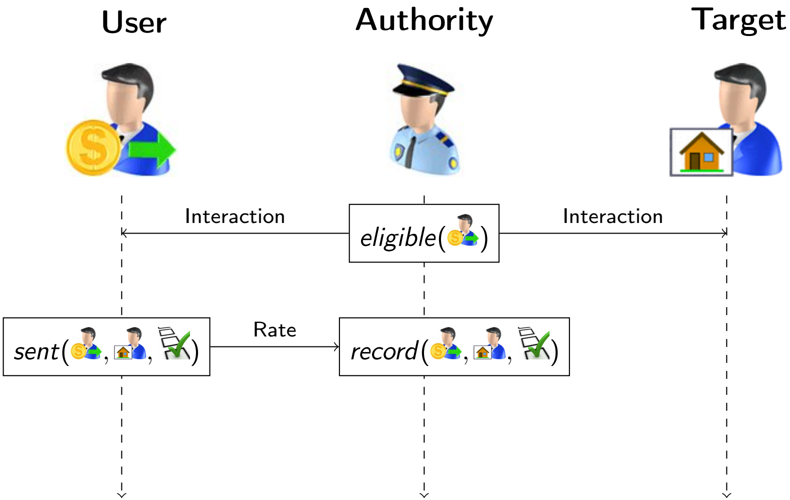
| | |
|---|---|
| $P, Q ::=$ | Processes |
| $0$ | null process |
| $in(u, x).P$ | message input |
| $out(u, m).P$ | message output |
| $\nu n.P$ | name restriction |
| if $m = m'$ then $P$ else $Q$ | conditional |
| $P \mid Q$ | parallel composition |
| $!P$ | replication |

Annotated using **events**

# Events



# Events

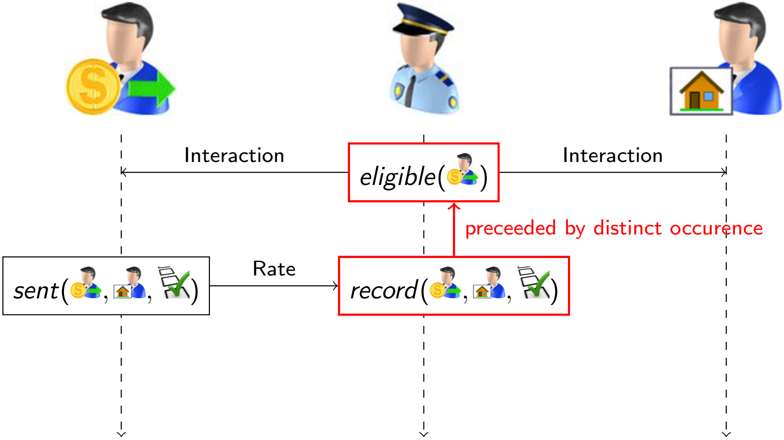

User
Authority
Target
Interaction
eligible( )
Interaction
sent( , , )
Rate
record( , , )

# Plan

# User Eligibility

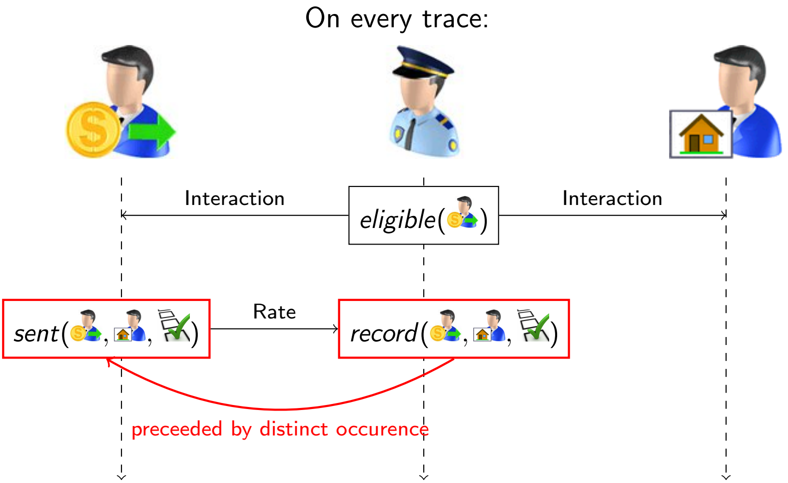
All recorded rates are casted by eligible users, and only one rate per user.

On every trace:



# Rate Integrity

Rates are recorded as casted without modification.

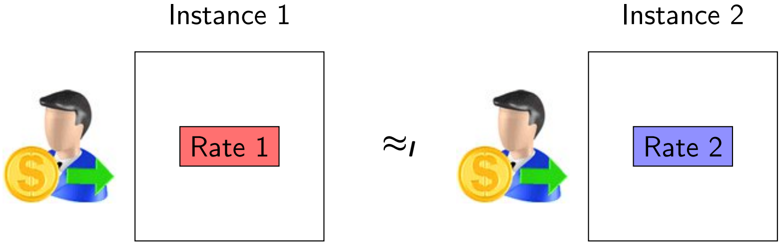


# Plan

# Rate Privacy

**No information** about the rates is leaked.

Observational equivalence of two instances

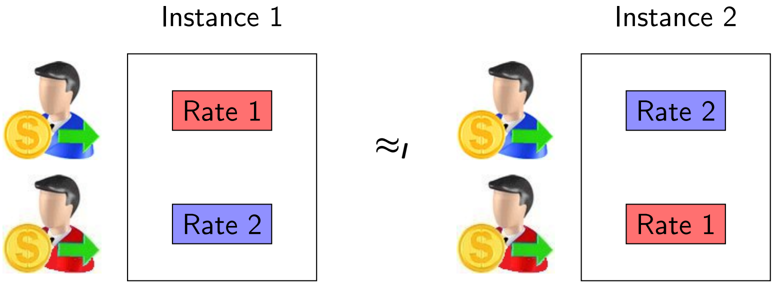



Can be considered with or without dishonest users.

# Rate Anonymity

An attacker cannot **link** a rate to a user.

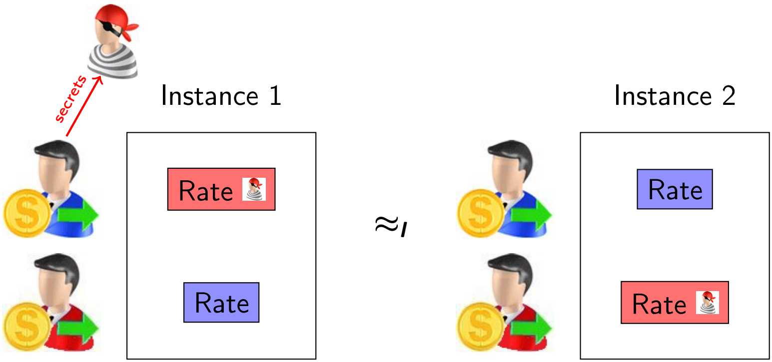
Observational equivalence of two instances




Can be considered with or without dishonest users and target.

# Receipt-Freeness

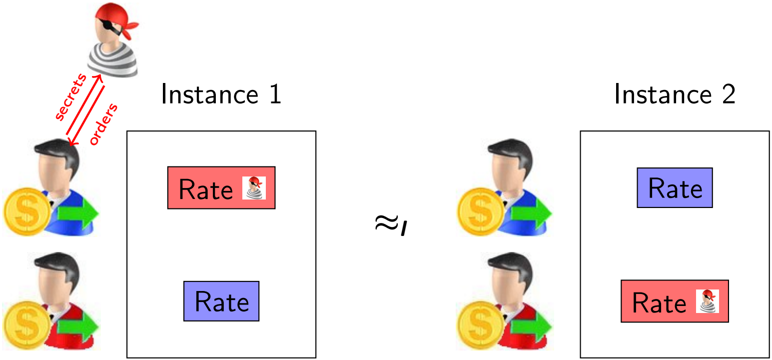
A user cannot **prove** to an attacker that he provided a certain rate




The coerced user cooperates with the attacker by **leaking secrets**.

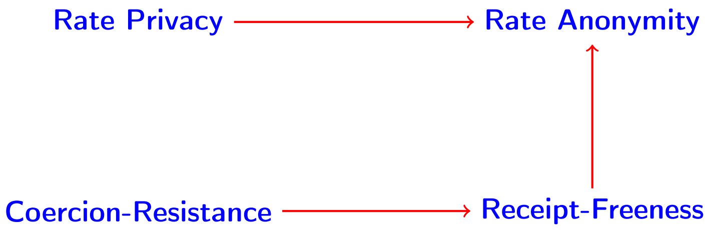
# Coercion-Resistance

Even when interacting with a coercer, the user can still provide a rate of **his choice**.




The coerced user is forced by the attacker to provide **Rate**.

# Relations


Rate Privacy
Rate Anonymity
Coercion-Resistance
Receipt-Freeness

# Plan

# Verifiability for Reputation Protocols

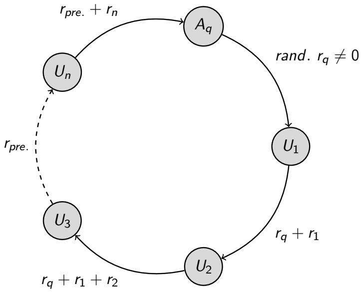
**Definition (Verifiability):**

A reputation protocol ensures *Verifiability* if there are Verification tests UEV, RSV respecting the following conditions:

1. **User Eligibility Verifiability (UEV):**
   - $UEV = true \Rightarrow$ all rates are casted by eligible users
2. **Reputation Score Verifiability (RSV):**
   - $RSV = true \Rightarrow$ the reputation score is computed correctly from the casted rates
3. **Completeness:** if all participants follow the protocol honestly, the above tests succeed.

# Plan

# Application: Pavlov *et al.* Protocol [?]




**Score:** $A_q$ subtracts $r_q$ from the summation.

**Assumption:** secure authenticated channels between users.

**Goal:** ensure rate privacy if all users act honestly

# Modeling in ProVerif

We model the protocol in ProVerif for two users in addition to $A_q$.

**Addition and Subtraction:**

$$
\begin{aligned}
sub(sum(x, y), x) &= y \\
sub(sum(x, y), y) &= x \\
sub(sum(sum(x, y), z), x) &= sum(y, z) \\
sub(sum(sum(x, y), z), y) &= sum(x, z)
\end{aligned}
$$

**Secure Authenticated Channels:**

- encrypt the exchanged messages
- include the unique identities of the sender and the receiver in the messages

# Results

Formal Verification with ProVerif [?]:

| Property | Result |
|---|---|
| Rate Privacy | ✓ |
| Rate Anonymity | ✓ |
| Receipt-Freeness | × |
| Coercion-Resistance | × |
| Rate Integrity | ✓ [2] |
| User Eligibility | ✓ |
| Reputation Score Verifiability | ✓[3] |
| User Eligibility Verifiability | × |

**Time:** less than one second with standard PC.

[2] without injectivity

[3] if the rates are published in a Bulletin Board

# Attacks

**Receipt-Freeness:** the shared symmetric **key k** can act as a **recipet**.

$$r_i = decrypt(r_p + r_i, k) - decrypt(r_p, k)$$

$\Rightarrow$ **Coercion-Resistance** is not ensured also.

**User Eligibility Verifiability:** users do not provide any proof (*e.g.*, certificate) of their eligibility.

# Plan

# Conclusion

**Conclusion:**

- **E-reputation** protocols have many applications
- **Secure** reputation protocols exist
- **Lack** of formal verification
- **First formal framework** for analysis of e-reputation:
  - Formal model in the **applied** $\pi$**-calculus**
  - **Definitions** for privacy, authentication, verifiability properties
- **Automated verification** in ProVerif of one case study.

# Future Work

**Future work:**

- Analyze more reputation protocols
- Study properties such as : correctness, accountability, . . .
- Verify other protocols such as: e-cash, . . .

# Thank you for your attention!

**Questions?**

ali.kassem@imag.fr
pascal.lafourcade@udamail.fr