A Framework to Provide Anonymity in Reputation Systems

Mobiquitous 2006

Hugo Miranda and Luís Rodrigues

Universidade de Lisboa
LaSIGE

Privacy is good...

- Users should be allowed to decide what to share
- Devices in ubiquitous networks leave a trail of users activities
  - Buying some medicine
  - Going somewhere
- Implementing privacy:
  - Anonymity is a good candidate
    - User ID is replaced by one pseudonym
    - The mapping between the real identity and the pseudonym is hidden
    - Users should frequently change their pseudonym

Reputation is good too. . .

- Reputation systems:
  - Nodes collaborate to spread the reputation of each participant
  - Reputation is derived from past experience
- Reputation systems help to detect (and punish)
  - Free-riders
  - Layers
  - Selfish users
- Not all detect
  - Users that forge their ID
  - Users that have multiple identities

Can we have both?

- No:
  - Users should frequently change their pseudonyms
  - How useful can reputation be if we don’t know to whom it belongs?
- Yes:
  - Give reputation to pseudonyms
  - Allow users to change pseudonyms, but
    - Prohibit more than one at once
    - Keep the link user ID⇔pseudonym hidden
  - Allow users to transfer reputation between pseudonyms

RuP: Reputation using Pseudonyms

- Concepts

  Certified Pseudonym (CP) The pseudonym of an user for some predefined time interval

  - An ID card that can be widely exposed
  - Should be asked by the peers to prevent fraud
  - Content: {start date, end date, pseudonym, public key}

  Pseudonym Certification Authority (PCA) Ensures that the user does not own more than one CP for each time interval

  - Accesses the real ID of the user
  - "Signs" the CPs
  - Facilitates the transference of reputation between pseudonyms

RuP: Properties

- Users can not avoid their own reputation

  No impersonation Users can not fake other pseudonyms

  No multiple personality Users can have at most one pseudonym

- Anonymity is preserved
  - not even the PCA can associate an user to a pseudonym

Basic concepts about cryptography

Asymmetric cryptography Uses a key pair

Public key K_u

Private key K_r

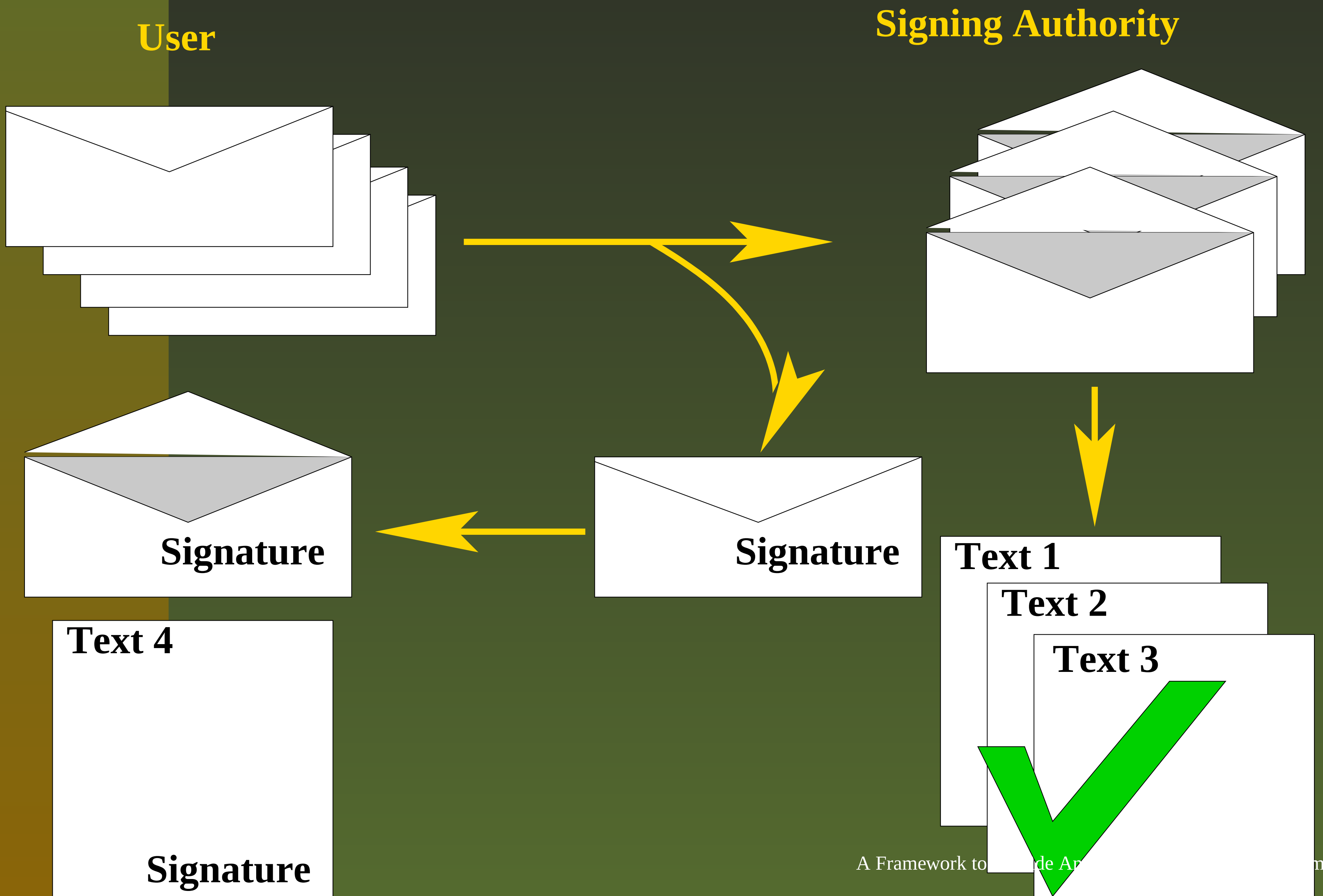
Encrypt/Decrypt $E_{K_u}(M) = C \Rightarrow D_{K_r}(C) = M$

Sign/Verify $D_{K_r}(M) = C \Rightarrow E_{K_u}(C) = M$

Blind signing Digitally signing something without being able to read it

$$\mathbb{S}_{K_r}(E_{K_x}(M)) = C' \Rightarrow D_{K_x}(C') = \mathbb{S}_{K_r}(M)$$

Probabilistic Blind Signing



Reputation Information

- The opinion of node B about node A
  - Different implementations in multiple reputation information frameworks
- Adaptation to RuP
  - Reputation information refers to pseudonyms
  - Node B signs the reputation information and gives a copy to A

Properties of RuP’s reputation

- A can prove to be the target of the information
- A can not deny to be the target of the information
- A can not fake reputation for himself
- A together with the PCA can change the pseudonym associated with the reputation
  - Two steps process:
    1. Remove the old pseudonym from the reputation information
    2. Attach the new pseudonym
  - At the end, the PCA:
    - will not be aware of the link between the old and new pseudonyms
    - is unaware of user’s real identity

Other aspects

- Connections to the PCA are occasional
  - Resource demanding operations can be performed by workstations
  - Certificates identify users, not devices
- Users are more likely to renew “good” reputation
- The duration of certificates trades-off
  - Impact of “bad reputation”
  - Efficiency of pseudonyms

Conclusions

- Anonymity is an important aspect in ubiquitous networks
- Existing reputation mechanisms are not prepared to handle anonymity expectations of the users
- RuP uses off-the-shelf cryptographic algorithms to
  - Improves current reputation systems
    - Prevents users from escaping to bad reputation
    - Prevents users from impersonating others
  - Preserve anonymity of the users
- See details and future work in the proceedings