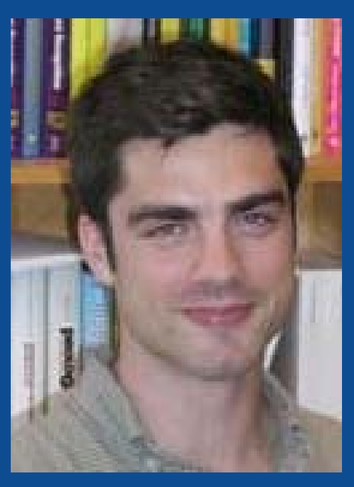
Reconciling Accountability with Anonymity in P2P Systems

John Jannotti, Anna Lysyanskaya (Brown University)



P2P systems as an economy:

- peers offer data and services for sale
- peers pay each other with anonymous e-cash
- peers have an incentive to participate, not just altruism
- accountability without sacrificing privacy: no reputation

Examples

1. File sharing (BitTorrent): peers pay each other for the data retrieved.
2. Onion routing (Tor): pay peers for routing traffic (motivate more peers to participate, increase anonymity).
3. Backup services.

Why can’t we afford to sacrifice privacy for the sake of accountability?

- Without privacy guarantees, P2P systems for anonymizing services, e.g. onion routing (Tor) and anonymous remailers, would be unattainable. Also, in P2P, users have expectation of privacy.

What is anonymous e-cash?

- Participants: bank, buyers, sellers

- Protocols: withdraw, spend, deposit

- A buyer withdraws an e-coin from the bank, spends it with a seller, the seller deposits (cannot transfer e-coin from the seller to anyone other than the bank).

- A coin is untraceable: the information the bank sees in the withdraw protocol does not allow it to tell when the coin was spent (even when colluding with the seller).

Research challenges

Building the Ecash System

- Fraudsters may try to spend the same e-coin twice.
  - Prevention requires the bank to be on-line
  - Detection & retaliation (off-line):
    - If the same coin is spent twice, how to catch the double-spender? *Can find out who he is.*
    - But how do we punish him? *Can use other money in his account if it is still there.*
    - How do we prevent him from double-spending again and again? *Fine-tune revocation and expiration measures to minimize damage.*
- Distributing the bank across peers [1]
- Who is the bank? Can anyone mint their own currency?

Ecash in Onion Routing

- Include a payment for each router
- The router must route everything correctly, else will not be paid [3].

Ecash in BitTorrent

- Fair exchange of large amount of data for an e-coin
  - Fairness is typically guaranteed by a disinterested third party. How do we make sure this party need not process large amounts of data? *Buy keys, not data!* [2]
- Mechanism design: how to prevent false advertisement, enable true advertisement of middleman services
  - Contracts describing precisely what you are paying for. *Content hashes, deadlines.*

Bibliography

[1] M.Belenkiy, M.Chase, C. Erway, J.Jannotti, A. Kupcu, A. Lysyanskaya. “Incentives for Outsourced Computation.” Manuscript, 2008.

[2] M. Belenkiy, M.Chase, C. Erway, J. Jannotti, A. Kupcu, A. Lysyanskaya, E. Rachlin. “Making P2P Accountable without Losing Privacy.” WPES 2007.

[3] J. Camenisch, A. Lysyanskaya, M. Meyerovich. “Endorsed Ecash.” IEEE Symp on Security and Privacy, 2007.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

Brown University