The Free Haven Project
A Reputation System to Increase MIX-net Rel

Roger Dingledine, Reputation Technologi
Michael Freedman, MIT Lab for Computer S
David Hopwood, Independent consultant
David Molnar, Harvard University

The Problem

- The current remailer infrastructure is
  - unreliable
  - inefficient
- Unreliability decreases anonymity

Improving Reliability

- Build protocols with provable reliability guarante
- Add reputation to "improve" reliability
- Provide economic incentives for reliability

- Distinction between reliability and robustness
  - Robustness:

Related Work

- MIXes (Chaum, Pfitzmann...)
- Robust MIX-nets (flash, Universally Verifiable)
- Probabilistic Anonymity (stop-and-go MIXes)
- Deployed Remailer Systems (cypherpunks, Mixm
- Remailer statistics (Levien's statistics, Jack B N

Need to Verify Failures

- Verifying successes is not useful: spoofing is eas
- Failures represent MIX unreliability
- Forcing failures *is* unreliability

Ways To Verify Failures

- Publish all intermediate messages (public ledger
- Web MIXes

others?

- Witnesses and Receipts

Witnesses and Receipts to Verify Failure

- N_{i+1} gives N_i a receipt for each accepted messa
- Each message has a deadline after which it has
- If N_i fails to deliver, he asks witnesses to try
- Witness returns receipt if success, else a failure
- Thus senders can check receipts and prove failu

Good MIXes demonstrate honesty

- Honest N_i delivers to N_{i+1} or to witnesses
- . . . and receives either a receipt or a set of witnes
- If sender challenges, he can provide receipt or s
  (Majority of statements wins)

Bad MIXes Are Caught

- Attacks: don't accept, or silently drop
- Witnesses will catch MIXes that don't accept
- MIXes that silently drop can't show receipts/sta

Reputation System Requirements

- Automated: sender software can automatically
- Verifiable: scorers can verify ratings, users can v
- Useful and dynamic: e.g. reflect recent trends i
- Must maintain anonymity provided by MIX-net

Our Reputation System

- Witnesses are scorers: tally failure claims from
  senders

- Scorers send test messages to get verified succe

- Scorers publish scores; sender software automatic
  paths

- Senders throw out MIXes without some thresh
  cesses, then weight remaining MIXes by number

Traffic Analysis

- Messages to witnesses unencrypted for public ve
- Adversary can get a higher reputation to get m
- Adversary can sabotage other nodes to get mor
- But greater reliability $\Rightarrow$ more users $\Rightarrow$ stronger

Future Directions

- Reliability metric and model (same with efficien
- Other reliability approaches, e.g. through paym
- Remove witnesses if possible (universally verifiab system), maintaining practicality.