AnonReddit
A Strongly Anonymous Public Forum

5/21/17
Theodor Lukin Yelin, Albert Kwon
Acknowledgements

- Albert Kwon
- Prof. Srini Devadas
- PRIMES Program
- Friends and Family
Motivation and Background
Forums

- Reddit

Title and Content

Votes

User

Comment

Votes
Forums
Problems of Current Forums

- Users can be personally attacked
- Opinions can be tied back to user, i.e. not shared freely
- In general, not Anonymous
- If Anonymous:
  - Double voting cannot be prevented as no way to track individual user
  - As votes are main reflection of support, this is a large issue
Why Anonymity?

- Prevent personal feuds, attacks from interfering with forum actions
  - Cannot be targeted based on identity if anonymous

- Whistleblowing (i.e. Edward Snowden)
  - Share information/opinion anonymously
  - Receive feedback/support anonymously

- Voting
  - In an election, voting must remain anonymous
Desirable properties of anonymous forums

- All registered users can Post, Comment, and Vote
  - Unregistered users cannot perform any of these actions
- All posting, voting, and commenting is completely anonymous
- No double voting
  - Same user cannot vote on the same post more than once
Threat model and Goals
Goal

- Provide Anonymity for all necessary forum actions
Threat Model
Goals

- Posting, Voting, Commenting is Anonymous
- User must be registered
- Double voting is not possible

Non-Goals

- A user registering should not be hidden
- Secure communications between client and server
- A single user registering multiple accounts
AnonReddit Design
Signature

Signer

Verifier
Linkable Ring Signature

Signing

Verifying

Private
Public

Public
AnonReddit
Experiments and Results
Methodology

- Scaling for number of Users (up to 50,000)
- Time measured for Posting
  - Client for creating signature
  - Server for verifying signature
- Network latency ignored
- Size of signature measured
Posting and voting latency

**TIME TO GENERATE/VERIFY SIGNATURE**

- Time to generate Sig
- Time to verify Sig

**SECONDS**

**NUMBER OF USERS**

0 10000 20000 30000 40000 50000 60000

0 20 40 60 80 100 120 140 160 180
Network Overhead
Conclusion and future work

- Improve signature generation efficiency to support ~1,000,000 users
  - Currently viable to scale up to ~100,000
- Use differential privacy
  - Hide exact number of votes on a post/comment
- Add options to be recognizable on certain posts
  - I.e. keep only specific posts anonymous
- Link posts in certain communities