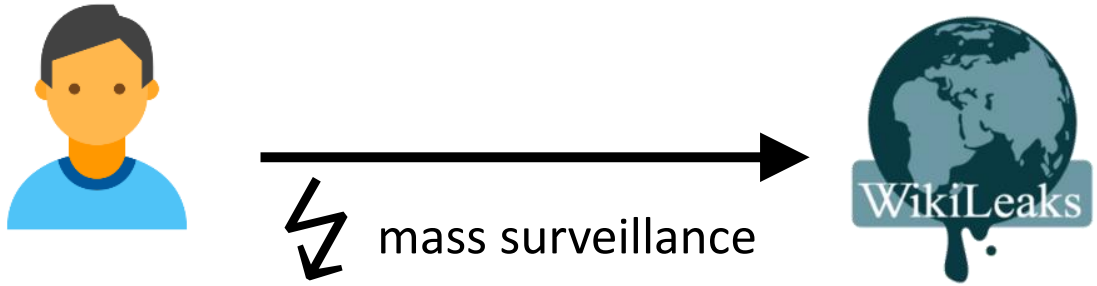
CoverUp: Upload and Download via Passive Participation

David Sommer, Aritra Dhar, Luka Malisa
Esfandiar Mohammadi, Srdjan Čapkun, Daniel Ronzani

Were you Ever Afraid to …

- … download something that is easily accessible?



- Maybe someone is watching?

whistleblowers

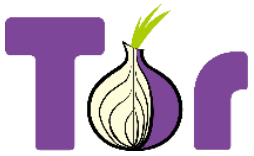
free speech

accessing primary sources (e.g., WikiLeaks)

(essential for an informed democracy)

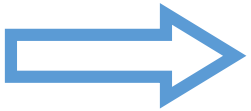
Motivation: Deniability and Participation

- ACN - Strong anonymity
  - Hide which users are connected to whom
  - Limits surveillance and censorship

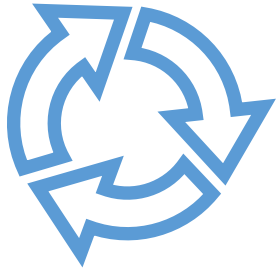


- Participation alone raises suspicion
  - Little deniability
- Bootstrapping Problem

Unattractive latency and/or bandwidth



Low number of connected users



unattractive degree of anonymity

small anonymity set

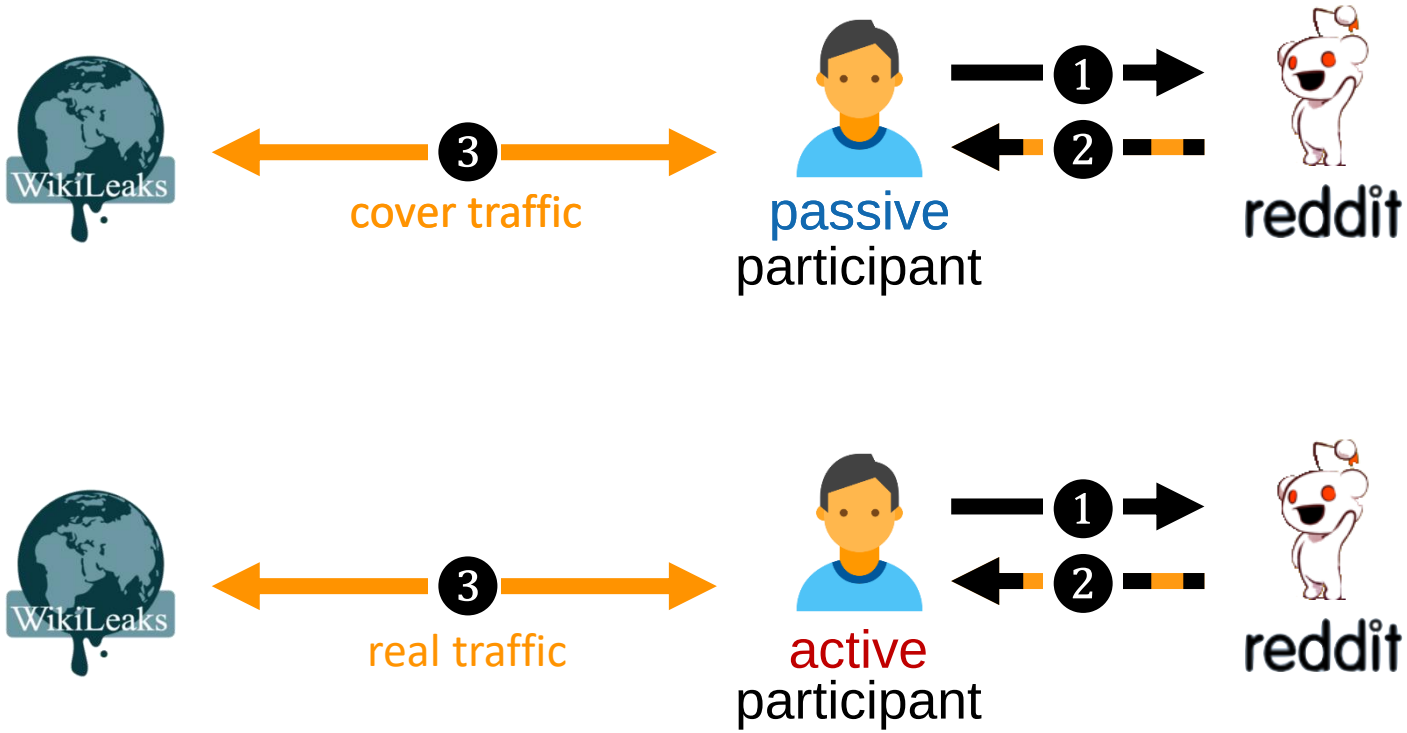
Our contribution: Passive Participation

- Web site visitors passively produce cover traffic

❶ User visits reddit

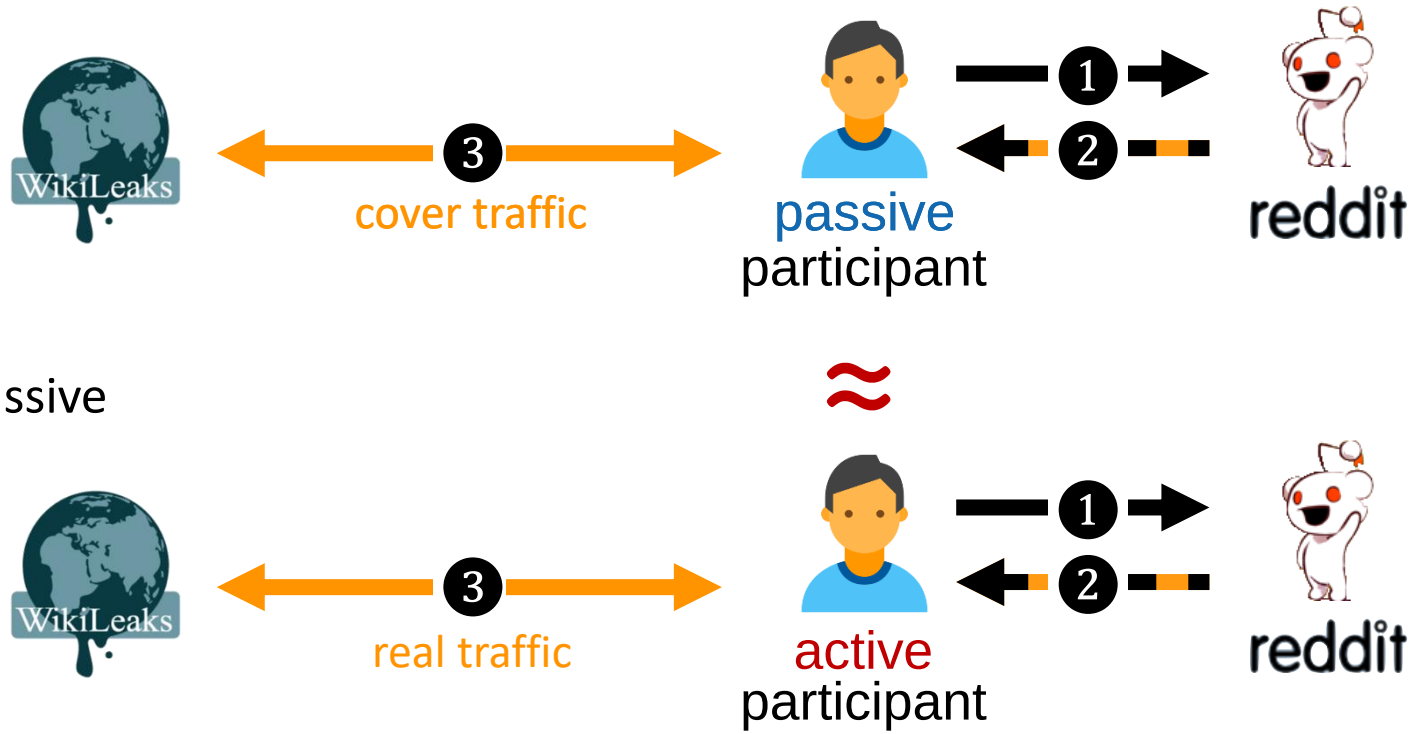
❷ Reddit responds and includes a piece of JavaScript code

❸ This JS code produces cover traffic



Our contribution: Passive Participation

- Web site visitors passively produce cover traffic
- Indistinguishability
  - Larger anonymity set
  - Anonymity set size = active + passive
  - Mitigates bootstrapping
- Provides deniability

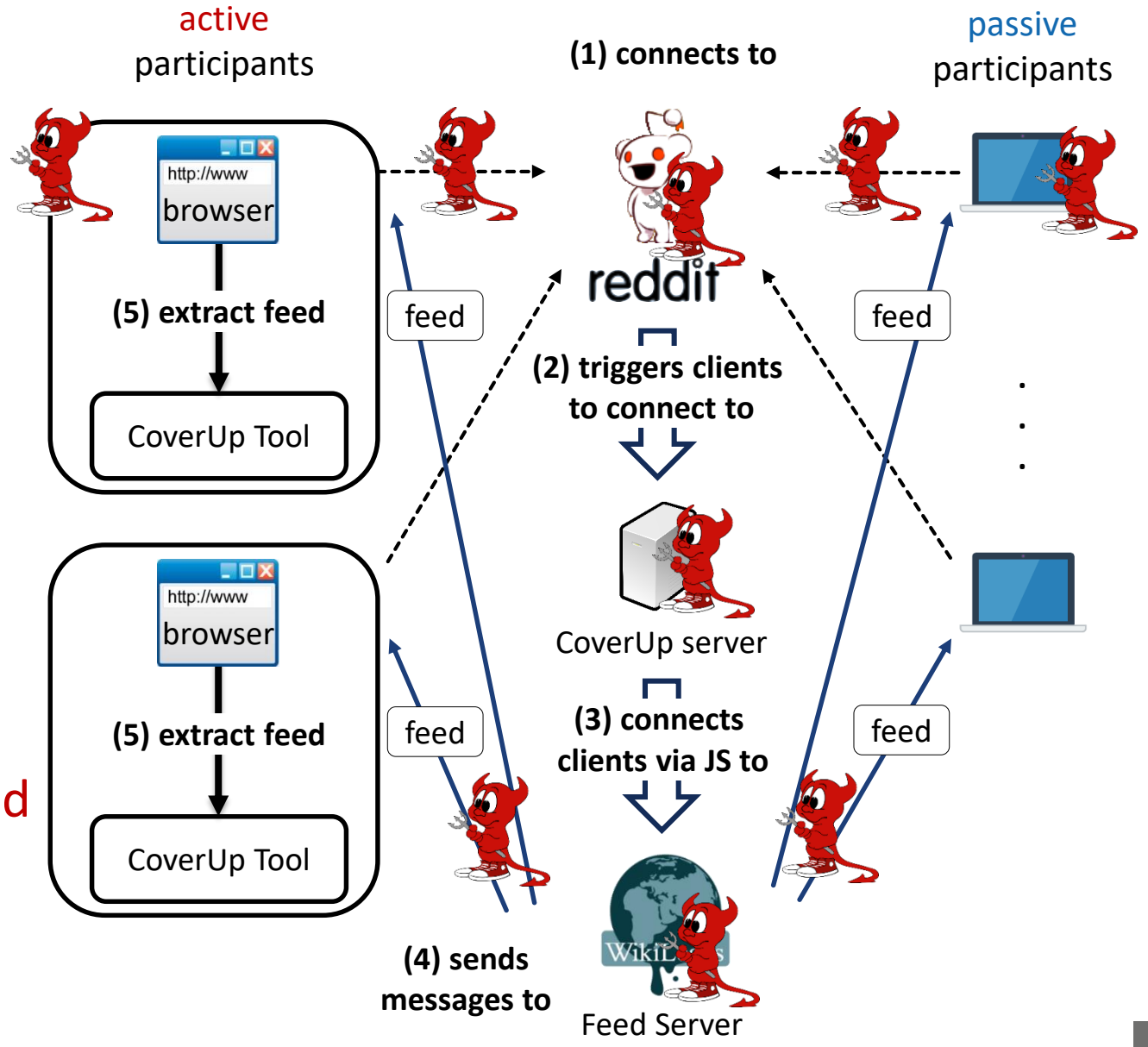


CoverUp: Contributions

- Uses Passive Participation
  - Uni-directional channel: Feed
  - Bi-directional channel: Transfer
- Working Prototype
- Analyzed Network Timing leakage

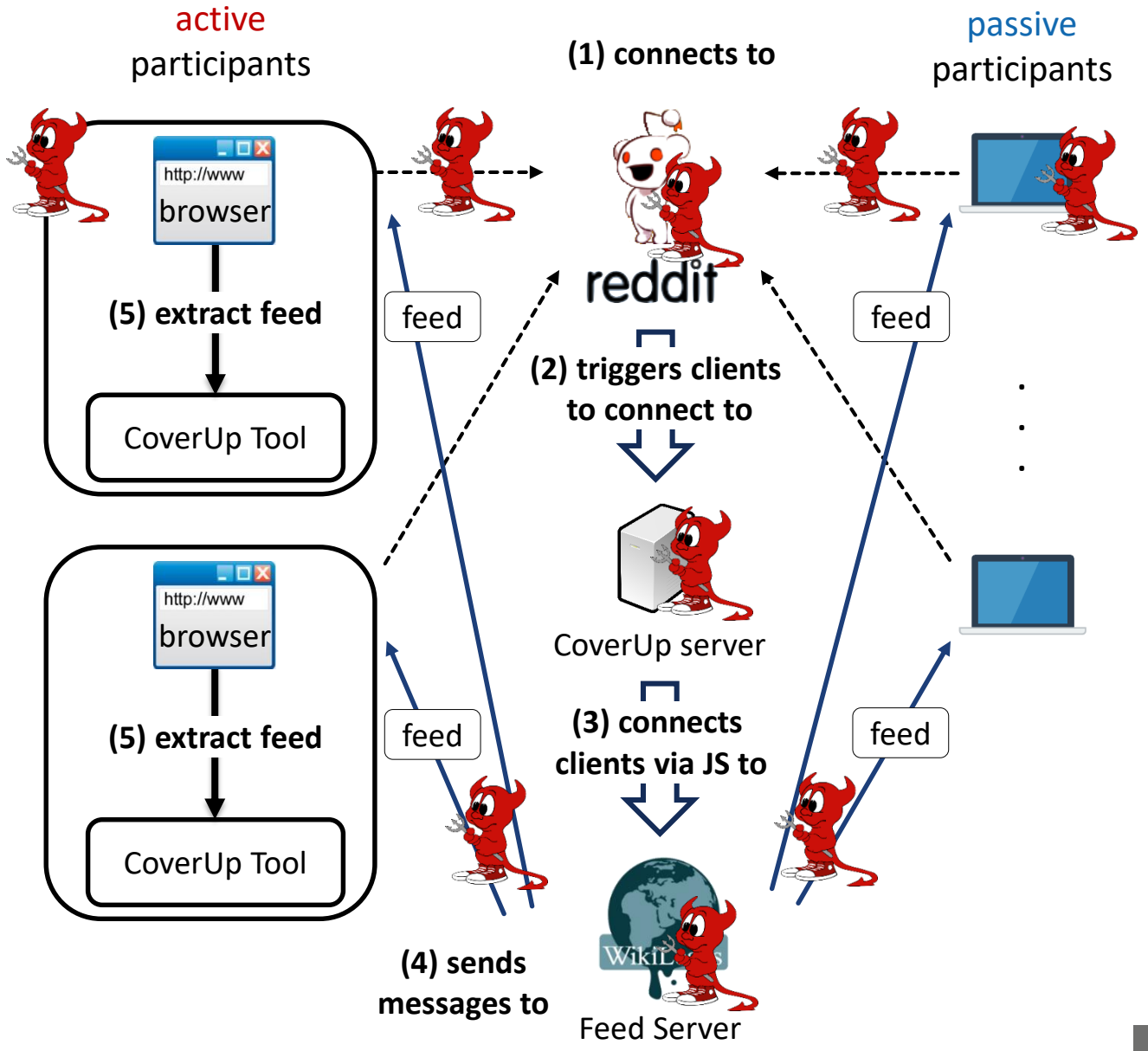
CoverUp: Feed

- JS code in sandboxed iframe due to Same-Origin-Policy
- Attacker controls:
  - Network (monitor/drop/fake)
  - Entry Server (reddit)
  - CoverUp server (delivers js code)
  - Feed Server (delivers feed)
- Active user's machine not compromised



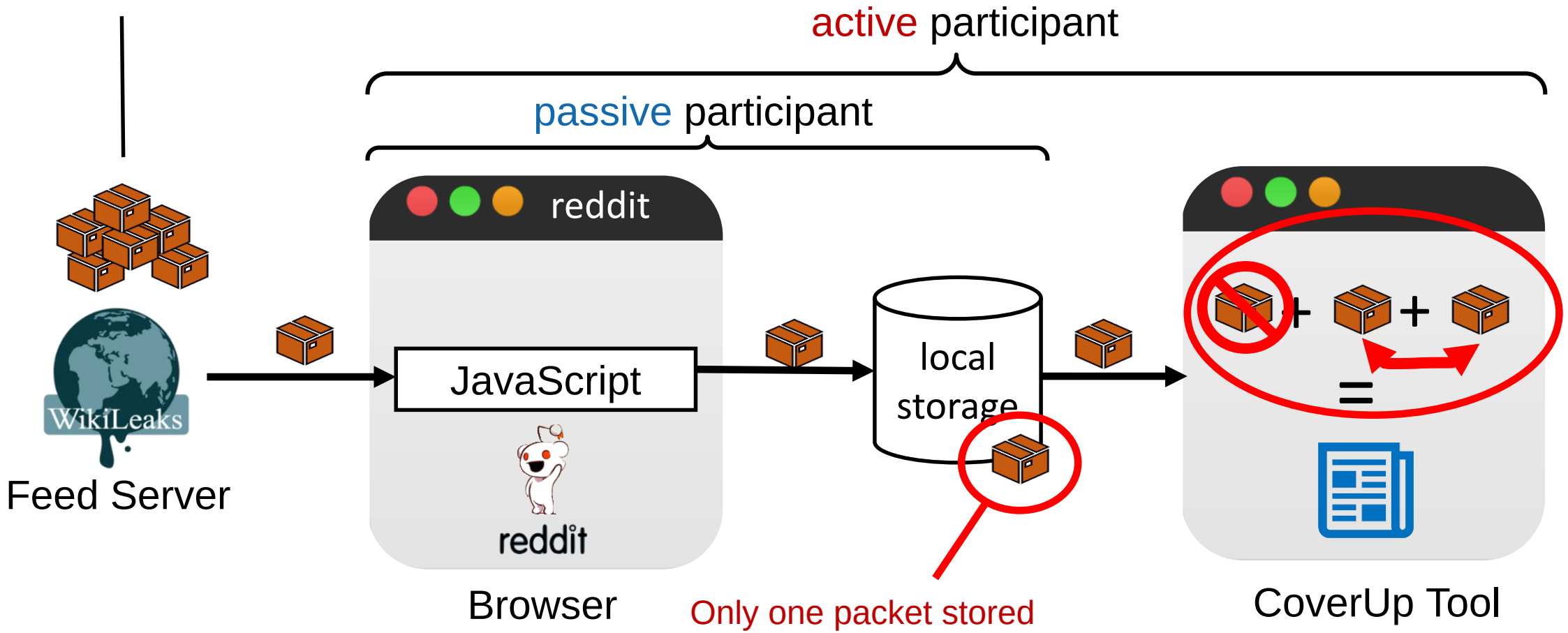
CoverUp: Feed

- Indistinguishability
  - Active and passive participants: same protocol
  - Difference: CoverUp Tool
  - Provides Deniability



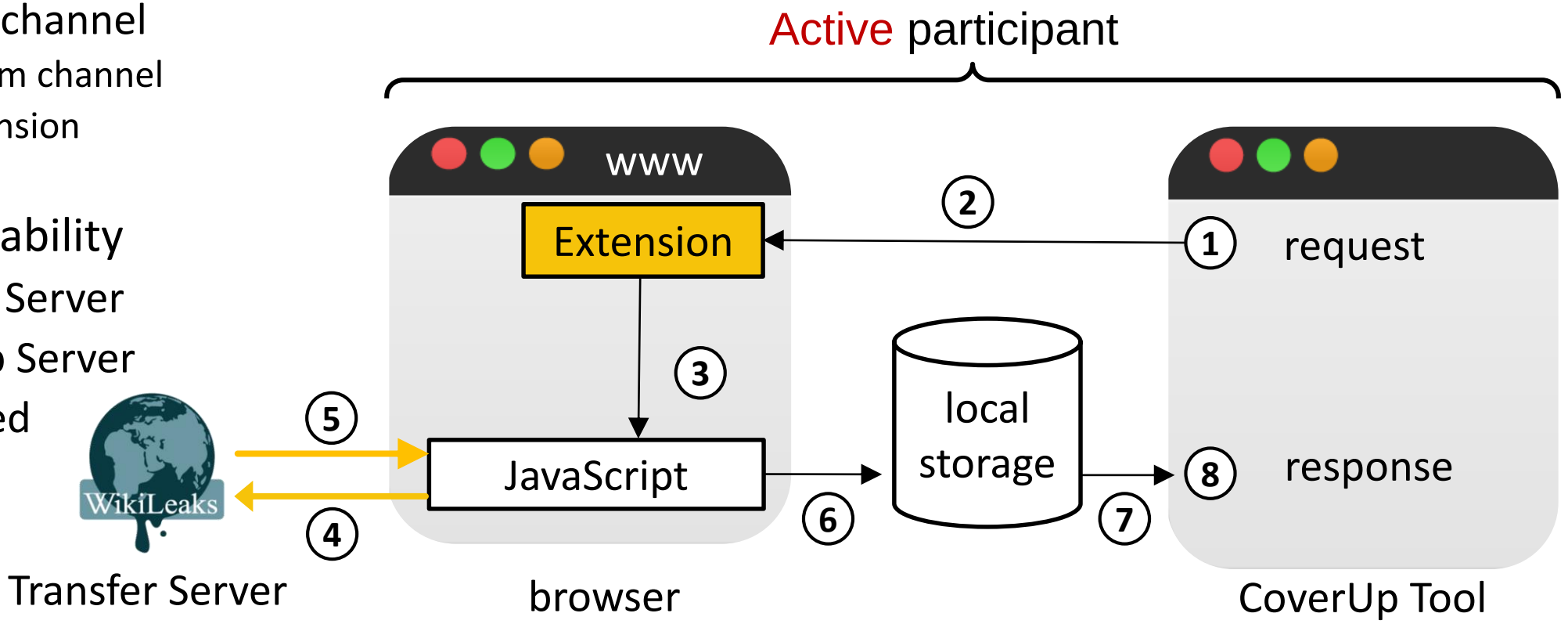
Protecting Passive Participants

Fountain Codes + All-or-Nothing Scheme



CoverUp: Transfer

- Bi-directional channel
  - Adds upstream channel
  - Involves extension
  - Using TLS
- Indistinguishability
- Trust Transfer Server
- Trust CoverUp Server
- Augments Feed

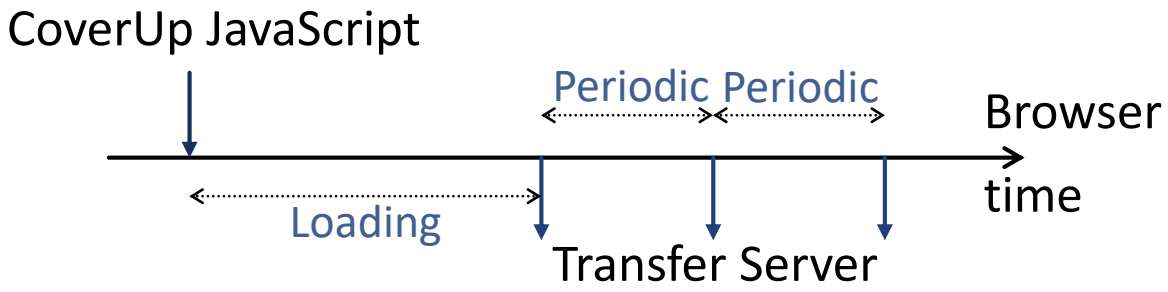


Evaluating the Indistinguishability Assertion

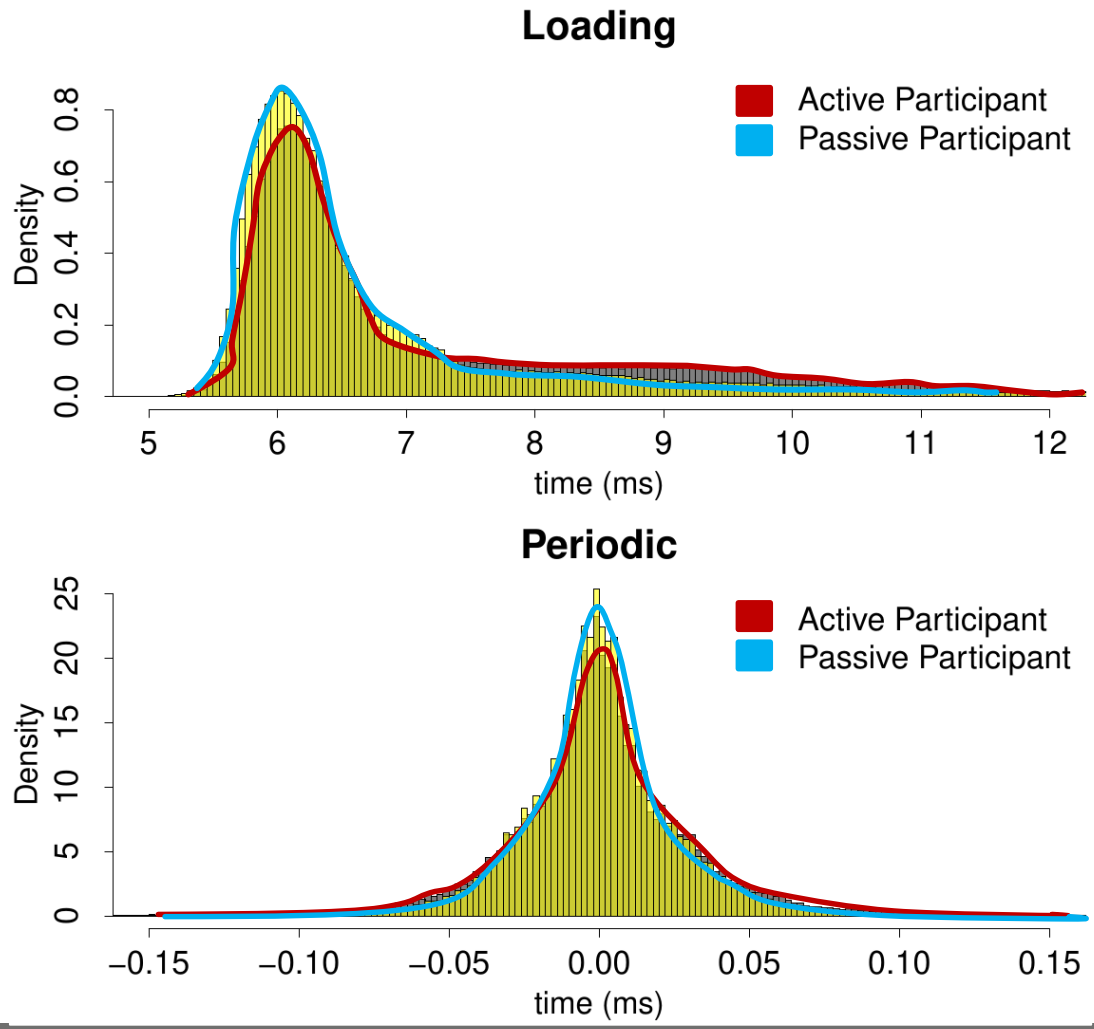
- Protocol transcripts are indistinguishable
  - Everything else identical?
  - But active users have CoverUp tool and browser extension (in Transfer)
- What can network attacker do?
  - Measure execution time by network timestamps
- Timing leakage
  - Evaluation
  - Mitigation

CoverUp: Experimental Setup

- Setup: LAN, entry, transfer, and feed server
- Feed and Transfer scenarios:

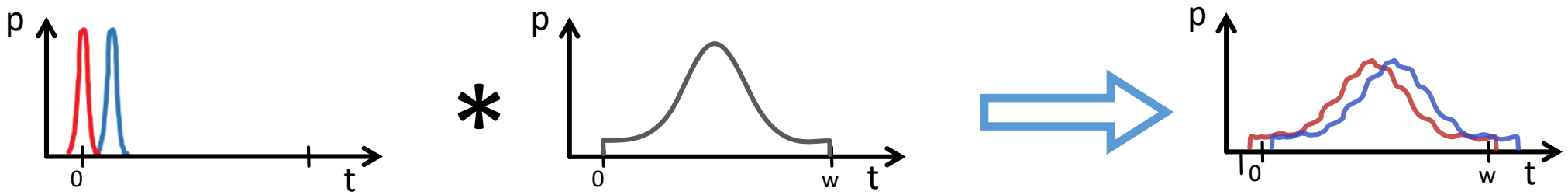


- *Strong attacker model*:
  - No other processes running on the system
  - High-precision time resolution
- 3 Million measurements

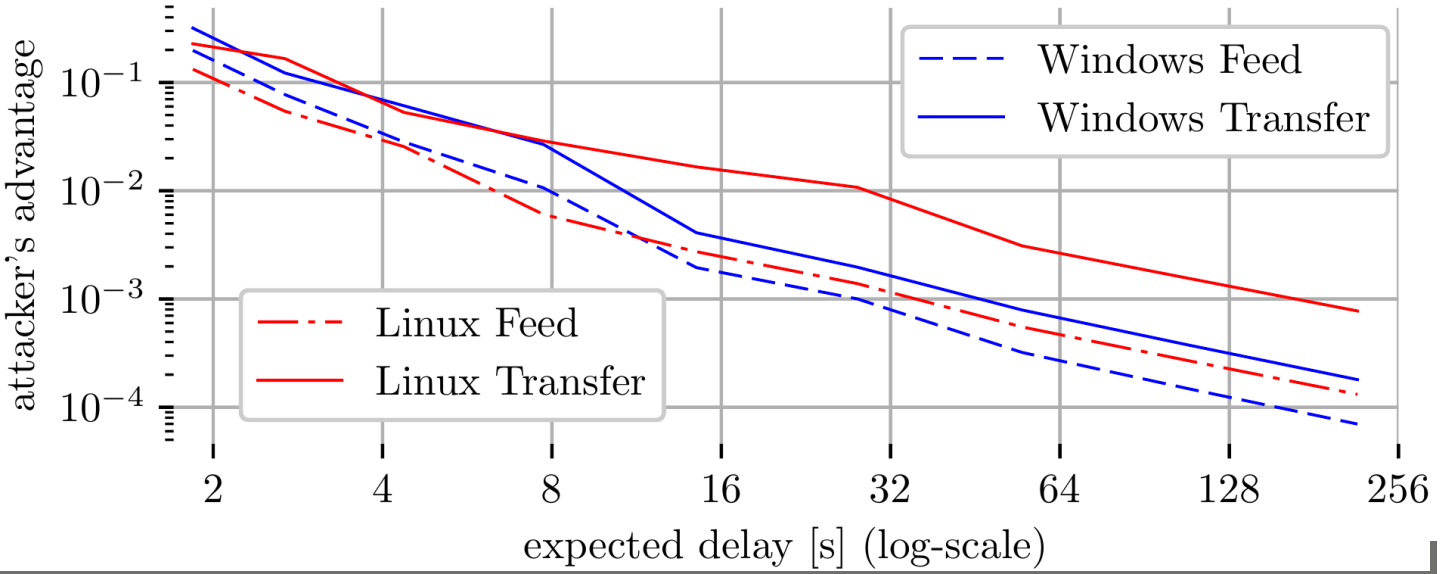


CoverUp: Privacy Budget

- Request dispatch time: add truncated Gaussian noise

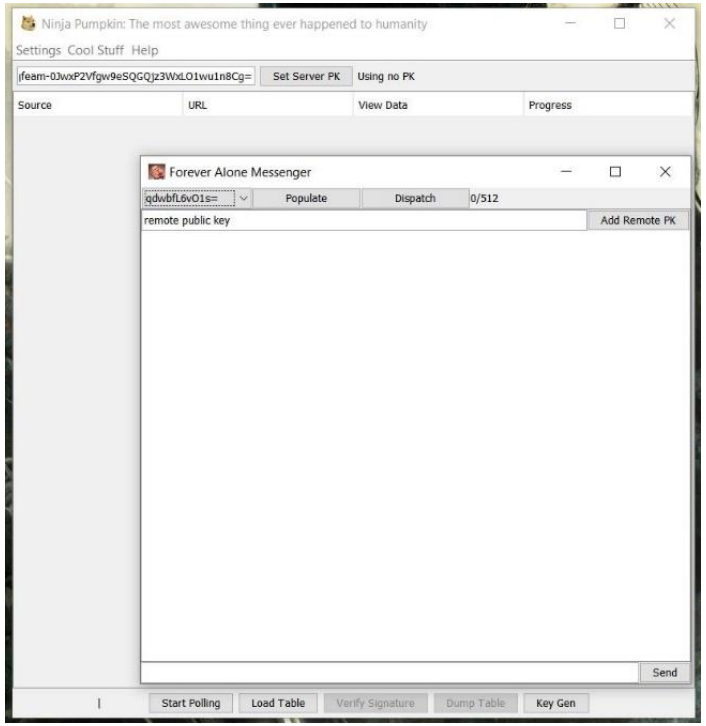


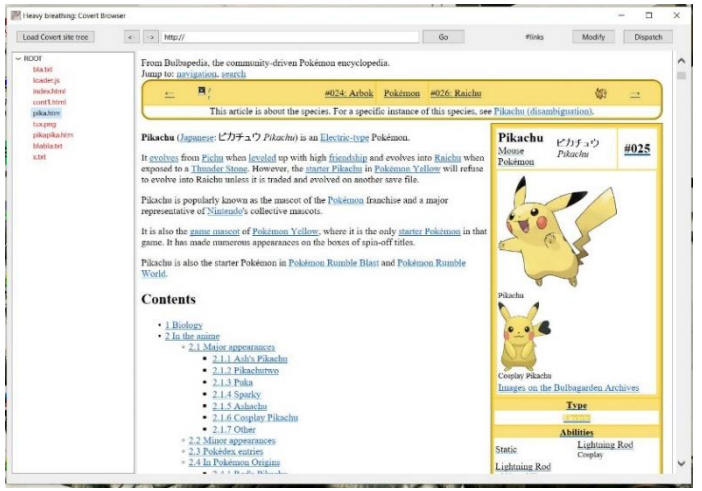
- Continual observation for half a year
  - < 5 hours of visiting the entry server (Periodic-observations) per day
  - < 50 connecting to the entry server (Loading-observations) per day



CoverUp: Implementation

- CoverUp Tool
  - Implemented in Java
  - Features: feed, chat and interactive browsing
  - Uses crypto APIs from whisper systems and JCA
- Browser extension
  - Chrome extension based on WebExtension API
- Feed/Transfer and CoverUp server
  - Implemented using Java EE Servlet API
  - Hosted on Apache Tomcat webserver





Available for download and testing: http://coverup.ethz.ch

CoverUp: Performance

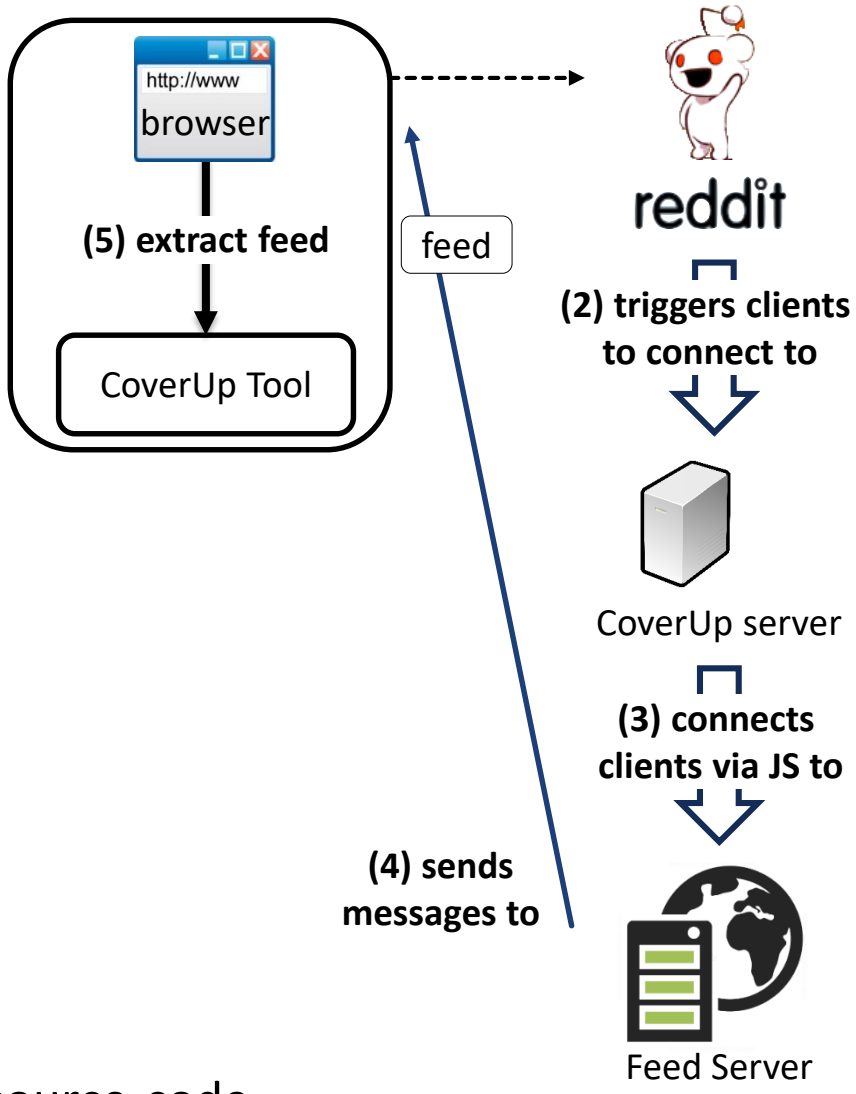
- Performance
  - Packet size: 75KB every 60s avg.
  - Goodput: 10KBit/s
- Per user overhead
  - Around 660 MB/month or 22MB/day
- Privacy guarantee
  - Attacker's advantage < $2 \cdot 10^{-3}$

cnn.com: 4.0MB
amazon.com: 5.0MB
alibaba.com: 5.4MB

google.com: 0.3MB

CoverUp: Summary

- Passive Participation
  - Increases anonymity set (Bootstrapping)
  - Hides Intention (Deniability)
- Adding Noise reduces Timing Leakage
  - Maintains feasible usability
- Measurements available



Available for testing: https://coverup.ethz.ch
Available for download: https://github.com/sommerda/CoverUp-source-code