rBridge: User Reputation Based Tor Bridge Distribution with Privacy Preservation

Qiyan Wang
Nikita Borisov

University of Illinois at Urbana-Champaign

Zi Lin
Nicholas J Hopper

University of Minnesota
The Internet helps political and social movements

5 voices on Egypt's 'unfinished revolution'

of entering an upcoming bicycle race but do not really know how to start or how to get yourself
“[It] is a force for democracy, because it permits citizens to communicate, to collaborate, and even to conspire uncontrolled by a central authority.”
Internet censorship

• **7 out of top 10** non-Chinese sites[^1] are blocked by the “Great Firewall of China”.

• The Chinese government employs an **Internet policy force** of over 30,000 people[^2].

<table>
<thead>
<tr>
<th>Top 10 non-Chinese sites</th>
<th>Blocked by GFW?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Partially</td>
</tr>
<tr>
<td>Facebook</td>
<td>Yes</td>
</tr>
<tr>
<td>YouTube</td>
<td>Yes</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>Partially</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Live</td>
<td>No</td>
</tr>
<tr>
<td>Twitter</td>
<td>Yes</td>
</tr>
<tr>
<td>Amazon</td>
<td>No</td>
</tr>
<tr>
<td>Blogspot</td>
<td>Yes</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>No</td>
</tr>
</tbody>
</table>

Censorship techniques

- IP blocking
- DNS hijacking
- Deep packet inspection
Censorship circumvention using Tor

reverse and even restore your hearing
Censorship circumvention using Tor

Recurring, directly connecting Chinese Tor users (past 180 days)

Cards will Appear in a variety
Censorship circumvention using Tor bridges

Bridges

Relays (publicly listed)
Censorship circumvention using Tor bridges

I heard that I could attract hummingbirds with Water.
How your entire world (as you perceive it) is created through SOUND,
Censorship circumvention using Tor bridges

How to avoid distributing bridges to malicious users?
Rate limiting

One bridge per IP address / Gmail address

Bridges

Relays

and what the paint store will not tell you
The Chinese government were able to enumerate all bridges in under a month in 2010.
Limited access

Only give bridges to highly trusted people

How can I pay these bills??? How can I pay these bills??? Why can’t I meet someone to really...
Limited Access

Only give bridges to
highly trusted people

Bridge distributor

Most of the potential (honest) users are unable to get bridges

SO, if you are mad of spending money for nothing, HERE YOU WILL FIND ANSWERS TO
Social Distribution

Conflict between robustness and openness!
Proximax [McCoy et al., FC’11]

the usefulness of magnetic sheets for ever-
Proximax [McCoy et al., FC’11]
Our basic idea: Incentives

That’s a very nice bridge you got there

It’d be a shame if something were to … happen to it

Pay users to keep bridges unblocked!

Why the hell would it? It’s time to get out of the comfort zone of tit for tat technique based training
rBridge: user reputation

*Earn credits from alive bridges*
rBridge: user reputation

*Earn credits* from *alive bridges*

These are big promises! Why should...
rBridge: user reputation

*Earn credits from alive bridges*
**rBridge: user reputation**

*Earn credits from alive bridges*

---

We make excuses. We don’t know what to do. We’re greedy. Habit. We think we
rBridge: user reputation

*Earn credits from alive bridges*

Shopping when you’re exhausted
**rBridge: user reputation**

*Earn credits from alive bridges*

*Spend credits to buy new bridges*

You don't have to gulp. You have
Defense against *Sybil attacks*: users with sufficient credits have the opportunity *to invite friends* to join the system.
Comparison with Proximax (the state-of-the-art scheme)

Proximax: less than 5% bridges can serve more than 20 user-hours before being blocked.

rBridge: over 80% bridges can serve at least 60 user-hours before being blocked, and about 60% bridges are never blocked.
In Tor, the selection of relays must be kept secret, even from the directory authority!
In Tor, the selection of relays must be kept secret, even from the directory authority!
In all previous schemes the distributor is fully trusted and knows which particular bridge is given to whom.
The basic rBridge scheme (without privacy preservation):
Use *Oblivious Transfer (OT)* to give out bridges, while *hiding which bridges are received by the user*. In your approval (or denial) letter that will help you determine your next best
rBridge: privacy preservation

Unable to compute credits without knowing the user’s bridges

Shock them, impress them, and melt
Delegate the task of computing reputation to users themselves.

Unable to compute credits without knowing the user’s bridges.
Delegate the task of computing reputation to users themselves.

We need to prevent user misbehavior, e.g., manipulating credit balance.
An Anonymous Credential

- Pseudonym $X$
- Credit balance $\Phi$
- ID of assigned bridge $B_i$
- Time $T_i$ when $B_i$ was given to $X$
- #Credits $\Phi_i$ earned from $B_i$

into some possible future scenarios
Anonymous Credential

- Pseudonym $X$
- Credit balance $\Phi$
- ID of assigned bridge $B_i$
- Time $T_i$ when $B_i$ was given to $X$,
- #credits $\Phi_i$ earned from $B_i$

Use *blind signature* to sign each part of the credential to *prevent manipulation*.
Anonymous Credential

- Pseudonym $X$
- Credit balance $\Phi$
- ID of assigned bridge $B_i$
- Time $T_i$ when $B_i$ was given
- #credits $\Phi_i$ earned from

Use **blind signature** to sign each part of the credential to prevent manipulation.

Use **zero-knowledge proofs** to prove the information on the credential is correct while hiding all the information from the bridge distributor.

in just a few minutes and seeing wonderful
1. Registration

Old technology, old procedures, old policies, old methods, or; Often produces
1. Registration

[Diagram showing a computer connected to a server via a bridge distributor]
1. Registration

My 3-second whisper to make
1. Registration

overlooked power of the CD/DVD/MP3
2. Update Credit Balance

Exactly the right amount of water that your
2. Update Credit Balance

Learn how to add in extra elements, rotate your card sketch
3. Bridge Exchange

Are you secretive? Are your muscles
3. Bridge Exchange

I adore key limes and am always on the lookout for new ways.
3. Bridge Exchange

TV? mance TV Robust Robust Robust Robust Robust strategy Inflexible Missed opportunities
Performance evaluation

Table 1: Performance (averaged over 100 runs)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Comp. (s)</th>
<th>Comm. (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>U</td>
<td>D</td>
</tr>
<tr>
<td>Registration</td>
<td>5.15</td>
<td>17.44</td>
</tr>
<tr>
<td>Updating credit balance</td>
<td>0.51</td>
<td>0.47</td>
</tr>
<tr>
<td>Getting a new bridge</td>
<td>5.35</td>
<td>17.62</td>
</tr>
<tr>
<td>Inviting new users</td>
<td>0.27</td>
<td>0.16</td>
</tr>
</tbody>
</table>

These operations are *infrequent!*
Performance evaluation

Table 1: Performance (averaged over 100 runs)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Comp. (s)</th>
<th>Comm. (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>U</td>
<td>D</td>
</tr>
<tr>
<td>Registration</td>
<td>5.15</td>
<td>17.44</td>
</tr>
<tr>
<td>Updating credit balance</td>
<td>0.51</td>
<td>0.47</td>
</tr>
<tr>
<td>Getting a new bridge</td>
<td>5.35</td>
<td>17.62</td>
</tr>
<tr>
<td>Inviting new users</td>
<td>0.27</td>
<td>0.16</td>
</tr>
</tbody>
</table>

In the current Tor network, each client needs to download 120 KB network-status file every 3 hours.

These operations are infrequent!
• Leverage *user reputation* to bridge the gap between robustness and openness in Tor bridge distribution.
  – High-reputation users can *buy* bridges and *invite* new friends
  – Much higher *robustness* than previous work
• Design the first *privacy-preserving* bridge distribution scheme
  – Use Oblivious Transfer, Commitment, Zero-knowledge Proof, and Blind Signature as building blocks.
Thank you!

Question?