Blindspot: Indistinguishable Anonymous Communications

Joseph Gardiner and Shishir Nagaraja

Security Lancaster Research Centre, Lancaster University

Problem

- Previous anonymous communication systems provide unlinkability, but do not provide unobservability
  - Under targeted surveillance an adversary can identify use of the system
- Unobservability is required, i.e. use of the system is hidden
- Previous attempts such as Collage [1] and Drac [2] still introduce new endpoints or change user behaviour in some way
  - Scope for detection through statistical traffic analysis
- We argue that indistinguishability is required for unobservability

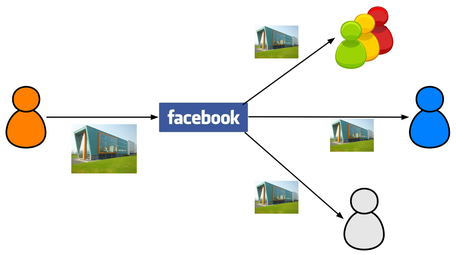

Figure 1: Image sharing in online social networks

Indistinguishability

- Required for full unobservability
- You cannot identify an user of the system with a probability greater than a random coin toss
- Traffic with hidden communication is statistically identical to traffic without hidden communication

Intended Uses

The system supports the sending of short messages. Some example uses are:

- Protest organisation
- Whistle-blowing

System Overview

The system works by using the (unmodified) image upload and sharing behaviour of users of online social networks (OSNs).

1. Message are embedded in images using steganography
2. Images are shared with friends
3. Friends using system download images and extract messages
4. Messages destined for others are included in next image upload

Routing and Anonymity Design

Blindspot requires a routing algorithm that can ensure low delay times and high delivery rates in an extremely low bandwidth network, which also means that control traffic must be minimized. Therefore, Blindspot makes use of a novel probabilistic routing algorithm:

- Routing aims to find lowest delay path, not shortest
- Makes use of convolution of random variables
  - Random variable is PDF of inter-upload delay for a user
  - Node stores the delay distribution convolutions of all possible 2-hop paths for which it is the middle node
- Node pulls all images from neighbours and adds to queue and assigns each message a score based upon convolution and overlap with neighbour list of previous node
  - $score_{m_i} = similarity_{prev} + min(cdf)_{prev}$
- Message list is sorted according to score, weighted coin toss applied to each message
  - Either include message in next upload, or discard

Anonymity is provided through the use of universal re-encryption [3]. This allows for onion-routing like anonymity without the requirement of knowing message routes.

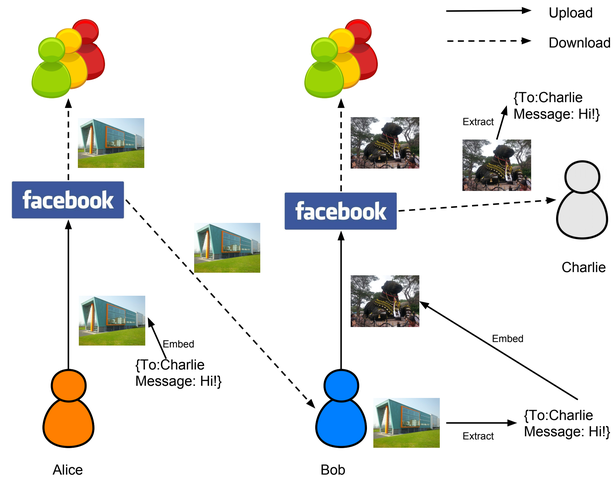

Figure 2: System Overview

Important Result

Blindspot provides the first fully indistinguishable communication system design, providing low-volume high-latency communication while also providing unlinkability. At its core is a novel, probabilistic, low bandwidth routing algorithm.

Results

The routing is tested on a dataset taken from Flickr of 7200 users and their monthly upload counts. We also test on a network of 7200 nodes generated using the Barabasi-Albert (BA) model and the upload data from Flickr.
Average delay is 1 day.

We also test with removing increasing percentages of nodes both at random, and in an targeted nature (by removing the nodes in descending degree order). The results are presented below.
The average delay remains at 1 day.

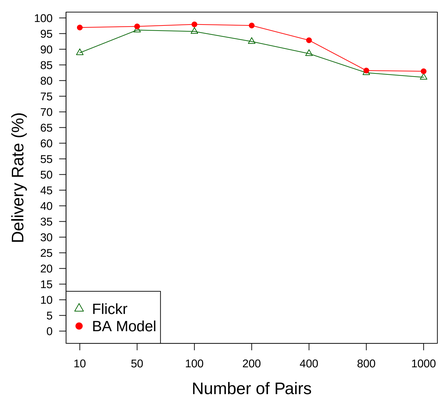

Figure 3: Delivery rate under increasing number of communicating pairs

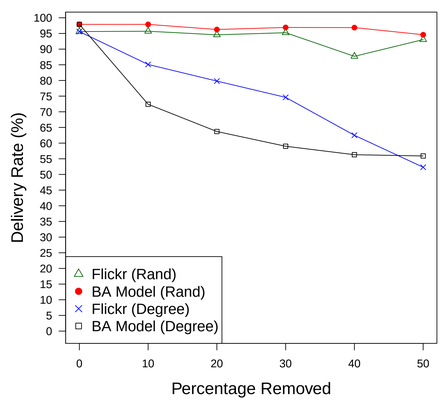

Figure 4: Delivery rate for 100 pairs after removing nodes

Conclusion

Blindspot allows for communication over online social networks while providing full unobservability. Use of the system does not change the user's internet traffic in any way, providing protection against targeted statistical traffic analysis. The system provides acceptable performance within the limited network environment in which it operates.

Future Work

Our next steps will be:

- Run simulations on an up-to-date, larger dataset
- Reduce key requirements for anonymity
- Allow routing over multiple social networks and media types
- Provide functionality for route reuse to improve performance

References

[1] Sam Burnett, Nick Feamster, and Santosh Vempala. Chipping away at censorship firewalls with user-generated content. 2010.

[2] George Danezis, Claudia Diaz, Carmela Troncoso, and Ben Laurie. Drac: an architecture for anonymous low-volume communications. 2010.

[3] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. Universal re-encryption for mixnets. 2004.

Contact Information

- Web: www.lancaster.ac.uk/pg/gardine1
- Email: {j.gardiner1,s.nagaraja}@lancaster.ac.uk

Security Lancaster | Lancaster University

InfoLab21

Read the full paper on arXiv