Why is it so hard to send unobservable messages across the internet?

Martin Gwerder (m.gwerder@unibas.ch)
Department of Mathematics and Computer Science, University of Basel

Objectives

This work emphasizes on the requirements needed to create a system that is capable to transfer unobserved messages across the internet. It focusses on:

- What is required to create unobservable messages?
- What parts are already available as well established technologies?
- Where do we have a lack of reliable and researched technologies?

In this poster, I emphasize on the result. If you are interested at the argumentation, I recommend the corresponding paper referenced at the lower right for further reading.

Introduction

There are lots of works[1][2][3][4] that relate to anonymous message transfer. However – none of these works (with exception to TOR[1]) has been widely adopted in the internet. The reason for this is usually that peoples tend to concentrate on the method to transport the message and fail at the same time completely to take the real world and its problems into account. I collected some information that helps to create sensible and reliable systems.

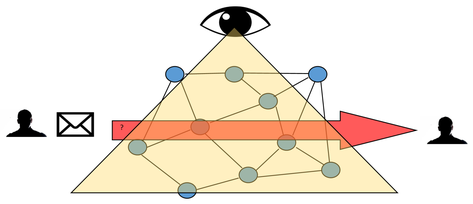

Figure 1: sending unobservable messages is not easy

Categorisation

In order to simplify the aspects of unobservability I categorized them into three categories.

- Acceptance
- Protocol
- Infrastructure

Acceptance

In order to get users to accept a solution we have minimum baselines to meet:

- Easy
- Fast
- Reliablee in order to be accepted.
- Not abuseable

Protocol

In order to succeed with the goal the protocol needs to support certain features:

- Unidentifiable
- Untagable
- Unreplayable
- Monolythic messages

Important factors

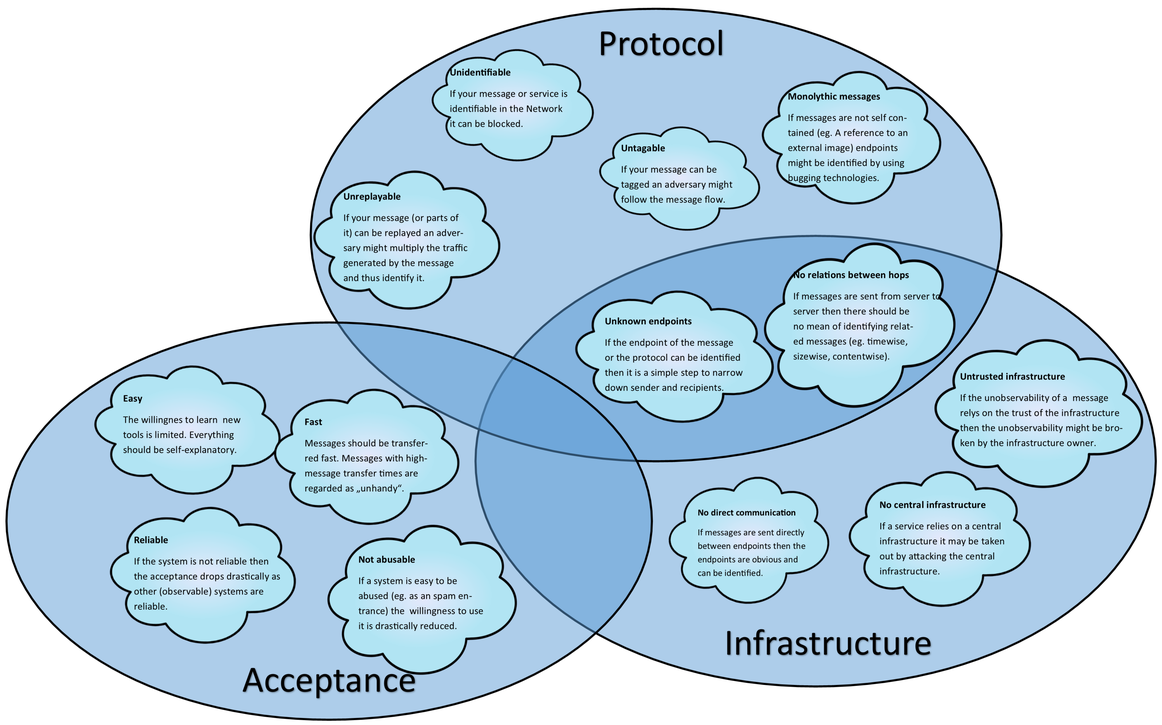

Figure 2: Important factors when designing an unobservable message channel

What is missing?

It is still unclear if researchers have done enough research in the past to build an unobservable system. Namely, the research of steganography seems to be in its childhood. Unlike in Cryptology there are no researched âĂIJbest practicesâĂİ and no mathematical language for it. We have been unable so far to research the characteristics of covert channels and attributes and we are unable to describe them with scientifically defined attributes in an elaborated language.
One thing seems to be clear when looking at the requirements for unobservable system. The costs in terms of bandwidth are tremendous compared to the normal (observable) messages. Cutting the costs of being unobservable should be one of our main goals in future.

Infrastructure

In order to succeed there are as well certain baselines for the infrastructure:

- Unknown endpoints
- No relations between single hops
- Untrusted infrastructure
- No central infrastructure
- No direct communication between endpoints

Conclusions

Sending unobservable messages thru a public network is not easy. It cannot be done by inventing a new identifiable service. It has to blend into today's traffic and look unsuspicious compared to all other traffic to be of any value. Yet it has to be easy to handle and simple to understand. Combining today's technologies might be sufficient but have to be researched further.

Additional Information

For additional information, please see the corresponding papers and presentations published at:
https://www.gwerder.net/~mgwerder/phd/how_unobservable/
or use the QR code in the top right corner.

References

[1] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[2] Ulf Möller, Lance Cottrell, Peter Palfrader, and Len Sassaman. Mixmaster Protocol — Version 2. IETF Internet Draft, July 2003.

[3] Shlomi Dolev and Rafail Ostrobsky. Xor-trees for efficient anonymous multicast and reception. *ACM Trans. Inf. Syst. Secur.*, 3(2):63–84, 2000.

[4] Brian Neil Levine and Clay Shields. Hordes — a multicast based protocol for anonymity. *Journal of Computer Security*, 10(3):213–240, 2002.