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

Martin Gwerder
Department für Mathematik und Informatik, Universität Basel

## Objectives

This work emphasizes on the requirements needed to create a system which is capable to transfer unobserved messages accross 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 technologies?

## Introduction

There are lots of works (FIXME CITE) which relate to anonymous message transfer. However – none of these works (with exception to TOR) 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 to take the real world and its problems into account. I collected some informations which helps to create sensible and reliable systems.

Placeholder

Image

Figure 1: Figure caption

## Materials

The following materials were required to complete the research:

- Curabitur pellentesque dignissim
- Eu facilisis est tempus quis
- Duis porta consequat lorem
- Eu facilisis est tempus quis

The materials were prepared according to the steps outlined below:

1. Curabitur pellentesque dignissim
2. Eu facilisis est tempus quis
3. Duis porta consequat lorem
4. Curabitur pellentesque dignissim

## Methods

Lorem ipsum dolor **sit amet**, consectetur adipiscing elit. Sed laoreet accumsan mattis. Integer sapien tellus, auctor ac blandit eget, sollicitudin vitae lorem. Praesent dictum tempor pulvinar. Suspendisse potenti. Sed tincidunt varius ipsum, et porta nulla suscipit et. Etiam congue bibendum felis, ac dictum augue cursus a. **Donec** magna eros, iaculis sit amet placerat quis, laoreet id est. In ut orci purus, interdum ornare nibh. Pellentesque pulvinar, nibh ac malesuada accumsan, urna nunc convallis tortor, ac vehicula nulla tellus eget nulla. Nullam lectus tortor, *consequat tempor hendrerit* quis, vestibulum in diam. Maecenas sed diam augue.

## Important factors

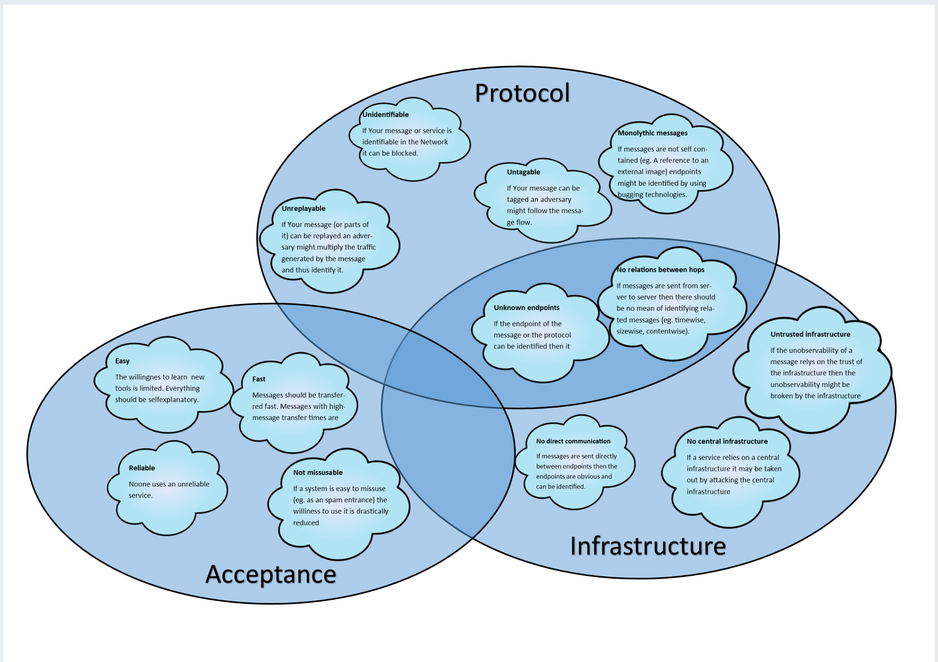


Figure 2: Important factors when designing an unobservable message channel

## Conclusion

Nunc tempus venenatis facilisis. **Curabitur suscipit** consequat eros non porttitor. Sed a massa dolor, id ornare enim. Fusce quis massa dictum tortor **tincidunt mattis**. Donec quam est, lobortis quis pretium at, laoreet scelerisque lacus. Nam quis odio enim, in molestie libero. Vivamus cursus mi at *nulla elementum sollicitudin*.

## Additional Information

Maecenas ultricies feugiat velit non mattis. Fusce tempus arcu id ligula varius dictum.

- Curabitur pellentesque dignissim
- Eu facilisis est tempus quis
- Duis porta consequat lorem

## References

[1] Lasse Øverlier and Paul Syverson.
Improving efficiency and simplicity of Tor circuit establishment and hidden services.
In Nikita Borisov and Philippe Golle, editors, *Proceedings of the Seventh Workshop on Privacy Enhancing Technologies (PET 2007)*. Springer, June 2007.

[2] Lasse Øverlier and Paul Syverson.
Valet services: Improving hidden servers with a personal touch.
In George Danezis and Philippe Golle, editors, *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006)*, pages 223–244. Springer, June 2006.

[3] Lasse Øverlier and Paul Syverson.
Locating hidden servers.
In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE CS, May 2006.

[4] Alessandro Acquisti, Roger Dingledine, and Paul Syverson.
On the economics of anonymity.
In Rebecca N. Wright, editor, *Proceedings of Financial Cryptography (FC '03)*. Springer-Verlag, LNCS 2742, January 2003.

[5] Carlisle Adams.
A classification for privacy techniques.
*University of Ottawa Law & Technology Journal*, 3:35–52, 2006.

[6] Ben Adida and Douglas Wikström.
How to shuffle in public.
In *Proceedings of the Theory of Cryptography 2007,*