Research Plan MailVortex

Martin Gwerder

January 2014

Abstract

It has never been so easy to collect huge amounts of data about people. The internet allows not only to quickly reach any point of the world but it also allows to automatically monitor all kind interaction which takes place on it. Mobile connection data, Instant messenger data, data from mail accounts and similar kind of data is available in masses and easy to collect and analyse. Ongoing discoveries show that message flows in the internet and our private life is being traced (see [1], [2], [3] and may more). The information obtained thru these channels is then being combined with other social streams to obtain a profile of a persons social network.

1 Investigators

This topic has been chosen as main topic for a PhD thesis of Martin Gwerder at the University of Basel. Main supervisor will be Prof. Christian F. Tschudin (Head of Computer Networks Group). A second supervisor has yet to be defined. Being a topic of a PhD thesis the work will be carried out by Martin Gwerder. Guidance and quality assurance is assured by the supervisors.

2 Research Questions

The following Question should be investigated: How is it possible to create a secure channel over existing, asynchronous message transfer protocols which is capable to hide Messages and Meta-Information. The information should be at least untraceable for third parties. Optionally the system may hide sender and recipient information.

3 Background and Significance

4 Research Method, Design and Analysis

The following working structure will be used to try to achieve the goals Listed above:

First I analyse current standard. Elaborate known strength and weaknesses thus getting the basic capabilities of the current transport channels.

Next I try to work out the current state of theory regarding transmission of anonymous messages. It has to be destinguished between three types of anonymity at this point. The sender anonymity is given if a sender can not be evaluated given a message which has been delivered or is being delivered. Recipient anonymity is given when the recipient of a message can not be evaluated even if the message content is completely known either at the beginning or the end of a transmission. Third party anonymity is given if a message can not be traced by an observer not involved in sending or receiving the message. This means he would be unable to determine neither the content of the message nor the sender nor the recipient. This part of the work will be very tempting as there are already solution which have been built which address similar topics.

By recombining strength and weaknesses of previous works the research should lead to the next step. A protocol definition which allows a controllable degree of anonymity while using already existing transport technology and thus blending into the regular transfer of the targeted media.

Last step is the verification of the newly designed protocol. It should be analysed based on attacks which are already known to be more or less successful on other anonymity systems.

5 Potential Risks

It is possible that despite careful design of a target solution no acceptable

6 Potential Benefits

7 Bibliography

References

[1] Temporary Committee on the ECHELON Interception System. REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system). 2001. url: `http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN`.

[2] Wikipedia entry on PRISM 2013. url: `https://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29`

[3] Wikipedia entry on TEMPORA 2013. url: `https://en.wikipedia.org/wiki/Tempora`