Technische Universität München, Department of Informatics

Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis B.Sc.

Thesis M.Sc.

Privacy Box – A Next-Gen Secure e-Mail-Like Service

tl;dr: Build a better OnionPi

Motivation

Our aim is to enable the average internet user (with regard to common services like the WWW, e-Mails, VoIP, file sharing...) to protect her privacy without having to rely on third party services which require payment as well as some amount of trust. We use a grass root approach where every user uses a *Privacy Box* which copes with all anonymization and traffic securing while the actual client device (computer, smart phone) does not need more setup than a VPN-connection.

Problem

Electronic mail is still the predominant solution for communication in corporate and private environments. Hence, solutions for secure e-mail based on GnuPG and S-MIME are important. However, S-MIME is typically a corporate solution and GnuPG has various problems concerning ease of use, key management, etc. Furthermore, GnuPG and S-MIME encrypted e-mails still reveal a lot of meta data, i.e., names and addresses of both communication partners. By this reason, thinking about a new mail-like communication service is important.
Our PrivacyBox concept provides a secure and privacy-preserving channel between such Boxes using encryption, TOR-like packet routing and fake traffic. Based on this PrivacyBox service, a mail-like service for communication in (smaller) social groups can be achieved.

Your Task

Your tasks include the elaboration, design and implementation of a concept for a secure and privacy-preserving e-mail-like communication service based upon the principles of our Privacy Box design. More specifically, the solution should provide the following properties/features:

- existing mail clients should be used as a user frontend which frees us from the need to implement a client for various platforms
- the legacy clients communicate with a SMTP/IMAP server on the Privacy Box
- the SMTP/IMAP service needs to be modified in such a way, that outgoing e-mails reaching the SMTP server are handed over to the Privacy Box service and transported to their destination. Vice versa, messages reaching the Privacy Box Service need to be added to the inbox of the IMAP server

Contact

Dr. Holger Kinkelin kinkelin@net.in.tum.de
Marcel von Maltitz, M. Sc. vonmaltitz@net.in.tum.de