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 – Security for Legacy e-Mails

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. While e-mail is insecure by default, open source tools such as GnuPG provide effective means of adding missing security to email. Unfortunately, the integration of GnuPG into email clients is non-trivial. Especially proprietary software products such as Outlook or Apple Mail are problematic. Most times, installation has to be repeated when a new version of the mail client comes out. Finally, the integration of GnuPG in email clients residing in particularly 'closed' environments, e.g., smart phones, cars, or smart TV sets, is almost impossible.

Your Task

Instead of integrating GnuPG directly into a plethora of different email clients, a trusted GnuPG email gateway appears to be a promising alternative. The email gateway connects to the SMTP and IMAP servers the user users to send/receive mail. Vice versa, mail clients of the user connect to the email gateway to send/receive emails.
The mail gateway is now able to transparently add GnuPG functionality to the mail service. When the gateway receives a signed and encrypted mail from an IMAP server, it performs validation and decryption of the mail. The result of the validation and the fact that this mail was received securely can be added as a remark into the email or the subject of the mail. Vice versa, the gateway receives unencrypted/unsigned mails sent by the user's mail client to others, adds the missing digital signature using GnuPG, performs encryption using GnuPG and finally transports the email to the outbound SMTP server.

Contact

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