Secure and Private Messaging – MIR2 project idea

revision 20250310 — project supervisor: martin.pirker@fhstp.ac.at

Setting / Scenario

Recently there was an attack in Austria, see for example this news article:
https://apnews.com/article/austria-stabbing-attack-syria-migration-a7b5c09085eacaff68dc738bfa1459fe

As the article says, the minister suggests "*Karner said that it will ultimately be necessary to carry out a mass screening without cause,*" — meaning, he demands an expansion of lawful mass surveillance of modern digital messaging services.

Review – State of the Art

In order to learn more about the state of the art in security and privacy of messaging services, the first task is a literature review:

What has been discussed/proposed in academic research in this domain in the last years? Review the paper titles, abstracts and if possible, the papers themselves of academic security&privacy conferences. First identify papers that are messaging associated. If yes, then take a closer look and out what they are writing about.

To get you started, in the following are some well-known security and privacy conferences:

I suggest you start at PETS https://petsymposium.org/popets/
as the proceedings of all their papers are freely available for download.
As an example, a noteworthy paper from 2024: "SoK: Metadata-Protecting Communication Systems"
https://petsymposium.org/popets/2024/popets-2024-0030.pdf

There is also IEEE Symposium on Security and Privacy
https://ieeexplore.ieee.org/xpl/conhome/1000646/all-proceedings
…where, for example, this State of Knowledge (SoK) paper was published in 2015:
https://www.ieee-security.org/TC/SP2015/papers-archived/6949a232.pdf

It would be great to find an updated survey/SoK paper like this—surely lots of research happened in the last 10 years?
There is the ACM Survey series: https://dl.acm.org/loi/csur
…maybe something is there to be found?

See also: IEEE European Symposium on Security and Privacy (EuroS&P)
https://ieeexplore.ieee.org/xpl/conhome/1813044/all-proceedings

and ACM CCS: Computer and Communications Security https://dl.acm.org/conference/ccs/proceedings

Also, ARES conference may have papers in this domain: https://dl.acm.org/conference/ares/proceedings

Of course, one can also just use Google Scholar or other search engines to find relevant papers.

See also the ongoing discussion in the EU on client side scanning for illegal material (e.g. child abuse) – “Chat Control”
https://www.patrick-breyer.de/en/posts/chat-control/

For some of the papers the full-text may not be available from the proceedings directly, but if one googles for them, one may find a version on the author’s homepage, an earlier preprint version on arXiv, etc. Please keep an archive of the papers you do review in detail, if possible, and then provide a download to me (so I don’t have to download them myself again)

Aggregation / Organization of Information

Prepare a report that summarizes your findings, use proper references to the papers you refer to. Group the papers you find into categories, e.g. traditional messaging (like Emails) versus modern messaging (like realtime chat), etc.

The report should reflect on the different properties in messaging services, for example:

1) What is an identity in a specific messaging service? An Email address? A cryptographic key? Does one have to identify somewhere first? …

2) Is a messaging service provider able to monitor its customers? How closely? For example, an Email provider can very easily examine every “From” and “To” information of every email - they are always in plaintext, by design.

3) How does a messaging service combat the spam problem? Can everyone send everyone a message? Is blocking of certain senders supported? Or does every message cost something? …

4) What would one need to participate? An app on a mobile phone? Just a webbrowser? ….

…. ….
more interesting properties

Future / Innovation

Propose a new design / infrastructure.

What features are currently missing? What would you like to have?

What are the trade-offs that are always there? What impossible to solve?

What privacy/security would you accept to give up in our modern, networked world?

Propose sub/tasks on how to to get there.

….