MORPHEUS

Paper: https://5x.fi/morpheus/paper.pdf

QR: https://5x.fi/morpheus/help

1495 UNIVERSITY OF ABERDEEN

Mikko Ilmonen
mikko.ilmonen.16@aberdeen.ac.uk
Department of Computing Science

Platform-Agnostic End-to-End Encryption for Modern Instant Messaging Platforms

BACKGROUND

Instant Messaging (IM) data transmitted over the Internet can be **personal, private and sensitive**. We may share data we **intend to keep private**, say things on impulse we later regret, and these **conversations** can potentially **stay stored for years**.

Many applications support IM, but **offer little to no information of the security of chat data**. Security is **implied**, **not proven to the user**.

MOTIVATION

While secure IM apps (such as **Signal**[1]) exist, many **unsecure ones are still being used**.

What if we could have **end-to-end encryption regardless of the platform** we're using?

An **open-source software** solution that users could **adapt to any IM platform?**

DESIGN

Morpheus is a software that **seamlessly integrates with IM platforms**, encrypting and decrypting messages automatically when they are sent and received, respectively.

Uses **PGP**[2] as the secure encryption algorithm. Written using **Go** and **JavaScript**.

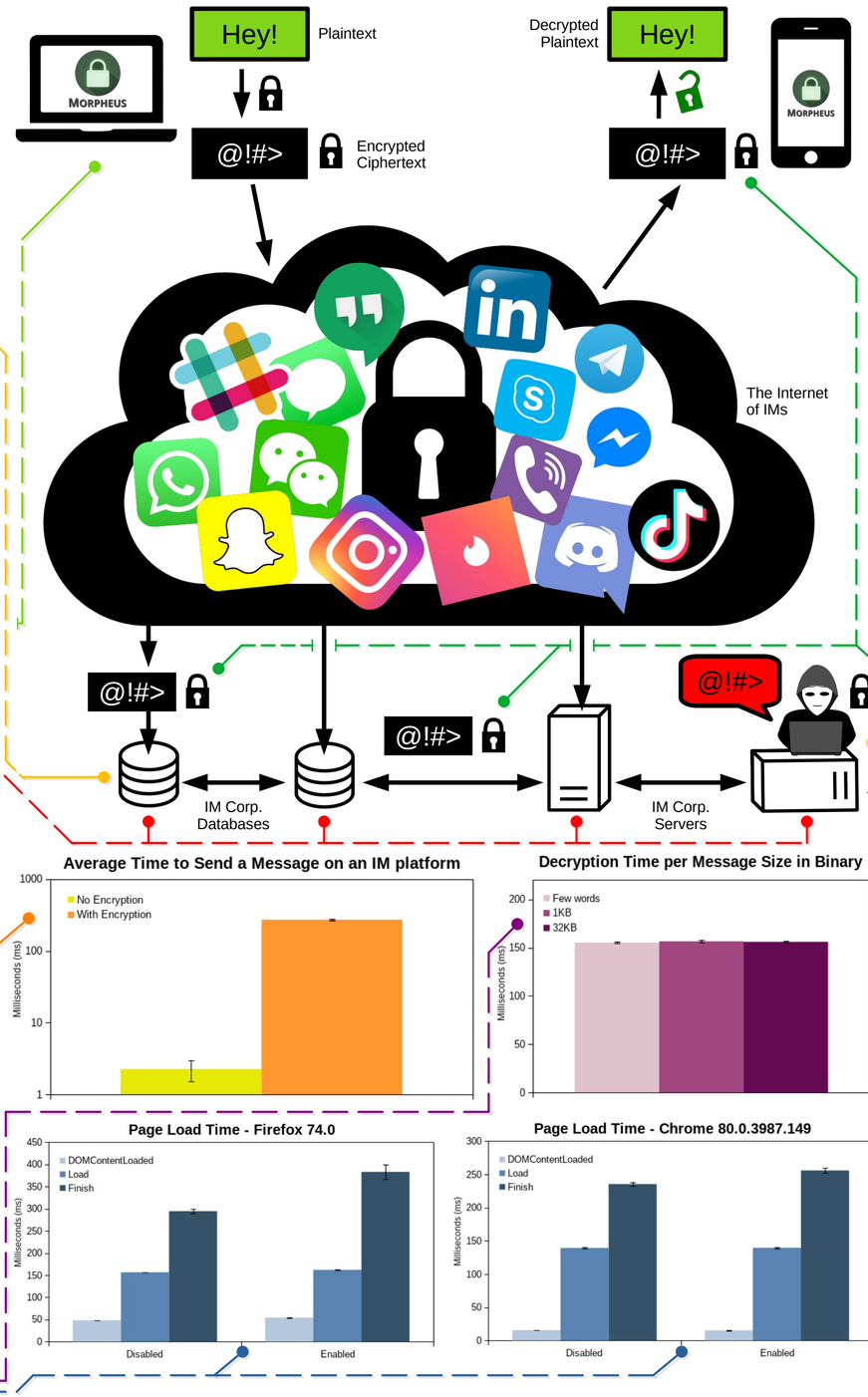
Works as a **Browser Extension** and interfaces with WhatsApp, Slack, Telegram & more.

EVALUATION

~200ms for **encryption**.

~20ms for **decryption** regardless of size.

25-100ms increase in **page load times**[3]



DISCUSSION

No noticeable difference in page load times. Encryption and decryption happen **almost instantaneously**.

Platform-agnostic software; easy module creation for any IM platform. Only **~15 lines of code required for integration** with any platform, after which **secure communication** is available.

CONCLUSION

Increased message security not only during transit, but **everywhere in the IM storage.**

While PGP and key exchange are **slightly difficult** for beginners, they **offer substantial security against both online and offline attacks**. Morpheus has a **help page** to let users get started.

Morpheus works very similarly to e-mail encryption. Software **does not disturb users' workflows**. Mobile is partially supported (via browser).

With some further software work and development, could be a **commercial software** or supported as **"Software as a Service"**.

FUTURE

Eye-dropper tool to pick elements to decrypt and encrypt, **removing need for a module.**

Move from **PGP** to the **Signal protocol**[4]. **Native interfacing** with IMs for desktop and mobile.

Automated **Secure Key Exchange** and establishment of **Trust Networks** in Morpheus.

ACKNOWLEDGEMENTS

Thank you:
- to the **205 Gang** for all the fun moments together.
- **Bruce** & **Wamberto** for your support.
- all the **incredible people** at **Google** who have helped (and still help!) me in my journey.

I wouldn't have made it without you all.

- Mikko

[1]https://signal.org/ [2]https://www.openpgp.org/ [3]depending on the browser [4]https://signal.org/docs/