MW4ALL: supporting identity-free and secure file transfers

Summary

MW4ALL consists of two NGI_Trust projects (Phase 1 and Phase 2, known as "MW4ALL 2.0") aimed at creating a viable product that can facilitate easy, fast and secure file transfers between two consenting devices. The Magic Wormhole protocol allows two parties to transfer files using a simple code, rather than personal data like an email address or username.

The MW4ALL projects investigated whether this open source technology can be scaled and commercialised without compromising on security or privacy. In the MW4ALL 2.0 project, we adapted the technology for web usage, developed an alpha version of the file transfer app, conducted rounds of user testing and further narrowed down a sustainability model. In doing so, we have created an application that makes secure and privacy-conscious file transfers accessible for everyone, which we will later release as a consumer product.

Keywords

Security, privacy, file transfer

Actors involved in the project

Least Authority TFA GmbH: https://leastauthority.com

The NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

The project

Sending files, which millions of us do on a daily basis, is not as easy as it first might appear. Email attachments have a maximum file size, some tools require the recipient to have a specific app/device to receive the files, and messaging apps require both parties to already be connected with each other (often exposing each other's contact information). Moreover, file transfer platforms tend to be able to read your files.

Ensuring people can communicate freely and enjoy the right to privacy is fundamental to a human-centric internet and a cornerstone of any free society. With this in mind, one potential solution to the question of secure and easy file transfer comes in the form of Magic Wormhole. It is an innovative open source protocol that allows two devices to establish a secure connection using a simple, single-use code (e.g. 8-rabbit-table), rather than by personal data like an email address or phone number. By foregoing the latter, Magic Wormhole provides connectivity without people needing to expose their identity to each other, or the service provider. With this protocol used in a file transfer application, sending files happens instantly (as both the sender and recipient need to have the application open simultaneously). Moreover, since files are end-to-end encrypted and the data is never stored in the cloud, neither party should be concerned that their files will be opened by a third party.

And so, in Spring 2020 and thanks to NGI_Trust funding, Least Authority, a Berlin-based technology company supporting people's right to privacy, sought to examine the commercial viability of the technology.

At the time, Least Authority had prior experience using Magic Wormhole for other tools and understood its potential. Over two rounds of funding (ending July 2021), Least Authority has aimed to determine whether Magic Wormhole could upgrade file transfers, a daily activity of millions of people, to a level of much greater security and privacy than is currently commonly used, and to execute on it. The projects were aptly named MW4ALL — Magic Wormhole for All — and MW4ALL 2.0.

From Kick-off to Alpha

To determine the viability of our idea, we worked on answering three questions:

1. How can we develop Magic Wormhole to create a product that best meets user needs (user research)?

2. Is it technically feasible to leverage the technology to meet these needs (technical development)?

3. How can we ensure the future of this product beyond the duration of the NGI_Trust grant (market research & long-term viability)?

The project kicked off with a survey of 100 people across the EU to determine user behaviour in terms of file transfers, including the methods adopted and the advantages and disadvantages of each. We learned how and why people typically use multiple tools and, by analysing over 200 other factors affecting participants' tool choice, we shortlisted Magic Wormhole's added value (table 1).

Table 1. Magic Wormhole's key differentiators

Convenience and speed	Users don't need to: sign up, enter their contact information of that of the recipient, or separately download/upload files. Instead, they simply drag and drop a file and pass on the generated code to the intended recipient.
Ability to send large files	The maximum file size is currently capped at 4 Gigabytes, though we can choose to remove this restriction.
Secure and Private	The protocol and application use end-to-end encryption. They are open source, and their code can be independently verified. The non-requirement of personal or contact information of the sender and recipient allows for anonymous file transfers.
Device/OS agnostic	The product has the potential to be platform agnostic: as an open protocol, it can be developed as an application for every major desktop (Windows, Mac, Linux) and mobile (Android, iOS) platform. As a web app, users needn't worry about what device or platform the intended recipient has.

Concurrently, we explored technical development needs and ways to scale the Magic Wormhole protocol, including how to ensure it can withstand certain types of attacks or adversarial network observers.

We have since adapted the Golang-implementation of Magic Wormhole (wormhole-william) for use with WebAssembly and made this implementation and the protocol compatible with websockets. This paved the way for using the protocol in any web browser. We also carried out several rounds of user testing, first with a wireframe prototype of the application, and later with the alpha prototype.

We still seek to make a number of improvements to the alpha version before we have a beta version and later a stable version for production use. In addition to bug-fixing and addressing tech debt, we are also making design and copy improvements, as we learned from user testing that people may not understand that both the sender and receiver need to be online simultaneously for file transfers to complete.

Despite this work ahead, having the tried-and-tested Magic Wormhole protocol now accessible in a web browser is a major achievement. With it, making file transfers in a secure and identity-free way, will be in reach for many more people.

Looking to the future

In the coming months, we will continue our work on our web product, finalize a product name and associated branding, and gear up for a public release. This process has been supported by NGI_Trust project coaches, who have generously shared insights, advice and asked us probing questions, which has helped us adopt a more business-minded approach as we prepare to launch to market.

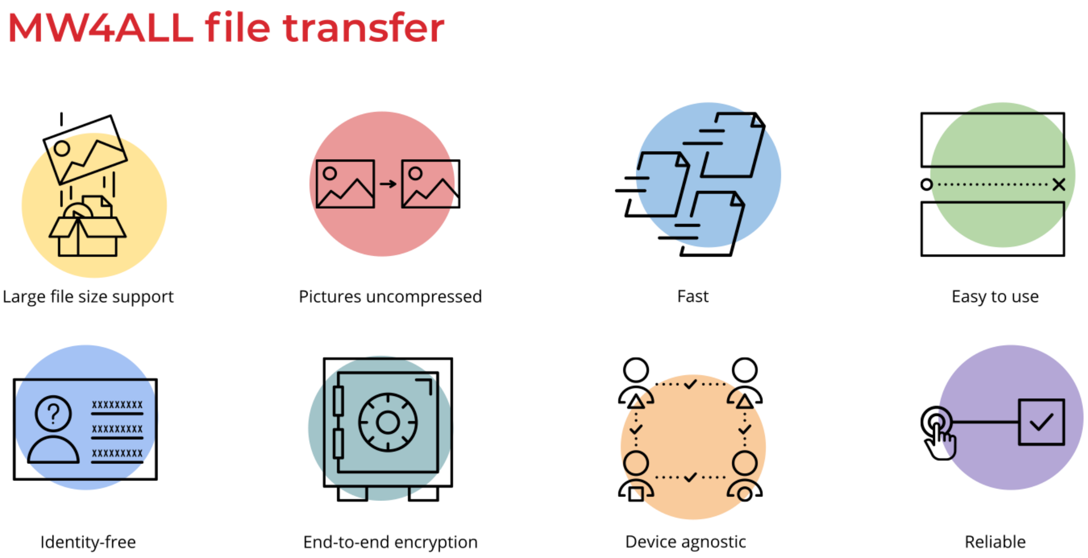

Figure 1. MW4ALL Icons

While our focus right now is web-to-web transfers, we plan to explore options to offer downloadable mobile and desktop applications for added functionality and security in the future. We also hope to support multiple files transfer, utilizing the 'Dilation protocol' for connection resumption and 'Seeds' for persistent connections / contact lists.

This project has helped us create something we believe in: usable technology solutions that advance digital security and privacy. We are grateful to NGI_Trust for their expertise and support in helping us further this important technology that contributes to a human-centric internet. And we are pleased to note that our product, like the protocol on which it is based, is open source code. We hope that researchers, innovators and technology developers will use this technology, develop it and contribute to it. It is, after all, only through our collective effort that we can hope to mainstream privacy and security in technology and preserve privacy as a fundamental human right.