Hermod: A File Transfer Protocol Using The Noise Protocol Framework

Markus Åkesson

June 11, 2020

Since the introduction of SSH File Transfer Protocol (SFTP) in Secure Shel version 2, SFTP has become the standard protocol for secure file transfer. Since there are no proper alternatives to SFTP, our options for conducting secure file transfers would be limited if any vulnerability relating to its security would be found. Hermod provides an alternative protocol for secure file transfer, built using the lessons learned from flaws in SSH and using a modern framework for constructing cryptographic protocols.

SSH and SFTP

SSH has since its release become a crucial part for performing remote system management as it enables the establishment of secure communications channels over potential insecure networks. Following the introduction of the SSH File Transfer Protocol, SSH has further strengthened its position by also enabling secure file transfer.

Due to the rather large scope of SSH, it has grown to become a large and complex protocol. The large scope also comes with extensive configuration and support for outdated ciphers. Users that are only interested in conducting secure file transfers still need to pull in support for remote execution, proxy services etc. The development of a new protocol, can ensure that the protocol focuses on providing secure file transfers using modern cryptography and with minimal complexity.

Noise Protocol Framework

The Noise Protocol Framework (Noise) is a newly released framework for building Diffie-Hellman based cryptographic protocols. Noise contains, among other features, support for mutual and optional authentication, identity hiding, forward secrecy and zero round-trip encryption, which makes it a promising alternative to use when securing the communication channel in a new file transfer protocol. By using Noise for designing a new cryptographic protocol, developers can rely on the framework for establishing a secure tunnel instead of needing to create their own handshake method.

Hermod

Hermod is the proposed new protocol for conducting secure file transfers. It uses the *KK-pattern* from Noise, ensuring that files are sent encrypted with strong Forward Secrecy. Similar to SFTP, a static key pair is used for both client and server authentication. The client is further identified with an ID-token, randomly generated when creating the clients key pair. Hermod defaults to generating a new set of credential, containing an ID-token and static key pair, for each individual server the client wants to exchange files with.

Compared to SSH and SFTP, Hermod provides a simple and minimal interface and no security related configuration options. While the security properties between Hermod and SFTP (through SSH) are similar, Hermod comes with a huge performance boost when transferring smaller files, up to 25x faster. For larger files, Hermod still outperforms SFTP, although with a much smaller margin.

The reference implementation of Hermod is written

in Rust, taking full advantage of its ownership-model for memory object. This ensures memory-safety and thread-safety for the binary resulting in a reliable and permanent implementation.