Anastasis - Multiparty key escrow service

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Christian Grothoff
Expert: Pierre-Yves Voirol (ABACUS Research AG)
Industrial partner: Taler Systems S.A., Erpeldange, Luxembourg; pEp Security SA, Zürich

Users of cryptography are frequently facing the challenge to secure their core secrets, and the contemporary default of asking them to remember strong passphrases is inadequate for mass adoption. With Anastasis we solve this issue by developing a system which allows its users to securely deposit shares of a core secret with an open set of escrow providers, and to recover the secret if the user lost it by using standard multifactor authentication methods.

Introduction

In many cases, losing a core secret means the loss of data availability and data confidentiality. In the case of a digital wallet, for example, the loss of the core secret can lead to great economic damage and even threaten the existence of a company. Unfortunately, there are no practical solutions known to us that on the one hand guarantee that the user can reliably restore the core secret without necessarily having to rely on another password or other key material, and on the other hand enable the user to remain in control of their data. We develop Anastasis as a Free Software solution for the described problem.

Procedure

Identity-based key derivation

Because the use of Anastasis without relying on a strong passphrase is essential for us, we derive keys used in Anastasis from hard to guess, semi-private and unforgettably inherent attributes such as name and passport number, social security number or AHV number. We use Argon2 as key derivation function, which makes brute forcing the keys harder. In addition, per provider salts flow into the key derivation process to ensure keys differ between providers. This obscures the link between the data stored at the different providers.

Multi-factor authentication

It is not impossible for someone to come into possession of the personal attributes of a user. That's why our design supports the use of several standard multi-factor authentication methods (such as SMS, email, security question, postident and videoident) to authenticate the user. This makes it more difficult for potential attackers to gain unauthorized access to data.

Share the core secret

We split the master secret of the user, which is used for symmetric encryption of the users core secret, into different shares and encrypt them with one of the derived keys. The different master key shares are each annotated with authentication instructions, such as the user's phone number if recovering the share is to be authorized via SMS authentication. The results are encrypted with a second key derived from the user's inherent attributes and uploaded to one or more escrow providers.

Recover the core secret

To recover the core secret, the user has to derive the identity-based keys again, provide the second key to the service providers and authorize recovery. When authorization is successful the providers return the encrypted shares of the master secret to the user who decrypts the shares with the first derived key and reassembles the master secret. The user can then decrypt their core secret.

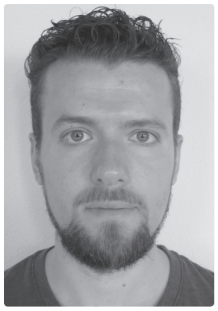
Result

We implemented Anastasis with a REST-API for HTTP-based operations and a client library to provide functions for secret sharing and secret recovery. Anastasis is designed to be extensible with different methods and payment solutions. A command line tool is available for interactive use. We also started to plan the graphical user experience.

Next steps

Because we see great potential in Anastasis, we want to further develop Anastasis and bring it to market. We have already been able to win business customers for this purpose and are now building up our company.

Dominik Samuel Meister



Dennis Neufeld