Resent-From: alias-bounces@ietf.org
Resent-To: lixia@cs.ucla.edu, ietf@dkutscher.net
From: Phillip Hallam-Baker <phill@hallambaker.com>
Subject: Decentralization workshop submission: Autonomy is the real goal.
Date: 5. May 2021 at 23:02
To: dinrg-chairs@irtf.org

The Mathematical Mesh 'Mesh' is a cryptographic security framework that has the goal of making each individual user of the Internet their own ultimate trust authority. Originally planned as a means of achieving a fully decentralized, zero-trust environment as the workshop CFP appears to envisage, it was realized that a less rigid, less ideological approach would better serve the real goal of autonomy.

Ten years ago, the doctrine of 'zero trust' led me to conceive the use of threshold encryption techniques to maintain a password vault for an individual user or a social media service for a group of users without being able to read any of the content hosted. Having engineered a situation in which the service is completely untrusted, I started to realize that this was not the optimum approach. What if a user loses their device and wants to prevent it accessing their encrypted password vault? The obvious solution was to allow the user to tell the service to refuse decryption requests for the device that was missing. This is clearly the right approach but in the process, the zero-trust service has become trusted.

This led to the realization that trust could not be eliminated, only managed. It is the ability to minimize the extent to which other parties are trusted and for what risks that is important. I can use encryption to provide complete protection of confidentiality with respect to my ISP but I can only mitigate exposure to service risks.

The paradox of the Web is that the attempt to decentralize the publication of ideas and knowledge has instead led to an unprecedented concentration of power over information. The Web gives anyone with access the ability to publish but only a very small number have the ability to be heard.

A core principle of the Mesh is that it grants users individual autonomy. If Alice decides to change her SMTP email provider from example.com to example.net, this requires her to advise every one of her contacts that she has changed her email from alice@example.com to alice@example.net. This switching cost is traditionally seen as an advantage to the provider at example.com as it discourages Alice from switching providers. That the disadvantage to the user is much greater will be understood by anyone who has been forced to change their email address because of a change of school, employment or broadband provider.

The lack of autonomy is even worse for messaging, voice and video applications. Like most established Internet users, I maintain accounts at a half dozen messaging services because there is no consensus on picking a single one and because

The Internet is for users but the Domain Name System and the WebPKI are only designed to identify organizations. DNS names are not owned, they are rented at an annual cost that exceeds the weekly wage of over a billion people. If the Internet is going to be for people, we need a naming system that is designed to meet the needs of people, not organizations.

DNS has long been recognized as the chief centralization point of the Internet and Web. As a result of architectural choices made when the Internet was small, DNS is also among the most expensive infrastructures to maintain. The cost of entering names in the registry is trivial. The cost of providing name query service to anyone on the Internet is vast and not least because over 95% of all queries received by core DNS services are abuse.

The Mesh Callsign registry began as a means of allowing Alice to transfer her account from one Mesh Service Provider to another with minimal switching cost. Unlike traditional accounts that are created by a service provider and bound to an account name that remains under control of that provider, all Mesh accounts are bound to a public signature key that serves as the root of trust for that account. Thus to transfer her account from example.com to example.net, allt that Alice needs to do is to sign an assertion to that effect and post it to some public registry that might be discovered by Bob.

This notion is of course closely related to that of Brian LaMachia's PGP key servers with the important difference that the Haber-Stornetta patent having expired, the obvious way to distribute such information is with an append only log authenticated by means of a Merkle tree (cf, NameCoin, Trans).

In this configuration Alice used the account name alice@example.com and a decentralized collection of autonomous registries provide the 'change of address' notification capability. Unfortunately, simulation studies suggested that the decentralization would be rather short lived. Network effects will inevitably lead to the emergence of a canonical registry which would provide a control point. Rather than attempt pure decentralization and end up with an unchecked control point, the interests of user autonomy are better served by minimizing the extent of the centralization and implementing separation of duties controls to mitigate the resulting risks.

The Mesh callsign registry emerged from these considerations. A callsign is a UNICODE label meeting specific constraints whose use is described in an entry in an append only log. Every callsign entry must specify the fingerprint of the public key representing the root of trust for interpreting that name. Entries MAY also contain addresses for Mesh service provision and for provision of other Internet services bound to that callsign.

Unlike DNS names, callsigns are issued for life and cannot be withdrawn except in specific circumstances. Unlike in the DNS model where the zone file is a trade secret and query service provided by the registry, the callsign registry log is a public document and Mesh service providers subscribe to updates so they can provide query providers to their customers (and others should they choose). This offloads virtually all costs associated with name registration from the registry making it possible to register names for life at a cost of less than $0.10 each.

Unlike DNSSEC or the WebPKI where name registration and key validation are performed as separate actions, the Callsign registry combines these functions as a single atomic function. By definition @alice is whoever controls the key that was bound to that name when the callsign entry was created.

Unlike NameCoin and other 'proof of waste' schemes, the integrity of the callsign registry is established through a process of cross notarization with the Mesh service providers using its services which in turn cross notarize with each of their customers. Thus to establish the integrity of a callsign entry published a week ago, Alice's device will validate a chain of notary assertions whose ultimate root of trust is Alice herself. To this extent the Callsign registry is more decentralized than any existing scheme (and does not require burning the Amazon rainforest to do so).

Thus the callsign registry provides Alice with the ability to register a name '@alice' that she can use for the rest of her life and to which she can bind any other type of communication identifier she might require. These include:

Alice's current Mesh Service provider (example.com or @example)
Alice's personal Web sites (https://alice.mesh/)
Alice's current SMTP email address (was alice@example.com, now alice@example.net).
Alice's PGP key and S/MIME cert
DNSSEC signing key for Alice's personal pseudo-domain alice.mesh
IP address for authoritative name service for alice.mesh

A technical specification and pathfinder implementation have been produced as proof of concept for the Callsign concept. Putting the concept into production would of course require the creation of a not-for-profit corporation to run the registry and a board to oversee disbursement of profits accruing from the operation of the registry if the project is successful.

Mathematical Mesh 3.0 Part VII: Mesh Callsign Service (ietf.org)