Project Neruda

isaac@freenetworkmovement.org

1 Objectives

- Create a unified identity mechanism based on existing tools and protocols.
- Build a secure, decentralized, and resilient path into the Santiago service discovery mechanism.
- Establish an open yet hardened overlay network by integrating cryptographic trust mechanisms into peering protocols.

2 Background

In order to guard against the natural failings of both human and technological systems, hackers in the first part of our millenium found it useful to build systems that were completely decentralized. One of the discoveries that made such efforts possible was the Distributed Hash Table. DHTs constitute a class of algorithm that allows for distributed storage and retrieval of key-value pairs.

Such decentralized systems are generally more resilient than centralized ones, but they are vulnerable to attack as long as their membership remains open. In particular, a vector known as a 'sybil attack' takes advantage of the fact that an adversary with sufficient resources can add an arbitrarily large amount of bad-actor nodes to an open system, thereby rendering the system unusable.

In 2008 and 2009, white papers were published by researchers such as Petar Maymounkov and Chris Lesniewski-Laas that theoretically established the possibility of hardening DHTs against sybil attacks by building trust mechanisms into their architecture.

There are existing free systems which have explored this possibility, and which might serve as a starting point for the development of Neruda. The three primary candidates are Cspace, RetroShare and Tonika. Cspace participates in a DHT which maps a public key to an IP address, but it is underdeveloped and does not appear to be currently maintained. RetroShare relies on the (unhardened) BitTorrent DHT to find addresses, and on GPG for identity verification, but these processes are distinct. Finally, Tonika is being written in Go by Maymounkov (the author of Kademlia). Tonika is perhaps the most promising candidate, though it is not well documented and (like RetroShare) includes a host of related, but superfluous functionalities.

3 Proposal

FreedomBox is a project that aims to allow users to easily own their own data (media, messages, etc) and to share that data securely with whomever they choose. In order to do so, users must be able first to find one another, and subsequently to discover usable modes of communication. Neruda is a project to solve for the first step, and is intended to be paired with the Santiago service discovery mechanism.

Of all current endeavors to decentralize and secure communications on the Internet, the FreedomBox project is uniquely positioned to effectively bootstrap a system with what Maymounkov calls 'organic security.' Because of its strong ties with the Debian community, which has built the world's most robust cryptographic trust network (the GPG strong set), FreedomBox can effectively launch a trust-backed distributed data store.

In particular, Neruda would be a distributed hash table whose search keys would be long-form GPG Key IDs, and whose values would be the IPv6 address currently associated with the key in question. (Search key and crypto key are therefore identical). The trust mechanisms built into the GPG protocols could be used to secure the hash table against both poisoning and sybil attacks by limiting the participation of untrusted nodes. Once a Key ID is hashed to a v6 address, that address can be queried using the Santiago mechanism, and secure, authenticated exchange of information can commence.