Freenet
The forgotten cryptopunk paradise

Arne Babenhauserheide

February 1, 2015

A long time ago in a chatroom far away, select groups of crypto-anarchists gathered to discuss the death of privacy since the NSA could spy on all communications with ease. Among those who proposed technical solutions was a student going by the name sanity, and he published the widely regarded first paper on Freenet: A decentralized anonymous datastore which was meant to be a cryptopunk paradise: true censorship resistance, no central authority and long lifetime only for information which people were actually interested in.

Many years passed, two towers fell, the empire expanded its hunt for rebels all over the globe, and now, as the empire's grip has become so horrid that even the most loyal servants of the emperors turn against them and expose their dark secrets to the masses, Freenet is still moving forward. Lost to the eye of the public, it shaped and reshaped itself - all the while maintaining its focus to provide true freedom of the press in the internet.

A new old hope

Once only a way to anonymously publish one-shot websites anonymously into Freenet that other members of the group could see, it now provides its users with most services found in the normal internet, yet safe from the prying eyes of the empire. Its users communicate with each other using email which hides metadata, micro-blogging with real anonymity, forums on a wide number of topics - from politics to drug-experiences - and websites with update-notifications (howto) whose topics span from music and anime over religion and programming to life without a state and the deepest pits of depravity.

All these possibilities emerge from its decentralized datastore and the tools built on top of a practically immutable data structure, and all its goals emerge from providing real freedom of the press. Decentralization is required to avoid providing a central place for censorship. Anonymity is needed to protect people against censorship by threat of subsequent punishment, prominently used in China where it is only illegal to write something

against the state if too many people should happen to read it. Private communication is needed to allow whistleblowers to contact journalists and also to discuss articles before publication, invisible access to information makes it hard to censor articles by making everyone a suspect who reads one of those articles, as practiced by the NSA which puts everyone on the watchlist who accesses freenetproject.org (reported by german public TV program Panorama). And all this has to be convenient enough that journalists to actually use it during their quite stressful daily work. As side effect it provides true online freedom, because if something is safe enough for a whistleblower, it is likely safe enough for most other communication, too.

These goals pushed Freenet development into areas which other groups only touched much later - or not at all. And except for convenience, which is much harder to get right in a privacy-sensitive context than it seems, Freenet nowadays manages to fulfill these goals very well.

The empire strikes the web

The cloud was "invented" and found to be unsafe, yet Freenet already provided its users with a safe cloud. Email was found to spill all your secrets, while Freenet already provided its users with privacy preserving emails. Disaster control became all the rage after hurricane Katrina and researchers scrambled to find solutions for communicating on restricted routes, and Freenet already provided a globally connectable darknet on friend-to-friend connections. Blogs drowned in spam comments and most caved in and switched to centralized commenting solutions, which made the fabled blogosphere into little more than a PR outlet for Facebook, but Freenet already provided spam resistance via an actually working web of trust - after seeing the non-spam-resistant forum system Frost burn when some trolls realized that true anonymity also means complete freedom to use spam-bots. Censorship and total surveillance of user behavior on Facebook was exposed, G+ required users to use their real names and Twitter got blocked in many repressive regimes, whereas Freenet already provided hackers with convenient, decentralized, anonymous micro-blogging. Now websites are cracked by the minute and constant attacks made it a chore for private webmasters simply to stay available, though Freenet already offers attack-resistant hosting which stays online as long as people where interested in the content.

All these developments happened in a private microcosmos, where new and strange ideas could form and hatch, an incubator where reality could be rethought and rewritten to reestablish privacy in the internet. The internet was hit hard, and Freenet evolved to provide a refuge for those who could use it.

The return of privacy

What started as the idea of a student was driven forward by about a dozen free-time coders and one paid developer for more than a decade - funded by donations from countless individuals - and turned into a true forgotten cryptopunk paradise: actual working solutions to seemingly impossible problems, highly detailed documentation streams in a vast nothingness to be explored only by the initiated (where RTFS is a common answer: Read The Friendly Source), all this with plans and discussions about saving the world mixed in.

The practical capabilities of Freenet should be known to every cryptopunk - but a combination of mediocre user experience, bad communication and worse PR (and maybe something more sinister, if Poul-Henning Kamp should prove to be farsighted about project Orchestra) brought us to a world where a new, fancy, half finished, partially thought through, cash-cow searching project comes around and instead of being asked "how's that different from Freenet?", the next time I talk to a random crypto-loving stranger about Freenet I am asked "how is Freenet different from X which just made the news?" (the answer which fits every single time is: "Even if X should work, it would provide only half of Freenet, and none of the really important features - friend-to-friend darknet, access dependent content lifetime, decentralized spam resistance, stable pseudonyms, hosting without a server").

Now, after many years of work have culminated in a big step forward, it is time for Freenet to re-emerge from hiding and take its place as one of the few privacy tools actually proven to work - and as the single tool with the most ambitious goal: Reestablishing freedom of the press and freedom of speech in the internet.

Since its focus has been on the big goals, there are lots of low hanging fruit: small tasks which allow reaping the fruits of existing solutions to hard problems. For example my recent work on freenet includes 4 hours of hacking the Python-based site uploader in pyFreenet which sped up the load time of its sites by up to a factor of 4. If you want to join, come to #freenet @ freenode and check the github-project.