Practical and Elite Chat Protocols

Presented by Jacob Welsh & Robinson Dorion

JWRD Computing – *Making Smart Tools for Smart People since 2015*

WoT: dorion, 54CCA1FC8C2E414C63BFB6CF0E48266E54D6B95A
WoT: jfw, 0CBC05941D03FD95C3A47654AE0DF306025594B3

Robinson's blog: http://dorion-mode.com
Jacob's blog: http://fixpoint.welshcomputing.com
WWW: http://jwrd.net
Email: sales@jwrd.net
Slides : `http://dorion-mode.com/junto-practical-and-elite-chat-protocols-20230802.pdf`

Wed, Aug 2, 2023

What is a Network Protocol ?

- A set of rules that determine how data is transmitted between computers across a network independent of any differences in their internal processes, structure or design.
- Publisher of a protocol implementations adhere to the rules and cannot change them, but can reliably build upon.
- Protocols empower publisher's and users alike by engendering competition and coexistence among implementations to meet the varying needs of a diverse market.
- A published has to respond to feedback received from his target market to innovate and find solutions for the problems his user's report if aims to grow the usage of his implementation
- Protocols treat publishers and users like adults and create an environment and incentives that enable them by opening up opportunities and thus engender higher quality, long term client service.

What is a Platform ?

- A centralized service in which its owners make all the rules and implementation decisions, both of which can be changed on a whim.
- Users must accept these changes or leave. If particular users don't like the changes and are in the minority, they either fall in line or are banned.
- Infantilize and disable users and close down horizons in the user's mind so as to facilitate their exploitation and ideally in a way they never manage to detect.
- Grow depends on fashion, being trendy.
- Repressing worthy minorities limits the horizons of the platform's development.
- Growth breeds bureaucracy, bureaucracy stifles and devolves to death.

An Eulora Message of the Day, published on Ossasepia

[1] "The strongest indication that you lost your way is to find a large majority in agreement with you."

[1] http://ossasepia.com/2022/06/23/all-tattoos-are-temporary

Signal's Official Development Ideology

"Truths which we believe to be self-evident :"

1. The answer is not more options. If you feel compelled to add a preference that's exposed to the user, it's very possible you've made a wrong turn somewhere.
2. The user doesn't know what a key is. We need to minimize the points at which a user is exposed to this sort of terminology as extremely as possible.
3. There are no power users. The idea that some users "understand" concepts better than others has proven to be, for the most part, false. If anything, "power users" are more dangerous than the rest, and we should avoid exposing dangerous functionality to them.
4. If it's "like PGP," it's wrong. PGP is our guide for what not to do.

From, *The ecosystem is moving on* by Mike Benham, Signal's creator, CEO until 2022 and Emeritus board member

"Cannibalizing a federated application-layer protocol into a centralized service is almost a sure recipe for a successful consumer product today."

A weak, noisy Signal

- A system is only as secure as its weakest link.
- Phone number, rather than encryption key is used as primary identity. User cannot own phone number, SIM swapping happens with regularly.
- Phones are a poor match for cryptographic applications because they have poor sources of entropy and any cryptographic system is only as secure and strong as the entropy source that lies at its root.
- The dependency of phones and phone numbers pretty much shoots any user's hopes of anonymity or pseudonymity in the head.

But it’s Open Source !!!

Open Source, yes ; Comprehensible ? Negativo.

- Before you can even compile the Signal code you have to compile some 90 –that’s nine zero– dependencies.
- Has anyone even read all of those, let alone begun to understand them and how they fit together ?
- If no one has the time to read and comprehend it does it matter if it’s open source ?
- Continual code turn over : even if you did read and understand it, they force updates about every quarter.

But you can run your own client and server !!!

Yes, but they discourage you.

To quote Benham from 2016

“I’m not OK with LibreSignal using our servers, and I’m not OK with LibreSignal using the name ”Signal.” You’re free to use our source code for whatever you would like under the terms of the license, but you’re not entitled to use our name or the service that we run.

And reiterated by one of the lackeys in 2020

“We really don’t want forked versions of the app maintained by other parties connecting to our servers.

Take away : if you run your own client or server, they want you isolated on an island.

Server issues : it's centralized platforms all the way down.

- Signal maintains no official documentation for installing the software.
- Per an unofficial guide, the requirements are :
  - SSL Certificate of your server's domain
  - Google Recaptcha
  - Firebase by Google
  - Twilio
  - Amazon Web Service S3 and Cloudfront
  - AWS SQS
  - AWS DynamoDB
  - Micrometer
  - Fixer

Terrorist question : Maybe, maaaaaybe, the Signal isn't selling user information directly, but what about the companies it is built atop of ?

Summary and next steps ?

- Signal cannot honestly be considered secure and only makes the claims to exploit users by giving a false sense of security.
- Use WhatsCrapp or similar centralized platform if you want convenience for talking with the masses.
- Write there as if you expect your text to be published on a widely read publication.
- Follow along and learn about IRC.

IRC's beginnings

- IRC was invented by a Finn called Jarkko Oikarinen and first published at the end of August 1988.
- Publicly and formally defined as a protocol in May, 1993, in RFC 1459 by Oikarinen and Darren Reed.
- Gained notariety for subverting "media blockades" in war zones :
  - Gulf War of 1991 ;
  - Gorbachev coup d'etat in '91

IRC structure

- There are several IRC networks and a wide variety of IRC implementations for both server and client code.
- JWRD runs an IRC server and implemented and maintains an IRC client called yrc.
- While the IRC protocol doesn't include strong encryption, strong encryption can and has been layered on top.

Bitcoin origins : IRC + PGP WoT

- In November 2010, Daniel Folkinshteyn (WoT: nanotube) implemented the Bitcoin Over the Counter (OTC) Web of Trust (WoT) leveraging another Internet Standard, OpenPGP.
- The interface for interacting with the WoT was implemented over the Freenode IRC network where parties authenitcated with encrypted challenge-response, communicated, negotiated trades and sent and received ratings.
- Everyone's using PGP already, exchange of ciphertexts readily available when needed.
- By 2011, all the relevant parties were communicating via IRC ; became the de facto public forum of Bitcoin politics, finance and development.
- Would Bitcoin have ever gotten off the ground without IRC + PGP WoT ?

Bootstrapping Bitcoin finance, politics and development

- Nurtured an innovative, Bitcoin-centric, framework for finance, politics and technical development.
- On the financial side, the GPG Contract was the instrument upon which the most innovative and biggest Bitcoin company was built : MPEX, the Bitcoin Securities Exchange.
- On the diplomacy side, when the SEC tried to open a real time communication channel with the leader of Bitcoin finance, Mircea Popescu, he required they use IRC and register a key in the WoT, thus taking steps towards implementing Bitcoin as a sovereign.
- On the Bitcoin governance side, when Gavin Bell and Luke-Jr attempted to hardfork the Bitcoin protocol, they made their futile pleas on IRC.

So why has IRC usage declined ?

- Most early Bitcoiners overlooked the value upon which they we sitting, n00bs are herded towards platforms.
- The perceived abundance of late stage socialism being fueled by an unprecedented credit bubble.
- “Hard times create strong men. Strong men create good times. Good times create weak men. And, weak men create hard times.” – *Those Who Remain*, by G. Michael Hopf
- Despite usage decline of the very open IRC over the years, it nevertheless endures and keeps serving new generations of users.
- Meanwhile, the “popular” platforms surf one wave of popularity while it lasts, corralling their users into centralised pens for as long as they are naive enough to stay docilely there to be shorn.
- The platforms change names and nothing much : AOL, Myspace, Facebook is now Meta, Twitter is now X, Tumblr is now Instagram, Blogspot turned to Medium turned to Substack, et cetera.

What are you going to do when the bubble burts ?

- Bitcoin is one tool, one very powerful tool, but is it enough in and of itself ?
- Or is it only one protocol that does its job very well, but needs to be combined with other protocols to create new markets to truly realize its potential ?
- Problem with central banks, and tyranical governments, sure. Why not apply that skepticism to centralized communications tools ?
- Does Meta survive the credit bubble bursting ? Does Twitter ?
- If you continue to rely on centralized communications platforms, to what extent are you increasing your exposure to social engineering (the primary threat market in security) and Sybil attacks ?

Learning is not compulsory, neither is survival.

Being a Bitcoiner means more than just owning some coin or even running a node it means adapting yourself to the Bitcoin model, which means learning the Variety Speak.

From *You're gonna have to learn that Variety Speak* on Trilema by Mircea Popescu

"In Bitcoin (the Variety Speak) means, IRC, the WoT and a small amount of phone number."

Take heed of the advice of the wolf in the ancient fable :

An ancient fable.

"The fox asks the wolf why's he sharpening his teeth when there's no one to fight, to which the wolf retorts that when there'll be someone to fight there's going to be no time to sharpen teeth."

How to IRC with JWRD

Demo Time.

Questions, Comments

Thank you for your time and attention.

Presentation Slides available for download at:

`http://dorion-mode.com/junto-practical-and-elite-chat-protocols-20230802.pdf`