Ricochet-Refresh, Gosling, and future work

blueprint for FREE SPEECH

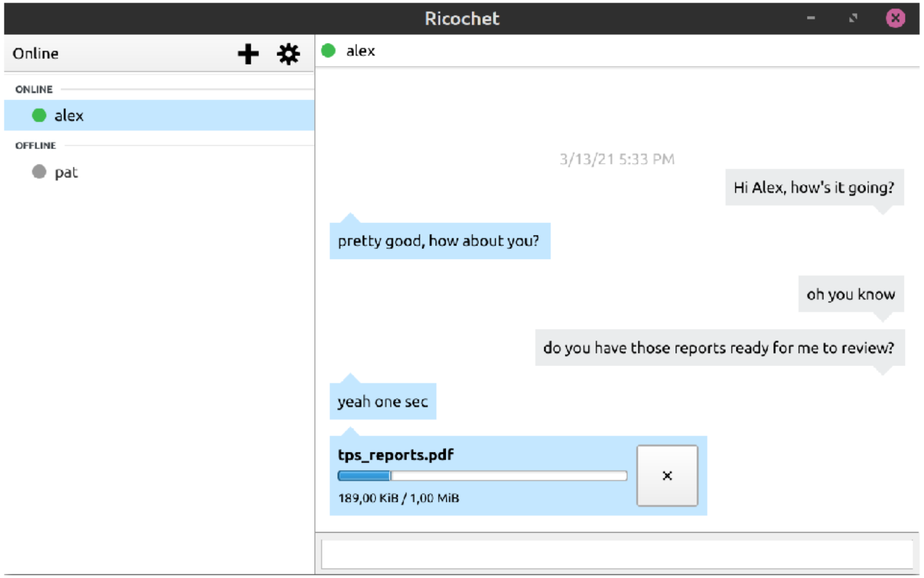
richard (they/them)
richard@blueprintforfreespeech.net

Introductions

- Blueprint for Free Speech is an international non-profit that promotes the right to freedom of expression
- Maintainer of Ricochet-Refresh
- Developing Gosling
- Find us in the **#tor-dev** channel on OFTC IRC:
    - **richard**
    - **msim**

Ricochet-Refresh

- Tor onion service based peer-to-peer instant messenging
- anonymous, decentralized, metadata-resistant
- Windows, macOS, Linux



3/13/21 5:33 PM

Hi Alex, how's it going?

pretty good, how about you?

oh you know

do you have those reports ready for me to review?

yeah one sec

tps_reports.pdf

189,00 KiB / 1,00 MiB

Ricochet-Refresh

- converted Ricochet-Refresh project to CMake
- added pluggable transport support
  - obfs4
  - Snowflake
  - meek-azure
- documentation updates
- various bug-fixes

Gosling

- peer-to-peer connection+authentication protocol over tor
- improvement and generalization on Ricochet-Refresh’s user authentication scheme
- built on onion services:
  - anonymous
  - meta-data resistant
  - end-to-end encrypted
- Rust reference implementation

Gosling

- specification mostly finalized after some iterations
  - Tor hackweek in July (thanks **nickm**!)
  - security review from Radically Open Security in October
- reference implementation in Rust with C FFI and C++ utility headers
- Rust and C++ unit and functional tests
- protocol documentation updates

What’s Next?

- Ricochet-Refresh
  - ongoing tor and pluggable-transport updates
  - Gosling integration
  - chat protocol review/revamp
- Gosling
  - resolve security review issues
  - bug fixes and usability improvements
  - example apps
  - Cargo integration
  - Arti backend
  - feedback collection

Links

- Blueprint For Free Speech: **blueprintforfreespeech.net**
- Ricochet-Refresh
  - website: **ricochetrefresh.net**
  - github: **github.com/blueprint-freespeech/ricochet-refresh**
  - manual: **github.com/blueprint-freespeech/ricochet-refresh/blob/main/doc/usage.md**
- Gosling
  - github: **github.com/blueprint-freespeech/gosling**
  - specification: **github.com/blueprint-freespeech/gosling/blob/main/docs/protocol.md**