

Ricochet-Refresh and Gosling Updates 2023



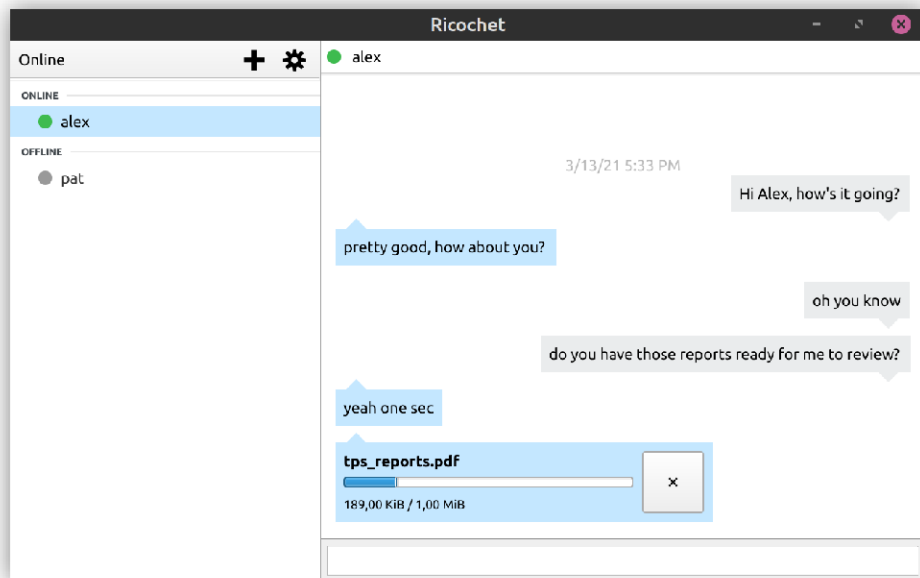
richard (they/them)
richard@blueprintforfreespeech.net

Introductions

- Blueprint for Free Speech is an international non-profit that promotes the right to freedom of expression
- Maintainer of Ricochet-Refresh
- Developing Gosling

Ricochet-Refresh

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



Ricochet-Refresh

- added Estonian (et-EE) locale support
- upgraded to OpenSSL 3.0.N series
- new app icon, installer icon, dmg background
- build-system updates
 - from-scratch re-write of ricochet-build
 - macOS signing migrated to rcodeesign
 - dependency upgrades: zlib, OpenSSL, Qt
 - macOS aarch64 builds
- added new pluggable transports:
 - conjure
 - WebTunnel



RICOCHET REFRESH



Gosling

- peer-to-peer connection+authentication protocol over tor
- improvement and generalization of Ricochet-Refresh's user authentication scheme
- built on onion services:
 - anonymous
 - meta-data resistant
 - end-to-end encrypted
- user-controlled visibility to peers
- Rust reference implementation
- Specification: **blueprint-freespeech.github.io/gosling/gosling-spec.xhtml**

Gosling

- protocol specification updates
- documentation updates
- website: **<https://blueprint-freespeech.github.io/gosling/>**
- crate refactor
- code cleanup (linting, formatting, etc)
- cbindgen generated C-header to JSON IDL conversion
- Github Actions CI/CD
 - build
 - unit+functional tests
 - fuzzing (Linux only)
 - website (specifications, code coverage, Rust & C/C++ documentation)
- crate published on crates.io: **<https://crates.io/crates/gosling>**

What's Next?

- Ricochet-Refresh
 - ongoing tor and pluggable-transport updates
 - chat protocol review/revamp
- Gosling
 - fuzz the C-FFI
 - example apps
 - language bindings (Python, Java)
 - complete the documentation
 - bridge support
 - security review
 - alternate Tor backends: arti-client, arti, TorVPN

Links

- Blueprint For Free Speech: **blueprintforfreespeech.net**
- Ricochet-Refresh
 - website: **ricochetrefresh.net**
 - github: **github.com/blueprint-freespeech/ricochet-refresh**
- Gosling
 - website: **blueprint-freespeech.github.io/gosling/**
 - github: **github.com/blueprint-freespeech/gosling**