PrivacySafe: owning one’s digital live

KWLUG September 2019 talk
Awesome hardware

- View in Modelo
- Physical board and scale
- Stack list at https://privacysafe.ai/?page_id=217
- Crowdfunding at https://www.indiegogo.com/projects/privacysafe-privacy-by-design
When you own space
Without Ownership of the space, we can only beg for privacy.
Ownership in physical space
Ownership in digital space
step 1: data creation, first copy
Ownership in digital space
step 2 today: service provider’s copy
Ownership in digital space
step 2 today: service provider’s copy

De facto loss of ownership
Simple solution: Give no copy to clouds!
Simple rules for client to server communication

- Never send any plain text content to server
- Never produce more metadata than is needed
- Nothing for server to copy, to abuse, or to loose
Simple rules for client to server communication

- Never send any plain text content to server.

End-to-End encryption

protection from wiretapping
Simple rules for client to server communication

- Never send any plain text content to server.
- Never produce more metadata than needed.
- Nothing for server to copy, to abuse, or to lose.

Onion routing, metadata hiding provides protection from surveillance.
Simple rules for client to server communication

True ownership of one’s digital space

- Nothing for server to copy, to abuse, or to lose
3N already proved itself offline
Mail / Messaging
Postal mail process
Electronic mail process

- User
- MSA
- MTA
- User
- MTA
- MDA
Do we need this complexity?
AweSome Mail process
Authenticated Secure Mail process
Classical federation
Web-style federation
3NWeb: set of self-supporting 3N-respecting protocols

• MailerId for non-tracking online identity service

• ASMail for mail & messaging

• 3NStorage for storing, syncing & sharing files
3NWeb

3NWeb is a set of 3N-respecting protocols.

Happy user

Cloud (3rd party servers) with nothing to steal (absolutely secure)
Overall view

Per-app isolation

Core

Client platform

Apps

Provider

3NWEB
Demo 3NWeb desktop client
Computational model server in charge
Computational model
client in charge
3NWeb client platform core

➢ Talks to servers all 3NWeb protocols for messaging, storage, identity

➢ Keeps keys, does all of encryption

➢ Provides to apps fine-grained capabilities. For example, app X will not see files of app Y.
3NWeb provider doesn't know what apps run on a client!

Police Officials: Google and Apple Should Censor Encryption Apps in Their Stores

Written by LORENZO FRANCESCHI-BICCHIERAI

April 19, 2016 // 01:01 PM EST

Law enforcement officials, led by the FBI, have been wringing their hands about how strong encryption
3NWeb apps

- Apps are simple to write, as one does not deal with keys, cryptography, etc.
- App uses capabilities, provided by core, like synchronized over several devices file systems.
- Apps are isolated from each other

Per-app isolation

Apps

Core

Client platform
Dive into details: desktop

- Apps
  - Per-app isolation
    - Electron's Renderer process with w3n object, loaded with capabilities allowed only for particular app, realizing Principle of Least Authority
  - Electron's IPC, with node-integration: false
- Core
  - Electron's Main process
- Client platform
Code

• Spec server implementation with test suites is available on GitHub under GPLv3.  
  https://github.com/3nsoft/spec-server

• Client side is available on GitHub under GPLv3.  
  https://github.com/3nsoft/core-platform-electron

• All 3NWeb protocols are open for everyone.  
  Help us to prepare RFCs for them.
Economics

- App developer doesn’t need a server farm for 3NWeb!

- 3NWeb service is chosen by user, be it one’s own servers or contracted from a provider.

- It’s like model on a desktop, and it’s unlike current model on a web, where app developers need to provision the likes of AWS’
What is your data ownership model?