

# diaspora\*

---

*an open-source, privacy-aware, personally controlled do-it-all web server.*

how the internet works



# the current model

---

- organic growth of internet into centralized hubs of communication.
- server-client model leads to middlemen.
- sharing data is convenient (though you might give up rights).

the Freedom Box

# drawing the line

---

- having all of your stuff in one place is the most essential feature.
- let it live anywhere.
- always on and connected is a major convenience factor.
- scope needs to be narrower (for now).

our approach

# one step closer

---

- raising the bar towards the Freedom Box.
  - change like this doesn't happen over night.
  - we need to make the initial change.
- mass usability, day one.
  - identical end user experience with a fundamentally secure and decentralized backend.

# diaspora core values

---

- an open-source, privacy-aware, personally controlled do-it-all web server.
- runs anywhere (shared/dedicated hosting, virtual machine, “under your bed,” on your cell phone).
- everyone scrapes and holds their own data.
- your ‘seed’ is your own web service
- all of your friends have permission based “friend keys” to access your stuff



how?

# the pillars

---

- decentralization.
- encryption.
- works with everything you already have

# decentralization

---

- how do seeds communicate?
  - since every seed is another instance of the same application, all diaspora seeds know how to access their friends data.
  - this communication is content agnostic; anything you want to share with people, diaspora can handle.
  - user never leaves his seed to view friend's data.
  - it's pretty simple to understand.

Max's seed: [www.max.com](http://www.max.com)

Dan's seed: [www.dan.com](http://www.dan.com)

*Every one of my friends has a unique friend key to my site*

Max's key to Dan's seed: 1234

Dan's key to Max's seed: 5678

**Dan's route for Max's pictures: [www.max.com/1234/photos](http://www.max.com/1234/photos)**

**Max's route for Dan's pictures: [www.dan.com/5678/photos](http://www.dan.com/5678/photos)**

*For Dan's site, when any request is made through the 1234 scope, Dan's server looks up Max's GPG public key, and encrypts all outgoing data to the requester.*

*(This route is public, but unless the recipient has Max's private key, the data is essentially garbage.)*

# rock-solid encryption

---

- GPG encryption for inter-instance communication
- user doesn't think about encrypting their data - it's all handled by your seed.
- “friending” gives another instance defined access rights to your data.
- exchange data via standard HTTP protocol.

# more routing

say Max wants to send Dan a message:

when I navigate to Dan's friend page and send him a message, I am actually saving it to my own database

then, when dan pings my server to view my information, he receives the message from me.  
he would ping

**[www.max.com/1234/](http://www.max.com/1234/) <- this is an index view which would contain my last X things, plus Dan's messages**

# what about existing services?

---

- flexible plugin architecture, via API or “scraping.”
- diaspora does three things
  - pulls in all of your preexisting content (now you have a copy)
  - now you can serve your own data to your friends
  - also acts as client to all services you have enabled (option)

# Employed Tech - Prototype

---

- Ruby on Rails
- MongoDB/MongoMapper
- GPG with full keychain support.
- Twitter/Flickr API's.



roadmap

# first sprint (end of summer 2010)

---

- full-fledged communications between Seeds (Diaspora instances)
- complete PGP encryption
- plugin architecture for scraping of most major services.
- version 1 of Diaspora's API.
- public github repository (completely free software).

# second sprint

---

- add-on modules (for new content).
- open-source developer network.
- further streamlining setup.

# infinity & beyond

---

- TahoeFS.
- XMPP.
- VOIP.
- Bittorrent content delivery network.
- Tor
- Provide own OpenID

what are you going to do about it?

# our summer++ plans

---

- we decided we would rather do this than get internships/jobs!
- We are raising money on kickstarter to fund us working on this project for three months FULL TIME.
- Kickstarter going live tomorrow
- Meeting with Eben Moglen on May 4th
- Also applied to the Awesome Foundation

thanks.

any questions?

[joindiaspora.com](http://joindiaspora.com)