It is called kinko

Easy E-mail encryption to protect your privacy:

encrypted email → secure connection → decrypted email

pretty easy privacy: 🤖 activated
Overview

› introduction
› spot the problem
› building good crypto tools
› challenges
› more than tools
› get involved
Snowden 2013...

...rekindled interest in privacy.

Privacy after 2013 means:

- a pretty secure means of communication
- user interfaces that are accessible to everyone
Spot the Problem
DE-Mail
DE-Mail
Lavabit
Posteo
Threema, Apple iMessage
Thunderbird/Enigmail
Heartbleed

OpenSSL

Cryptography and SSL/TLS Toolkit
The diagram shows the following problems:

**Sender**
- Difficult to use
- No end-to-end encryption
- Browser/desktop vulnerabilities

**Operator**
- Not open source
- Trust issue
- No end-to-end encryption

**Receiver**
- Difficult to use
- Browser/desktop vulnerabilities
What has kinko learned

- easy-to-use
- OpenSource
- end-to-end encryption
- vibrant community
- do not make cryptography yourself
- consider browser and desktop security challenges
<table>
<thead>
<tr>
<th>Feature</th>
<th>kinko</th>
<th>DE-Mail</th>
<th>LavaBit</th>
<th>CryptoCat</th>
<th>Threema</th>
<th>Thunderbird/Enigmail</th>
<th>OpenSSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>easy-to-use</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>OpenSource</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>end-to-end encrypted</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>vibrant community</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>know your cryptography</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>consider browser and desktop security challenges</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>no need to trust the operator</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Challenges

- Usability
- Mobility
- Desktop OS
- Identity
- Trust
- Security
- Community
- Fun
- Reaching Out
- Funding
CHALLENGE ACCEPTED
Challenge: Usability

- Usability determines mainstream adoption
- PGP exists for > 20 years: how many people are using it?
Usability

- Easy setup
- Nothing changes in the way you use email
- Keep your mail client, or...
- ...use kinko webmail
- Keep your email address
Why you gotta love (using) me

I´m so cute...

...and pretty

...and likeable

...and cuddly
Challenge: Mobility

- Yesterday: one person = one computer
- Today: one person = several computers, phones, tablets, toasters...
Mobility

- A proxy in extra hardware
- with all your devices (Android, Linux, iOS, OSX)
- accessible from everywhere
- using default protocols (IMAP, SMTP, Browser)
- secure connection via port forwarding & SSL certificates
Challenge: Desktop OS

Everyone is root. Everything is perfectly fine!
Challenge: Desktop OS

- Installation as root
- Complex operating systems and software
- Browsers are more and more complex
  - many potential vulnerabilities
Desktop OS challenges

- A dedicated device for crypto
- Minimal, Linux based OS
- Components secured against each other (different accounts, etc.)
- Optional: access to configuration available only from local network
Challenge: Identity (Key Exchange)

Whom are you talking to?

Is it really you, Trinity?
Challenge: Identity (Key Exchange)

Whom are you talking to?

Yes, check my fingerprint
Identity: technical approaches

- TOFU: parsed from emails
- Key server
- Fingerprint verification
Identity: social approaches

Out of channel verification

- Identity verification (PostIdent)
- Signing Service (e.g. heise.de key signing)
- Web of trust (key signing party)
- Pseudonym: Business card with email address and fingerprint
- add your idea here..
Challenge: Trust

Do you trust your mail provider?
Trust

- sensitive information (private keys) must be in the user`s hands only!
- tools must be Open Source and reviewed
Challenge: Security

Do you trust us to be masters of math? Would you trust our home made cryptography?

its alright

I'm from the internet
Security

- use trusted tools like GnuPG
- stay up to date with security developments
- keep tools up to date
- build a vibrant community
More Than Tools
Challenge: Community

A vibrant community is key for a good crypto project.

But how to get people enthusiastic to support your project?
Community

- Licenses
- Approachable source code and project organization
- Communication Tools
- Newsletter
- Contributing must be fun!

https://github.com/kinkome/
Challenge: Fun

Fun with cryptography.
Fun

I think, we've managed so far...
Challenge: Reaching out!

I don't need crypto, I've got nothing to hide!
Reaching out!

- engage people in conversation
- use social media as a weapon
- use educational videos
- use educational games
- cause scandals
Challenge: Funding

- Privacy projects need to stay independent of corporate funding
- So how to cover the costs?
Crowdfunding

- Crowd Funding for kinko in August
- independent source of income
- a means to reach people and media attention on privacy
- please back kinko in August!

https://kinko.me/crowdfunding
Get involved!

- subscribe to our newsletter at https://kinko.me
- spread the word
- contribute to the code
- help educate the public about privacy
- contribute with whatever you are best in
- back us in August

THE FUTURE IS ENCRYPTED