BitmaskK: encryption for mere mortals

FOSDEM 2018

kali - meskio - kwadronaut

https://leap.se
Problem: encrypted email is complicated...
gpg - GNU Privacy Guard

Message that could get source killed

BEGIN PGP MESSAGE
Version: GnuPG v1.4.10 (GNU/Linux)

... PGP message content...

END PGP MESSAGE

Public GPG Key

Public GPG Key

JOURNO

INTERNET

SOURCE
How to use PGP to verify that an email is authentic:

Look for this text at the top:

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Hey,

First of all, thanks for taking care of. If it's there, the email is probably fine.
Problem: providers
My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on—the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund here.
Peer to peer?
Better federation!

- Protect providers from their users
- Protect users from the provider
What does LEAP do?

- **LEAP Platform:**
  toolkit to make it easier to run a service provider
- **New protocols:**
  so no need to trust your connection provider
- **Bitmask client:**
  smooth working client with compatible providers
leap mail service

- End-to-end encryption
- Backwards compatible with email and current OpenPGP usage
- Service provider has no access to user data
- Automatic key discovery and validation
- Cloud synchronized for high availability on multiple devices
email service
soledad
mx
transitional key validation

generic rules for automatic key management, transition from TOFU to more advanced ruleset.

- bind key <-> email address
- key directory
- endorser (provider)
- binding info: evidence for "educated guess"
- verified key transition (automatic)

[leap.se/en/docs/design/transitional-key-validation]
TOFU

With a bunch of exceptions
1. First Contact

When one or more keys are first discovered for a particular email address, the key with the highest validation level is registered.
2. Regular Refresh

All keys are regularly refreshed to check for modified expirations, or new subkeys, or new keys signed by old keys.

This refresh SHOULD happen via some anonymizing mechanism.
3. Key Replacement

A registered key MUST be replaced by a new key in one of the following situations, and ONLY these situations:

- Verified key transitions.
- If the user manually verifies the fingerprint of the new key.
- If the registered key is expired or revoked and the new key is of equal or higher validation level.
- If the registered key has never been successfully used and the new key has a higher validation level.
- If the registered key has no expiration date.
VPN

- Prevent eavesdropping.
- Circunvent internet censorship.
- Prevent leaks (DNS, IPv6, ...).
LEAP platform

sudo gem install leap_cli
leap new example --domain example.org
cd example
leap add-user --self
leap cert ca
leap cert dh
leap cert csr
leap node add blueberry services:openvpn \  
ip_address:1.1.1.1 openvpn.gateway_address:1.1.1.2
leap node add raspberry services:couchdb,webapp \  
ip_address:1.1.1.3
leap init node
leap deploy
sysadmins are human
and deserve usability too
"leap deploy"
user control panel

varac@demo.bitmask.net

Welcome varac.

- Created 2014-03-21 10:06:38 UTC
- Updated 2014-03-21 10:06:38 UTC
- Enabled true

- Destroy your account.
- Create and check support tickets.

To use bitmask services:

- Download Bitmask
your right to whisper
leap.se
show me the code!

https://0xacab.org/leap/

- ~10 important repos
- GPL code
current state
Email Beta (0.10...)  
works on Linux  

Bitmask VPN  
works on Linux && Android
next steps

- OSX and windows
let a thousand providers bloom
thanks! questions?

https://bitmask.net

https://leap.se

katzenpost.mixnetworks.org
**Bitmask** is an open source application to provide easy and secure encrypted communication. You can choose among several different service providers or start your own. Currently, Bitmask supports encrypted internet (VPN) and encrypted email.
Bitmask Thunderbird Extension

REQUIRES RESTART

After installing the extension, do the following:

1. Make sure that Bitmask is running and you are logged in.
2. In Thunderbird, click the main menu, then "Preferences" - "Account Settings".
3. Click "Account Actions" - "New Bitmask Account...".

⭐⭐⭐⭐⭐ (1) · 286 users
2. ability to use multiple devices
Synchronization Of Locally Encrypted Data Among Devices
data = 💌 + 🔑
bitmask keymanager
requires no user interaction
interoperability is a must
many projects converging
(Watch AUTOCRYPTO: Enigmail, K9, Mailpile, Bitmask)
SOLEDAD

- Synchronization of Locally Encrypted Data Among Devices
- auth: srp
- kdf: scrypt
- AES-256-GCM
- built on top of canonical's u1db
- vector clocks
- clientside: sqlcipher backend
- serverside: couchdb cluster
Problem: Attachments

- Syncing blobs in a convoluted store
- Pluggable BlobsIO backend for server (in dev)
- FS as MVP, others welcome!
Validation levels

low == less trust on the source
1. Weak Chain

sks key servers, email attached key, OpenPGP header, ...
2. Provider Trust

webfinger, provider mailvelope
3. Provider Endorsement

NickNym
4. Historical Auditing

CONIKS, google's transparent keyserver
5. Known Key

client pinned keys
6. Fingerprint
manual verification