Keybase and PGP

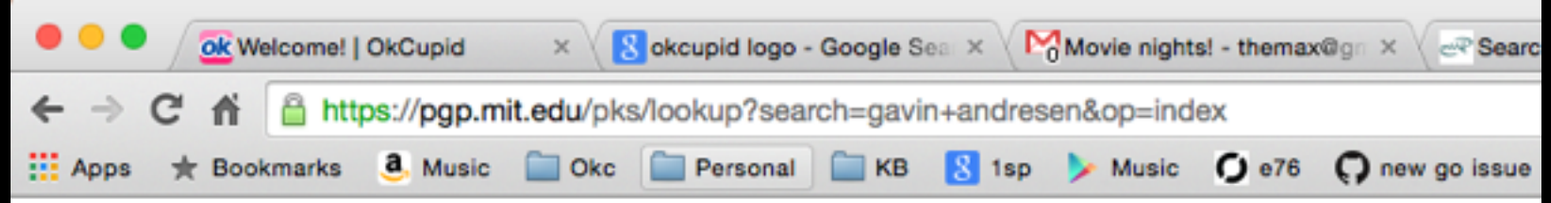
Max Krohn
@maxtaco
https://keybase.io/max

Mini-Talk Overview

- A short history of Keybase
- What we're focusing on
- Keybase and PGP

Quick History of Keybase


bitcoin



Search results for 'gavin andresen'

Type	bits/keyID	Date	User ID
pub	1024R/1F281E36	2014-01-01	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	1024R/03DDF953	2014-01-01	Gavin Andresen <gavinandresen@gmail.com>
pub	4096R/1FC730C1	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/C3E16446	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/ECDAC457	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/000ECC0A	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/075CDF63	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/ABFBDAB5	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/942973E8	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/3FB9CA59	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/EA1B3F36	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/1B719FBE	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/E3B1D902	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/16D21C85	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/8EF9233B	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
pub	4096R/73FBE314	2011-12-15	Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>

Public Key Lookup 2.0

- Based on pre-established social identities
- A new notion of identity that worked for Internet friends and meatspace friends
- A complement to PGP

JS-Based PGP

- For both Web and Node.js command-line app
- Concurrent with the OpenPGP-JS effort, so wound up with a parallel implementation

Early Learnings While Implementing PGP

- Worried that key servers could reassemble keys with impunity
- And/or withhold revocations
- Proof of email ownership could not easily be replayed to third parties

CT-Style Append-Only Log

- Every user gets a “signature chain”
    - Each link is a signed statement, including the hash of the previous tail
- The server makes a Merkle Tree of all signature chains
- Publishes the signed tree continuously
- Let users corroborate with third-party authorities (Twitter, Github, etc) or independent mirrors

Identify Steps

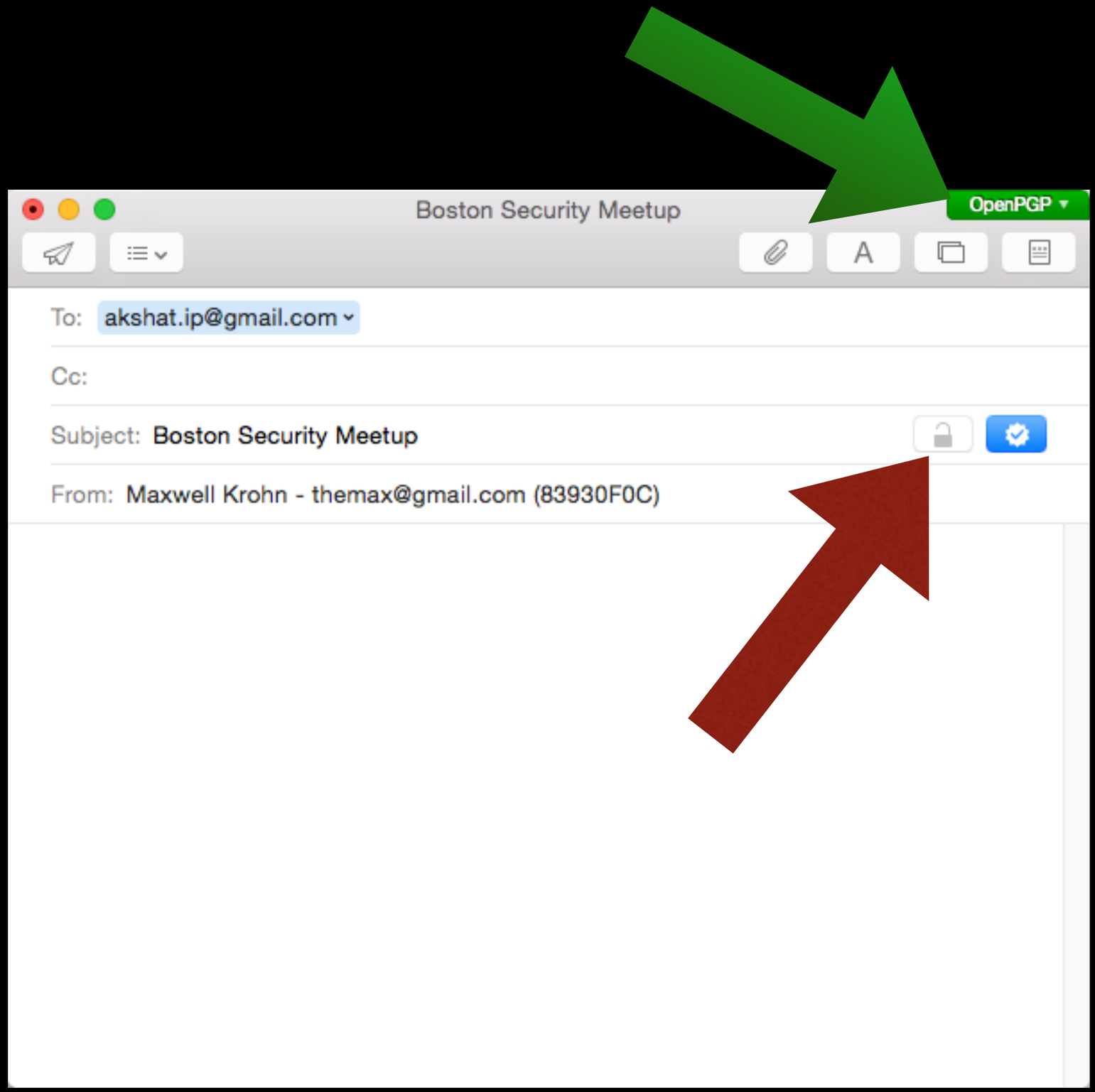
- Lookup user's sigchain starting with Merkle root:
  - https://keybase.io/_/api/1.0/merkle/path.json?username=awendland
- Replay "sigchain" and ensure that it stops at signature advertised above
  - https://keybase.io/awendland/sigchain
- Corroborate with third parties

PGP-Style WoT: Tracking

- “I track you” (sort of like: “I follow you”)
  - I identify you
  - I sign a summary of your public identity into my sigchain

Shortcomings

- Key mobility only if protected with a human-memorizable password
  - Prone to server hacks
  - No story for lost devices
- Couldn’t see how to make this product grow past initial pool of enthusiasts


Boston Security Meetup
OpenPGP
To: akshat.ip@gmail.com
Cc:
Subject: Boston Security Meetup
From: Maxwell Krohn - themax@gmail.com (83930F0C)

Recent Releases

- Per-device keys
- KBFS
- Native apps for 5 platforms

Per-Device Keys

- Each device generates its own public/private key pair
- Keeps the private key local, and signs the public key into the user's sigchain
    - Reciprocal signatures of signer and signee, as in PGP subkey signatures
- All keys are equally powerful; can revoke or add other devices, including your first or "eldest" key

PDK Implications

- Easier to recover from lost device; can just revoke that device
- When Alice encrypts for Bob, encrypts for all of his devices individually

KBFS

- Online file system with E2E security via Keybase key exchange
- As in PGP, each folder gets a symmetric key, encrypted for all recipient's public keys
- Designed for viral recruitment of users

Keybase and PGP

- A PGP key is part of a user “identity” like a Twitter or Github Handle
    - When I track you, I sign your “eldest” key, and your social identities, including your PGP fingerprints
- PGP keys are “siblings” to per-device keys, and can provision or revoke devices
- Users can have multiple PGP keys per “key family”