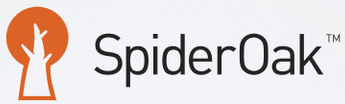
ANTI-SOCIAL NETWORKING

How we can have nice (datamining-free) things

DAVID DAHL

SpiderOak / Crypton

Defcon 23
8 August 2015



I AM A TWITTER ADDICT

NOT ANOTHER E2E CHAT APP!?

NO

Kloak is a “status, location and image sharing” app!

“KLOAK”

(COLOR, ICONS, UI DEV IS IN PROGRESS)

Kloak concept is a tongue in cheek reference to Mark Zuckerberg’s hoodie. The Dudebro Silicon Valley persona “changing the world” through VC cash and better data mining algorithms

ITS CASUAL

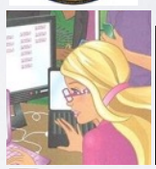
Like Twitter, but private

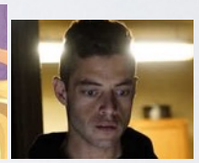
KLOAK THREAT PROTECTION MATRIX

- **Privacy** from the Chinese Army **NO**

- **NSA**? **FUCK NO**

- folks in **this** room? **LOL**





- Biz-Intel-Data-Mining-d-Bags? **YES**

DATA-MINING IS THE 99% THREAT

Our data is collected by Silicon Valley firms, is being **stored forever** to be used for **what**?

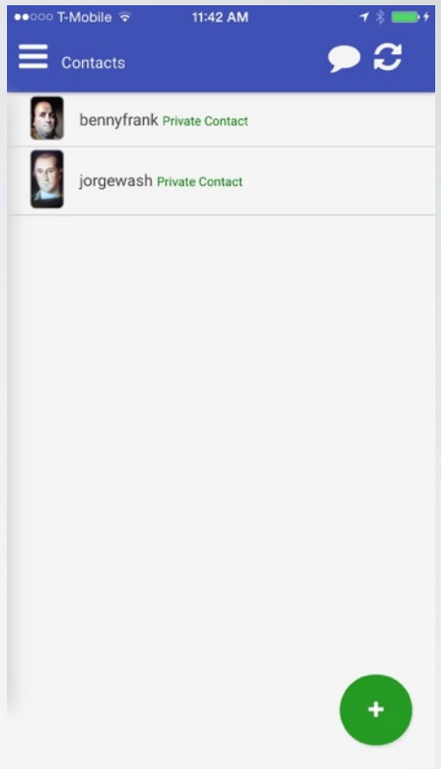
Normals are happily typing all their thoughts and dreams and indiscretions in to the free black boxes Silicon Valley provides. What becomes of this data? how long is it kept? who is it sold to?

Ello and MeWe are offering users a “Bill of Rights”, but they still have plain text and VC cash. LOL. Kloak uses e2e - so the Bill of Privacy Rights is enforced by your key ring.

KLOAK IS A UX EXPERIMENT

UX OF FOLLOWING OTHERS

…in E2E apps is difficult

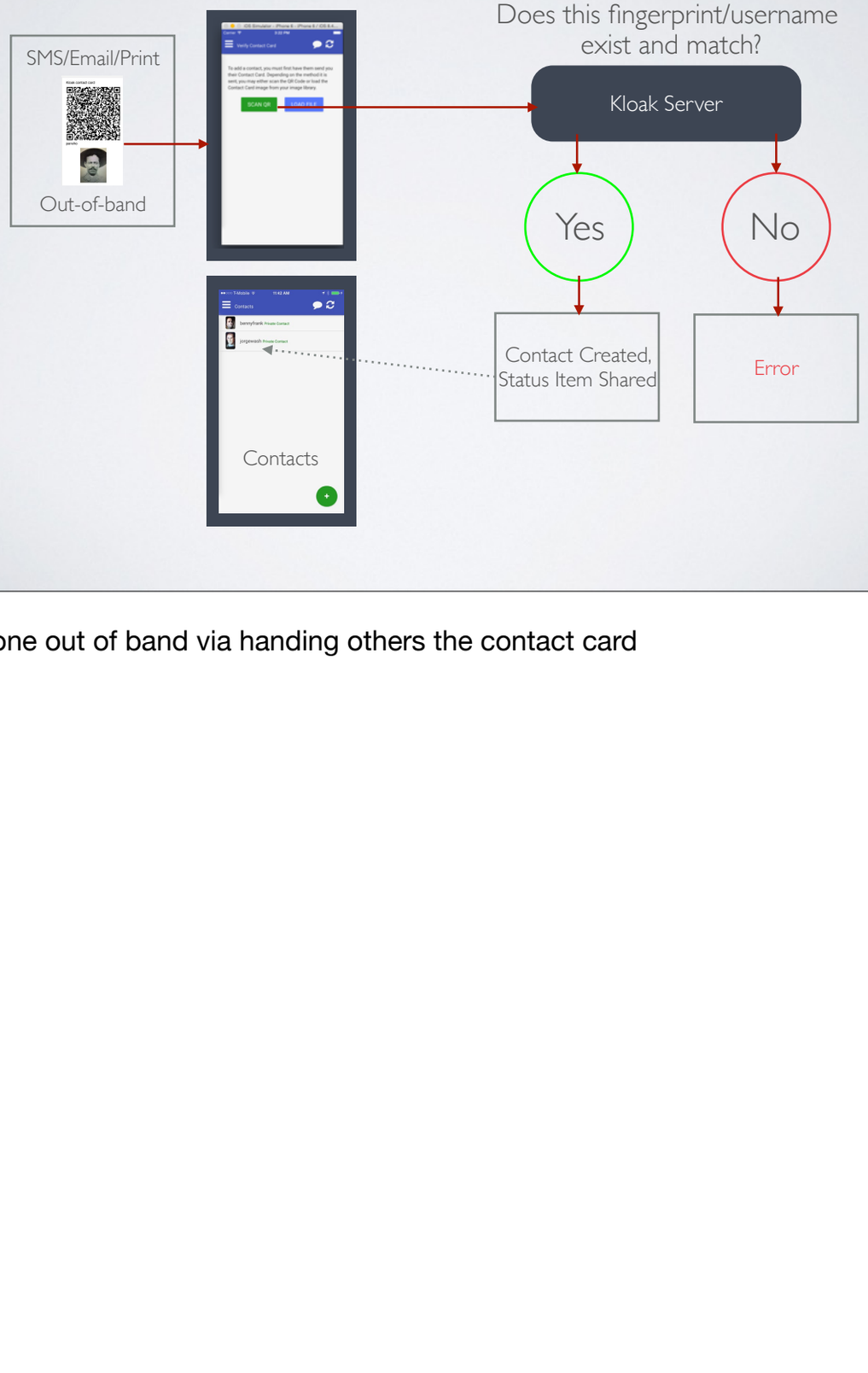


This is not just a “follow button” operation. Nor should it be. There needs to be a simple and smooth operation to achieve exchanged keys, but what should it look like. This should also “feel” private

CONTACT CARDS

- Allow for out of band verification

CONTACT CARD WORKFLOW



There is no interface to “find users”, all pairing is done out of band via handing others the contact card

LESS JARGON MORE FAMILIARITY

A more familiar "contact card" or business card and "rolodex" concept is totally understood by users

CARNEGIE MELLON CAPSTONE PROJECT

- Summer 2015
- UX research: Contact Cards
- Focus groups
- Surveys

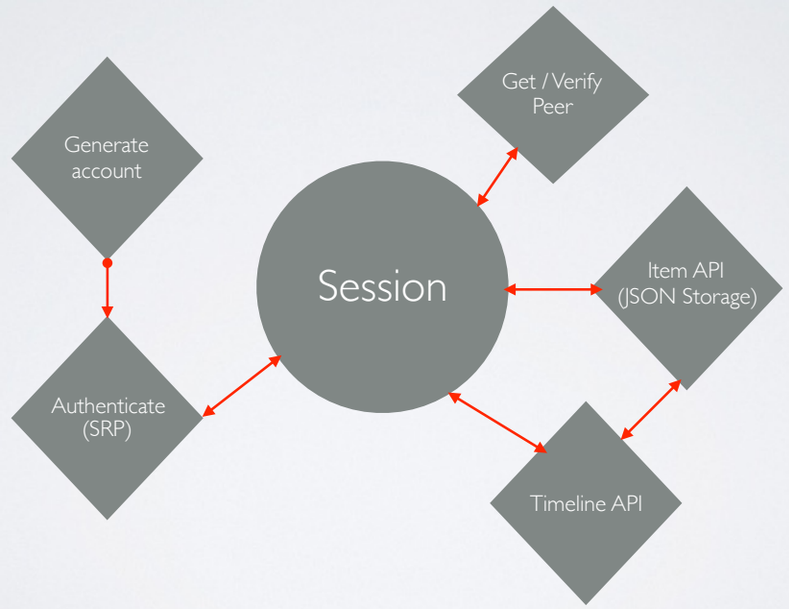
We will be publishing the paper and results of this study soon.

FRAMEWORKS & TOOLS

Crypton

SpiderOak's Application Framework

CRYPTON IN A NUTSHELL



SJCL

Stanford's JS Crypto Library

(We will move to NaCl)

CORDOVA

Apache's (PhoneGap) mobile framework

NODE.JS & SOCKET.IO

Servers

POSTGRESQL

Anything else would be **weak** and **silly**

CRYPTON KEY RING

- Each account's keyring contains 2 sets of public/private key pairs
  - One for signing and one for encryption
- An HMAC key for encrypting identifiers
- A PBKDF2 wrapping key

APIS AT A GLANCE

```
crypton.generateAccount('username', 'password',
  function (error, account){});

crypton.authorize('username', 'password', function (error, session){});

session.getOrCreateItem('wineList', function (error, item){});

session.items.wineList.value.reds = [{cabernet: 'sonoma'}];

session.items.wineList.save(function (err) {});

session.getPeer('alice', function (err, alice) {});

session.items.wineList.share(alice, function (err) {});
```

Not to get too far into the APIs crypton provides, but Crypton's APIs read like any other web API. All of the crypto is encapsulated inside functions anyone can use, and all of the normal parameters that developers need to choose are set for you to "smart defaults" - that have been audited by professionals. This is UX *too*, making the framework APIs simple. The developer never deals directly with the encryption. When you call "getFoo()", decryption happens even before you are handed the plain text object.

KLOAK DATA STRUCTURES

Crypton "**Items" API**

```
session.getOrCreateItem('myStatus', function callback (err, item) {
  if (err) {
    console.error(err);
    return;
  }

  item.value = {
    status: 'Just drank a super hoppy beer at a hip bar can you imagine???'
  };
  // item is lazily auto-saved
});
```

The new object is now available at **session.items.myStatus**

SHARING ITEMS

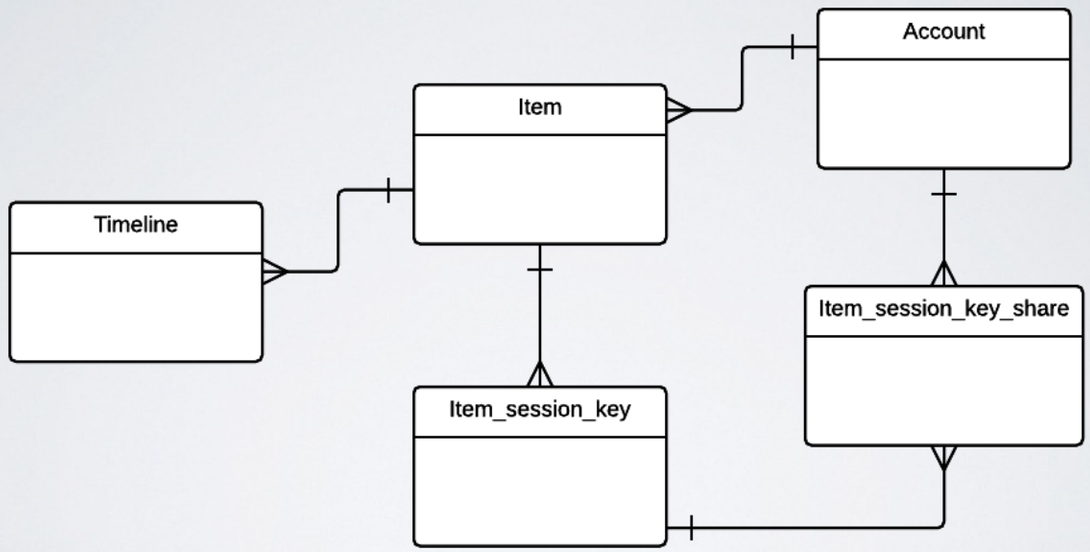
```
session.getPeer('alice', function callback (err, peer) {
  if (err) {
    console.error(err);
    return;
  }

  // Share the status item with Alice:
  session.items.myStatus.share(peer, function callback (err) {
    if (err) {
      handleError(err);
    }
    // Every time this item is updated, the new value will be
shared with each sharee
  });
});
```

SHARING NOTIFICATION

Via: Socket.io in real time - if both parties are currently connected

or Via the "**Timeline**" API, which is the "feed"

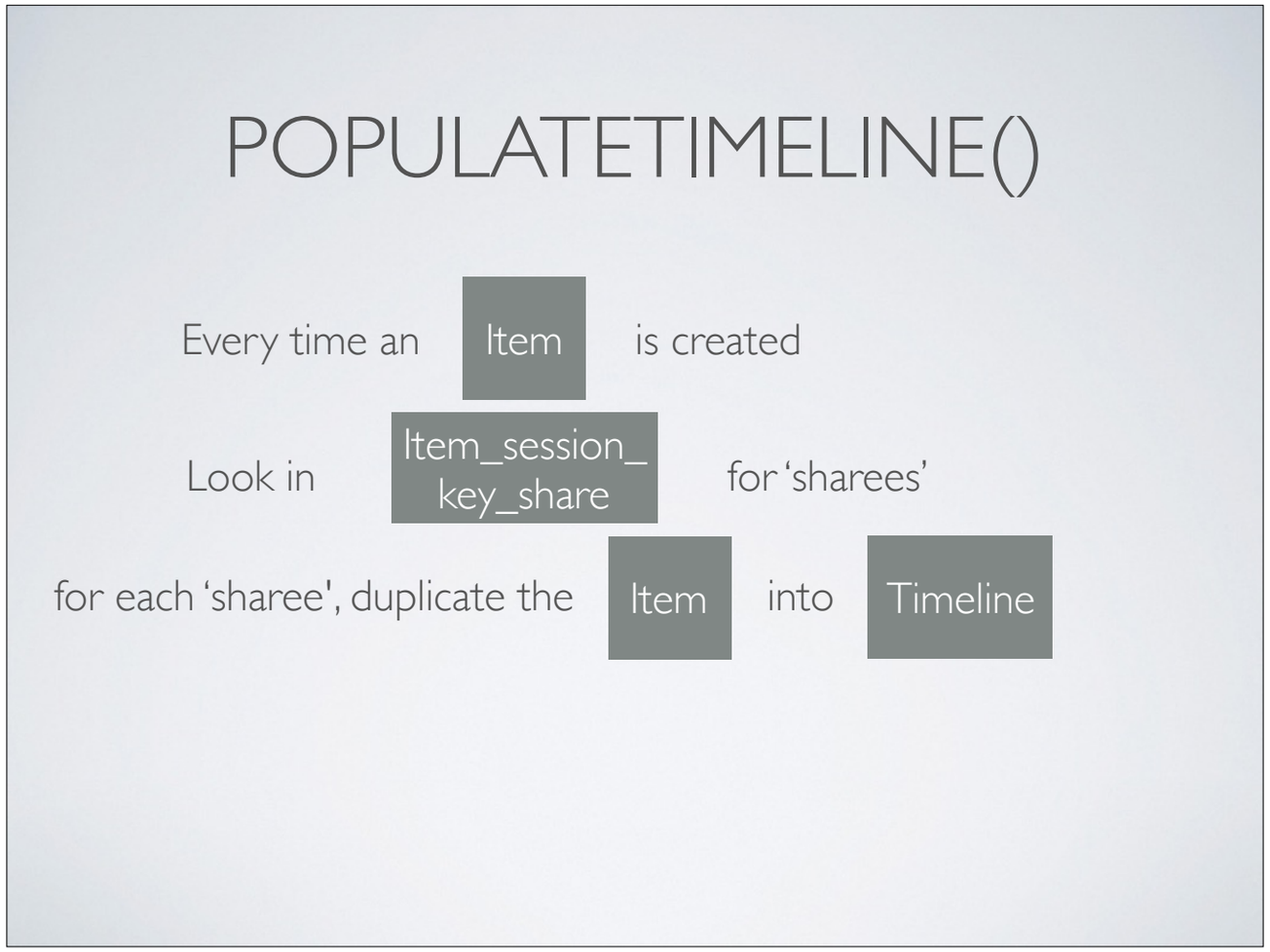
POSTGRESQL SCHEMA



https://github.com/SpiderOak/crypton/blob/master/server/lib/stores/postgres/sql/setup.sql#L624

HEAVY LIFTING!

```
CREATE OR REPLACE FUNCTION populateTimeline() RETURNS TRIGGER AS $$
  DECLARE
    item_row RECORD;
  BEGIN
    FOR item_row IN
      SELECT s.item_session_key_share_id,
        s.account_id, s.to_account_id, k.item_id,
      a.username AS toUser, b.username AS fromUser
        FROM item_session_key_share s
        JOIN item_session_key k ON
          (s.item_session_key_id = k.item_session_key_id)
        JOIN account a ON
          (s.to_account_id = a.account_id)
        JOIN account b ON
          (s.account_id = b.account_id)
        WHERE k.item_id = NEW.item_id AND k.supercede_time IS NULL
    LOOP
      -- Insert a timeline row for each session_key_share
      INSERT INTO timeline (item_id, creator_id, receiver_id, creation_time, value)
      VALUES (NEW.item_id, item_row.account_id, item_row.to_account_id, NEW.creation_time,
NEW.value);

    END LOOP;
    RETURN NULL;
  END;
$$ LANGUAGE PLPGSQL;
```



Still not sure what kind of policy to enforce over ownership of shared status updates, for now going with if its shared it is always shared.

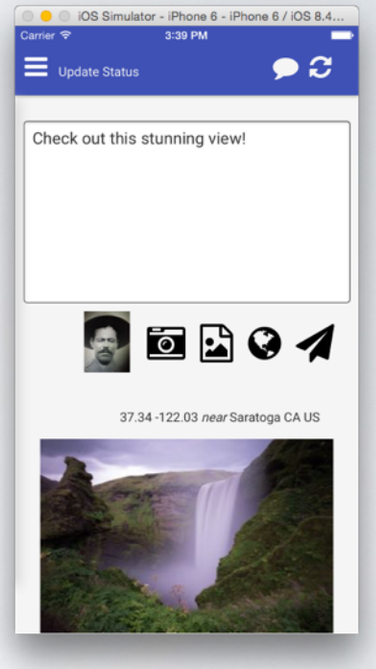
TIMELINE API

- Each account has its own timeline
- Upon login, the latest items in the timeline are loaded, decrypted locally and displayed
- "get latest" timeline items API method
- "get previous" timeline items (from timeline ID)

POSTING STATUS

User can post 512 characters, location and an image

Location Data is also **private**, no external mapping APIs are used, the app is packaged with "GPS to city name" db



RELEASE?

- Soon (Late Summer 2015)
- https://github.com/Crypton/statusapp
- Android builds can be had now, but the server is our staging server

Thanks!