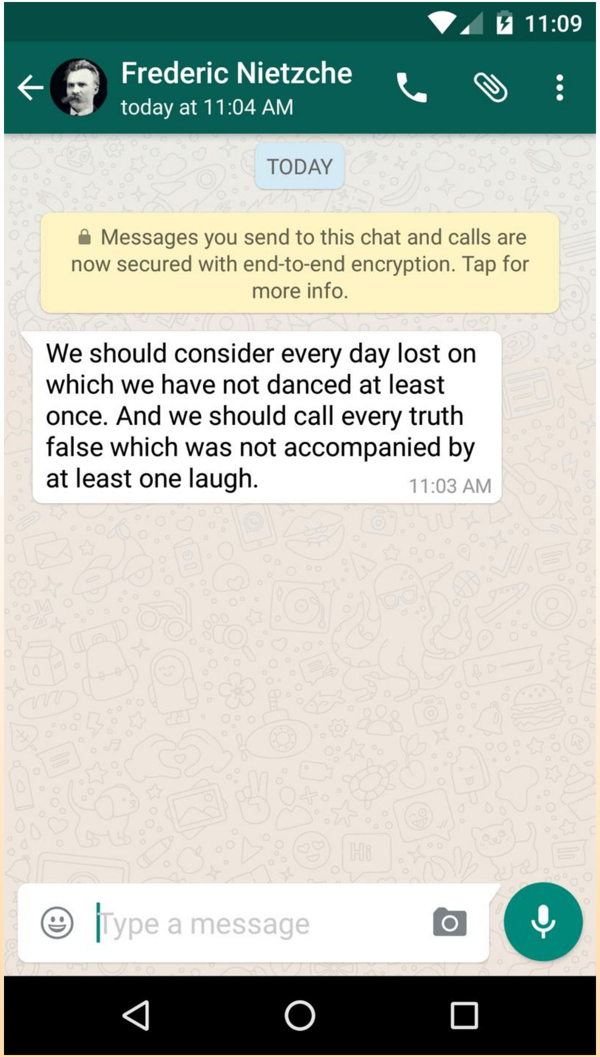
Presented at PETS'2016,
July 20th 2016

Beeswax

a platform for private web apps

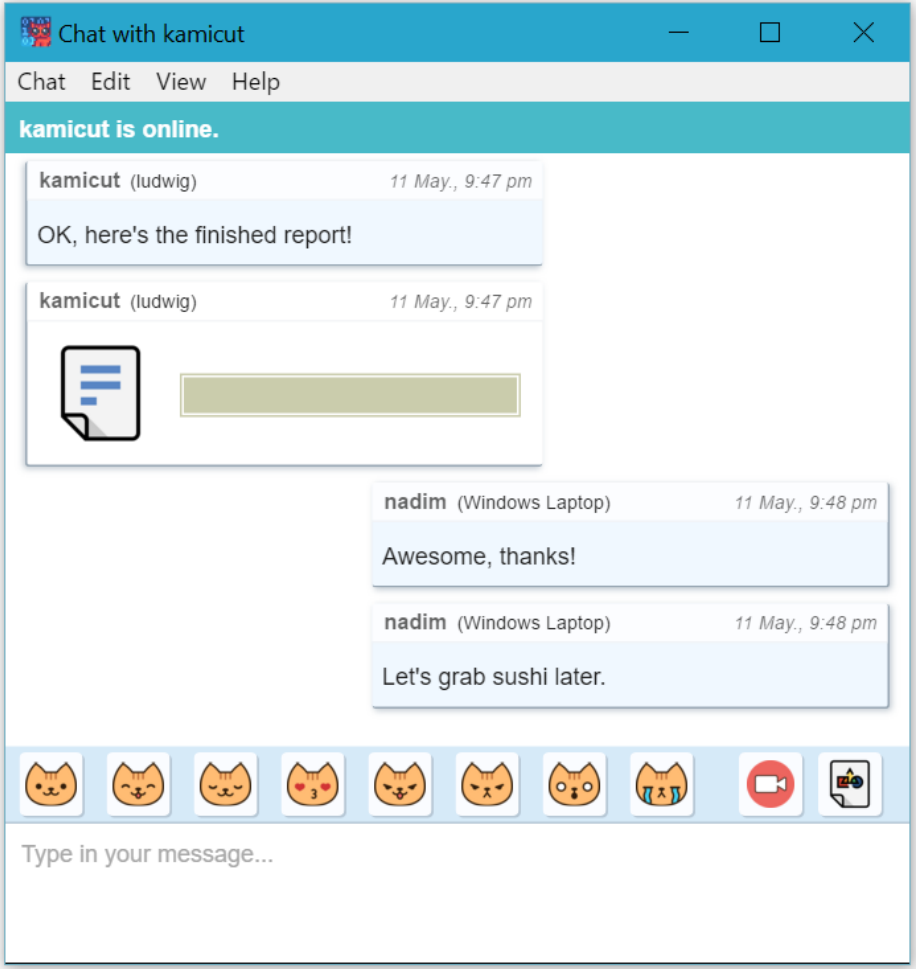
Jean-Sébastien Légaré*, Robert Sumi and William Aiello
UBC NSS Lab

The University of British Columbia



Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.

We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh. 11:03 AM



kamicut is online.

kamicut (ludwig) 11 May., 9:47 pm

OK, here's the finished report!

kamicut (ludwig) 11 May., 9:47 pm

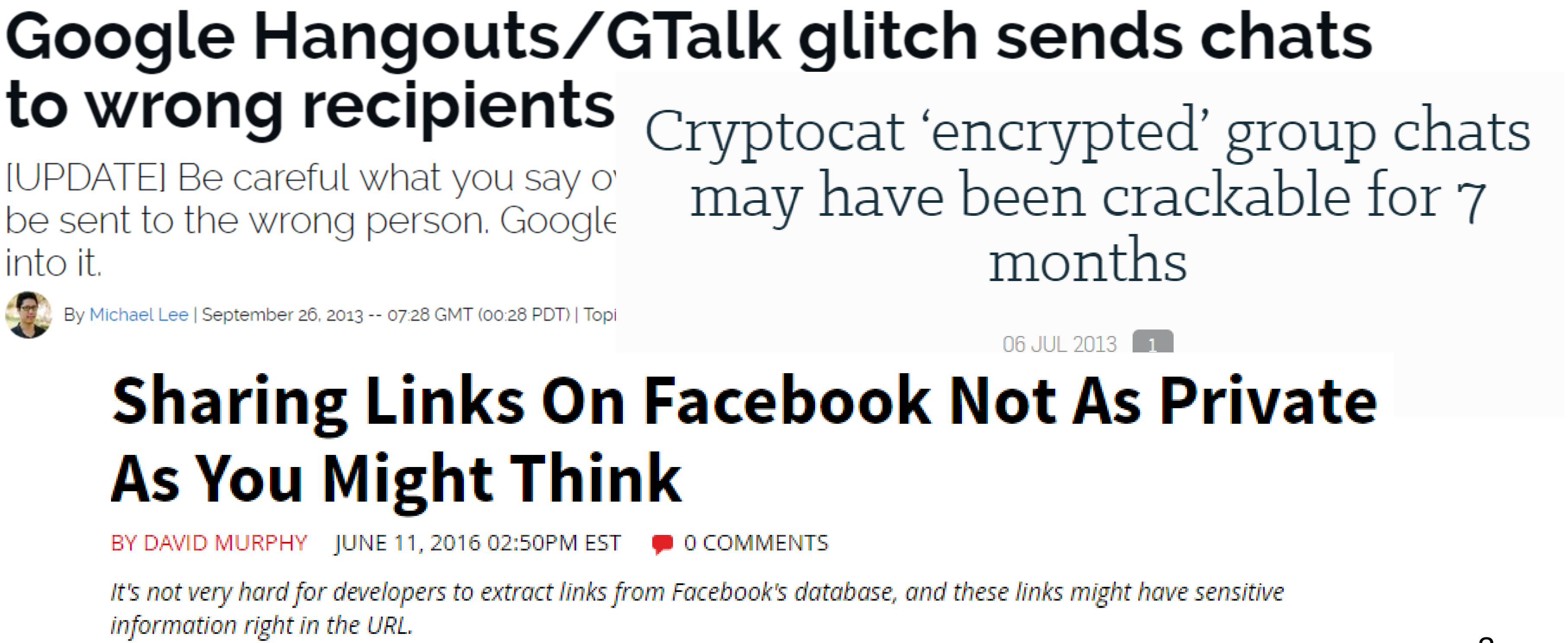
nadim (Windows Laptop) 11 May., 9:48 pm

Awesome, thanks!

nadim (Windows Laptop) 11 May., 9:48 pm

Let's grab sushi later.

Are they secure? Is it really Private?



Google Hangouts/GTalk glitch sends chats to wrong recipients

[UPDATE] Be careful what you say o
be sent to the wrong person. Google
into it.

By Michael Lee | September 26, 2013 -- 07:28 GMT (00:28 PDT) | Topi

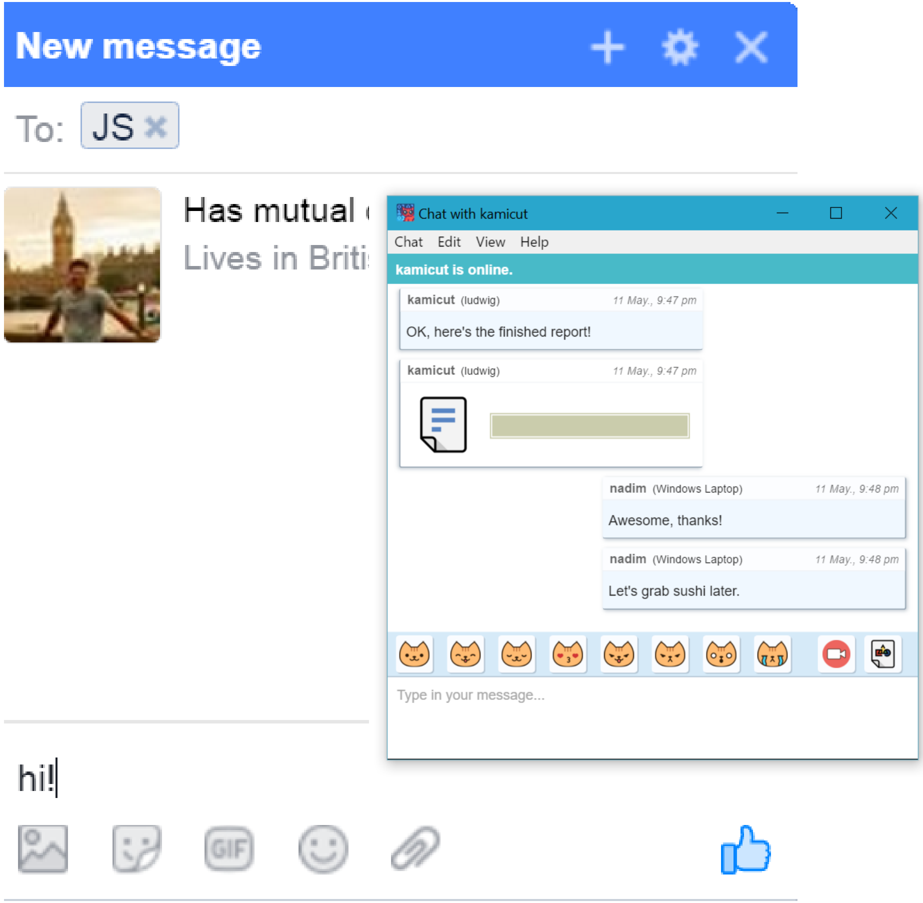
Cryptocat ‘encrypted’ group chats may have been crackable for 7 months

06 JUL 2013 1

Sharing Links On Facebook Not As Private As You Might Think

BY DAVID MURPHY JUNE 11, 2016 02:50PM EST 0 COMMENTS

It's not very hard for developers to extract links from Facebook's database, and these links might have sensitive information right in the URL.



kamicut is online.

kamicut (ludwig) 11 May., 9:47 pm
OK, here's the finished report!

kamicut (ludwig) 11 May., 9:47 pm

nadim (Windows Laptop) 11 May., 9:48 pm
Awesome, thanks!

nadim (Windows Laptop) 11 May., 9:48 pm
Let's grab sushi later.

hi!

Ex: Facebook Messaging, cryptocat, google talk otr.

How could one gain assurance?

- Audit the code?
- Rely on conclusions of a diligent self-identified community of experts?
- Do it again for every app?

Root of the Problem

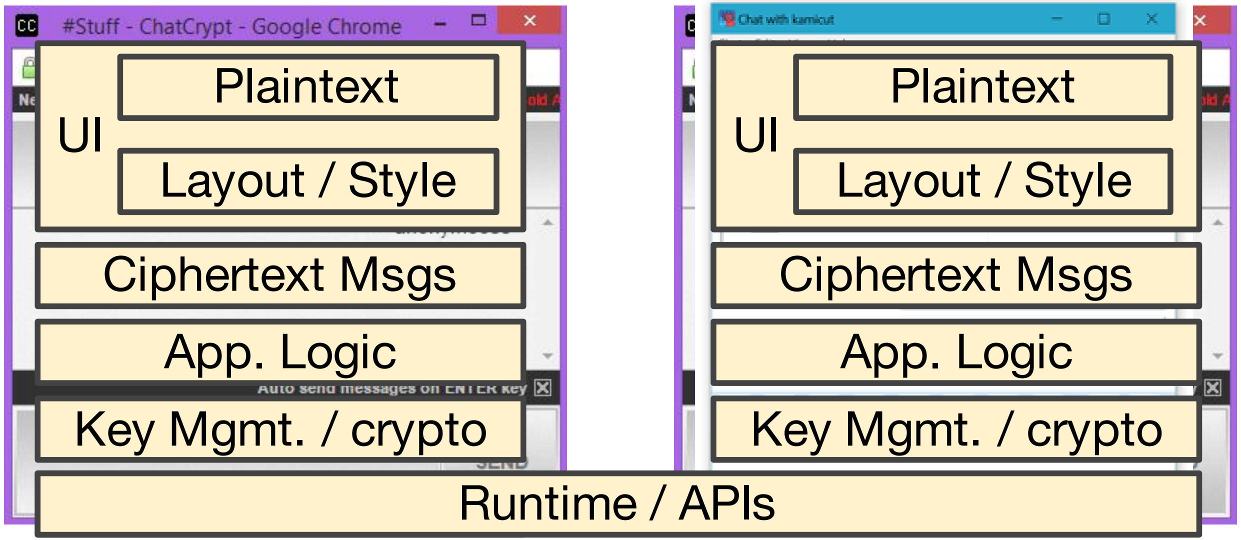
- Client-Side code of private apps contains private information – The keys.
- W/O containment of keys, plaintext, crypto functionality, app must be in TCB
- Moreover, *every* app performing end-to-end security must be trusted

+ TCB of *all* applications

Beeswax

- A security platform to reduce the TCB of private *web* applications.
- Disaggregation, and containment of security-critical data & functionality.
- Sharing of this functionality provided in well-defined APIs.
- Allows scrutiny to be focused on the platform (*Instead of every app)*
- Implemented as a Google Chrome (v40) extension, (5K lines of code)
- Deployable now and allows rich web application development

TCB Grows Larger



#Stuff - ChatCrypt - Google Chrome
Chat with kamicut
Auto send messages on ENTER key
SEND

UI

Plaintext

Layout / Style

Ciphertext Msgs

App. Logic

Key Mgmt. / crypto

UI

Plaintext

Layout / Style

Ciphertext Msgs

App. Logic

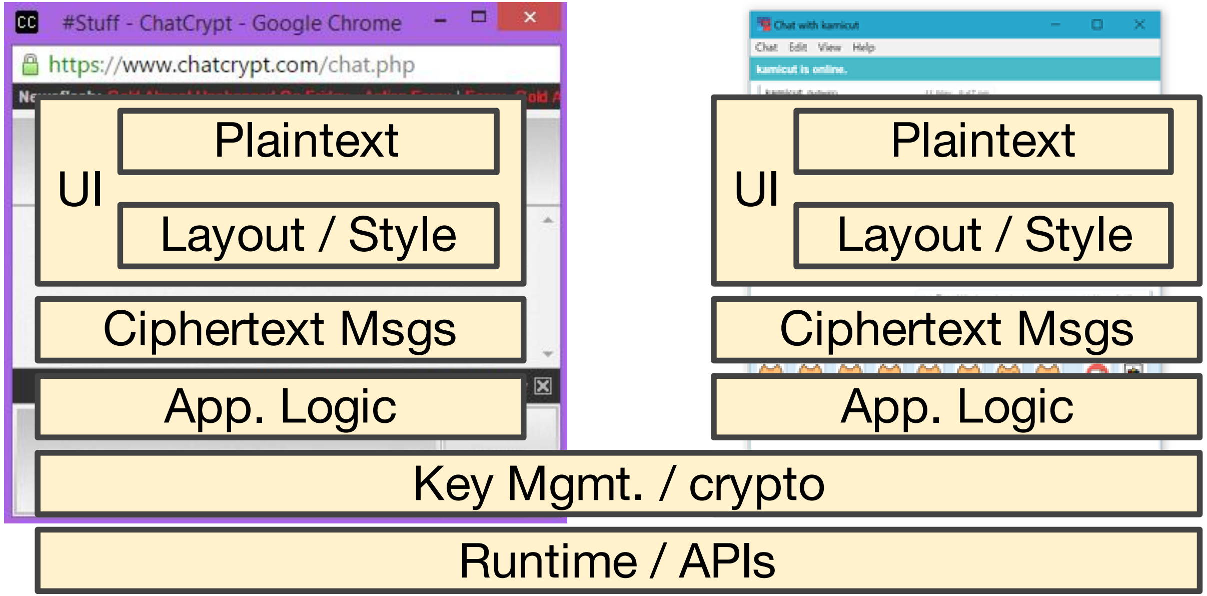
Key Mgmt. / crypto

Runtime / APIs

Repeats for each app.

Vulnerabilities in application code can exfiltrate data.

□ Must be in TCB

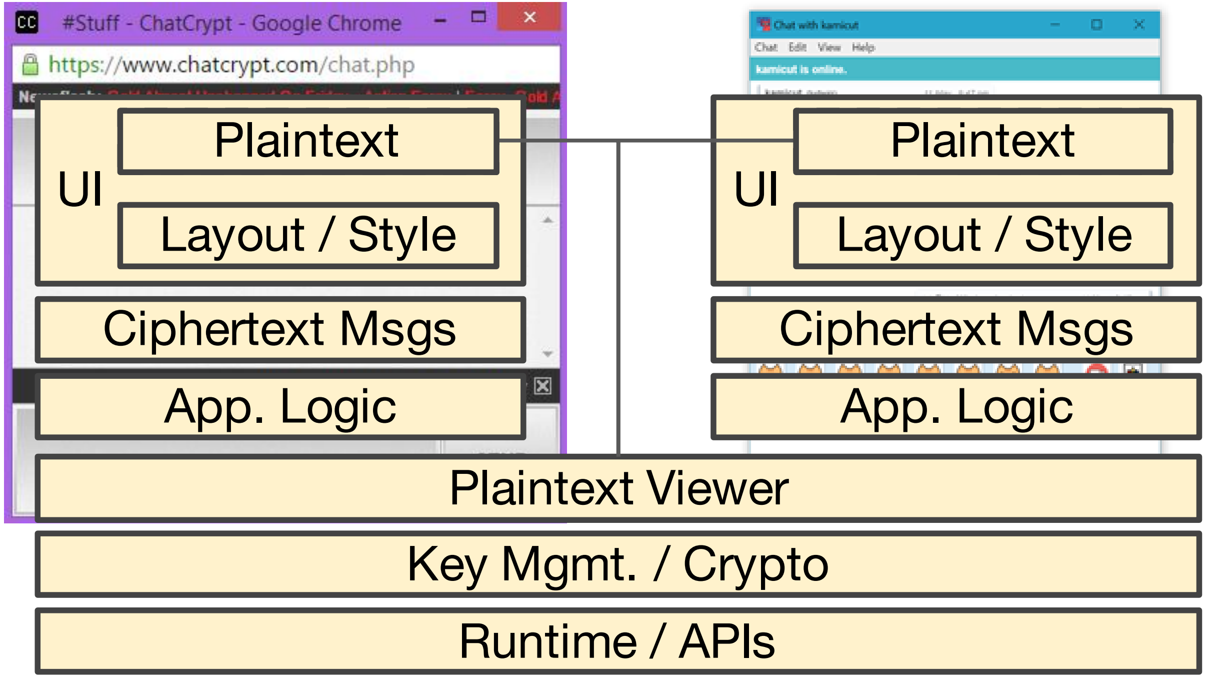


Protect Keys

- Move them to platform
- Application gets key handles

🟨 Must be in TCB

🟦 Needs no trust



#Stuff - ChatCrypt - Google Chrome
https://www.chatcrypt.com/chat.php
Chat with kamicut
Chat Edit View Help
kamicut is online.

UI: Plaintext, Layout / Style

Ciphertext Msgs

App. Logic

UI: Plaintext, Layout / Style

Ciphertext Msgs

App. Logic

Plaintext Viewer

Key Mgmt. / Crypto

Runtime / APIs

🟨 Must be in TCB

🟦 Needs no trust

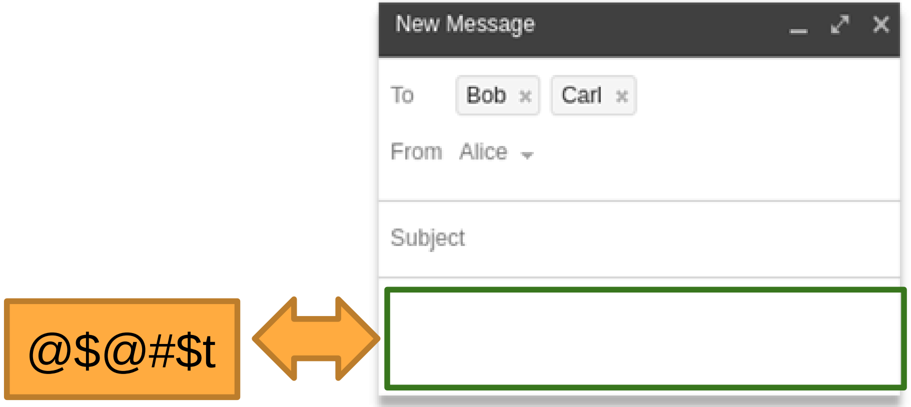
Also protect plaintext

- Provide opaque handles to the application

- Challenges:
  - Keep look n feel
  - Maintain current dev practices.

Challenge - Isolating plain text

Plaintext isolated in “private areas” taken in charge by Beeswax.



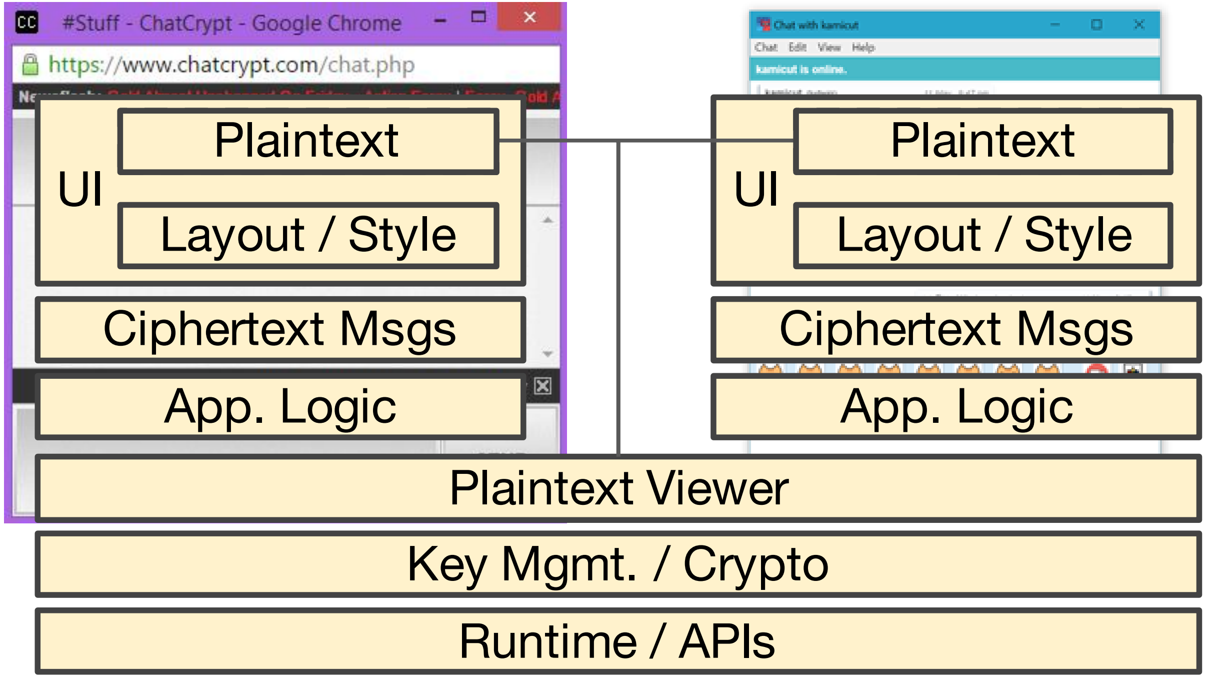
1. API call designates region of DOM to display confidential info.

2. Platform protects region of DOM from access by page JS.**

3. API call to display and inputs ciphertext in/out private area.

**Isolation uses ShadowDOM [W3C], similar to ShadowCrypt [CCS2014].

**We perform JS environment changes to protect access and allow events.


CC #Stuff - ChatCrypt - Google Chrome
https://www.chatcrypt.com/chat.php
Chat with kamicut
Chat Edit View Help
kamicut is online.

UI

Plaintext

Layout / Style

Ciphertext Msgs

App. Logic

UI

Plaintext

Layout / Style

Ciphertext Msgs

App. Logic

Plaintext Viewer

Key Mgmt. / Crypto

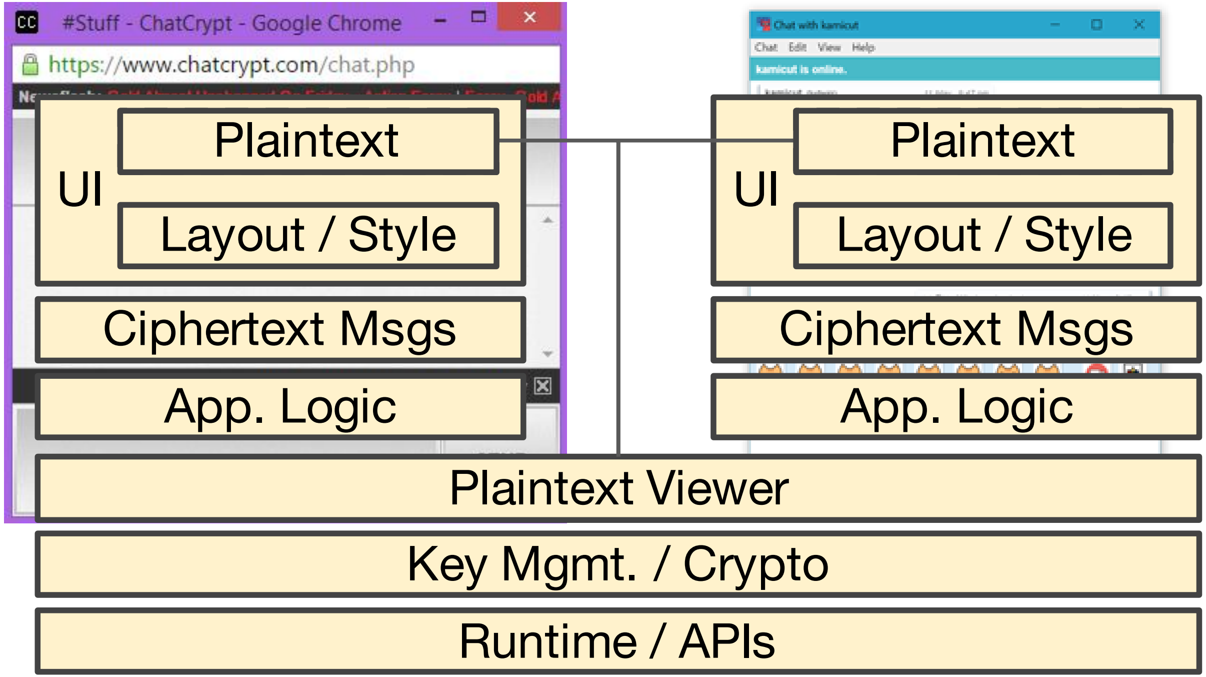
Runtime / APIs

- Beeswax isolates keys and plaintext
- Isolated data cannot be exfiltrated

Are we done?
Can we turn the app stacks blue?

🟨 Must be in TCB

🟦 Needs no trust


#Stuff - ChatCrypt - Google Chrome
https://www.chatcrypt.com/chat.php
Chat with kamicut
Chat Edit View Help
kamicut is online.

UI

Plaintext

Layout / Style

Ciphertext Msgs

App. Logic

UI

Plaintext

Layout / Style

Ciphertext Msgs

App. Logic

Plaintext Viewer

Key Mgmt. / Crypto

Runtime / APIs

🟨 Must be in TCB

🟦 Needs no trust

NO!

Blue means we must assume app can be malicious.

A malicious app can spoof the UI.

Challenge – Defeating UI spoofing by app

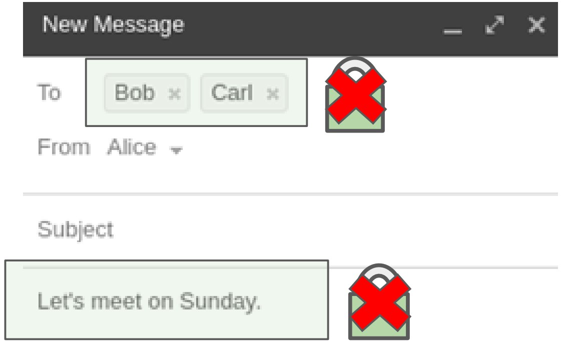
Application may or may not use Beeswax APIs.

App might try to provide its own "privacy" markers

- E.g. "Bob's in the 'To:' field. Is this message really being sent to Bob?"

- Application could show "green locks" or "green borders", but can't be trusted.

Beeswax could change the page to add indicators, but the app controls the window.



Let's meet on Sunday.

Beeswax Privacy Indicator

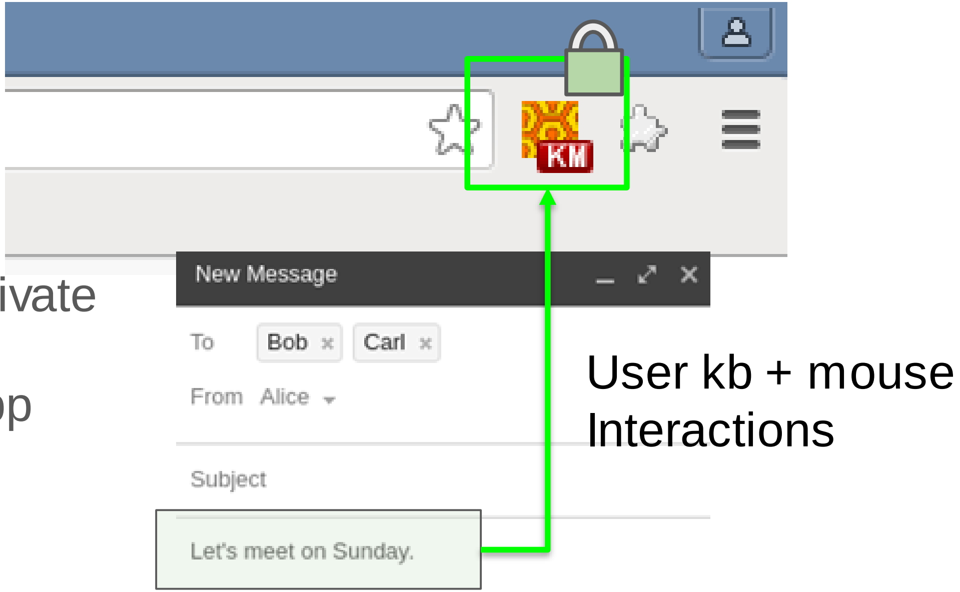
We add an indicator of privacy in an *unspoofable* region of the tab

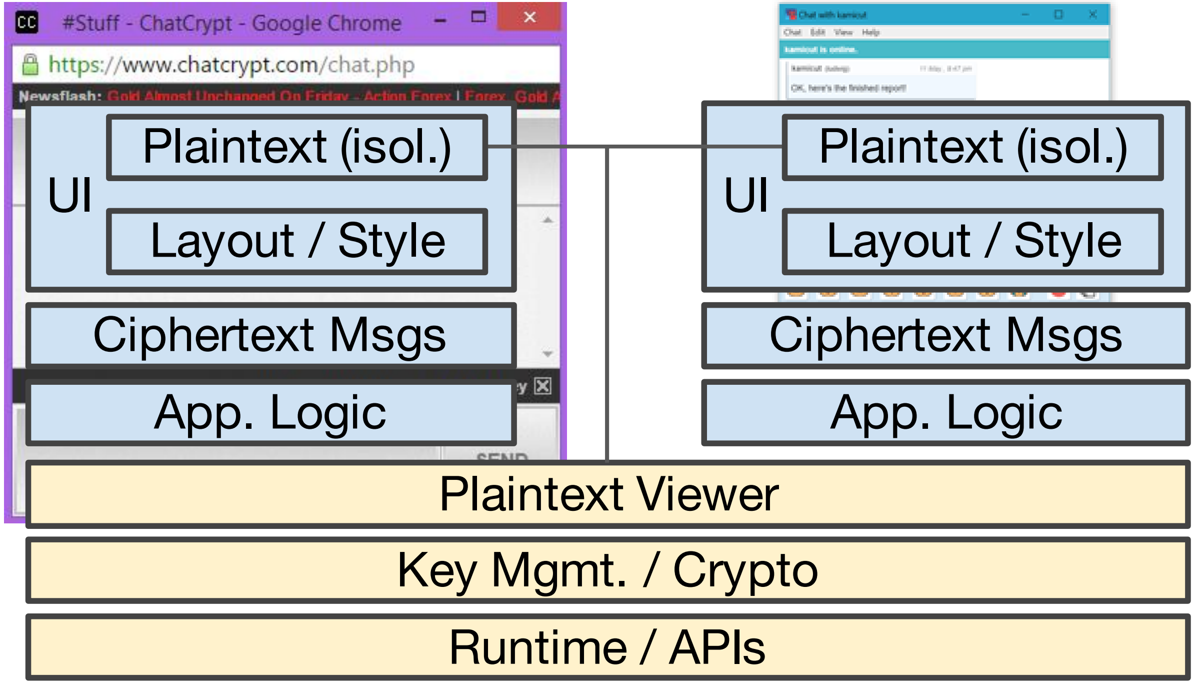
User interactions in private areas toggle the privacy indicator.

Tells if DOM region of interest is private

Content is hidden from the app

Events locked* to region




#Stuff - ChatCrypt - Google Chrome
https://www.chatcrypt.com/chat.php
Newsflash: Gold Almost Unchanged On Friday - Action Forex | Forex Gold A
SEND
Chat with kamicut
Chat Edit View Help
kamicut is online.
OK, here's the finished report!

UI

Plaintext (isol.)

Layout / Style

Ciphertext Msgs

App. Logic

UI

Plaintext (isol.)

Layout / Style

Ciphertext Msgs

App. Logic

Plaintext Viewer

Key Mgmt. / Crypto

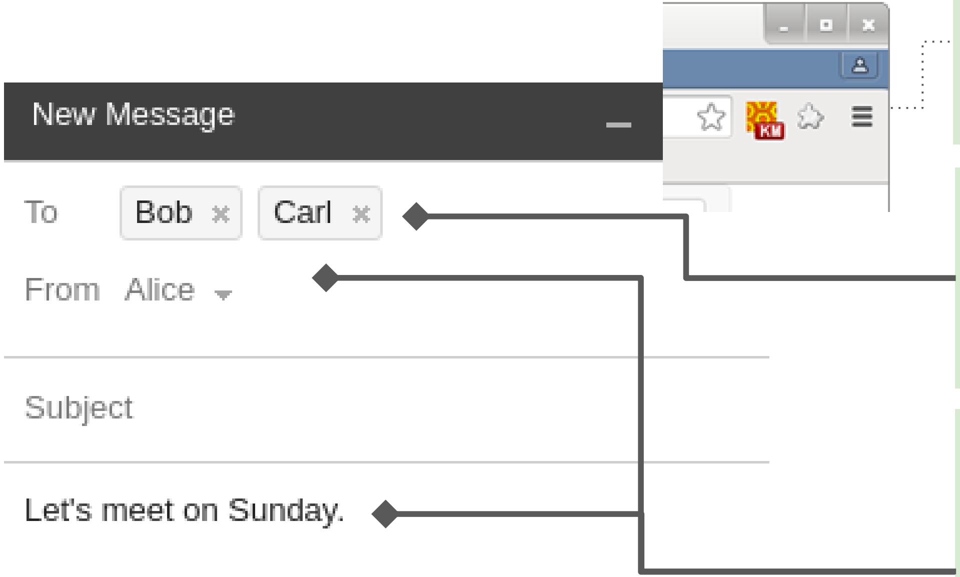
Runtime / APIs

🟨 Must be in TCB

🟦 Needs no trust

- Keys/plaintext are unavailable to the application
- P.I. indicates where events and text go.
- In TCB: Beeswax YES, Apps: NO

Split Functionality: Platform and App



New Message

To Bob Carl

From Alice

Subject

Let's meet on Sunday.

When interacting with a private area, the platform allows the user to verify true recipients of a message.

Application provides functionality and takes care of sharing. Intention: “User wants to write a message to Bob+Carl”

Platform manages keys and identities.

Platform establishes secure end-to-end data streams between users. (crypto).

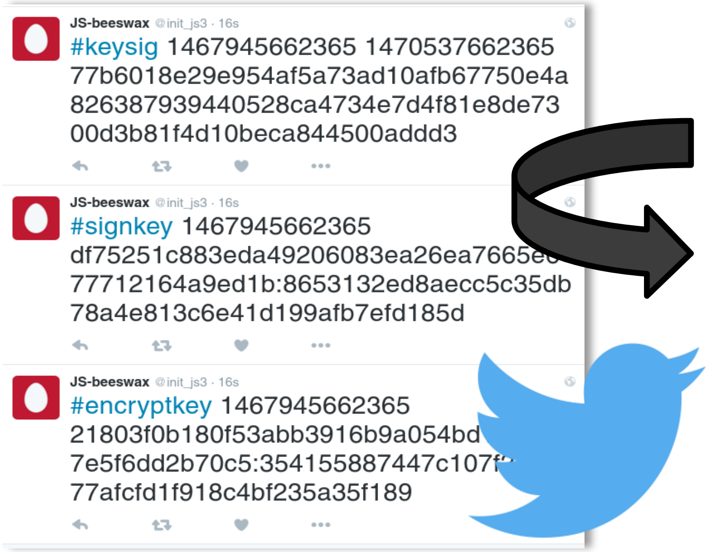
Transparent Key Management and Distribution

Beeswax has Built-in key management:

- Automatic distribution of Public Keys
- Key Agreement Protocol between pairs of users (“friendships”)
- Symmetric key crypto API (“streams”)

Beeswax Identities

At setup, a user’s Beeswax browser extension will generate 2 keypairs (sign, encrypt) and post a self signed cert of both to a configured twitter account..



JS-beeswax @init_js3 · 16s
#keysig 1467945662365 1470537662365 77b6018e29e954af5a73ad10afb67750e4a 826387939440528ca4734e7d4f81e8de73 00d3b81f4d10beca844500addd3

JS-beeswax @init_js3 · 16s
#signkey 1467945662365 df75251c883eda49206083ea26ea7665e 77712164a9ed1b:8653132ed8aecc5c35db 78a4e813c6e41d199afb7efd185d

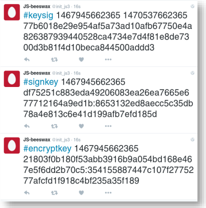
JS-beeswax @init_js3 · 16s
#encryptkey 1467945662365 21803f0b180f53abb3916b9a054bd 7e5f6dd2b70c5:354155887447c107f 77afcfd1f918c4bf235a35f189

The Beeswax background process in the extension monitors and reposts certs periodically.

*A similar process allows users to retrieve and monitor friend’s keys based on twitter IDs

Beeswax Key Distribution

The application initiate friendships with other users. (Triggers the KAP).

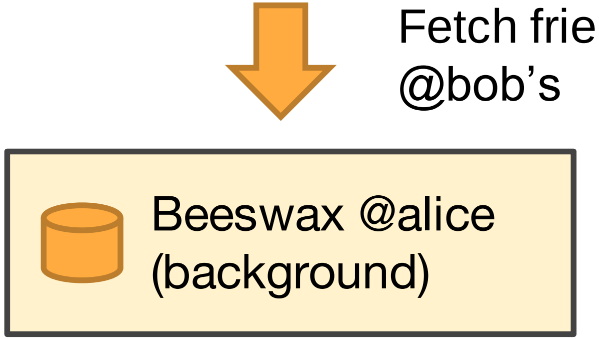


JS-beeswax @init_js3 · 16s
#keysig 1467945662365 1470537662365 77b6018e29e954af5a73ad10afb67750e4a 826387939440528ca4734e7d4f81e8de73 00d3b81f4d10beca844500addd3

JS-beeswax @init_js3 · 16s
#signkey 1467945662365 df75251c883eda49206083ea26ea7665e6 77712164a9ed1b:8653132ed8aecc5c35db 78a4e813c6e41d199afb7efd185d

JS-beeswax @init_js3 · 16s
#encryptkey 1467945662365 21803f0b180f53abb3916b9a054bd168e46 7e5f6dd2b70c5:354155887447c107f27752 77afcfd1f918c4bf235a35f189

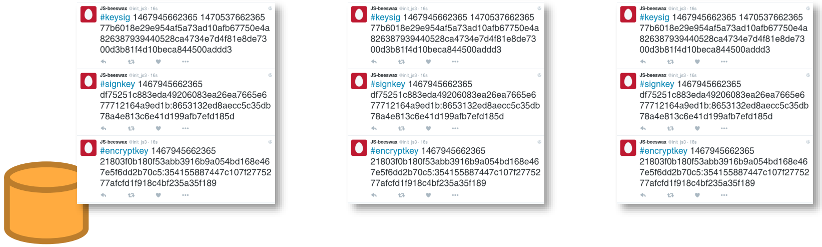
@bob's certs



Fetch friend @bob's

Beeswax @alice (background)

Beeswax periodically monitors online certs against those in DB. Handles revocation.*



JS-beeswax @init_js3 · 16s
#keysig 1467945662365 1470537662365 77b6018e29e954af5a73ad10afb67750e4a 826387939440528ca4734e7d4f81e8de73 00d3b81f4d10beca844500addd3

JS-beeswax @init_js3 · 16s
#signkey 1467945662365 df75251c883eda49206083ea26ea7665e6 77712164a9ed1b:8653132ed8aecc5c35db 78a4e813c6e41d199afb7efd185d

JS-beeswax @init_js3 · 16s
#encryptkey 1467945662365 21803f0b180f53abb3916b9a054bd168e46 7e5f6dd2b70c5:354155887447c107f27752 77afcfd1f918c4bf235a35f189

JS-beeswax @init_js3 · 16s
#keysig 1467945662365 1470537662365 77b6018e29e954af5a73ad10afb67750e4a 826387939440528ca4734e7d4f81e8de73 00d3b81f4d10beca844500addd3

JS-beeswax @init_js3 · 16s
#signkey 1467945662365 df75251c883eda49206083ea26ea7665e6 77712164a9ed1b:8653132ed8aecc5c35db 78a4e813c6e41d199afb7efd185d

JS-beeswax @init_js3 · 16s
#encryptkey 1467945662365 21803f0b180f53abb3916b9a054bd168e46 7e5f6dd2b70c5:354155887447c107f27752 77afcfd1f918c4bf235a35f189

JS-beeswax @init_js3 · 16s
#keysig 1467945662365 1470537662365 77b6018e29e954af5a73ad10afb67750e4a 826387939440528ca4734e7d4f81e8de73 00d3b81f4d10beca844500addd3

JS-beeswax @init_js3 · 16s
#signkey 1467945662365 df75251c883eda49206083ea26ea7665e6 77712164a9ed1b:8653132ed8aecc5c35db 78a4e813c6e41d199afb7efd185d

JS-beeswax @init_js3 · 16s
#encryptkey 1467945662365 21803f0b180f53abb3916b9a054bd168e46 7e5f6dd2b70c5:354155887447c107f27752 77afcfd1f918c4bf235a35f189

Key Agreement -- Friendship Channel

Key-Agreement-Protocol (KAP) creates secure bi-directional control channel between pairs of users, **Friendship Channel.** E.g. used for invitations and exchanging key information (see below).

API get_friend(@accountid) -> friendship

Establishes a set of symmetric keys used for secure communication of app signalling, such as invitations to streams.

Streams

Streams are media channels. Stream creators can invite other users over friendship channels.

API invite(<friendship>, <streamid>) -> invitation

Invite participants to a stream by messages over friendship channel

API accept_invite(<invitation>) -> streamid

Application receives a key handle for this stream (handle to a symmetric key).

Application relays ciphertext attached to streams.

Evaluation

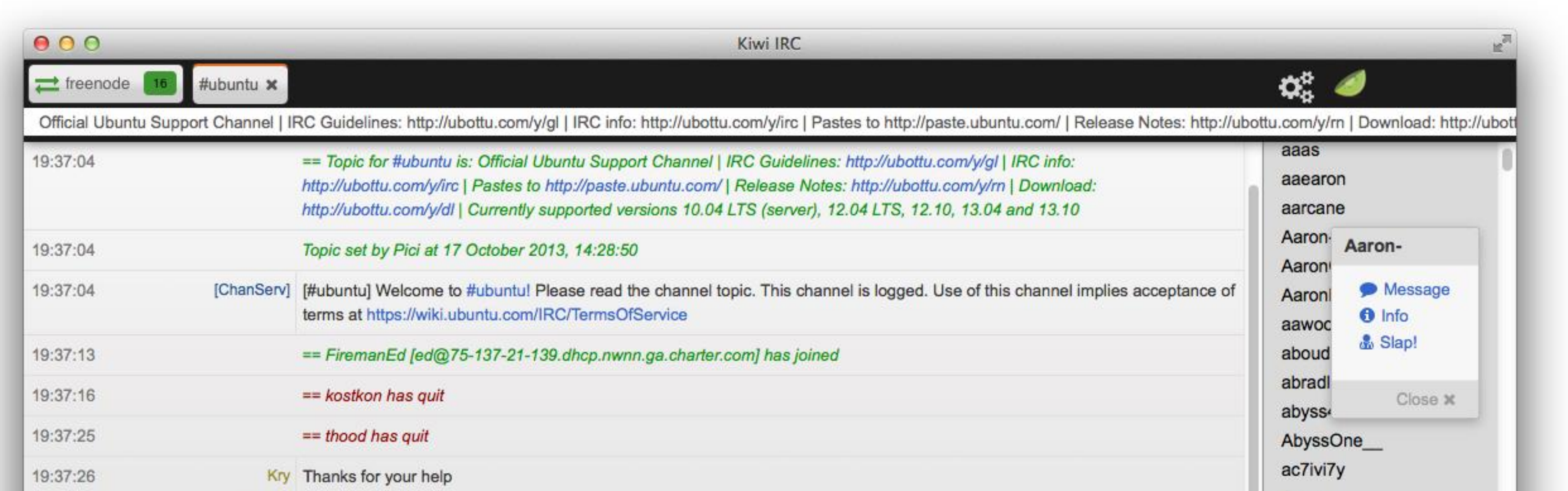
- Mechanisms fit for the development of modern web application
- Transformed existing web communication application (IRC) to support encrypted messaging between groups of users
- Created new encrypted photo gallery to demonstrate ability to handle richer media types
- Acceptable performance

Evaluation - Encrypted IRC Client

Adding encrypted messages to an IRC client:

Beeswax users can create encrypted IRC channels

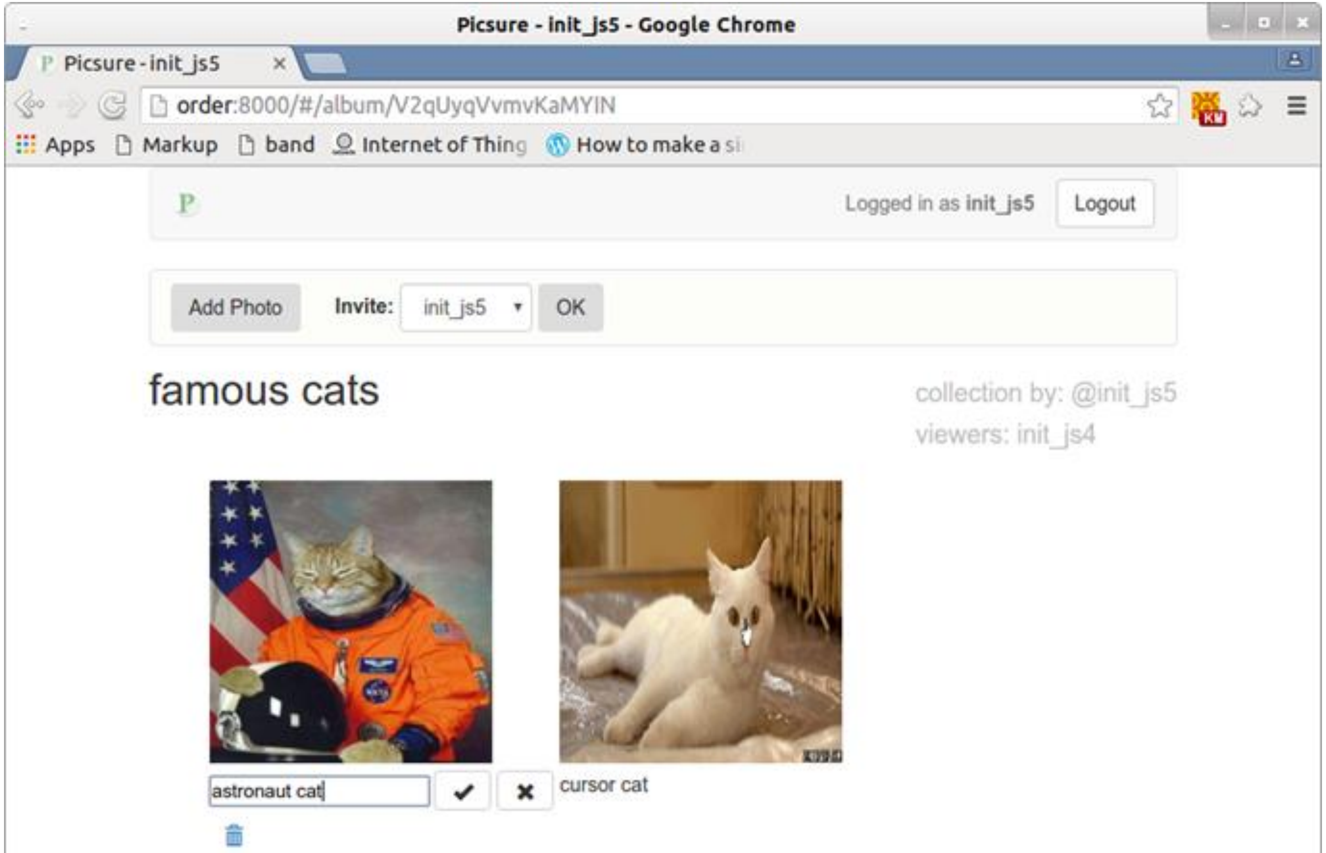
Modified KiwiIRC v0.9.0: 400 LOC added to client-side (7%)



Official Ubuntu Support Channel | IRC Guidelines: http://ubottu.com/y/gl | IRC info: http://ubottu.com/y/irc | Pastes to http://paste.ubuntu.com/ | Release Notes: http://ubottu.com/y/rn | Download: http://ubott

```
19:37:04              == Topic for #ubuntu is: Official Ubuntu Support Channel | IRC Guidelines: http://ubottu.com/y/gl | IRC info:
                      http://ubottu.com/y/irc | Pastes to http://paste.ubuntu.com/ | Release Notes: http://ubottu.com/y/rn | Download:
                      http://ubottu.com/y/dl | Currently supported versions 10.04 LTS (server), 12.04 LTS, 12.10, 13.04 and 13.10
19:37:04              Topic set by Pici at 17 October 2013, 14:28:50
19:37:04   [ChanServ] [#ubuntu] Welcome to #ubuntu! Please read the channel topic. This channel is logged. Use of this channel implies acceptance of
                      terms at https://wiki.ubuntu.com/IRC/TermsOfService
19:37:13              == FiremanEd [ed@75-137-21-139.dhcp.nwnn.ga.charter.com] has joined
19:37:16              == kostkon has quit
19:37:25              == thood has quit
19:37:26          Kry Thanks for your help
```

Evaluation - Secure photo sharing (PicSure)



famous cats

collection by: @init_js5

viewers: init_js4

astronaut cat

cursor cat

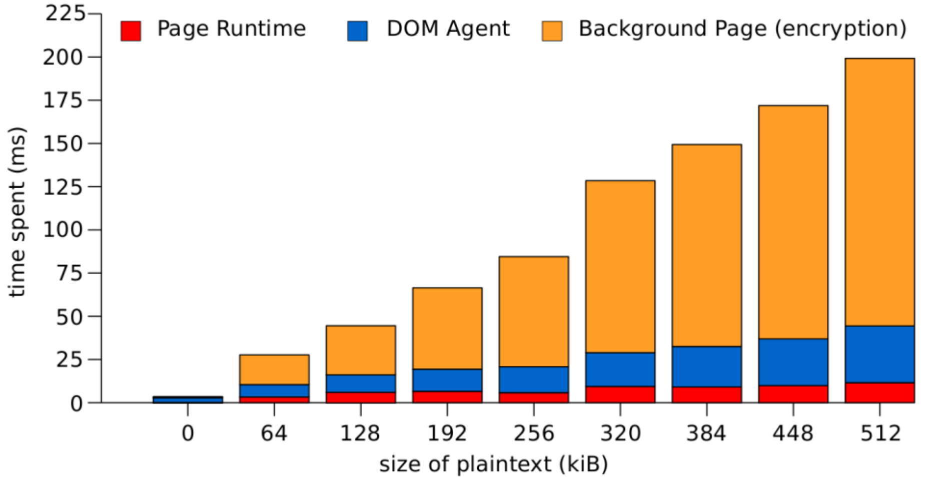
Regular tools: jquery, bootstrap, node.

Richer media type support: private areas supporting images (Beeswax photo chooser)

Performance - Microbenchmarks

Takeaways:

- Encryption cost is predictable, linear with plaintext size.



Re: runtime

- ~52 ms average page load increase
- 2.5x slower event processing to sanitize events from confidential information in private areas

Why just the web. What about mobile?

- Android OS does not have an architecture for secure modules to be loaded
- No allocation for an unspoofable area of the screen (privacy indicator)

Discussion

- Provides protection against exfiltration by the application provider
- Like any platform, features can be added as platform matures
- Key distribution easy and automatic, deployable now.
- Focus scrutiny on platform, not apps

Platform and apps are open source, available on github:

`https://web-priv.github.io/beeswax/`

END OF RIBBON.
RESERVE SLIDES FOLLOW

Privacy indicator states

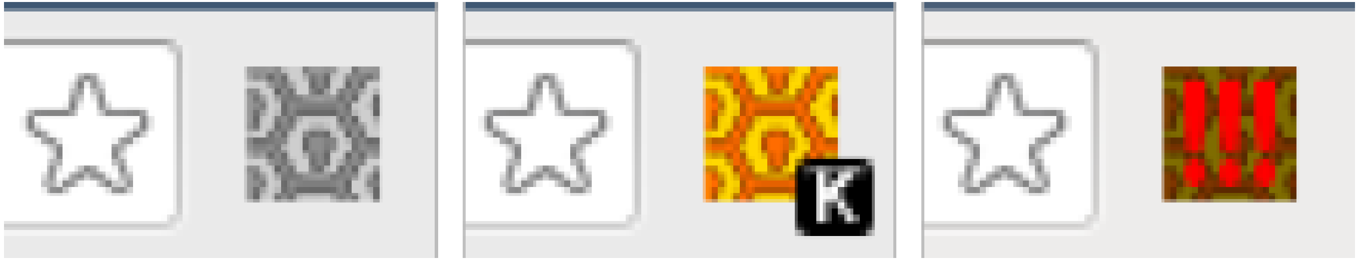


Fig. 2. The Privacy Indicator “unprotected" (left), “protected" due to keyboard events (“K") in a private area (middle), and showing a security warning (right).

Other spoofing

Talk about other ways to spoof there?

- Lying about recipients
- Overlaying elements
- Stealing events from private areas
- Locking mechanism

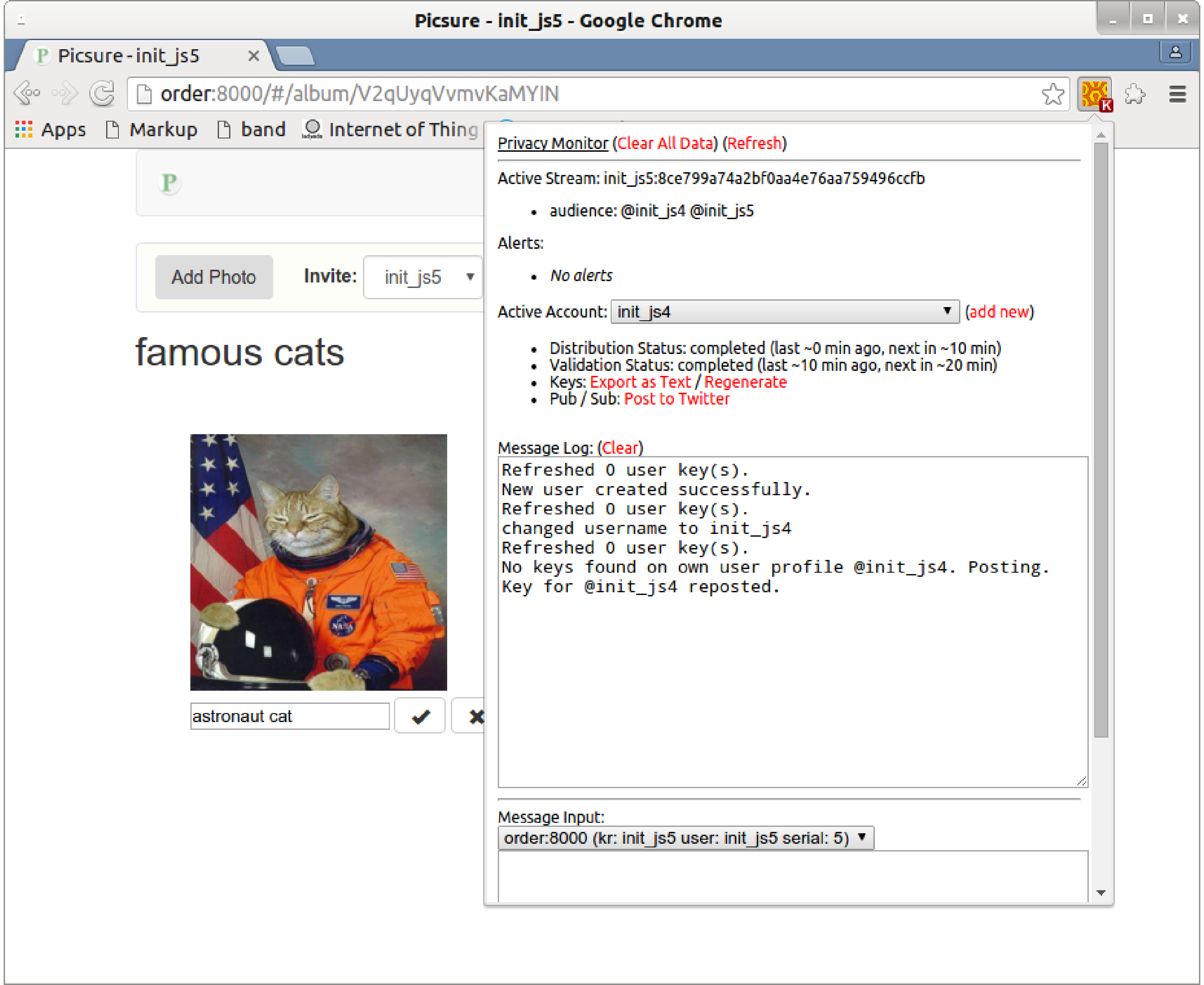
Refer to paper?

Beeswax Identity Management

Users are registered to a Pub/Sub service

Users verify binding between P/S account ID and person they want to communicate with

Only account owner can post to that account



Privacy Monitor (Clear All Data) (Refresh)

Active Stream: init_js5:8ce799a74a2bf0aa4e76aa759496ccfb

- audience: @init_js4 @init_js5

Alerts:

- *No alerts*

Active Account: init_js4 (add new)

- Distribution Status: completed (last ~0 min ago, next in ~10 min)
- Validation Status: completed (last ~10 min ago, next in ~20 min)
- Keys: Export as Text / Regenerate
- Pub / Sub: Post to Twitter

Message Log: (Clear)

```
Refreshed 0 user key(s).
New user created successfully.
Refreshed 0 user key(s).
changed username to init_js4
Refreshed 0 user key(s).
No keys found on own user profile @init_js4. Posting.
Key for @init_js4 reposted.
```

Message Input:

order:8000 (kr: init_js5 user: init_js5 serial: 5)