



The Open Privacy Stack: Privly

@privly

Lead Developer: Sean McGregor @seanmcgregor

Community Manager: Jennifer Davidson @jewifer

Outline

1. How the web is broken for security
2. "Injectable Applications" as a solution
3. How Privly implements injectable applications
4. More on injectable applications
5. The Privly Foundation and the way forward

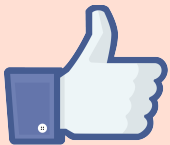
How Security on the Web is Broken



PRISM: Online service providers cannot protect users from the governments under which they operate

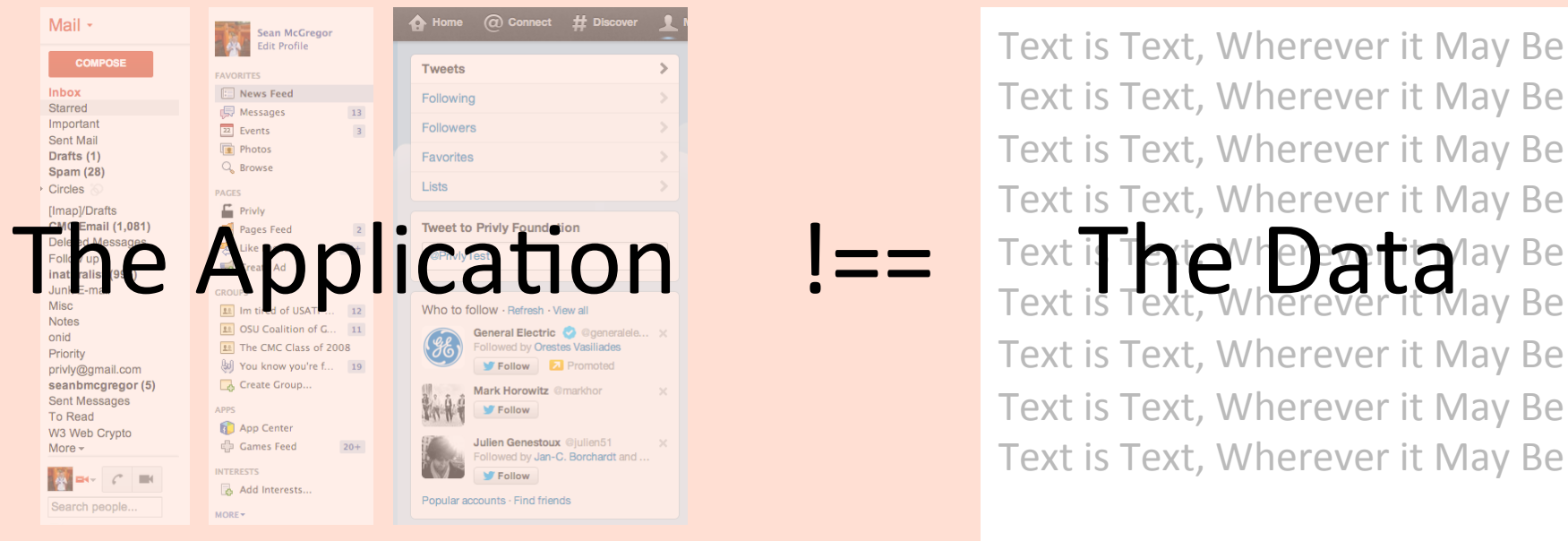


Hushmail: Online services cannot protect users from themselves



Facebook “Like” Button: Security and functionality are difficult to combine

Solution: Stop Reinventing Security



- Your site is unique, but your data is not!
- Wrap content in its own application viewed inside your web application

OSCON 2013

priv.ly/pages/download

Text is Text, Wherever it May Be

Privly Presentation

Sean McGregor



Join Google+


 **Test Account** <test@privly.org> 11:10 AM (0 minutes ago) ☆

to Sean ▾

Text is text, wherever it may be. Text is text, wherever it may be. Text is text, wherever it may be. Text is text, wherever it may be. Text is text, wherever it may be.



Click here to [Reply](#) or [Forward](#)

 Sean McGregor _ ↗ ✕


   More ▾

me:

Text is text, wherever it may be. Text is text, wherever it may be. Text is text, wherever it may be. Text is text, wherever it may be. Text is text, wherever it may be.

Sent at 10:54 AM on Sunday

Sean is busy. You may be interrupting.
Press Enter to send your message.

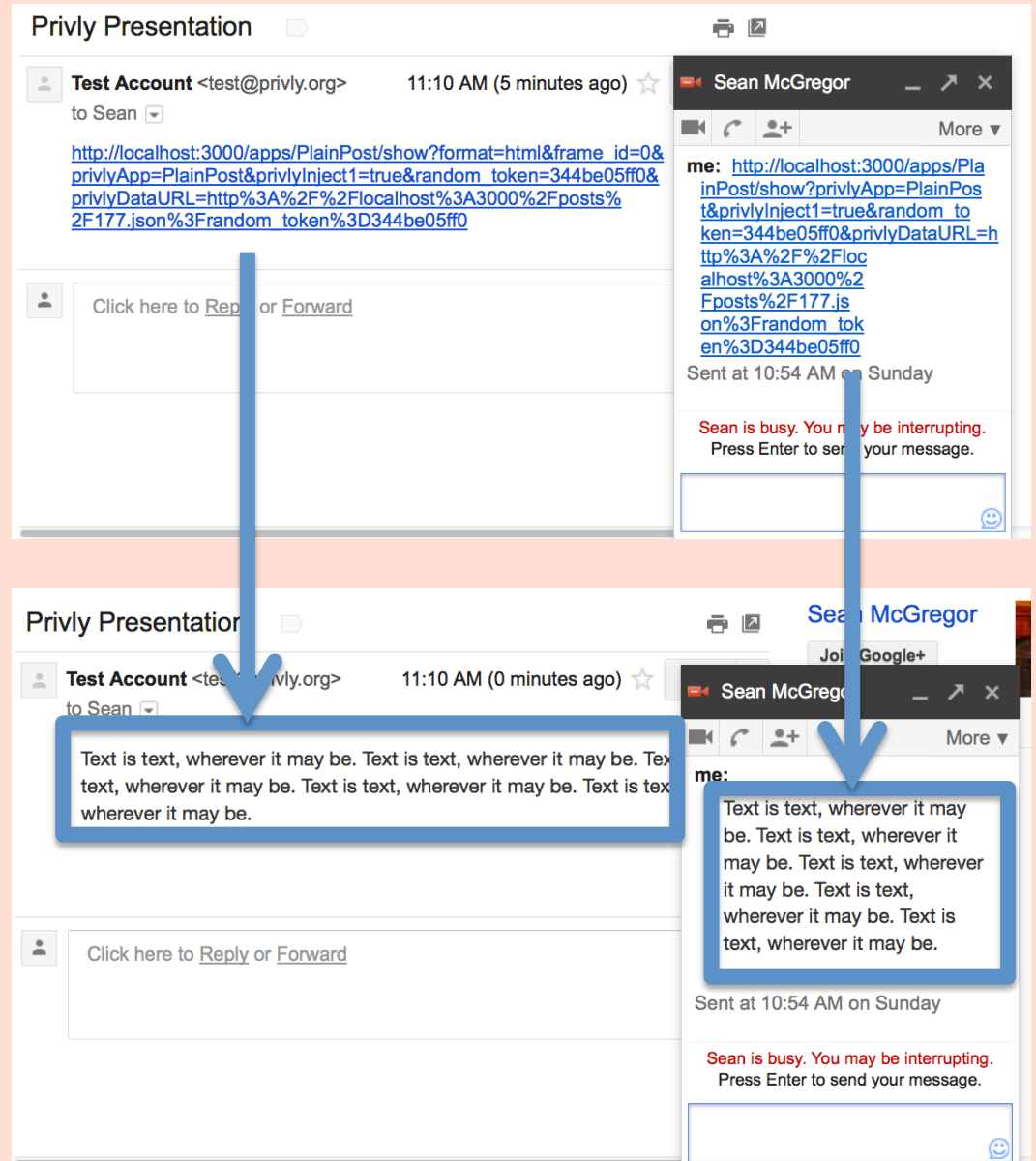


OSCON 2013

priv.ly/pages/download

That Was Privly at Work

1. Browser Extension discovers specially formatted link
2. “Injects” the link



Text is Text, Wherever it May Be

Privly Presentation

Sean McGregor









Join Google+

 **Test Account** <test@privly.org> 11:10 AM (0 minutes ago) ☆
to Sean ▾

This is a Complete Web Application

 Click here to [Reply](#) or [Forward](#)

 Sean McGregor  



   More ▾

me:

This is a Complete Web Application

Sent at 10:54 AM on Sunday

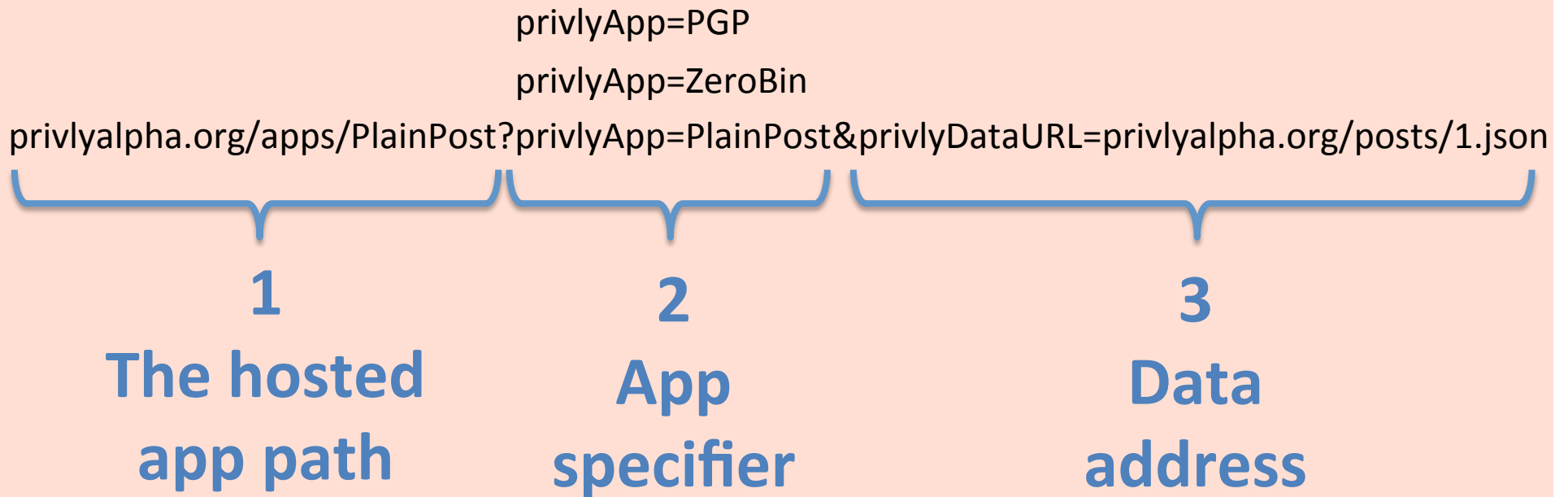
Sean is busy. You may be interrupting.
Press Enter to send your message.

OSCON 2013

priv.ly/pages/download

The Privly URL



[https://Privlyalpha/apps/
PlainPost?
privlyApp=PlainPost&privlyDataU
RL=https://privlyalpha.org/posts/
2342536674.json](https://Privlyalpha/apps/PlainPost?privlyApp=PlainPost&privlyDataURL=https://privlyalpha.org/posts/2342536674.json)



Extended Browser

This is a demonstration of Privly's capabilities. The host page, Twitter, does not have access to the Tweet's contents. It is also not limited by the length imposed by Twitter.



-47

Tweet

Host Page

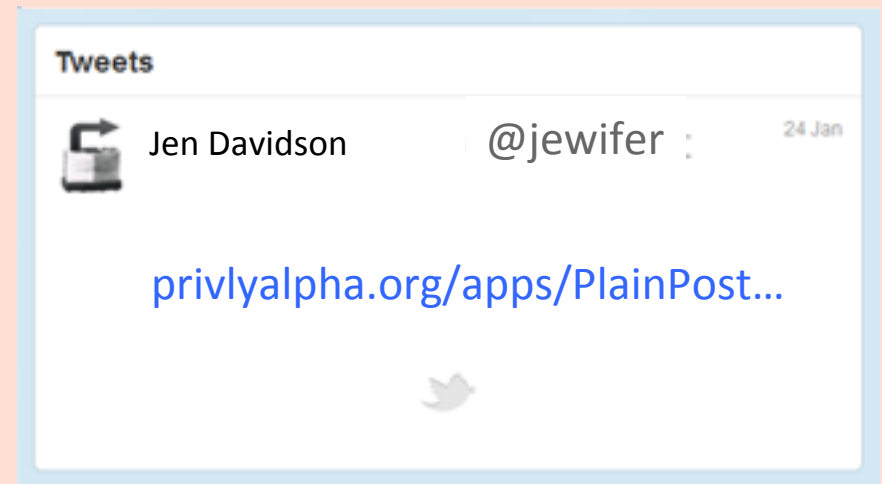
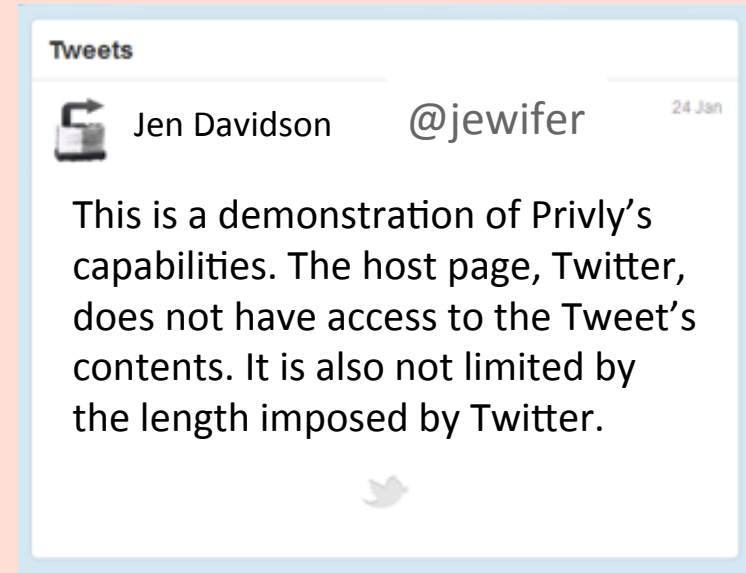
OSCON 2013

priv.ly/pages/download

Extension

No

Extension





Javascript Cryptography Considered Harmful

?privlyApp=PlainPost&

2

App
specifier

Pre-Distribute the
Apps

Privly

Javascript Cryptography **Potentially** Not Harmful

What if the User Doesn't Have the App?

`privlyalpha.org/apps/ZeroBin`



1

**The hosted
app path**

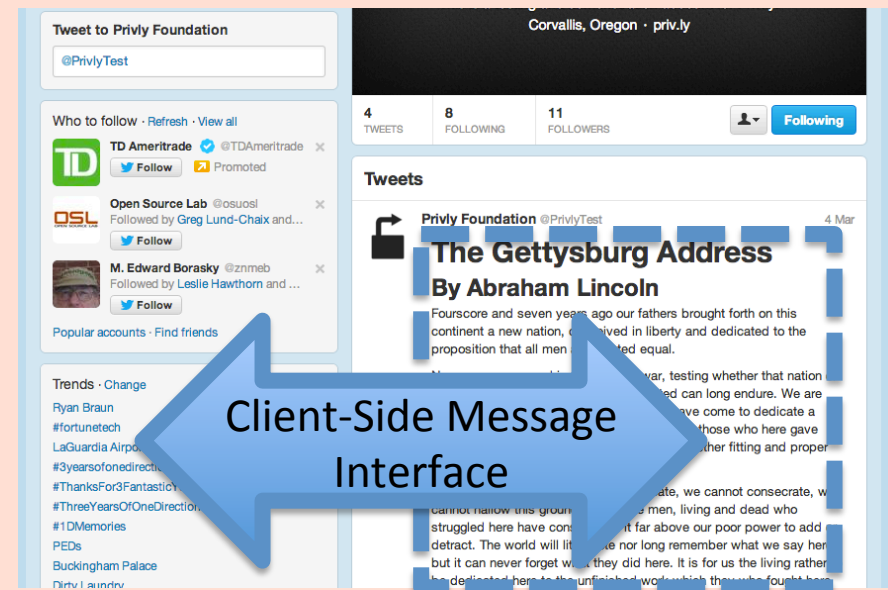
- Optional hosted fallback
 - Posting users can choose an app where hosted fallback is possible
 - You do not protect users from the host
 - Best case, you host it yourself
 - ZeroBin App is a compromise

More About these “Injectable Apps”

- Current
 - PlainPost: Most universal application
 - ZeroBin: Encrypted by the anchor text
- In Development
 - PGP: Strong Public Key Crypto
 - IndieData: Personal Semantic Datastore
- Planned
 - OTR: Encrypted chat application
 - various other specific use cases

Cool Potential Functionality

- Host page API
- Hooks into distributed hash table
- Seamless integration with social networks for sharing lists



Are Websites the Adversary?

- Only from a security perspective
 - Have to account for worst case scenarios
- Privly increases time-on-site
 - Increased add revenues
 - Time-on-site is more valuable than being able to target advertising to private message contents

Privly Development Status



- Google Chrome Extension is the most advanced
- Use the Chrome Extension to develop Injectable Apps
- Google Summer of Code students are developing iOS and Android version

Content Servers

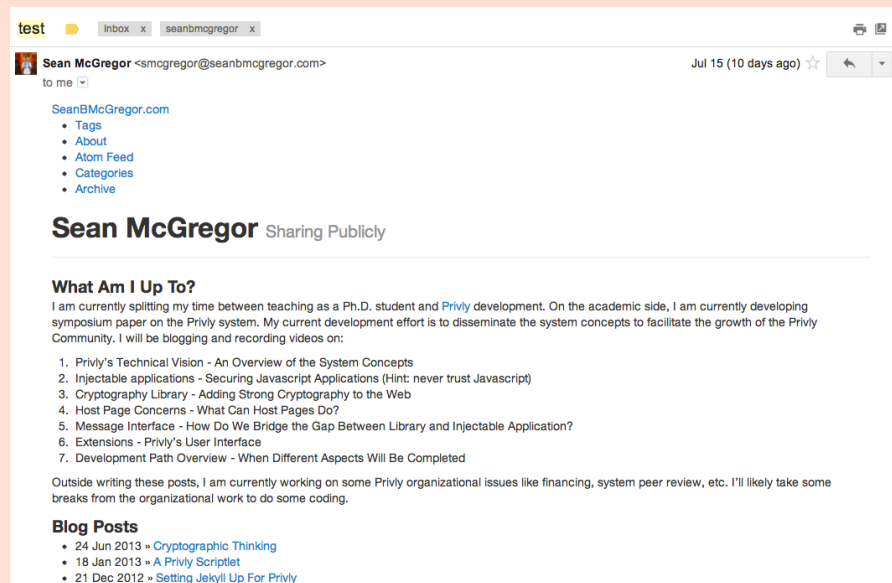
Sophistication



GitHub Pages

BACKBONE.JS

- Data driven
- Advertises extensions
- Privly-applications runs from static folder



OSCON 2013

priv.ly/pages/download

What's Next

- Security is hard, innovation is **dangerous**
- Put warnings on **everything** and release/iterate



Making an Injectable Application

- Start with the Chrome extension:
github.com/privly/privly-chrome
- Easiest way to start is by editing the PlainPost application

Resources

- Info/Download: priv.ly
- Communicate: privly.org
- Code: <https://github.com/privly>
- Latest Content Server: <https://privlyalpha.org>
- Slides: github.com/privly/privly-organization/tree/master/presentations/2013-07-25-OSCON/OSCON.ppt

Get Connected

#privly on irc.freenode.net

Join our mailing list, <http://bit.ly/privly-group>

Techno-Activism 3rd Mondays

- August Event:
<http://ta3m-pdx-3.eventbrite.com>
- TA3M Wiki:
http://wiki.openitp.org/events:techno-activism_3rd_mondays



Free (As in Beer)

- The handouts at the front have directions for getting credentials on on privlyalpha.org

Wait...what?

- Privly allows you to post “private” content anywhere on the web
- Privly allows you to offer your users protection from your servers (because what if they get compromised? Onooo!)
- Privly is a flexible framework – you can add all kinds of applications

Legal

- All logos are property of their respective owners
- Graphics in this presentation are used under a Creative Commons License
- This presentation is licensed under Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) (<http://creativecommons.org/licenses/by-sa/3.0/>)

Questions?

Thanks to O'Reilly Media!

<https://priv.ly>

<https://groups.google.com/group/privly@privly>

Sean: @seanmcgregor

Jen: @jewifer