



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

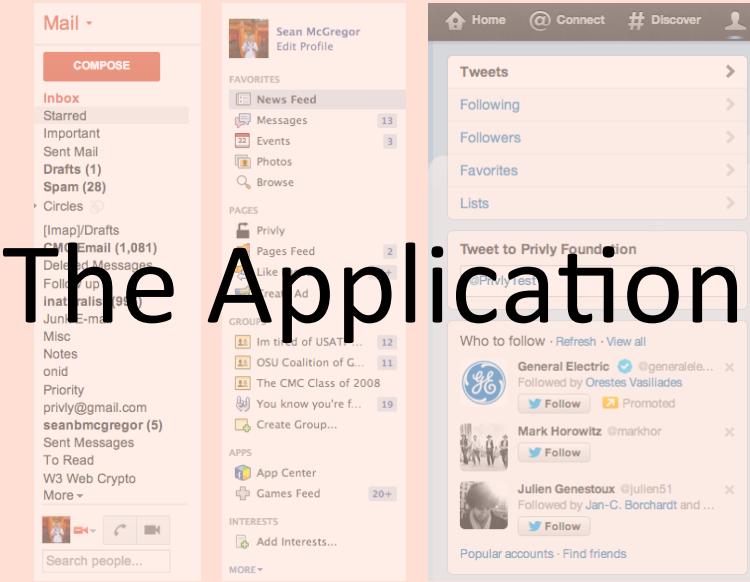


Hushmail: Online services cannot protect users from themselves



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

Solution: Stop Reinventing Security



The Application

!== The Data

Text is Text, Wherever it May Be
The Data
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

- 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.

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

me:

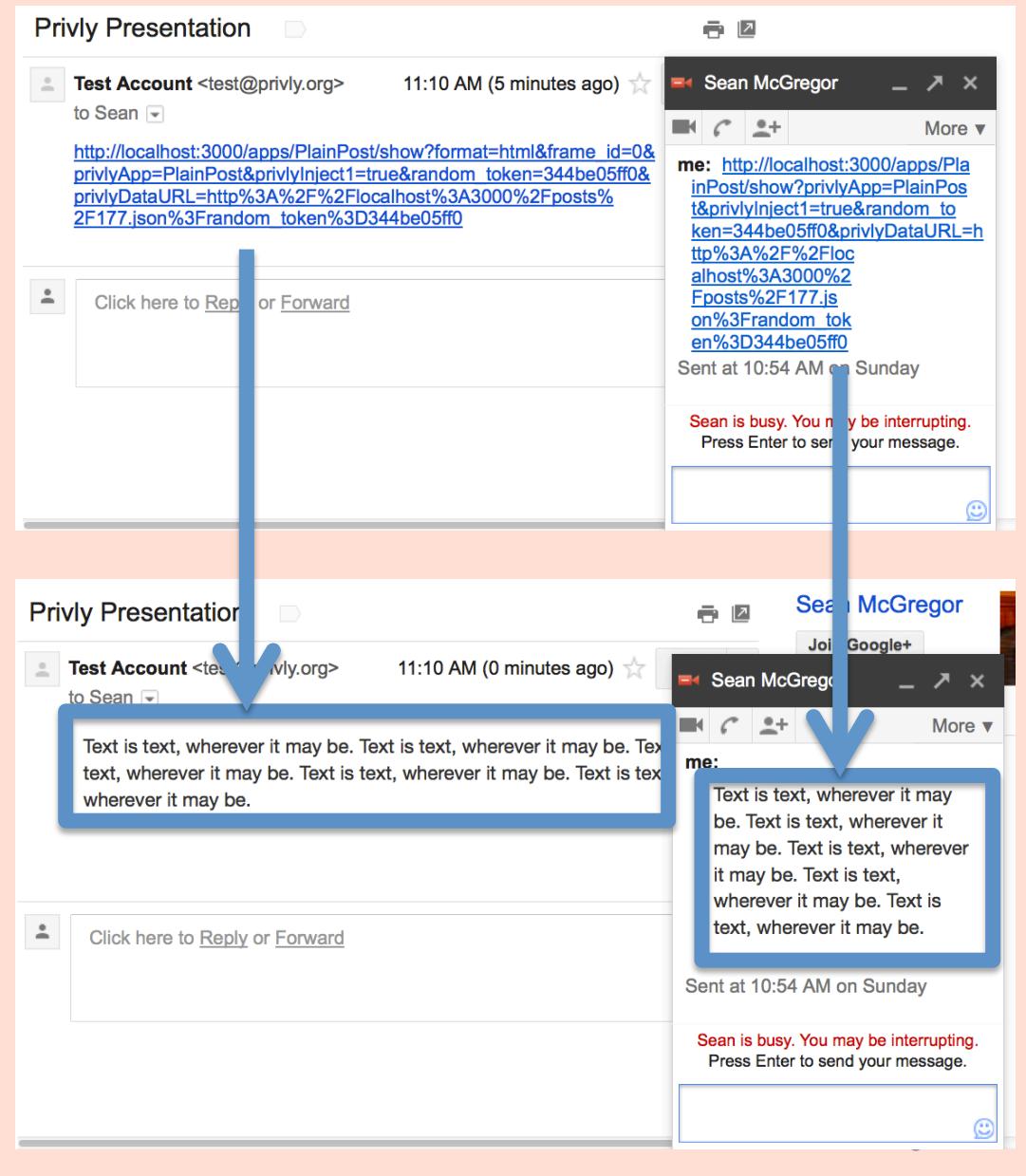
Text is text, wherever it may be. Text is text, wherever it may be.

Sent at 10:54 AM on Sunday

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

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

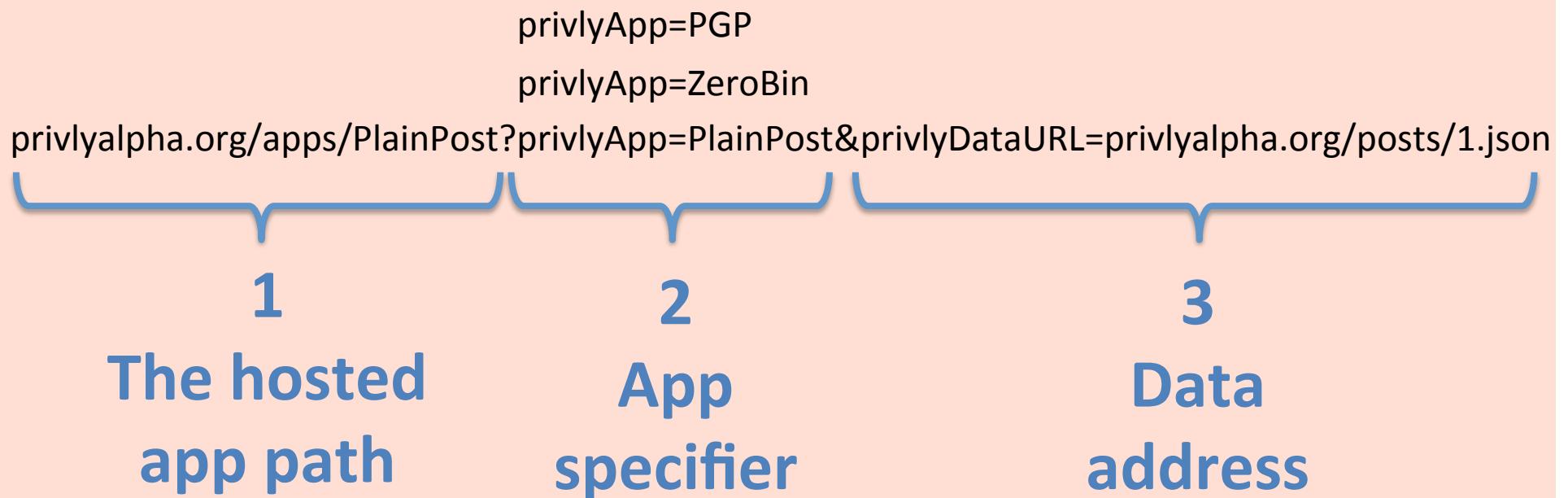
Sean is busy. You may be interrupting.
Press Enter to send your message.



OSCON 2013

priv.ly/pages/download

The Privly URL





Extended Browser

OSCON 2013

priv.ly/pages/download

[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)

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

Extension No Extension

OSCON 2013

priv.ly/pages/download

Tweets



Jen Davidson

@jewifer

24 Jan

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.



Tweets



Jen Davidson

@jewifer :

24 Jan

privlyalpha.org/apps/PlainPost...





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

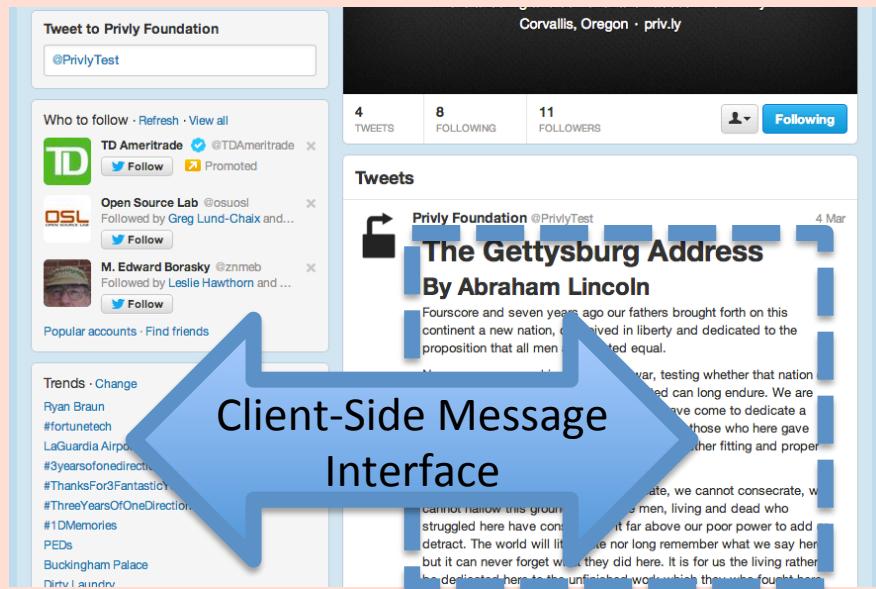
- Optional hosted fallback
 - Posting users can choose an app where hosted fallback is possible
 - You do not protect users from the host
 - Best case, you host it yourself
 - ZeroBin App is a compromise

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

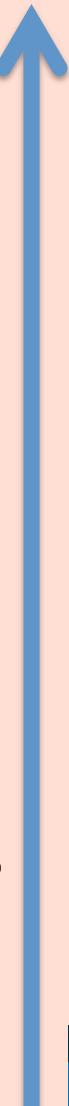
Privly Development Status



- 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

OSCON 2013

priv.ly/pages/download

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

test Inbox seanbmccgregor Jul 15 (10 days ago)

Sean McGregor <smcgregor@seanbmccgregor.com>
to me ↗

SeanBMcGregor.com

- Tags
- About
- Atom Feed
- Categories
- Archive

Sean McGregor Sharing Publicly

What Am I Up To?

I am currently splitting my time between teaching as a Ph.D. student and [Privly](#) development. On the academic side, I am currently developing symposium paper on Privly system. My current development effort is to disseminate the system concepts to facilitate the growth of the Privly Community. I will be blogging and recording videos on:

1. Privly's Technical Vision - An Overview of the System Concepts
2. Injectable applications - Securing Javascript Applications (Hint: never trust Javascript)
3. Cryptography Library - Adding Strong Cryptography to the Web
4. Host Page Concerns - What Can Host Pages Do?
5. Message Interface - How Do We Bridge the Gap Between Library and Injectable Application?
6. Extensions - Privly's User Interface
7. Development Path Overview - When Different Aspects Will Be Completed

Outside writing these posts, I am currently working on some Privly organizational issues like financing, system peer review, etc. I'll likely take some breaks from the organizational work to do some coding.

Blog Posts

- 24 Jun 2013 » [Cryptographic Thinking](#)
- 18 Jan 2013 » [A Privly Scriptlet](#)
- 21 Dec 2012 » [Setting Jekyll Up For Privly](#)

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](https://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](http://wiki.openitp.org/events:techno-activism_3rd_mondays)



Free (As in Beer)

- The handouts at the front have directions for getting credentials 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

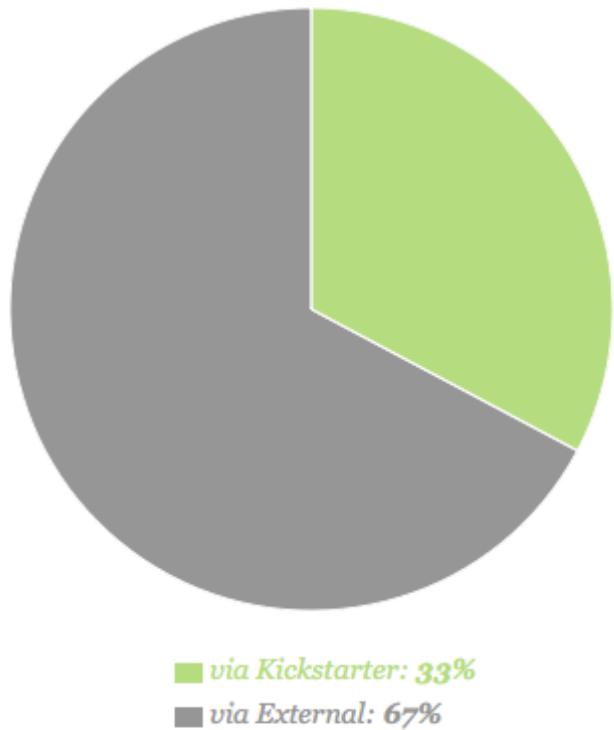
Jen: @jewifer

Extra Time Resources

Kickstarter

Our Kickstarter Experience

REFERRERS



Dollars pledged via Kickstarter

\$8,814

Dollars pledged via external referrers

\$18,077

Average pledge amount

\$47.60

Kickstarted in April 2012

↗ PROJECT ACTIVITY



OSCON 2013

priv.ly/pages/download

Sell

A Product -Or- A Cause

SLIDES WE MAY USE

- SLIDES WE MAY USE



Host Page Script: privly.js

from:public-webcrypto@w3.org OR to:public-web

Privly.js HTML Document 8 of about 190

Our sponsor needs the Crypto API to enable JavaScript programs to be able to request: "Hey, please sign

Privly.is Converts to iframe

HTML iframe

In all of the following cases, the user must be prompted for his PIN prior to signing with the smart card. Also, the system must know what he is signing.

Using smart cards to sign data submitted to internal company web apps:

a. An employee accesses the company web app where he can make changes to his employee benefits (dental, medical, eye). He enters the changes and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes the benefits changes.

b. After an employee makes a business trip he accesses a company web app which allows him to fill in the trip expenses - hotel, car rental, airfare - for reimbursement. He enters the expenses and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement.

c. An employee is on a business trip. At the end of each day he accesses his company's web app to enter

Business Cards \$8.50

People (11)

Davenport, James L.

Add to circles

Show details

Ads - Why these ads?

2012 Dodge® Avenger

Learn About Models, Colors & More!

Locate a Dealer in Your Area Now!

www.dodgecurrentoffers.com

How To Publish A Book

Free How To Guide For First Time Author in Publishing a Book.

www.Xlibris.com/HowToPublish

Charitable Trust

What's In Jim's Charitable Trust Portfolio? Sign Up Today To See.

www.thestreet.com/charitabletrust

VistaPrint- Official Site

Save on Business Cards, Postcards, Brochures, Magnets and Letterhead!

www.VistaPrint.com

OSCON 2013

priv.ly/pages/download



Host Page Script: privly.js

from:public-webcrypto@w3.org OR to:public-web

Privly.js HTML Document 8 of about 190

Our sponsor needs the Crypto API to enable JavaScript programs to be able to request: "Hey, please sign [math] \left[1 - \frac{\kappa_D}{(1 + x^2)^{1-\delta}} \right]^{-1}"

COMPOSE

Inbox
Starred
Important
Sent Mail
Drafts (1)
Spam (6)

» Circles
[Imap]/Drafts
CMC Email (1...)
Deleted Mess...
Follow up
inaturalist (83)
Junk E-mail
Misc
Notes
onid
Priority

Chat
Search people...
✉ Sean McGregor

HTML Document

Privly.js
HTML iframe
Sends resize message
Privly iframe
Using smart cards to sign data submitted to internal company web apps:

a. An employee accesses the company web app where he can make changes to his employee benefits (dental, medical, eye). He enters the changes and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes the benefits changes.

b. After an employee makes a business trip he accesses a company web app which allows him to fill in the trip expenses - hotel, car rental, airfare - for reimbursement. He enters the expenses and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement.

c. An employee is on a business trip. At the end of each day he accesses his company's web app to enter

Business Cards \$8.50
People (11)
Davenport, James L.
Add to circles
Show details
Ads - Why these ads?
2012 Dodge® Avenger
Learn About Models, Colors & More!
Locate a Dealer in Your Area Now!
www.dodgecurrentoffers.com
How To Publish A Book
Free How To Guide For First Time Author in Publishing a Book.
www.Xlibris.com/HowToPublish
Charitable Trust
What's In Jim's Charitable Trust Portfolio? Sign Up Today To See.
www.thestreet.com/charitabletrust
VistaPrint- Official Site
Save on Business Cards, Postcards, Brochures, Magnets and Letterhead!
www.VistaPrint.com

OSCON 2013

priv.ly/pages/download

Host Page Script: privly.js



from:public-webcrypto@w3.org OR to:public-web

Privly.js HTML Document 8 of about 190

Our sponsor needs the Crypto API to enable JavaScript programs to be able to request: "Hey, please sign this document."

Privly.js

HTML iframe

Resizes iframe

In all cases, the user must be prompted for his PIN prior to signing with the smart card. Also, the app displays to the user the data that is being signed, so that he knows what he is signing.

Privly iframe

Using smart cards to sign data submitted to internal company web apps:

a. An employee accesses the company web app where he can make changes to his employee benefits (dental, medical, eye). He enters the changes and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes the benefits changes.

b. After an employee makes a business trip he accesses a company web app which allows him to fill in the trip expenses - hotel, car rental, airfare - for reimbursement. He enters the expenses and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement.

c. An employee is on a business trip. At the end of each day he accesses his company's web app to enter

Business Cards \$8.50

People (11)

Davenport, James L.

Add to circles

Show details

Ads - Why these ads?

2012 Dodge® Avenger

Learn About Models, Colors & More!

Locate a Dealer in Your Area Now!

www.dodgecurrentoffers.com

How To Publish A Book

Free How To Guide For First Time Author in Publishing a Book.

www.Xlibris.com/HowToPublish

Charitable Trust

What's In Jim's Charitable Trust Portfolio? Sign Up Today To See.

www.thestreet.com/charitabletrust

VistaPrint- Official Site

Save on Business Cards, Postcards, Brochures, Magnets and Letterhead!

www.VistaPrint.com

OSCON 2013

priv.ly/pages/download

Host Page Script: privly.js



A screenshot of a web browser window displaying a signed HTML document. The browser interface includes a search bar at the top with the query "from:public-webcrypto@w3.org OR to:public-web", a search button, and a "More" dropdown. The main content area shows a red-themed email client interface with a sidebar containing links like "Compose", "Inbox", "Starred", "Important", "Sent Mail", "Drafts (1)", "Spam (6)", "Circles", "[Imap]/Drafts", "CMC Email (1...)", "Deleted Mess...", "Follow up", "inaturalist (83)", "Junk E-mail", "Misc", "Notes", "onid", "Priority", "Chat", and a search bar for "Search people...". The main pane displays an "HTML Document" with the title "Privly.js" and a sub-section "HTML iframe". Inside the "HTML iframe", there is another "Privly iframe" containing the text "Protected content". At the bottom of the main pane, there is a note: "Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement." The bottom left corner of the browser window shows the text "OSCON 2013".

priv.ly/pages/download

Extension Level: Decryption



The screenshot shows a web browser window with an email inbox on the left and an "HTML Document" view on the right. The inbox sidebar includes links for Compose, Inbox, Starred, Important, Sent Mail, Drafts (1), Spam (6), Circles, [Imap]/Drafts, CMC Email (1...), Deleted Mess..., Follow up, inaturalist (83), Junk E-mail, Misc, Notes, onid, Priority, Chat, and a search bar. The main area displays an email message with the subject "HTML Document". The message content is as follows:

Our sponsor needs the Crypto API to enable JavaScript programs to be able to request: "Hey, please sign [math]1 - \frac{\kappa_0}{(1 + x^2)^{1-\epsilon}}"

from:public-webcrypto@w3.org OR to:public-web

HTML Document

More 8 of about 190

Privly.js

HTML Document

Privly.js

HTML iframe

Smart Card Use Cases

In all of the following use cases the user must be prompted for his PIN prior to signing the data using his smart card. Also, the system must display to the user the data that is being signed, so that he can verify that it is what he wants to sign.

Privly iframe

Using smart cards to sign data submitted to internal company web apps:

a. An employee accesses the company web app where he can make changes to his employee benefits (dental, medical, eye). He enters the changes and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes the benefits changes.

b. After an employee makes a business trip he accesses a company web app which allows him to fill in the trip expenses - hotel, car rental, airfare - for reimbursement. He enters the expenses and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement.

c. An employee is on a business trip. At the end of each day he accesses his company's web app to enter

A large white arrow points from the "Decrypts" text down towards the "Privly iframe" area. A black curved arrow in the top right corner points towards the Firefox logo.

OSCON 2013

priv.ly/pages/download

Extension Level: Decryption



A screenshot of a Gmail inbox interface. The main message is from "from:public-webcrypto@w3.org OR to:public-web" with the subject "HTML Document". The message body contains several redacted sections and includes the following text:

Our sponsor needs the Crypto API to enable JavaScript programs to be able to request: "Hey, please sign [REDACTED]"

The message body is heavily redacted, with only the following visible text remaining:

Sends resize message
HTML iframe
Privly iframe
Using smart cards to sign data submitted to internal company web apps:

a. An employee accesses the company web app where he can make changes to his employee benefits (dental, medical, eye). He enters the changes and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes the benefits changes.

b. After an employee makes a business trip he accesses a company web app which allows him to fill in the trip expenses - hotel, car rental, airfare - for reimbursement. He enters the expenses and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement.

At the bottom of the message, there is a link: "An employee is on a business trip. At the end of each day he accesses his company's web app to enter [REDACTED]".

The left sidebar shows the user's inbox with 190 messages, including categories like "Inbox", "Starred", "Important", "Sent Mail", "Drafts (1)", "Spam (6)", "Circles", "[Imap]/Drafts", "CMC Email (1...)", "Deleted Mess...", "Follow up", "inaturalist (83)", "Junk E-mail", "Misc", "Notes", "onid", "Priority", "Chat", and "Sean McGregor".

OSCON 2013

priv.ly/pages/download

Extension Level: Decryption



from:public-webcrypto@w3.org OR to:public-web

Privly.js HTML Document 8 of about 190

Our sponsor needs the Crypto API to enable JavaScript programs to be able to request: "Hey, please sign

Inbox Starred Important Sent Mail Drafts (1) Spam (6)

Circles [Imap]/Drafts CMC Email (1...) Deleted Mess... Follow up inaturalist (83) Junk E-mail Misc Notes onid Priority

Chat Search people... Sean McGregor

Privly.js **Resizes iframe** HTML iframe Privly iframe

Using smart cards to sign data submitted to internal company web apps:

a. An employee accesses the company web app where he can make changes to his employee benefits (dental, medical, eye). He enters the changes and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes the benefits changes.

b. After an employee makes a business trip he accesses a company web app which allows him to fill in the trip expenses - hotel, car rental, airfare - for reimbursement. He enters the expenses and presses Submit. The changes are signed using the employee's smart card and then sent to the web app which validates the signature and processes for reimbursement.

c. An employee is on a business trip. At the end of each day he accesses his company's web app to enter

Business Cards \$8.50 People (11) Davenport, James L. Add to circles Show details Ads - Why these ads? 2012 Dodge® Avenger Learn About Models, Colors & More. Locate a Dealer in Your Area Now! www.dodgecurrentoffers.com How To Publish A Book Free How To Guide For First Time Author in Publishing a Book. www.Xlibris.com/HowToPublish Charitable Trust What's In Jim's Charitable Trust Portfolio? Sign Up Today To See. www.thestreet.com/charitabletrust VistaPrint- Official Site Save on Business Cards, Postcards, Brochures, Magnets and Letterhead! www.VistaPrint.com

OSCON 2013

priv.ly/pages/download



Extension Level: Decryption

A screenshot of a web browser window displaying an email message from "public-webcrypto@w3.org". The message subject is "HTML Document". The body of the email contains several nested "Privly.js" and "HTML iframe" components, which are highlighted with white boxes. A large blue rectangular area covers the bottom portion of the message body, containing the text "Protected content". The browser interface includes a sidebar with various links like "Compose", "Inbox", "Starred", etc., and a right sidebar with ads for "Business Cards \$8.50", "People (11)", and "Davenport, James L.". The bottom left corner shows "OSCON 2013" and the URL "priv.ly/pages/download".