Site and user security concerns for real time content serving

Chris Mejia, IAB
Sean Snider, Yahoo!
Prabhakar Goyal, Microsoft

Agenda

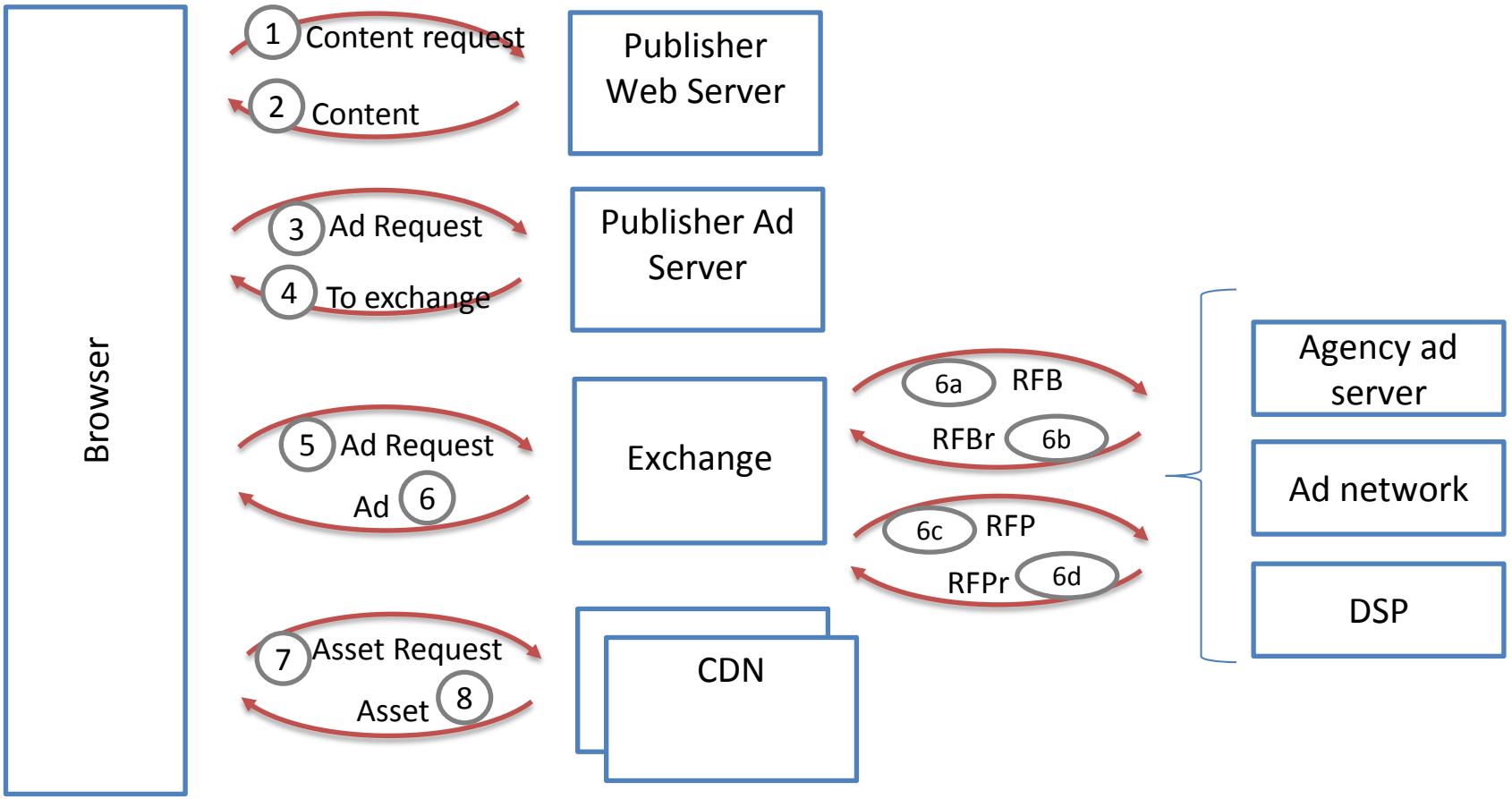
- Introduction: what is IAB?
- Use case
- SafeFrame Overview
- HTML5 Sandbox/CSP – Asks
- Next Steps and Q&A


OK, YES, WE DO WANT TO BID ON THAT 8:04AM AD SLOT IN THE SAN DIEGO MARKET.
THAT WAS LAST FEBRUARY.
YES
TOM FISH BURNE
ONLINE ADVERTISING IS EVOLVING. ARE YOU?
media LIFESTREET
CREATED BY marketoon studios
LIFESTREETMEDIA.COM

Introduction: what is IAB?

- Interactive Advertising Bureau
  - Membership-based trade organization, based in NYC
  - Founded in 1996
  - Members are online media publishers
  - Over 600 members in the US
  - 86% of digital advertising in US runs on IAB member sites
  - IAB develops digital advertising & publishing standards
- How do our interests align?
  - Ad content is served from 3rd parties in real time
  - Publishers are concerned with site and user security
  - Most Web content is paid for by advertising & sponsorship
  - We believe in the power of a “free” Web

Use case: Real time content serving



Publisher areas of concerns

- **Isolation**
  - Separation between publisher and 3rd party code
  - Prevent data leakage – page content, cookies, other data
  - Prevent JS and CSS collision
- **Functional / UI**
  - Allow rich interactions without providing full access
  - Restrict certain media types
  - Control autoplay
- **Ability to control other “attack surface areas”**
  - Prevent downloads
  - Plugin activation
  - Navigation
  - Messaging
  - ..

Covered by Iframe+SafeFrame

Topic of today’s discussion

SafeFrame Overview

What is SafeFrame?

- A cross domain IFRAME
- Standard definition of APIs between the top level browsing context and the content inside the IFRAME
  - Said IFRAME MUST be a direct child of the top, it cannot be nested.
- API establishes functionality for ‘heavy interactions’ with the top level browsing context:
  - Expand/Resize the Frame
  - Draw additional elements
  - Etc.
- Each piece of functionality can be allowed or disallowed by the top level browsing context
- API allows for some data sharing
  - Geometric information
  - Relevant DOM events

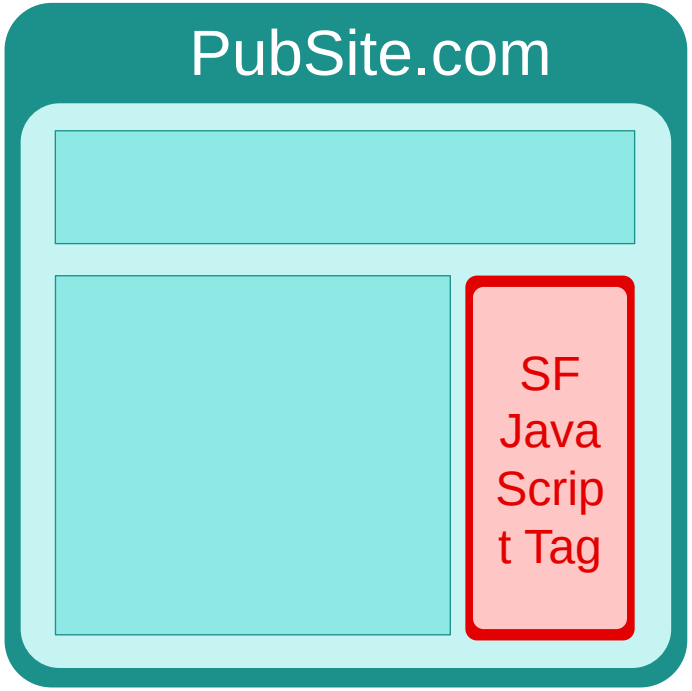
What is SafeFrame?

Content Domain

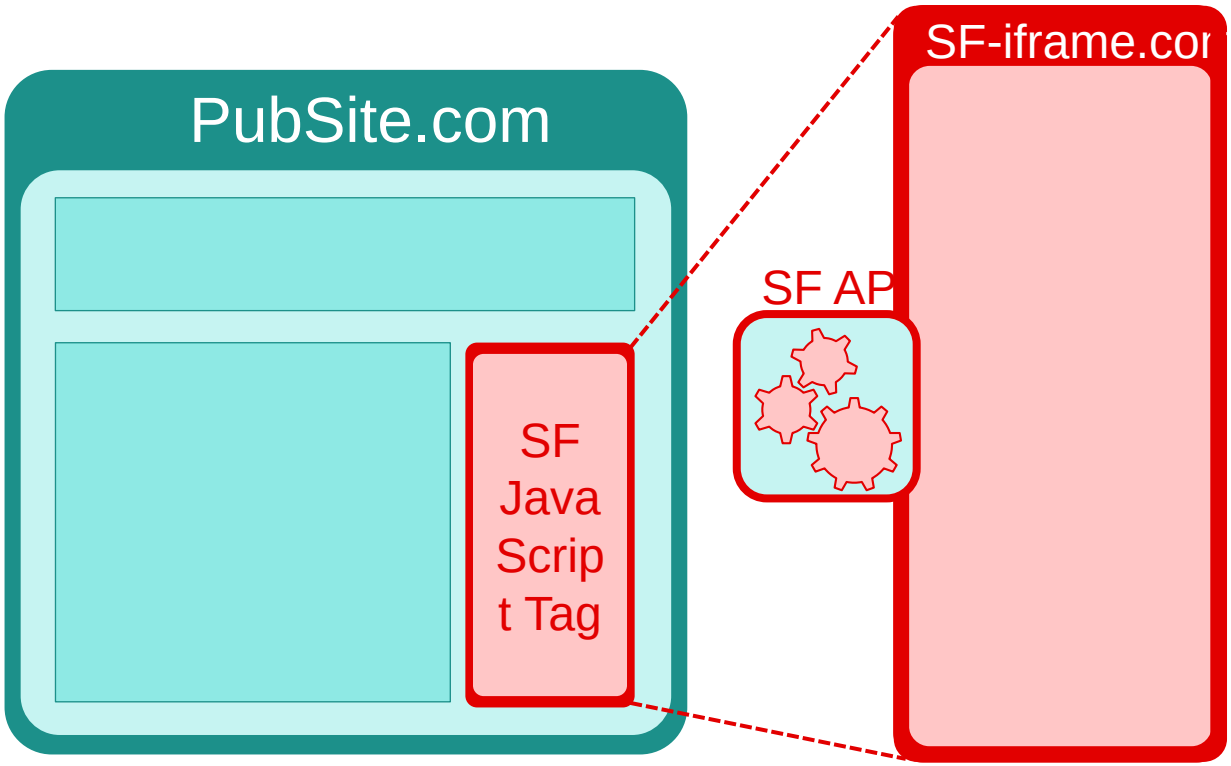
Cross Domain (“agnostic”) IFRAME for 3rd party content

- Creates one or more IFRAME(s) using a **Secondary agnostic origin**
  - But content is injected, rather than loaded from a given URL, mitigating the need for an HTTP request per IFRAME.
    - Typically document URI for the IFRAME is a **CDN** (content delivery network) URI
    - Document and it’s initial resources are cacheable
- 3rd party content is typically free form HTML and JavaScript

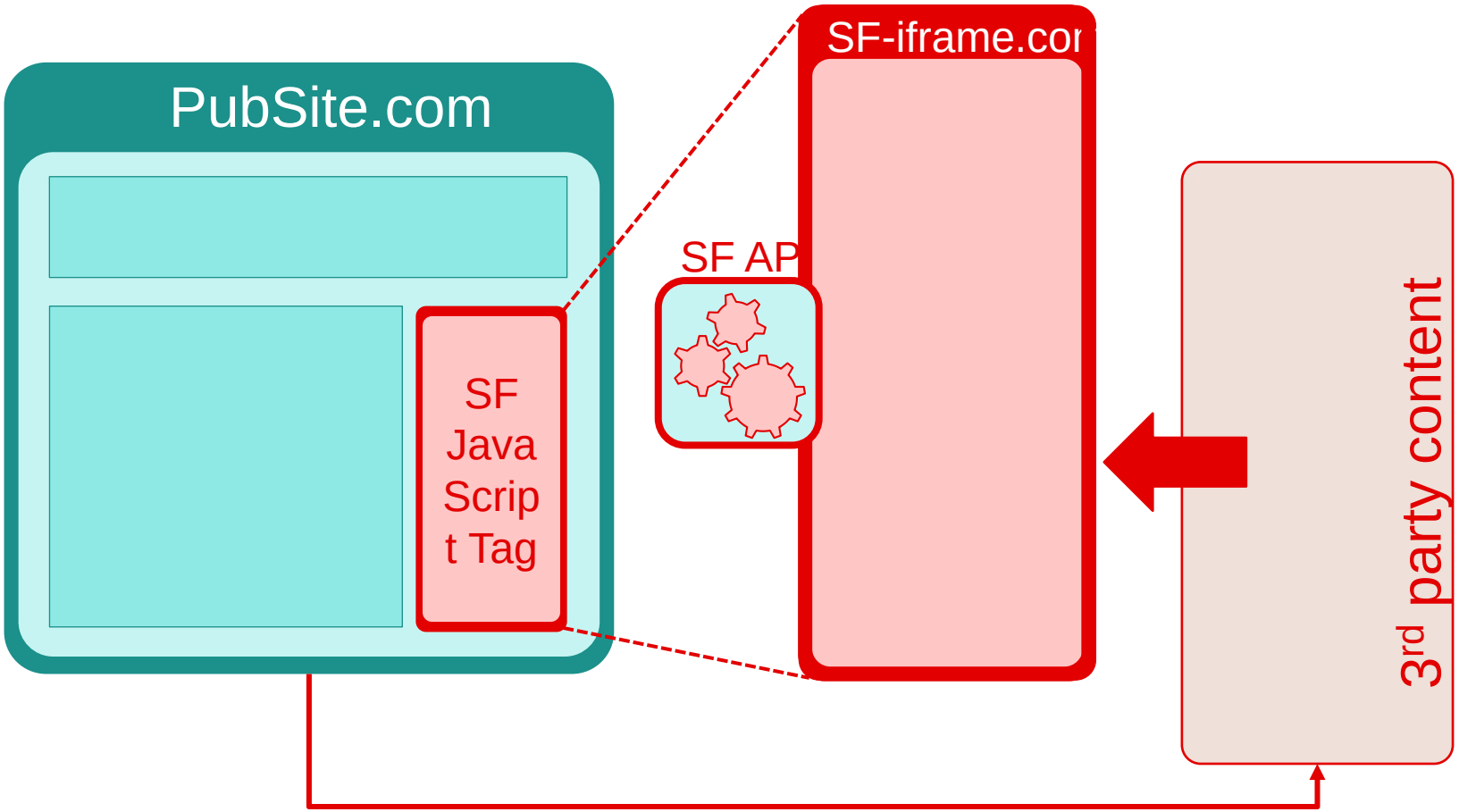
How it Works



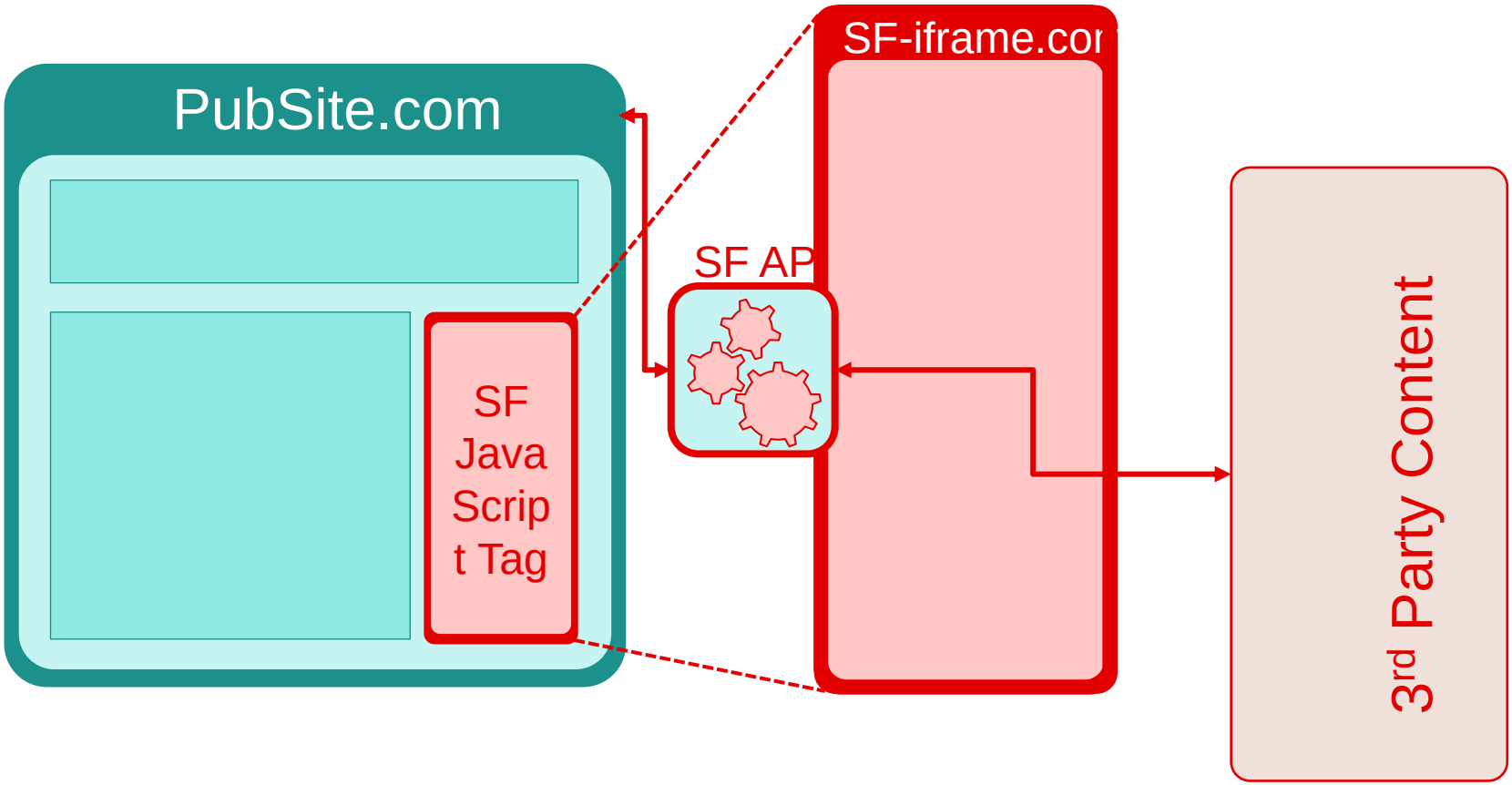
How it Works



How it Works


PubSite.com
SF
Java
Scrip
t Tag
SF-iframe.cor
SF AP
3rd party content

How it Works


PubSite.com
SF
Java
Scrip
t Tag
SF-iframe.cor
SF AP
3rd Party Content

Proposed Extensions

HTML5 Sandbox and CSP

- Limitations (as we see it)
  - Current sandbox attributes/directives are too coarse grain
  - There are additional areas of control publishers desire

- Ask
  - Enhancement to allow finer controls, i.e., ability to restrict
    - Individual plug-ins (Sandbox)
    - Allow / Deny access to a given IFRAME via JavaScript
    - Downloads
    - Alternate navigation

SafeFrame, Sandbox and CSP

Desired Feature	Covered by HTML5 Sandbox?	Included in by CSP 1.1?	Comments
allow-plugins	No	Yes	HTML 5 sandbox
plugin-types	No	Yes	Support for enabling/disabling specific plugin types
media-types	No	No	Restrict use of certain type of images, audio, video
require-user-initiation	No	No	Prevent autoplay of audio/video without user initiation Prevent navigation without user initiation

SafeFrame, Sandbox and CSP

Desired Feature	Covered by HTML5 Sandbox?	Included in by CSP 1.1?	Comments
file-download	No	No*	Rule to allow / disallow using navigation or an iframe to load content that triggers a download
restrict-script	No	No	Javascript in an IFRAME restricted to itself regardless of origin Allow storage/cookie read/write
force-self-nav-top/force-self-nav-new	No	No	Force navigation target to self or new
message-src	No	No	Rule allowing/disallowing x-origin messaging

Next Steps

- Define details around the proposed extensions (write the spec)
- Communicate the proposal to W3C via the established processes - bugzilla items and spec extension draft
- Discuss other areas of collaboration

Thank You!

- **Contacts**
  - Chris Mejia: chris.mejia@iab.net
  - Sean Snider: ssnider@yahoo-inc.com
  - Prabhakar Goyal: pgoyal@microsoft.com
- **References**
  - SafeFrame: http://www.iab.net/safeframe
  - Digital advertising ecosystem overview: https://www.youtube.com/watch?v=1C0n_9DOlwE