Web SAMP and Private Network Access

Mark Taylor (University of Bristol)

Applications WG
IVOA Interop
Sydney
(presented remotely)

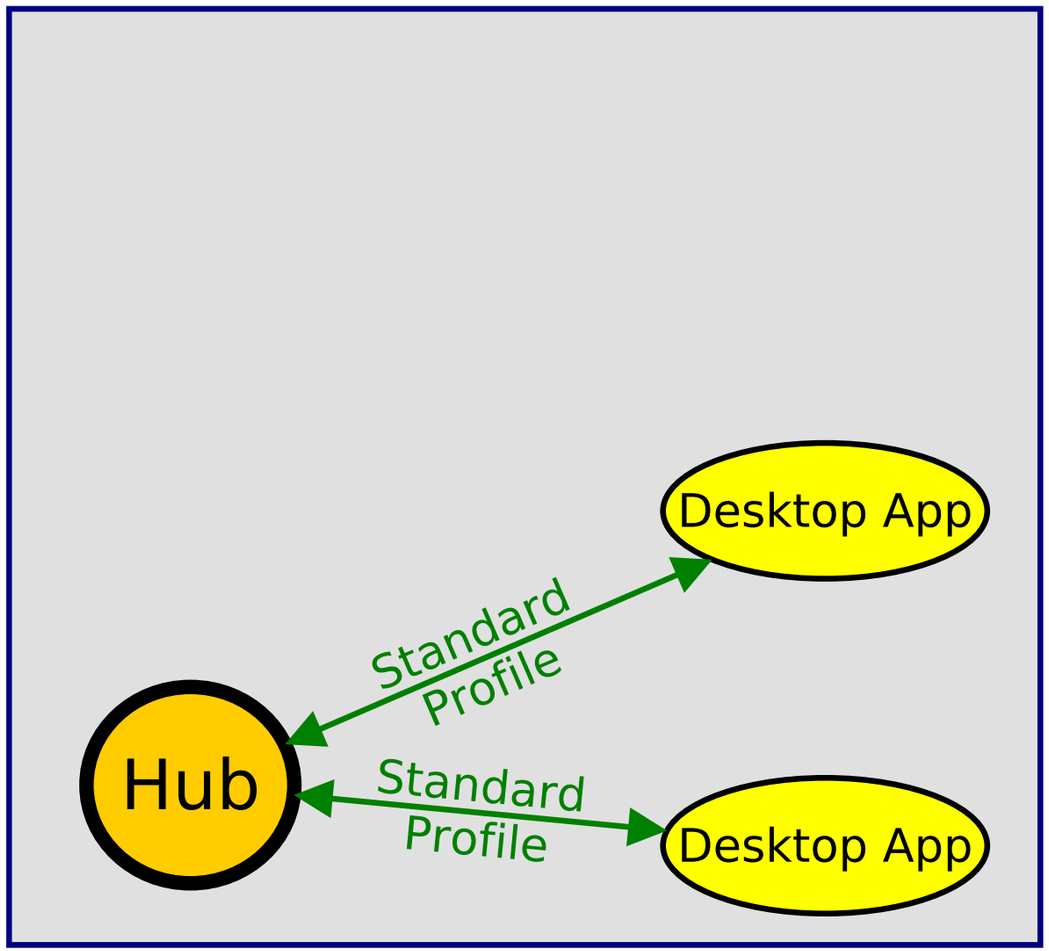
20 May 2024

$Id: samp-pna.tex,v 1.15 2024/05/17 12:33:23 mbt Exp $

Outline

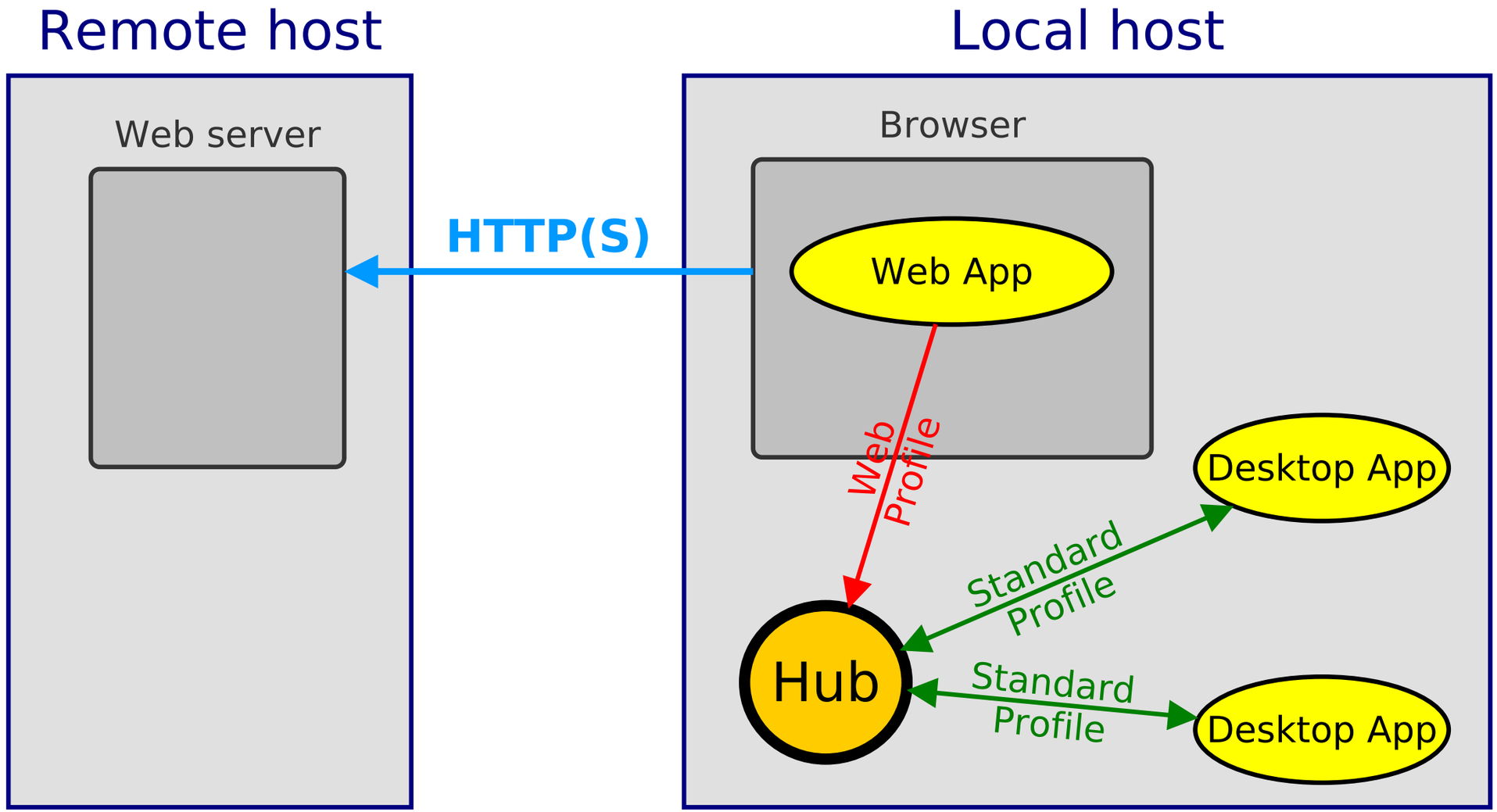
- (Web) SAMP refresher
- Technical details
  - Why is this complicated?
  - What details are changing?
- Summary/Recommendations

Simple Application Messaging Protocol



SAMP 1.11 (2009)

Simple Application Messaging Protocol



SAMP 1.3 (2012)

Issue

SAMP Web Profile: Web app talks to Hub over HTTP

- Well-known URL: `http://localhost:21012/`
- (there are good reasons this can't be an HTTPS localhost URL)

Browsers sometimes deliberately block these calls from web apps for security reasons (CSRF)

- Mixed Active Content: HTTPS web page talking to HTTP localhost server
  - ▷ HTTPS→HTTP considered insecure in general W3C Mixed Content TR (since around 2014)
  - ▷ But exception is made for local host W3C Secure Contexts draft TR (since around 2019)
    ⇒ Since around 2019, Web SAMP from HTTPS works for all browsers except Safari/WebKit (see WebKit bug 171934)
- Private Network Access: Public web page talking to localhost server
  - ▷ Specification is W3C Private Network Access draft report (since around 2023?)
    - This is a *Community Group Report*, not on the W3C standards track
    - Google initiative?
    - At least Chrome is moving to implement it; maybe other browsers in future
  - ▷ Implications:
    1. Localhost HTTP server (Hub) must explicitly allow requests from web pages (by CORS header manipulation)
       ⇒ Hubs need updating (JSAMP and Astropy done)
    2. Only HTTPS web pages will be permitted to talk to localhost HTTP server
       ⇒ In future SAMP from HTTP may not work for some/all browsers

    (Original discussion was on apps mailing list)

Hub Change

- Hub behaviour in CORS preflight request required by PNA:

  If incoming `OPTIONS` request contains header:

  ```
  Access-Control-Request-Private-Network:  true
  ```

  then insert header in response:

  ```
  Access-Control-Allow-Private-Network:  true
  ```

- Implemented in JSAMP v1.3.8 (PR#5), Astropy 6.1.0rc1 (PR#16193)
- Thanks to Bogdan Nicula (Royal Observatory Belgium) for alerting me

Timeline

		HTTP		HTTPS		
		FF+others	Chrome	FF+others	Chrome	Safari
2009	SAMP 1.11	—		—		
2012	SAMP 1.3: Web Profile	OK		?		
2014	W3C Mixed Content	OK		Blocked		
2016	W3C Mixed Content update	OK		Blocked	OK	Blocked
2020	Browser updates	OK		OK	OK	Blocked
2023?	Private Network Access	OK	Blocked	OK	Warning	Blocked
2024	Hub upgrades	OK	Blocked	OK	OK	Blocked
Future	Browser updates	Blocked?	Blocked	OK	OK	OK?

(Try your browser now! Start a Hub e.g. TOPCAT, then go here for HTTP and here for HTTPS.
See also WebSampHttps wiki page.)

Summary:

- In the past, Web SAMP mostly worked from HTTP pages but not HTTPS
- In the future, Web SAMP may mostly work from HTTPS pages but not HTTP

  — but make sure you're using a Hub with CORS updates for PNA (JSAMP $\geq$1.3.8, Astropy $\geq$6.1?)