Web SAMP from HTTPS: Impossible?

Mark Taylor (Bristol)

IVOA Interop
Sydney

31 October 2015

$Id: samp-https.tex,v 1.17 2015/10/31 04:07:38 mbt Exp $

Outline

- (Web) SAMP refresher
- HTTPS + SAMP: the problem
- Possible solutions
- Conclusions

SAMP Refresher

Simple Applications Messaging Protocol

- Allows clients to communicate with each other via a Hub
- Clients can be desktop applications or web applications:

  Desktop application: runs directly on OS with user privileges, can access filesystem
  Web application: runs in a browser (typically HTML+JavaScript), sandboxed

- To make it work, each client has to set up communications with the Hub (not each other)
- The set of rules a client uses for Hub discovery and communication is called the Profile
- Desktop applications use the Standard Profile, web applications use the Web Profile
- Both use XML-RPC over HTTP, but with some differences:

  Standard profile:

  - hub URL is read from lockfile `~/.samp`
  - HTTP communication uses normal user socket

  Web Profile:

  - hub is found at the well-known URL `http://localhost:21012/`
  - HTTP communication uses `XMLHttpRequest` with CORS

  (There are some other differences, but not relevant here)

→ SAMP from an HTTP page works (pretty) well

HTTPS

- HTTPS is HTTP Over TLS
  - RFC 2818, which defines HTTPS, says:

    > **2. HTTP Over TLS**
    > Conceptually, HTTP/TLS is very simple. Simply use HTTP over TLS precisely as you would use HTTP over TCP.

  - TLS = Transport Layer Security ≈ SSL = Secure Sockets Layer
  - Host authentication is mandatory in HTTPS (though it's optional in TLS)
- Some web pages are served over HTTPS
  - Encrypts communications
  - Assures the client that it's talking to the web server it thinks it is
  - Required to support secure authentication
    (e.g. serving restricted data to authenticated users)

HTTPS web page + HTTP SAMP

You might want an HTTPS web application to use SAMP:

- Browser retrieves web page from remote host using HTTPS `https://example.com/query.html`
- Web page JavaScript talks to Hub on localhost using HTTP `http://localhost:21012/`

→ what's the problem?

HTTPS web page + HTTP SAMP

You might want an HTTPS web application to use SAMP:

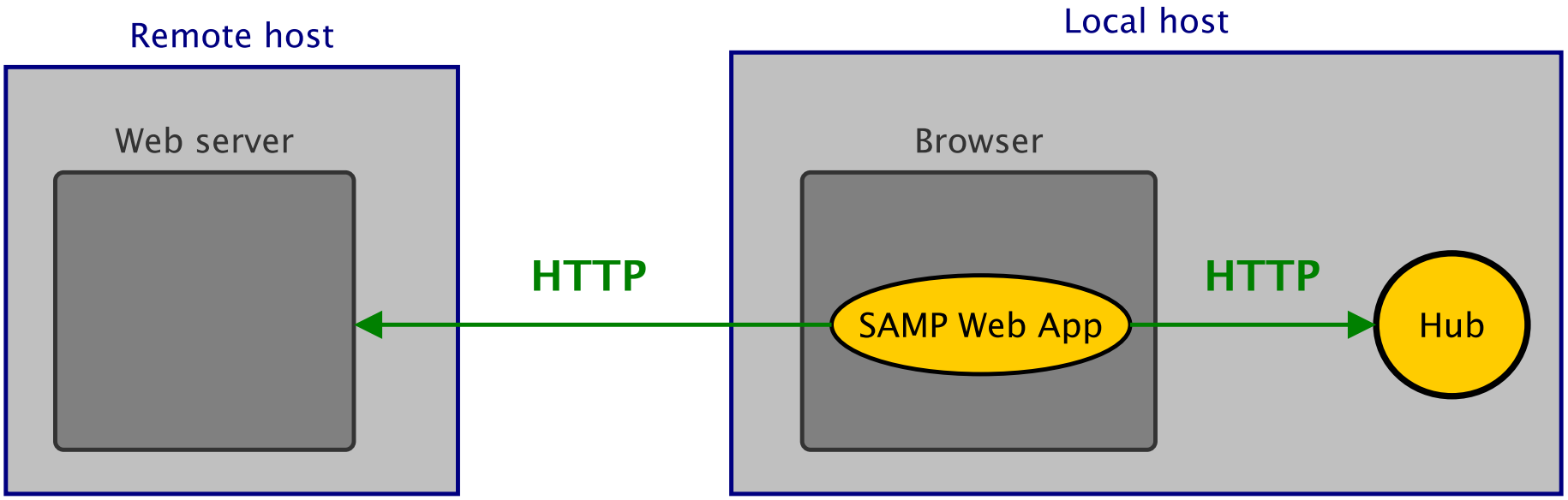
- Browser retrieves web page from remote host using HTTPS `https://example.com/query.html`
- Web page JavaScript talks to Hub on localhost using HTTP `http://localhost:21012/`

→ what's the problem?

Most browsers block "mixed active content"

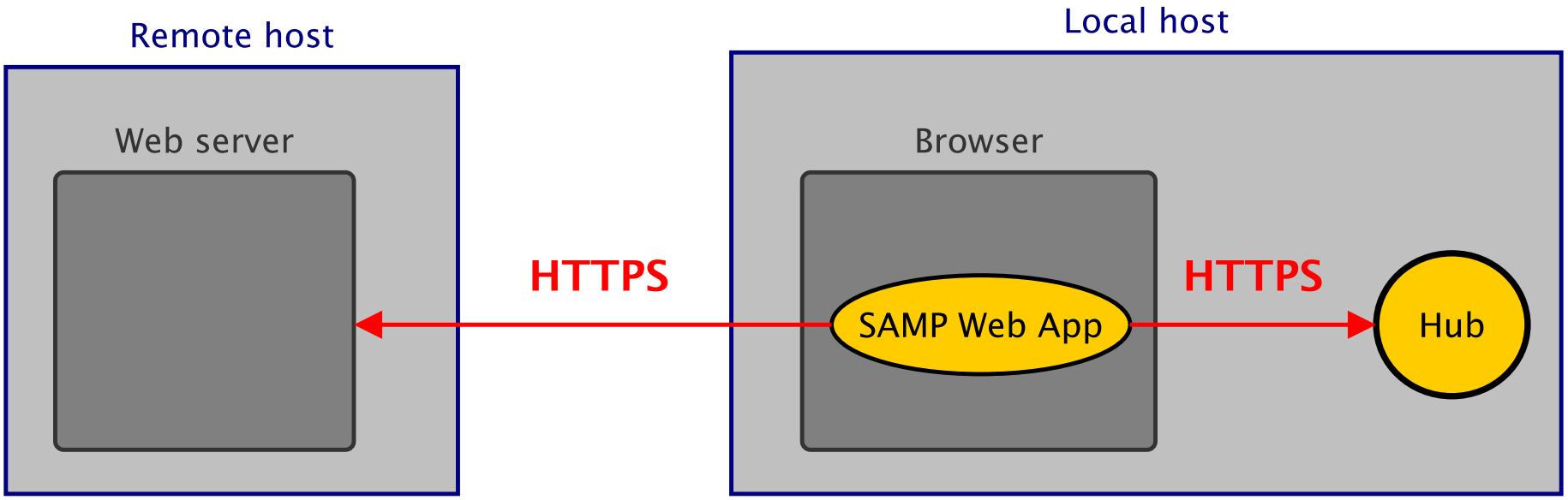
- That is (certain kinds of) HTTP communications within an HTTPS page
- If allowed, they would be vulneralble to "Man-In-The-Middle" attacks, which would compromise the integrity of the HTTPS communications

Unmixed/Mixed Active Content



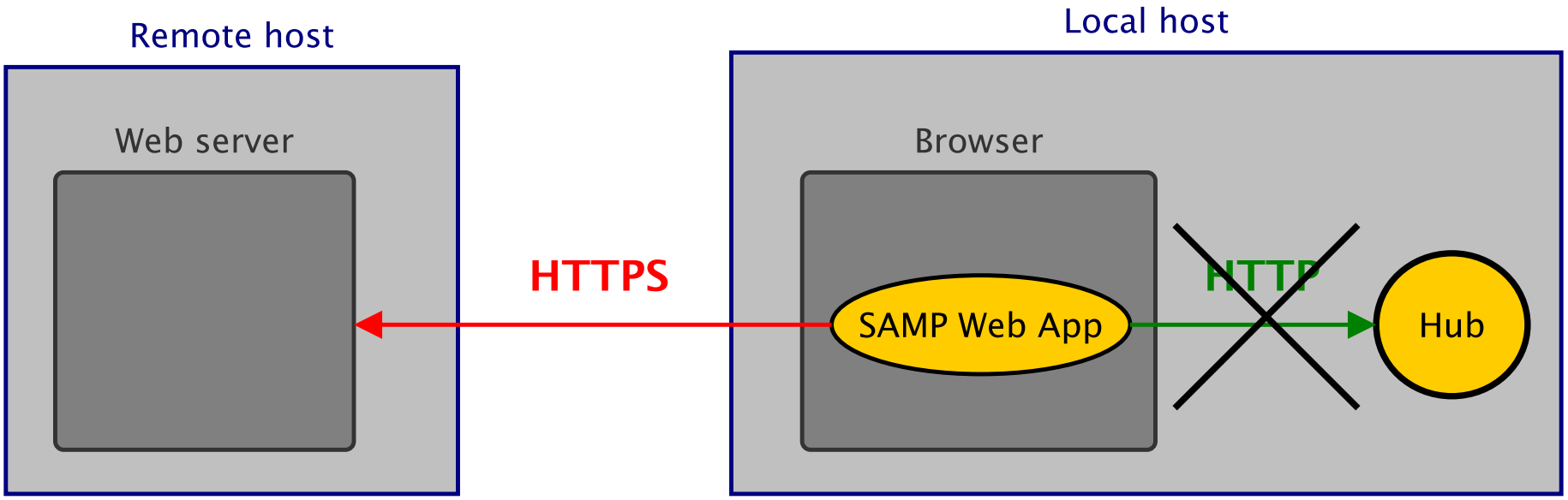
☑ OK

Unmixed/Mixed Active Content



☑ OK

Unmixed/Mixed Active Content



☒ Blocked by browsers

HTTPS web page + HTTPS SAMP

Mixed content disallowed ... so unmix it!

- Define a new HTTPS variant of the Web Profile:
  - Web Profile http://localhost:21012/ (existing)
  - Web-HTTPS Profile https://localhost:21013/ **(new)**
- Communications can be all HTTPS → browser is happy:
  - Browser retrieves web page from remote host `https://example.com/query.html`
  - Web page JavaScript talks to Hub on localhost `https://localhost:21013/`
- All we need to do is define a new Profile:
  - Small update to SAMP standard (define Web-HTTPS Profile like Web Profile)
  - Update web client libraries to use Web-HTTPS Profile if hosted from HTTPS
  - Update hub implementations to run an HTTPS server alongside HTTP one

→ Easy?

HTTPS on localhost

Web-HTTPS Profile has to run (Hub) HTTPS server on localhost

- This is not as easy as it sounds ☹
- HTTPS requires server TLS authentication
- The Hub HTTPS service needs to present a certificate
- The certificate needs to identify the service with its hostname
- The hostname for the Hub is the local host:
  - ▷ "`localhost`", *or*
  - ▷ a DNS record that resolves to 127.0.0.1, *or*
  - ▷ the network name of the current host *(would that work??)*
- The browser needs to trust the certificate or it will reject the HTTPS connection

Localhost Certificate

How do you get a trusted certificate for the local host?

- Force SAMP users to acquire trusted certificates for their own hosts?
  - ☹ Far too much difficulty and expense for end users
- Acquire a certificate for the `localhost` domain and bundle it with the SAMP hub?
  - ▷ There are a few ways you could try to do that:
    - Self-signed?
      ☹ Browsers won't trust it
    - Buy a certificate for domain "localhost" from a root CA?
      ☹ CAs are not permitted to issue certificates for localhost domain
    - Acquire a hostname that DNS-resolves to 127.0.0.1 and buy a cert for that?
      ☺ You can do this! e.g. `samp.localtest.me`
  - ☹ But this requires distributing public/private key pairs publicly
    - This certainly feels deeply wrong
    - Where CAs have spotted it in the past, they have revoked the certificate
- SAMP hub issues IVOA-certified certs automatically for current host at runtime?
  - ☹ Expensive or difficult for IVOA to issue trusted certs
  - ☺ letsencrypt.org ("Free, automated and open CA arriving Q4 2015") might help?
  - ☹ Still requires distributing some kind of private key with Hub

Localhost Certificate

How do you get a trusted certificate for the local host?

- Force SAMP users to acquire trusted certificates for their own hosts?
  - ☹ Far too much difficulty and expense for end users
- Acquire a certificate for the `localhost` domain and bundle it with the SAMP hub?
  - ▷ There are a few w could try to do that:
    - Self-signe
      - ☹ Browsers w
    - Buy a certificate fo lhost" from a root CA?
      - ☹ CAs are not permitte ificates for localhost domain
    - Acquire a hostname that DN 127.0.0.1 and buy a cert for that?
      - ☺ You can do this! e.g. `samp.lo`
  - ☹ But this requires distributing public/private key pairs publicly
    - This certainly feels deeply wrong
    - Where CAs have spotted it in the past, they have revoked the certificate
- SAMP hub issues IVOA-certified certs automatically for current host at runtime?
  - ☹ Expensive or difficult for IVOA to issue trusted certs
  - ☺ letsencrypt.org ("Free, automated and open CA arriving Q4 2015") might help?
  - ☹ Still requires distributing some kind of private key with Hub

DOOMED?

Other Options?

Remote-HTTPS→Local-HTTP mixed active content:

- This communication model is not unique to Web SAMP
  - Other people want to do it for similar reasons to us (web app↔desktop app communications)
- Are there workarounds?
  - Browser-specific configuration: there are sometimes options for users to unblock it
  - There might be some more or less wacky/hacky content-based possibilities, but I haven't seen anybody else using them in anything like a robust way
- Is it really harmful?
  - Security reasoning seems different than Remote-HTTPS→Remote-HTTP case
  - ... but I'm not smart enough to know whether it's really safe
  - My guess:

    either it is harmless, and browsers will learn to permit it in the future

    or it really is dangerous, in which case we probably(?) shouldn't even try to work round it in SAMP

Further reading for enthusiasts:

`http://developer.mozilla.org/en-US/docs/Security/MixedContent`
`http://stackoverflow.com/questions/6793174`
`http://readme.localtest.me/`
`http://github.com/Daplie/localhost.daplie.com-server`
`http://letsencrypt.org/`

Conclusions

As far as I can see:

- Web SAMP from an HTTPS page can't be made to work out of the box

  ... at least not without a a lot of work *and* questionable practice

- If we wait and see, the problem might just go away
  - ▷ Browsers may evolve to permit remote-HTTPS⟶local-HTTP mixed active content
  - ▷ ... or they might not
  - ▷ ... and it probably won't be very soon

- In the mean time, web apps wanting to do Web SAMP (still) have to:

  either migrate to HTTP
  or not use SAMP (e.g. save file to disk & load into desktop application?)
  or advise users how to workaround (e.g. unblock mixed active content per-browser)
  or *(half-baked)* open new HTTP page with SAMP link from HTTPS page??

Have I missed something?