Edge conf session writeup

Session:	*Security*
Moderated by:	*Dan Appelquist, W3C TAG Co-Chair*
Notes by:	*George Crawford, Financial Times*
Slack channel:	*#panel-security*

Moderator

Dan Appelquist, W3C TAG Co-Chair

Panel

Yan Zhu, Yahoo!, **Patrick Hamann**, Financial Times, **Mike West**, Google, **Virginie Galindo**, Gemalto / W3C WebSec IG, **J. Alex Halderman**, Uni. of Michigan / Let's Encrypt

Opening talk

Yan Zhu, Yahoo!

- We need to make security easy by default
- Two main problems:
    - XSS (code injection)
        - Tweetdeck emoji script injection hack
        - Still an issue in 2015
        - How do we fix?
            - CSP: only allow resources of type X from resource Y
                - HTTP header limiting usage, throws an error in the browser
                - http://csptester.io
    - MITM
        - HTTPS everywhere
            - www.google.com/ads still presents sign-in button on an http page
                - SSL is expensive and tedious
                - Solution: https://letsencrypt.org/
                    - A new CA giving free certificates
                    - Server package to automate validation of domain, cert renewal, SSL configuration: https://github.com/letsencrypt/acme-spec

Discussion

Tom Parker / Yoav Weiss: Third party content such as adverts can lead to mixed content and therefore become one of the main blockers in the move to HTTPS. Do we need changes from third parties (such as the ad networks) or is this a browser problem?

- Patrick
  - don't think moving to TLS is an issue (esp. with letsencrypt)
  - not just a problem with adverts
  - need to tackle root cause
  - 30% of adverts are from doubleclick - Google has the power to prevent serving non-secure assets
  - Need to work with IAB to create new rules and adhere to them
  - FT has created guidelines for the ad-ops team
- Mike
  - People need to understand that moving to TLS is in a company's financial interest
  - Less technical, more about convincing people
  - Doubleclick: allows https for all adverts
- Yan
  - why not use the 'stick' and force advertisers to use HTTPS?
- Mike
  - HTTP2 and TLS has great attraction
- **Jonathan Fielding:**
  - possible to have a special kind of iframe?
- Mike
  - what should the properties be?
- **Paul Downey, GDS**
  - certs are great, but how do we trust the infrastructure they're on?
- Alex:
  - TLS & PKI help reduce the amount of trust we need to place in DNS
  - main problem is too many trusted CAs

Patrick Hamann & Ernesto Jimenez: Mozilla recently announced that they are planning to deprecate insecure-HTTP, which includes denying new features from sites that are served over HTTP connections. Is this a mistake?

- Mike:
  - Google moving this way too
  - Changing the way we display security in the UI - showing insecure rather than secure
  - Withholding new features from HTTP
  - 'carrots' are hard to find in this area
  - Features are powerful:
    - GeoIP - needs to be granted to the origin, not any MITM

- Patrick:
  - it's a UI/UX trust issue
  - vendors need to improve the way they present this - permissions API is also problematic
- Mike
  - we start this by ensuring the origin is correct
- **Yoav Weiss, Akamai**
  - if you eliminate new features from HTTP, you're hampering developers and adoption. There are no benefits: you're applying pressure on the wrong people. Developers aren't lazy. Should apply on 3rd-parties - reduce cookie persistency on HTTP?
- Yan
  - setting up HTTPS is too hard
- Mike
  - removing everything? CSS?
  - GeoIP is totally legitimate to remove
  - we have the same goal, so target the problematic features first rather than block a new CSS feature
- Virginie:
  - need to keep up the movement: infrastructure, browser vendor strategy, then educate the devs and users
  - we need a plan
  - collect feedback, educate. W3C can help with a consistent consortium plan
- Alex
  - we need pressure from a larger set of actors
  - remove pain points like ads
  - how are we still using uncrypted transport in 2015? Like posting root passwords over telnet a while ago
- **Remy Sharp, Left Logic**
  - Security is good, no doubt. Barrier for entry to new devs is so high. Many use FTP. Do these new barriers mean driving devs away from new features?
- Mike
  - Deploying a server should just include SSL. Letsencrypt, https://sslmate.com/

Andrew Betts: Is letsencrypt essentially just making it possible for people to use self-signed certs? What differentiates a letsencrypt cert from self-signed? And is "a letsencrypt" for EV certs a feasible concept? How would that work?

- Alex
  - not self-signed. Just like a real CA, audited, but cheap
  - Race to the bottom - CA used to request legal documents to confirm validity. With domain validation, it's just done by email with a nonce.
  - With LE, we'll be no weaker than traditional CAs, but will pave the way for stronger methods in the future.
  - Problem with PKI is that attacker can pick a weak CA
- Mike
  - domain verification means ???
  - different to self-signed cert. I could create one for google.com. Verifying I have

control over the domain is a critical step
- **Guido Bouman, Q42**
  - not the same as self-signed, which is great. When every site has cert, you might get phishing as every site seems more safe. Might be a form of phishing - automating the process might open route to more attacks
- Alex
  - you can do that today
- Dan
  - but with a secure SSL lock icon?
- Mike
  - we should drop the lock, as it doesn't indicate much
- Dan
  - how do you inform the users?
- Mike
  - users don't care!

Jonathan Fielding: Some CDNs make implementing SSL trivial by securing the 'last mile' but doing regular HTTP to origin. Is this OK? Should users be informed, and if so, how?

- Yan
  - SSL doesn't mean it's encrypted end-to-end
- Mike
  - Cloudflare gives a free cert, connects to backend
  - can work with a self-signed on endpoint
  - last-mile is many fewer hops, and less of a concern
- Patrick
  - what about open proxies, government proxies, telco interference?
- **Guy Podjarny, Akamai**
  - hot on last-mile security
  - what about microservices inter-communication?
  - better off not signalling security to user than signalling whilst unsure
- Mike
  - agree completely. Problem is not getting the encryption working, it's user expectations
- Alex
  - i would start to worry about liability when implying security. May see litigation to push insecure processes
- **Jonathan Fielding**
  - Cloudflare great, but need to educate devs about last mile. How can we do that?
- Patrick
  - "It's a performance problem". No, it's not. Netflix say it's more of a money problem.
- Dan
  - https://istlsfastyet.com/

Dan Appelquist: How can we surface security capabilities such as encryption through javascript to the (front end) web application developer - a la the “extensible web”?

- Virginie
  - HTTPS is one way
  - having the capability for the dev to use an encryption API will help. Build their own security model
- Alex
  - everyone can come up with good security models, but you only think of the issues you are aware of
  - web crypto is a good set of products, but it’s not the same as TLS
  - Netflix simulated SSL over HTTP, but it didn’t work
- Virginie
  - use the tools to protect your own credentials, not to write your own encryption
- **Katy Moe, Kahoot!**
  - Don’t use pure JS Math.rand, use web crypto
- **Robert Knight, Mendeley**
  - what about providing the same APIs and algorithms across browsers?
- Virginie
  - not yet standardised, need to work on profiles and tests
- Dan
  - how about an informal breakout on webcrypto?

Andrew Betts: Often HTTPS is used to 'punch through' middleboxes that might otherwise interfere with data that they don't understand or don't like. But some of these things are trying to be helpful - can the competing agendas be reconciled?

- Alex
  - things middleboxes can do: censor, inject ads and scripts
  - lots of business operate them
  - that model doesn’t survive the transition to HTTPS - need trust between user/client and source, should be able to deauthorise interference
- Dan
  - companies monitoring employeed
- Mike
  - fine, but use a self-signed cert on the user’s machine
  - don’t intercept in the middle
- **Mike MacCana, CertSimple**
  - Chrome Android doesn’t show cert
- Dan
  - good for web advocacy - user sees security in the UI
- Mike
  - we show a lock because we expect sites to be insecure. Instead, expose insecure
- Mike MacCana, CertSimple
  - should we expose the extent of the validation?

- Mike
    - does this help users? perhaps only worries them
    - value of TLS is encrypted connection. Users don't understand the ownership of the chain
- **Guido Bouman, Q42**
    - low-bandwidth in South Africa? Providers use lots of mechanisms to help reduce bandwidth consumption
- Dan
    - one of the key cases for middleboxes
- Mike
    - user can explicitly opt-in (e.g. Opera Mobile) to a middleman viewing all your data. But what about NSA?
- Patrick
    - yes.

Yoav Weiss: TLS is great, and more secure than HTTP, but not perfect. Are there plans to improve or replace it in the future?

- Alex
    - TLS 1.3 protocol in the works: https://tools.ietf.org/html/draft-ietf-tls-rfc5246-bis-00
    - lots of attacks recently
    - need to get to the point where the protocol is streamlined and free of technical debt
- **Jake Archibald, Google**
    - HSTS - should there be a TLD which is always secure? Can it be secured on the DNS level?
- Mike
    - we can add secure TLDs, why not?