No Half Measures: Advertisers Must (Properly) Adopt HTTPS

Greg Norcie
Staff Technologist
Center for Democracy & Technology

Full white paper at https://cdt.org/files/2015/05/ad-https-w3c.pdf

(Or search “No Half Measures HTTPS” on DuckDuckGo)

What is HTTPS?

- HTTPS = HTTP over TLS (originally SSL – but don't use that)
- Confidentiality: no eavesdropping in transit
- Integrity: data not modified in transit
- Authentication: Am I actually talking to my credit union?

HTTPS Protects Us From Mass Surveillance

The IETF has stated that
"*Pervasive monitoring is an attack*" (RFC7258)

W3C TAG states HTTPS is now a
"*baseline requirement*" to prevent monitoring

Even federal CIO ordered all federal websites must uses HTTPS and HSTS by 12/31/16

[1] https://tools.ietf.org/html/rfc7258
[2] Securing The Web TAG Finding http://www.w3.org/2001/tag/doc/web-https
[3] OMB Memo M-5-13
https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

Mixed Content is Harmful

Mixed Content - mixture of HTTP and HTTPS elements on same page

Research by Bonneau showed that web analytic & advertising were a major source of mixed content [1]

Mixed content can be sniffed and/or injected

No confidentiality, no data integrity

Interactive Advertising Bureau (IAB) agreed, noting ~20% of advertisers do not currently support, and called on advertisers to adopt HTTPS [2]

[1] http://www.jbonneau.com/doc/KB15-NDSS-hsts_pinning_survey.pdf
[2] http://www.iab.net/iablog/2015/03/adopting-encryption-the-need-for-https.html

A Real Example of Improperly Configured HTTPS

- New South Wales, Australia had an electronic voting system
- Site itself used properly configured HTTPS
- 3rd party Javascript used an outdated version of TLS vulnerable to the FREAK attack
- Theoretically attacker could have modified data in transit (in practice no evidence of attack)

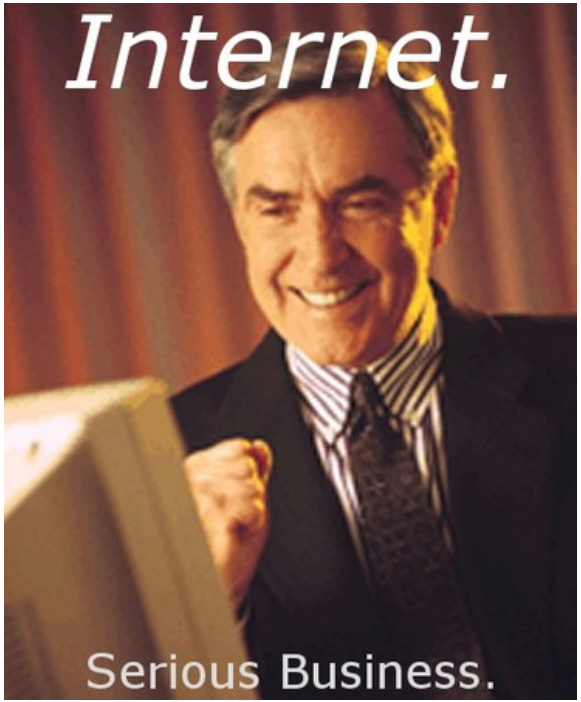
[1] https://freedom-to-tinker.com/blog/teaguehalderman/ivote-vulnerability/

HTTPS Best Practices Must Be Used

- Use HTTP Strict Transport Security (HSTS) when possible
  - When enabled with HSTS a site will refuse any connections over plain HTTP
- Support certificate pinning when possible
  - Cert pinning allows you to specify (“ping) which certificate authorities have authority to issue certs
- Support the latest TLS version possible
  - NEVER use SSL
  - attacks exist on several versions of TLS as well

Economic and Regulatory Effects of Failure to Adopt

- Customers will increasingly gravitate to ad providers who support HTTPS
- Data breaches due to failure to implement HTTPS may be seen as an unfair business practice under FTC's section 5 authority



Conclusions

1. Encrypt all the things.
2. Encrypt the things well.
3. If you don’t encrypt things well, people will spy on you
4. If you don’t encrypt things well, people may fine you.
5. If you don’t encrypt things well, people will find an ad provider who does.