Encrypting the Web

Robert Boedigheimer
@boedie

About Me

- Microsoft MVP – Developer Technologies
- ASPInsiders
- Pluralsight Author
- Progress Developer Expert – Fiddler
- 3rd Degree Black Belt, Tae Kwon Do

- @boedie
- robert@boedie.dev
- www.boedie.dev

Fiddler

- Tracing tool built specifically for HTTP(S)
- Eric Lawrence (@ericlaw)
- Acquired by Telerik in 2012

- https://www.telerik.com/fiddler (free)

- Can configure to decrypt HTTPS

What is HTTPS?

- A **secure** communication protocol
- HTTP over an encrypted channel (TLS or SSL)

- *Browsers indicate if HTTPS is in use or not*

TLS and SSL

- **TLS** - Transport Layer Security
  - *v1.3 – 2018*
  - **v1.2** - 2008
  - ~~v1.1 - 2006~~
  - ~~v1.0 - 1999~~
- ~~SSL - Secure Sockets Layer~~
  - *v3.0 -1996*
  - *v2.0 - 1995*
  - *v1.0 – never released*

Why HTTPS?

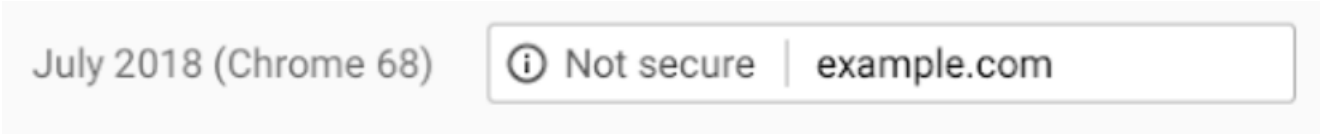
- **Confidentiality**
- Integrity

- Authentication (Server, optional client)

- Trust
- *Browser vendors will eventually make you…*

Chrome 68+

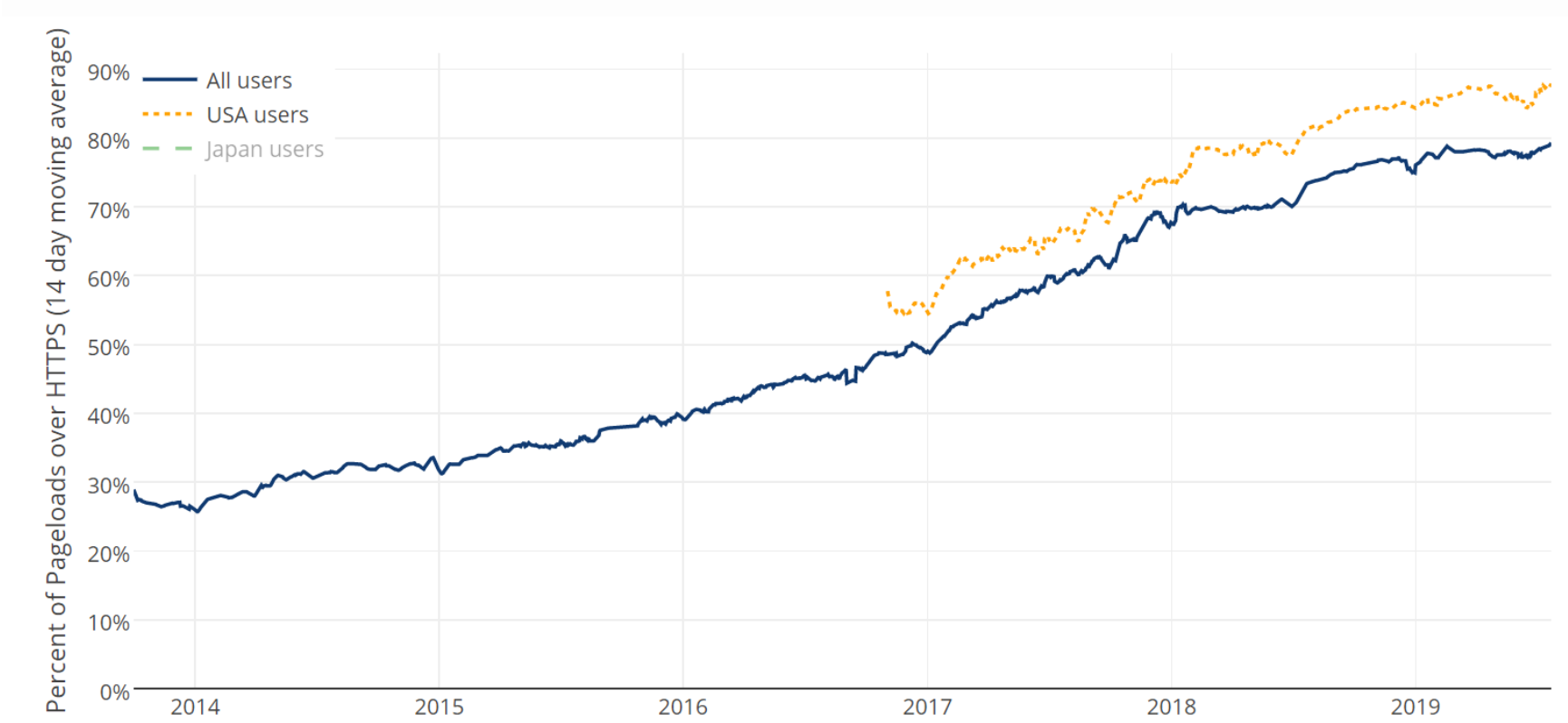
- **ALL** sites using HTTP marked as “Not Secure”



HTTPS By Default (% sites)

- https://trends.builtwith.com/ssl/SSL-by-Default
  - 90% of Top 10k sites
  - 85% of Top 100k sites
  - 64% of Top 1m sites

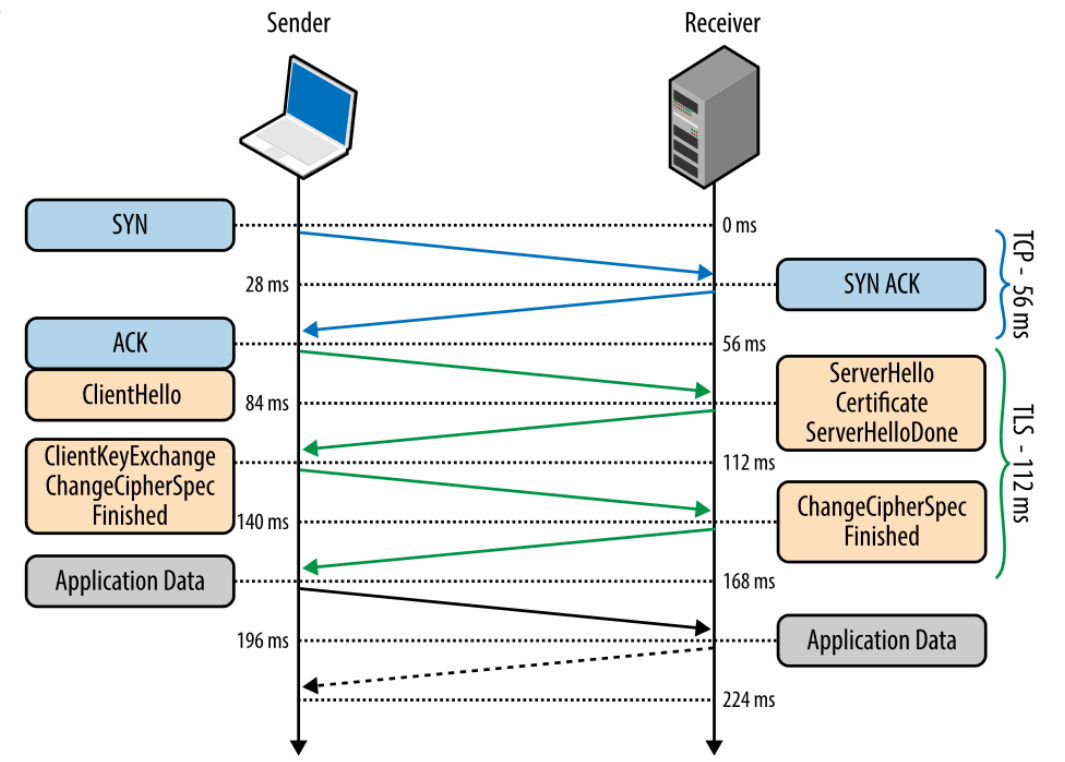
HTTPS (% Firefox pages loaded)



https://letsencrypt.org/stats/#percent-pageloads

How does HTTPS work?

- *TCP handshake*
- TLS handshake
  - TLS version(s)
  - Cipher suite(s)
  - Server certificate
  - Symmetric key



tinyurl.com/ybq33nb2

Certificates (Server)

- Types
  - **Domain Validation** (DV)/Organization Validation (OV)

  - Extended Validation (EV)
    - Indicator dropped in Chrome 77, Firefox 70

- Certificate Authority (CA)
  - letsencrypt.org
- Self-signed
- www.certificate-transparency.org/

What Is **Not** Encrypted?

- IP address/port of web server
- Hostname

- Duration
- Amount of data transmitted

Problems

- Social Counts
- Mixed content
  - Passive
  - Active

- Fixes
  - Protocol-less (protocol-relative) URLs
  - Content Security Policy
    - upgrade-insecure-requests
    - block-all-mixed-content

Moving to All HTTPS

- Configure to support HTTPS

- 302 redirect
- 301 redirect
- HTTP Strict Transport Security (HSTS)
  - *https://hstspreload.org/*

Features that Require HTTPS

- HTTP/2
- JavaScript
  - Service Workers
- Geolocation (Chrome)
- Referer request header
- Brotli Compression

- Major browsers will only support new features for HTTPS

Concerns

- Performance
  - istlsfastyet.com
- Cost
  - letsencrypt.org
- Troubleshooting
  - Fiddler/WireShark

Miscellaneous

- Fiddler decrypt HTTPS
- WireShark decrypt HTTPS (tinyurl.com/kbhzzs6)
- Browser connection information

Tools

- badssl.com
- www.ssllabs.com/ssltest
  - Client
  - Server
- *securityheaders.io*

Resources

- High Performance Browser Networking (hpbn.co)
- doesmysiteneedhttps.com
- **tinyurl.com/y9gzlptt** (static sites need HTTPS)
- whynohttps.com

Questions

- @boedie
- robert@boedie.dev
- www.boedie.dev

- Slides and code - https://tinyurl.com/y6o5f42y