HTTPS in 2018

Fundamentals of securing your website

Presented by Peter Hebert

Vancouver WordPress Meetup

August 8, 2018

About Me

- Full-stack WordPress and Drupal developer
- 20+ years web development experience

Owner/Developer:

Rex Rana Design and Development Ltd.

Developer:

CoLab Cooperative

Overview

- Definitions - HTTP vs HTTPS
- Why HTTPS?
- How HTTPS works
- How to serve websites securely over HTTPS

Definitions

HTTP

- Hypertext Transport Protocol
- Original protocol for web page delivery
- Plain text transport between client/server
- Unauthenticated
- Insecure

HTTPS

- S for Secure
- HTTP over TLS (Transport Layer Security)
- Encrypted communication between client/server
- Trust provided through certificate validation process

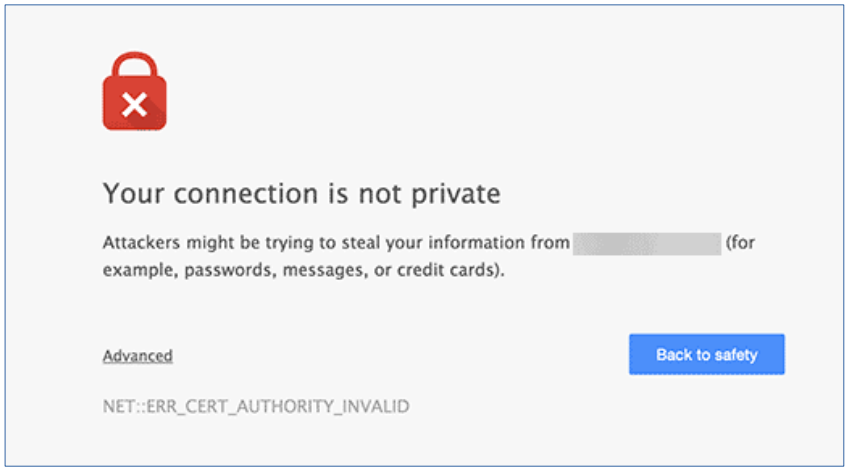
Why HTTPS?

HTTPS is rapidly becoming a requirement of running a website

- Ranking factor in search results (Google, Bing, etc)
- SEO penalty for using plain HTTP
- Browsers now warn users that a site is “not secure” if using plain HTTP
- Privacy concerns
- Complying with legislation (GDPR)

Why HTTPS?

You want to avoid these



Why HTTPS?

Encryption

Identification / Trust

Encryption

Encodes data so third parties cannot decipher the contents

- Public/private key pairs
- Protects personally identifiable and financial information
- Essential for e-commerce, and membership sites

SSL/TLS Encryption process

Before encrypted communication begins, a “Handshake” occurs between client/server to determine encryption method

1) Client Hello
2) Server Hello
3) Authentication and Pre-Master Secret
4) Decryption and Master Secret
5) Encrypted communication using Session Key

Identification / Trust

Makes sure the server you are communicating with is the legitimate server you made the request to

- Servers are identified by certificates signed by trusted authorities
- Validation process done by Certificate Authorities to verify that the person or organization requesting certificates are legit
- All data is encrypted signed by trusted certificate

How SSL/TLS works

- Organization asks Certificate Authority (CA) for a certificate
- After verification, CA issues and signs certificate
- Signed Certificate installed on the web server
- Web browsers have Root certificates – certificates of trusted CAs
- Browser only trusts websites whose certificates can be verified against a root certificate
- Once server is verified as trusted, then green lock icon appears in address bar of browser

Certificate validation

3 levels of validation provided by CA - (lowest to highest level of trust):

- **Domain validation (DV)**
  - only proves that you own the domain
  - Automated verification
- **Organization Validation (OV)**
  - verifies organization details – name, location, contact info, etc
  - Human verified
- **Extended validation (EV)**
  - extensive vetting by CA
  - Verifies legal entity of organization, physical location
  - Extensive investigation to verify against public records
  - Browser shows green address bar

Let’s Encrypt

- A free, automated, and open certificate authority
- Provides Domain Validation (DV) certificates
- Easy setup
- Automated process of validation, certificate issuance, renewal and revocation, web server configuration
- Many web hosts now integrate Let’s Encrypt into their user control panels, for 1-click certificate installation

Resources

- Article:
  - Understand SSL/TLS Handshake processs in 3 minutes
- Videos:
  - How SSL works
  - SSL TLS HTTPS process explained in 7 minutes
- Let’s Encrypt:
  - Getting Started
  - How it Works