HTTPS
HTTPS Everywhere

Stew Edelman

Using the Internet Securely

➢ Brief History of TLS/SSL and HTTPS

➢ Why HTTP is not sufficiently secure
➢ The use of HTTPS rather than HTTP
➢ The HTTPS Everywhere project from The Electronic Frontier Foundation
➢ Some of the best practices regarding using the internet securely

What is the Terminology ?

- HTTPS
  - HTTPS
    - Hypertext Transfer Protocol Secure
    - Secure means the same as saying HTTP over SSL
  - HTTPS SSL
    - Secure Socket Layer prevents eavesdropping, tampering, or message forgery over the Internet.
  - HTTPS SSL/ TLS (newest and most secure)
    - Transport Layer Security providing primarily privacy and ensuring data integrity

Brief History of HTTPS and TLS/SSL

- ➤ 1994 Netscape creates HTTPS

- ➤ 1995 Netscape creates SSL version 2.0 (SSL Version 1.0 is never made public)

- ➤ 1996 Netscape SSL version 3.0

- ➤ 1999 TLS 1.0

- ➤ 2006 TLS 1.1

- ➤ 2008 TLS 1.2

- ➤ TBD TLS 1.3

- ➤ Today HTTPS is referred to as only SSL/TLS or just as TLS

HTTPS

- ➢ HTTP over SSL, HTTP over TLS, HTTP Secure
- ➢ HTTPS is about securing the client/browser and the web/server

- ➢ HTTPS data is encrypted between your web client and the web site
- ➢ HTTPS makes sure the web site is who they say they are through certificate verification

HTTPS, VPN, or Both

- ➢ HTTPS uses encryption to establish secure communication in a client/server environment (web browser to web server)
- ➢ VPN uses encryption to provide secure communication tunnel between a device and a VPN server
  - ➢ Alan Baker's VPN presentation Nov. 2016
    - – https://sjpc.org/baker/presentations/vpn.pdf

- ➢ Both HTTPS and VPN should be used. This will secure the client/server transaction, also ensure the entire connected networks are secure

HTTPS Everywhere

- ➢ EFF Website home of HTTPS Everywhere
  - ➢ HTTPS Everywhere is an effort between EFF and TOR

    HTTPS Everywhere

    - ➢ (https://www.eff.org/https-everywhere)

    "HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. "

- ➢ If a web site offers both HTTP and HTTPS, HTTPS Everywhere will make the browser use HTTPS instead of HTTP.

Basic Security Best Practices

- ➢ Install HTTPS Everywhere plugin from eff.org
  - ➢ HTTPS offers strongest security for web today
  - ➢ HTTPS helps guarantee secure and private connection
- ➢ Apply software updates
  - ➢ OS, browser, anti-virus...helps protect from virus and malware
- ➢ Turn off autorun (when you plug-in USB stick)
- ➢ Clear web browser cache and cookies (I perform this task daily)
- ➢ EFF Surveillance and Self-Defense
  - – https://ssd.eff.org/en

HTTPS on Wikipedia

EFF HTTPS Everywhere

Encrypting the Web

HTTPS and your online security

Don't Get Pwned: A Guide to Safer Logins

Surveillance Self-Defence

US-CERT - United States Computer Emergency Readiness Team

Alan Baker's Virtual Private Networking - VPN Presentation