Why Do We Need HTTPS
Topics

- Background of HTTPS
- Discussion on SSL/TLS
- Major Implementations and Issues
- Digital Certificate
- Advanced Configurations
## Benefit of Using HTTPS

<table>
<thead>
<tr>
<th>Improve</th>
<th>Improve</th>
<th>Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>the network communication security</td>
<td>the ranking in Google</td>
<td>the branding</td>
</tr>
</tbody>
</table>
您即將前往詐騙網站

攻擊者可能會試圖透過 yahoo.digitaladvertising.com.hk 誘使你做一些危險行為，例如安裝軟體或提供個人資料 (包括密碼、電話號碼或信用卡資料)，瞭解詳情。

- 自動傳送部分系統資訊和網頁內容給 Google，協助偵測危險的應用程式和網站，遵守隱私權政策。

詳細資訊 返回安全性瀏覽
SSL & TLS

Secure Sockets Layer (SSL)
- a protocol for establishing an encrypted connection between a client and a server
- well-known version is SSL 3.0
- a legacy term

Transport Layer Security (TLS)
- improvement of SSL using stronger encryption algorithms
- recent version is TLS 1.3 for better performance and security
- secure sites are using TLS 1.2 or 1.1 at the moment
Applications of SSL/TLS

- Web (i.e. the HTTPS)
- Email
  - POP3 over SSL/TLS (i.e. port 995)
  - IMAP4 over SSL/TLS (i.e. port 993)
  - SMTP over SSL/TLS (i.e. port 465)
- Any applications that are encrypting the network traffic
  - antivirus software gets update from vendor’s server
  - mobile apps
  - syncing information between smartphone and manufacturer
SSL/TLS Implementations

- OpenSSL
- LibreSSL
- BoringSSL
- GnuTLS
Security of the SSL/TLS

• Protocols Vulnerabilities
  • BEAST
  • CRIME
  • Heartbleed
  • POODLE
  • BREACH
  • FREAK
  • Logjam
  • NOMORE
  • DROWN
  • Bar Mitzvah
  • SWEET32

• Operations Risk
  • Patch Management
  • Trustworthy of Digital Certificates
  • Protection of Keys
  • Configuration of the Protocols (Cipher Suite)
  • Configuration of Servers
    • version, setting, patches
## Cipher Suites

<table>
<thead>
<tr>
<th>Modern Compatibility</th>
<th>Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, Java 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intermediate Compatibility</td>
<td>Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7</td>
</tr>
<tr>
<td>Old:</td>
<td>Windows XP IE6, Java 6</td>
</tr>
</tbody>
</table>
Mozilla SSL Configuration Generator

- Apache
- Nginx
- Lighttpd
- HAPrxy
- AWS ELB

Server Version: 2.4.28
OpenSSL Version: 1.0.1e
HSTS Enabled: [on/off]

Oldest compatible clients: Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, and Java 8

Apache 2.4.28 | modern profile | OpenSSL 1.0.1e | link

```html
<VirtualHost *:443>
  ...
  SSLEngine on
  SSLCertificateFile  /path/to/signed_certificate_followed_by_intermediate_certs
  SSLCertificateKeyFile /path/to/private/key

  # Uncomment the following directive when using client certificate authentication
  #SSLCACertificateFile /path/to/ca_certs_for_client_authentication

  # modern configuration, tweak to your needs
  SSLProtocol  all -SSLv3 -TLSv1.1
  SSLTlsCipherOrder  on
  SSLCompression  off
  SSLSessionTickets  off

</VirtualHost>
```

https://mozilla.github.io/server-side-tls/ssl-config-generator/
Digital Certificate

is required to exchange information securely over the Internet using the Public Key Infrastructure (PKI).
How to Get a Certificate

1. Filling a Certificate Signing Request (CSR)

2. Submit to CA to validate our identity

3. CA send back the necessary file to configure the web server
Certificate Authorities

• Symantec, GoDaddy, GlobalSign, GeoTrust, RapidSSL, Thawte, DigiCert, Comodo, Hongkong Post, Let’s Encrypt ...

• Self-signed
# Distrust Symantec Certificates

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>Release Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>65</td>
<td>6 Mar 2018</td>
<td>Distrusts the certs issued before 1 Dec 2017</td>
</tr>
<tr>
<td></td>
<td>66</td>
<td>17 Apr 2018</td>
<td>Distrusts the certs issued before 1 Jun 2016</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>30 Aug 2018</td>
<td><strong>Distrusts all certs signed with Symantec hierarchy</strong></td>
</tr>
<tr>
<td>Firefox</td>
<td>60</td>
<td>9 May 2018</td>
<td>Distrusts the certs issued before 1 Jun 2016</td>
</tr>
<tr>
<td>Microsoft</td>
<td>63</td>
<td>16 Oct 2018</td>
<td><strong>Distrusts all certs signed with Symantec hierarchy</strong></td>
</tr>
<tr>
<td>Safari</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No Plan Yet</td>
</tr>
</tbody>
</table>
Action Required if ...
Credibility of CAs

- Mozilla removed CNNIC CA certificate in the Firefox 37 +
- Google removed CAs StartCom and WoSign in the Chrome 56 +
Certificate Types by Trustworthiness

• DV - Domain Validated
• OV - Organization Validated
• EV - Extended Validation
Certificate Types by Features

• Wildcard Certificate
  • *.example.com
  • secure unlimited number of sub-domains with a single SSL certificate

• Multi Domain SSL (SAN) Certificate

• UCC Certificate
  • for Exchange Servers
  • Multiple Domains

• Code Signing Certificate

• Document Signing Certificate

• Personal Certificate
How Does SSL/TLS Work (simplified)

1. Client makes a connection to Server
2. Server sends a certificate to Client
3. Client validates that the certificate:
   • signed by an organization it trusts
   • name is match
   • not expired
   • not in the blacklist
4. Then client generates a random key, encrypts it with the public key in the certificate, and sends it back to the server
5. Server decrypts the key and uses this shared secret to secure further communications
Test the HTTPS Configurations

- Qualys SSL Labs tool: https://www.ssllabs.com/ssltest
Advanced Configuration - HSTS

• HTTP Strict Transport Security
  • cache the certificate for a designated period in browsers
  • connect via HTTPS only
• Support in Apache & Nginx Web Servers
• Domain owners can submit to https://hstspreload.org
Question?
Thank You!