



Topics

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

Benefit of Using HTTPS

Improve	Improve	Improve
the network communication security	the ranking in Google	the branding



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

D 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



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

Modern	Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9,
Compatibility	Android 5.0, Java 8
Intermediate	Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android
Compatibility	2.3, Java 7
Old:	Windows XP IE6, Java 6

C

٨

Mozilla SSL Configuration Generator

 Apache Modern O Intermediate O Nginx O Old HSTS Enabled ☑ **O** HAProxy

Server Version 2.4.28 OpenSSL Version 1.0.1e

O Lighttpd

<VirtualHost *:443>

SSLEngine on

SSLCertificateFile

SSLCertificateKeyFile

O AWS ELB

apache 2.4.28 | modern profile | OpenSSL 1.0.1e | link Oldest compatible clients: Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, and Java 8

Mozilla SSL Configuration /path/to/signed_certificate_followed_by_intermediate_certs Generator

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

/path/to/private/key

https://mozilla.github.io/server-sidetls/ssl-config-generator/

modern configuration, tweak to your needs all -SSLv3 -TLSv1 -TLSv1.1 SSLProtocol SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1 SSLHonorCipherOrder on SSLCompression off SSLSessionTickets off

Digital Certificate

 is required to exchange information securely over the Internet using the Public Key Infrastructure (PKI) ----BEGIN CERTIFICATE-----

MIIDVzCCAj+gAwIBAgIJAJMjCeUS0cILMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNV BAYTAkhLMRUwEwYDVQQHDAxEZWZhdWx0IENpdHkxHDAaBgNVBAoME0R1ZmF1bHQg Q29tcGFueSBMdGQwHhcNMTgwNTI0MDkxNDUyWhcNMTkwNTI0MDkxNDUyWjBCMQsw CQYDVQQGEwJISzEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5MRwwGgYDVQQKDBNEZWZh dWx0IENvbXBhbnkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA vTDwgCFSKylUumHSc1gXOjM5rJrKnMK/NxL9cghDGO1zhJDUgpLRbd1YZUGG8zLo Z7EZKyZTSfSo7lvoSy20XApKYtVR7T5CbkD6Wo2HT4qz2DBRN1jJ69VHRdGOMo07 E/BQcT+Vj5za1MCmihu/SNeEzwzGcbCKUKYVWW/SGL9RUG6jif49bm6Hkf6dAdg/ d2bkq+bsZJ6Y/KFNa0LD5oqhxR+OuOP3L9NCLApqNjagPD7aVkZFUe2i5ug135zH 5aNplz1MtDrrU0jW6zn32w+zuQbQh9Z405/D4Cn1pLLNChIj1kvTMyKG5nC8ohjR 40gBOT5h78TsAwcrL+fb2QIDAQABo1AwTjAdBgNVHQ4EFgQUlgBztpUxbuoAlK65 TyGIuDs3HfcwHwYDVR0jBBgwFoAUlgBztpUxbuoAlK65TyGIuDs3HfcwDAYDVR0T BAUwAwEB/zANBgkghkiG9w0BAQUFAAOCAQEAuTPoGtc8Y0Lloa9+nZTto/+Fu48i czsKlJKRz0jVzHtUTf+54qrno/g5u9FTZK6Z6cwSHMawBTJ0G3ChISFyPiaRzaUa F4HwTFnF4TW/XSuhFrez5Vk4FD0cPdvQ2/x4FbPZTtF0FwMPbuCbm3W0ezwAP55D LDjRwGEUdaw6zV8JhEHsludPDXt7IZuqvnLynfAGiqCJQRHG73u9TSVlb07s0A+7 8pSH+ZhH/cFsPMqqWHxsagq6oNE1NSg2xdI1CUTLFz0LgKOtcFnAuePaZL0s4PwP RU4eXP+4MNi0u/3LQe0xFTTK07YA9b7BlafoxMSU8CVEs2SWKIBwm2vMNw== ----END CERTIFICATE----

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

 Symantee, GoDaddy, GlobalSign, GeoTrust, Rapid
SSL, Thawte, DigiCert, Comodo, Hongkong Post, Let's Encrypt

Self-signed

Distrust Symantec Certificates

Browser	Version	Release Date	Action
Chrome	65	6 Mar 2018	Distrusts the certs issued before 1 Dec 2017
	66	17 Apr 2018	Distrusts the certs issued before 1 Jun 2016
	70	30 Aug 2018	Distrusts all certs signed with Symantec hierarchy
Firefox	60	9 May 2018	Distrusts the certs issued before 1 Jun 2016
	63	16 Oct 2018	Distrusts all certs signed with Symantec hierarchy
Microsoft			No Plan Yet
Safari			No Plan Yet

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 +

Mar State Mar Revoking Trust in one CNNIC Intermediate Certificate Mar Intermediate Certificate Mar State Ma

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Distrusting WoSign and StartCom Certificates October 31, 2016

Posted by Andrew Whalley, Chrome Security

Certificate Authorities (CAs) play a key role in web security by issuing digital certificates

Certificate Types by Trustworthiness

- DV Domain Validated
- OV Organization Validated

🚹 (1) Facebook	× +	
← → ♂ ଢ	🛈 🛡 🔒 https://www.facebook.com	
f Poorth		0

• 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

憑證層級(出)	
✓COMODO ECC Certification Authority	
✓COMODO ECC Domain Validation Secure Server CA 2	
sni30128.cloudflaressl.com	
憑證欄位 (E)	
──延伸金鑰用法	
- 憑證政策	
透證廢止清冊發佈點	
授權資訊存取	
憑證主體替代名稱	
物件識別符 (13614111129242)	
-憑證簽章演算法	
憑證簽章值	
欄位值 (⊻)	
DNS 名稱: tomkranz.com	
UNS 名稱: tschudin-haustechnik.ch DNS 名稱: wirr org	
DNS 名稱: wsyoung.com	
DNS 名稱: yardgardenharrow.info	
DNS 名稱: yarnparadise.net DNS 名稱: yarnpibaok an	
DNAS 名相: yen1000K.ga	

開閉 (C)

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

Qualys. SSL Labs			Home Projects	Qualys.com Con
ou are here: <u>Home</u> > <u>Projects</u> > SSL Server Test				
SSL Server Test				
his free online service performs a deep analysinformation you submit here is used only to vill.	is of the configuration of any SSL provide you the service. We do	web server on the n't use the doma	e public Internet. Plea in names or the test	se note that the results, and we neve
Hostname:	Do not show the results on the boards		Submit	
Recently Seen	Recent Best		Recent Worst	
alumni.wm.edu	tomharris.tech	A+	scotss.org.uk	т
adwords.google.com	www.physiotherapie-dirsch.de	A+	mobile.hafod.org.uk	F
www.yellowpages.co.th	support.groupeboa.com	A	accounts.ctrip.sq	т
abnamro.nl Err	secure.ctrip.my	A	kis.console.ksyun.com	F
pursingup it	redbulk org	•	mortoncommunity.net	т

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 <u>https://hstspreload.org</u>



