



**Has Tenido Tiempo Para Securizarlo:
Te Lo Suplico, no Sigas Solo Leyéndolo**

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL



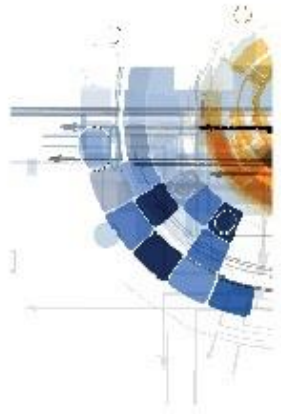
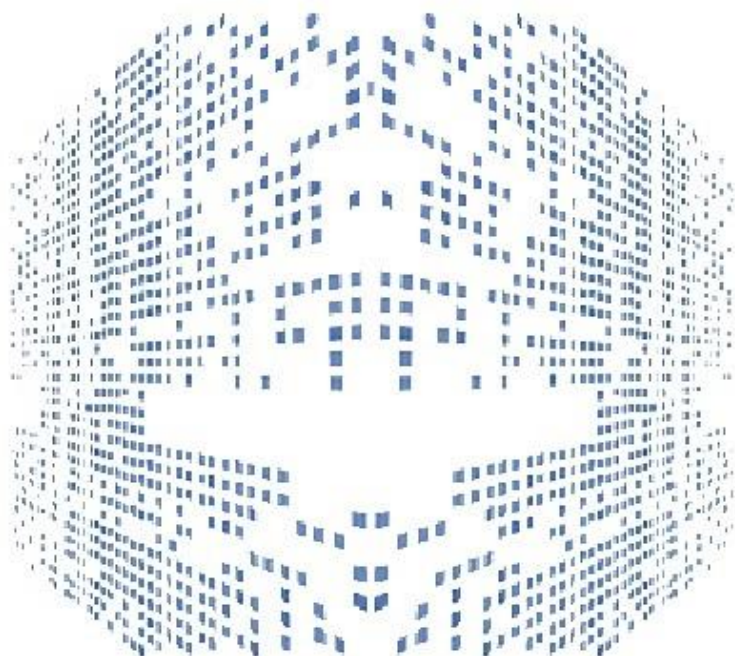
Noviembre
de 2007...



DinoSec

- Raúl Siles
- DinoSec (www.dinosec.com)
- raul@dinosec.com

(40 minutos...)



X Jornadas STIC CCN-CERT

Diez años fortaleciendo la ciberseguridad nacional

Madrid, 13 y 14 de diciembre 2016

X Jornadas: Otra orientación - Defensiva vs. Ofensiva

A word cloud featuring various SSL/TLS related terms. The most prominent word is 'OCSF' in the center. Other visible words include 'DROWN', 'TSL', 'PFS', 'RSA', 'Must', 'Renegotiation', 'Heartbleed', 'Padding', 'CRL', 'HTTP', 'Transparency', 'Staple', 'ALPN', 'Certificate', 'Stapling', 'SSL', 'SNI', 'SSLv3', 'OneCRL', 'NP', 'Secure', 'CR sets', 'Oracle', 'CS', 'SCS', 'BEAST', 'RC', 'AES', 'CSP', 'MD5', 'SHA256', 'CAA', and 'Stapling'. To the right of the word cloud is a red heart icon with red liquid dripping down from its base.

Has Tenido Tiempo Para Securizarlo: Te Lo Suplico, no Sigas Solo Leyéndolo

HTTPS: TLS, no SSL

#movingtoHTTPS

¿Qué ha pasado en 2016? ¿Qué va a pasar en 2017?

Terminología: SSL o TLS



Terminología: HTTP**S**

La importancia de la letra "S"

https://



"Pues le ponemos la **S** y ya está, ¿no?"

Aplicar también TLS al resto de protocolos: SMTP**S**, IMAP**S**, POP3**S**...

Índice

1. HTTP
2. Herramientas
3. Ataques sobre HTTPS...
4. TLS
5. Recomendaciones (en la implementación de HTTPS)
6. HSTS
7. CSP
8. HPKP
9. Clientes HTTPS
10. Conclusiones

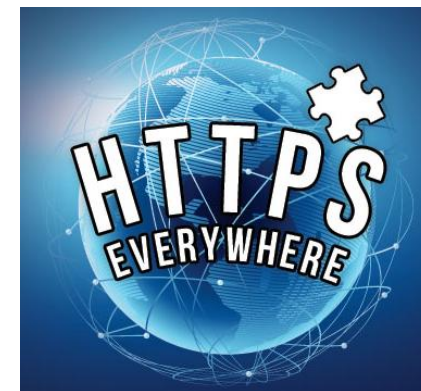
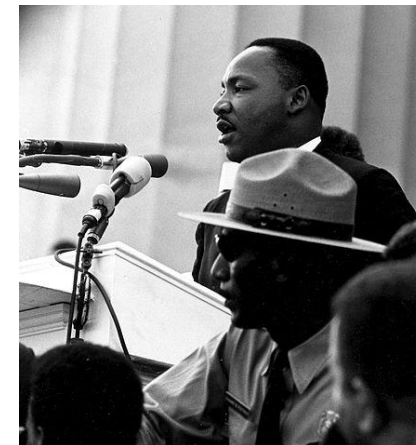


"La web es segura": HTTP^S



"Yo tengo un sueño..." ("I Have a Dream...")

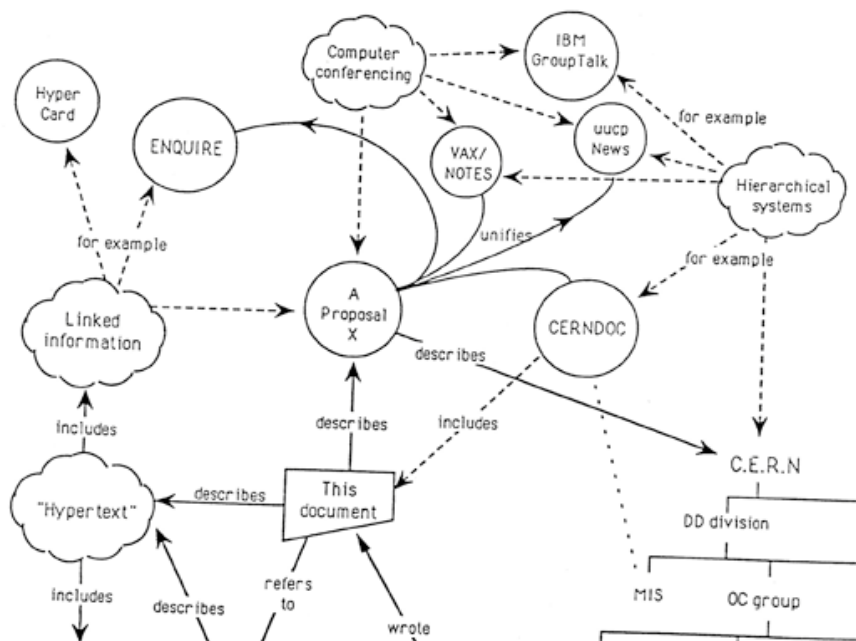
- Martin Luther King Jr (28/8/1963)
 - "Deseo un futuro en el cual la gente de tez negra y blanca pudiesen coexistir armoniosamente y como iguales."
- Raúl Siles (14/12/2016) 😊
 - "Deseo un futuro en el cual las webs cifradas (HTTPS) y no cifradas (HTTP) no pudiesen coexistir armoniosamente y como iguales."
 - "Un futuro dónde la web sea sólo HTTPS, y todos los puertos TCP/80 estén cerrados. ¡Viva el puerto TCP/443!"
 - Excepto: <sitio web>





HTTP

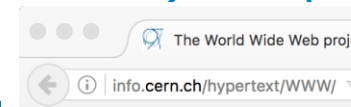
Todo comenzó con una propuesta en marzo de 1989...



<https://www.w3.org/History/>

HTTP

- Tim (John) Berners-Lee (el "padre" de la Web) - UK
 - Primera comunicación cliente/servidor usando HTTP: noviembre 1989 (HTTP, HTML y URLs)
 - <http://info.cern.ch/hypertext/WWW/TheProject.html>
- HTTP/0.9 (1991; 25 años), HTTP/1.0 (05/1996), HTTP/1.1 (06/1999), HTTP/2 (05/2015)
- Número de servidores/sitios web (1 en 1991)
 - 19.000 en agosto de 1995 (comienzo de Netcraft)
 - 1 M en abril de 1997
 - 10 M a comienzos de 2000 (≈50% activos)
 - 1.000 M (1B) en septiembre 2014 (<20% activos)



World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#), [Policy](#), November's [W3 news](#), [Frequently Asked Questions](#).

[What's out there?](#)

Pointers to the world's online information, [subjects](#), [W3 servers](#), etc.

[Help](#)

on the browser you are using

[Software Products](#)

A list of W3 project components and their current state. (e.g. [Line Mode](#), [X11 Viola](#), [NeXTStep](#), [Servers](#), [Tools](#), [Mail robot](#), [Library](#))

[Technical](#)

Details of protocols, formats, program internals etc

[Bibliography](#)

Paper documentation on W3 and references.

[People](#)

A list of some people involved in the project.

[History](#)

A summary of the history of the project.

[How can I help?](#)

If you would like to support the web..

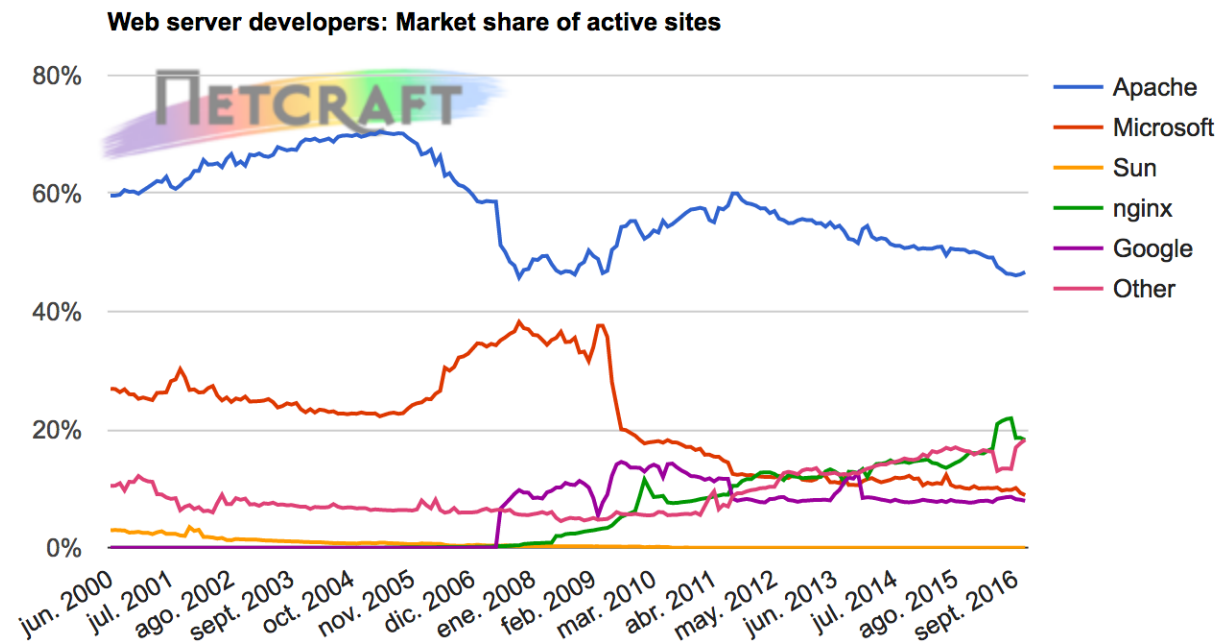
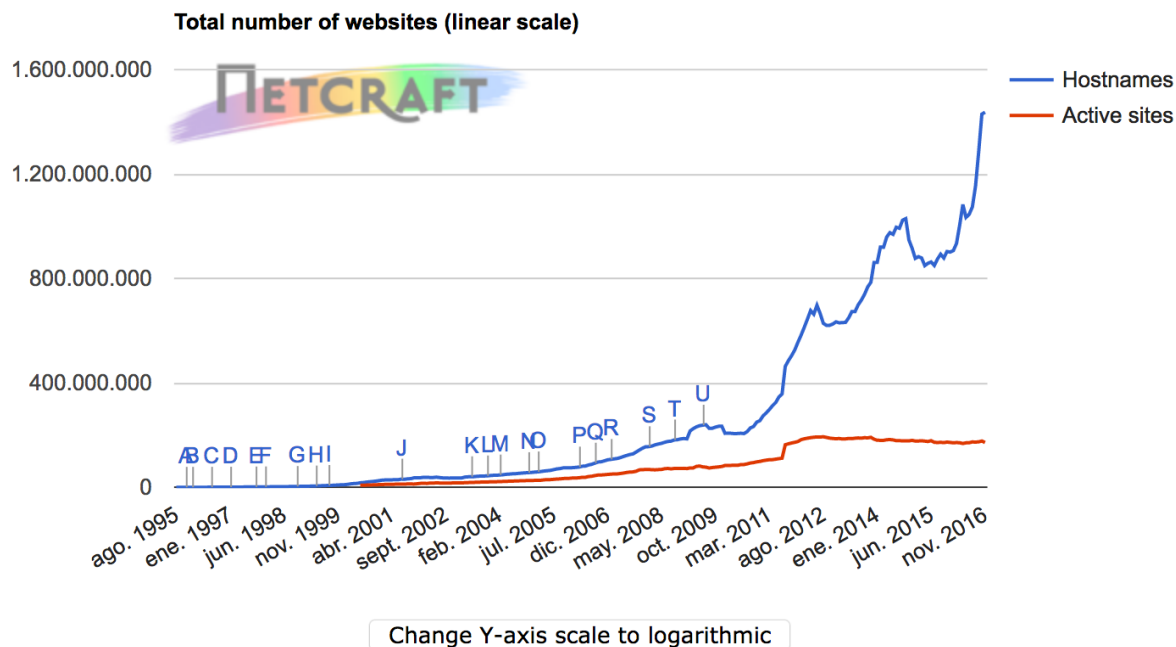
[Getting code](#)

Getting the code by [anonymous FTP](#), etc.

Número de sitios, servidores y tecnologías web



- Noviembre 2016
 - + 1.436 M sitios web (+171 M "activos") y +6 M servidores
 - Activos: Apache (46%), nginx (18%), IIS (9%), Google (8%)...

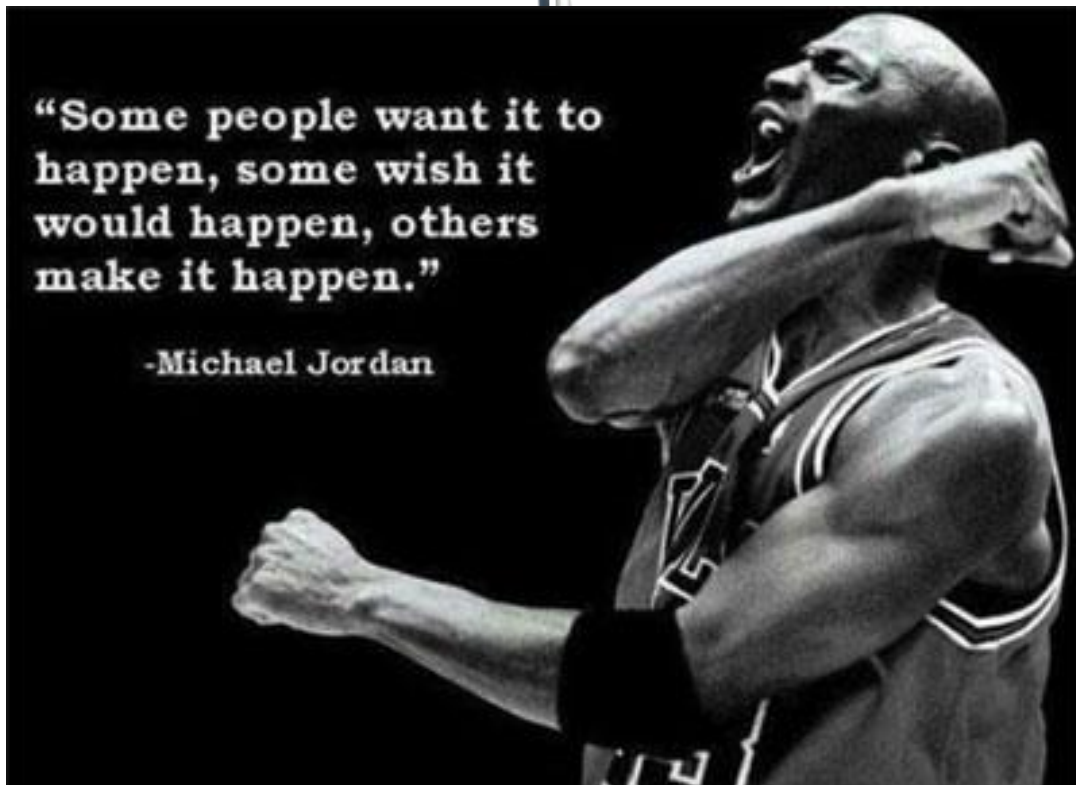


<https://news.netcraft.com/archives/2016/11/22/november-2016-web-server-survey.html>

¿Por qué tantos números y la historia de HTTP?

No aprendemos de la historia...

Motivación



VERGÜENZA





Herramientas

Herramientas

- Inspeccionar los logs de los servicios y aplicaciones web
 - Pruebas con distintos clientes/navegadores web (tradicional y móvil)
- Proxies de interceptación web
 - OWASP ZAP & Burp Suite & ...
- Herramientas "en la nube"
 - SSL Labs (¿minimizar exposición pública?)
 -
- Herramientas locales
 - Privacidad y accesibilidad (Intranet)



Ataques sobre HTTPS...

Ataques sobre HTTPS... (HSTS, HPKP...)

- Exploiting changes on DNS server configuration (L. Nve) – SSLStrip2
 - <https://www.blackhat.com/asia-14/archives.html#Nve> (DNS subdomains)
- Bypassing HTTP Strict Transport Security (J. Selvi) – Delorean
 - <https://www.blackhat.com/eu-14/archives.html#Selvi> (NTP MitM)
 - <https://www.defcon.org/html/defcon-23/dc-23-speakers.html#Selvi>
- Privacidad: HSTS & HPKP
 - <https://zyan.scripts.mit.edu/presentations/toorcon2015.pdf>
 - <http://www.radicalresearch.co.uk/lab/hstssupercookies>
- HSTS & HPKP: Batman y Robin (C. Torrano/P. Glez) – PinPatrol
 - <http://es.slideshare.net/elevenpaths/hsts-hpkp-los-batman-y-robin-de-la-seguridad-web>
- MitMf, BetterCap, y nuevos ataques en el futuro...



SSL / TLS

TLS

Transport Layer Security (TLS)

- SSL (Secure Sockets Layer) – Netscape: 1994 & 1995
- TLS: TCP (ej. HTTPS) y UDP (DTLS)
- Seguridad
 - Autenticación (servidor y/o cliente)
 - Cifrado (confidencialidad)
 - Integridad (datos)
- HTTP/2 (05/2015): HTTPS opcional ☹️
 - Implementación de los navegadores web: HTTPS obligatorio
- Mejor ranking SEO

<https://hpbn.co/transport-layer-security-tls/>

Versiones del protocolo TLS

- SSL 2.0 (Nov'94) & SSL 3.0 (Nov'95) (RFC 6101 – por documentación)
 - SSL 2.0 prohibido en RFC6176 (Mar'11) y SSL 3.0 en RFC 7568 (Jun'15)
- TLS 1.0 – RFC 2246 (Ene 1999)
 - <https://tools.ietf.org/html/rfc2246>
- TLS 1.1 – RFC 4346 (Abr 2006)
 - <https://tools.ietf.org/html/rfc4346>
- TLS 1.2 – RFC 5246 (**Ago 2008**)
 - <https://tools.ietf.org/html/rfc5246>
- **TLS 1.3** ("TLS 2 ó 4") – Borrador (v18 – Oct 2016) - Exp: Abr 29, 2017
 - <https://tools.ietf.org/html/draft-ietf-tls-tls13-18>

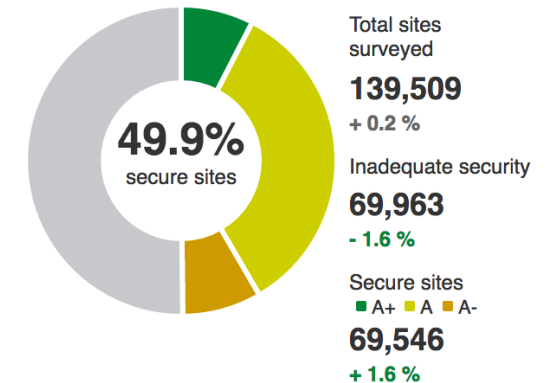
TLS ≈ 46

Número de sitios web HTTPS...

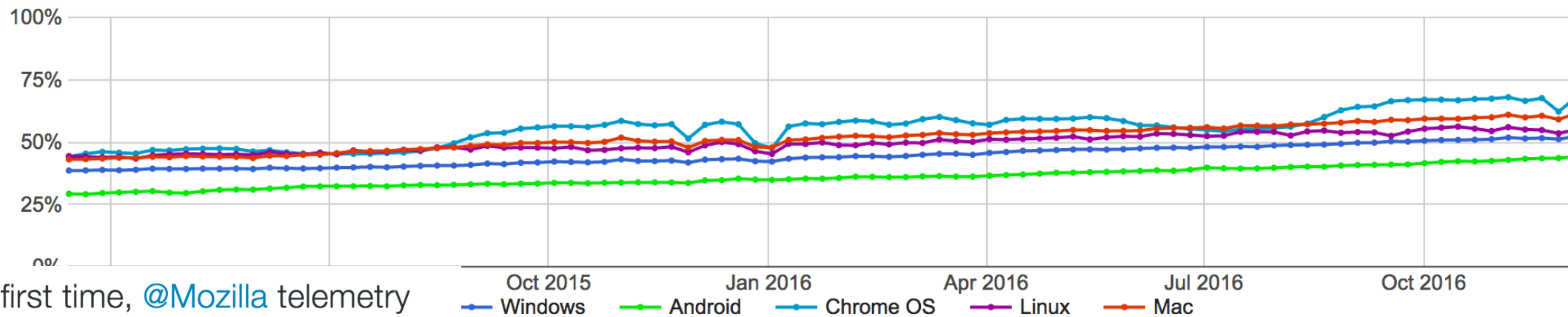
- SSL Pulse (by SSL Labs) - TIM: Trustworthy Internet Movement
 - <https://www.trustworthyinternet.org/ssl-pulse/>
- Censys: <https://censys.io>
- Crt.sh: <https://crt.sh>
- "HTTPS on Top Sites" (Google Transparency Report)
 - <https://www.google.com/transparencyreport/https/grid/>
 - Top 100 sitios web (no Google) $\approx$ 25% tráfico total
 - HTTPS at Google: <https://www.google.com/transparencyreport/https/>
- Netcraft SSL Survey (Ej. Enero 2015 – suscripción anual)
 - <https://www.netcraft.com/internet-data-mining/ssl-survey/>

Published Date: **December 04, 2016**
Comparisons are made against the previous month's data.

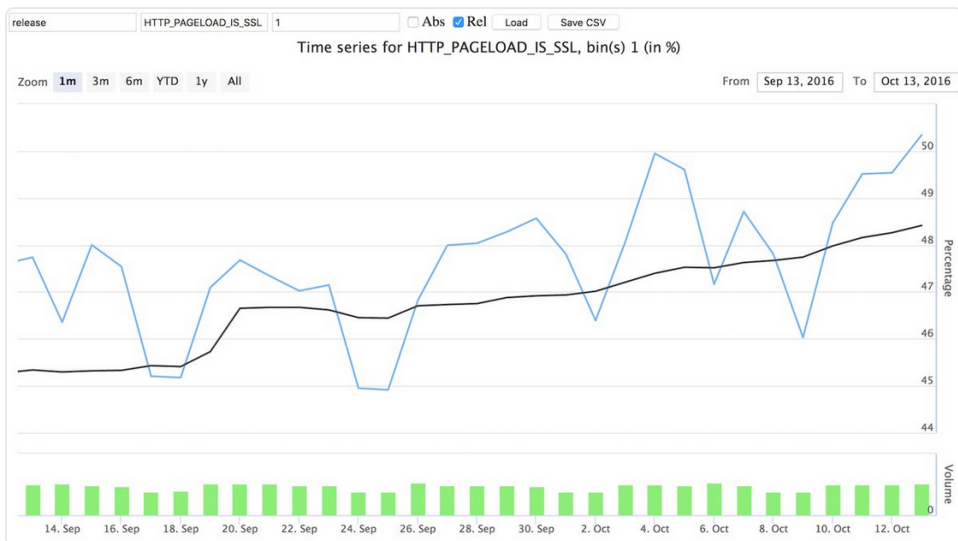
SSL Security Summary



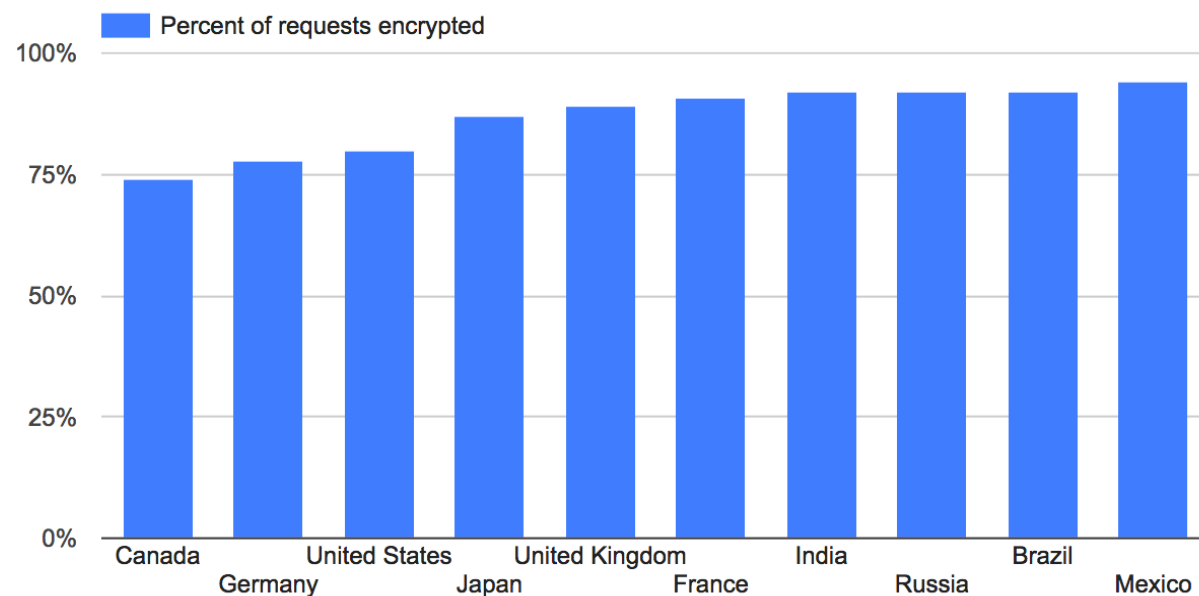
Percentage of pages loaded over HTTPS



Yesterday, for the first time, @Mozilla telemetry shows more than 50% of page loads were encrypted with HTTPS.



RETWEETS 1.085
ME GUSTA 1.177



Tráfico HTTPS a los servicios de Google por país
(sólo monitorizan esos 10 países)



Let's Encrypt

- CA gratuita, abierta y sin ánimo de lucro (<https://letsencrypt.org/stats/>)
 - Noviembre 2015
- Certificados digitales gratuitos
 - Campaña de donación (crowdfunding)
- Herramientas de gestión automatizadas
- Chain of trust
 - <https://letsencrypt.org/certificates/>
- Guías...
 - <https://scotthelme.co.uk/setting-up-le/>
 - <https://scotthelme.co.uk/lets-encrypt-smart-renew/>

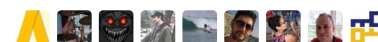


We've issued 20M+ certificates! Help us continue our work:



RETWEETS
176

ME GUSTA
254



12:30 - 27 nov. 2016



Rendimiento de HTTPS



- Overclocking SSL (2010)
 - <https://www.imperialviolet.org/2010/06/25/overclocking-ssl.html>
- STARTTLS, False & Snap Start
- *Session resumption*
- Cachear contenidos públicos
 - No contenidos sensibles
- *OCSP stapling*

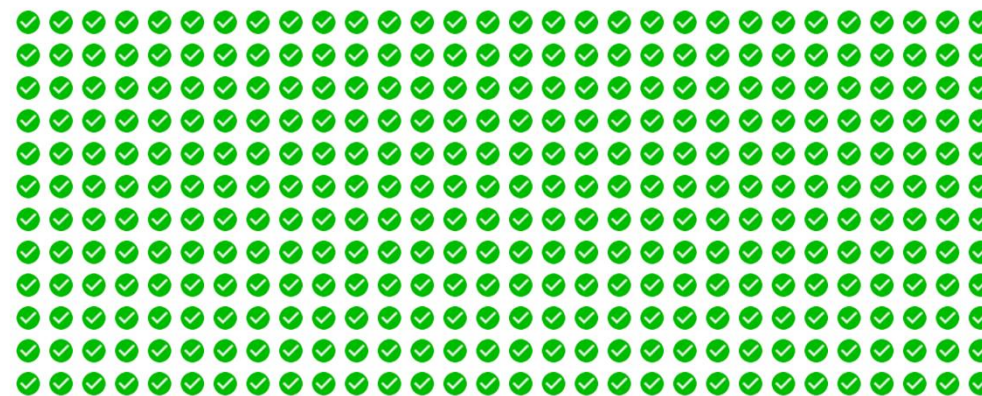
HTTP vs HTTPS Test

Encrypted Websites Protect Our Privacy and are Significantly Faster
Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (0.62 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

HTTP HTTPS

2.162 s

Done! Please try HTTP.



<https://www.httpvshttps.com>

Can I use... TLS 1.1 & TLS 1.2?

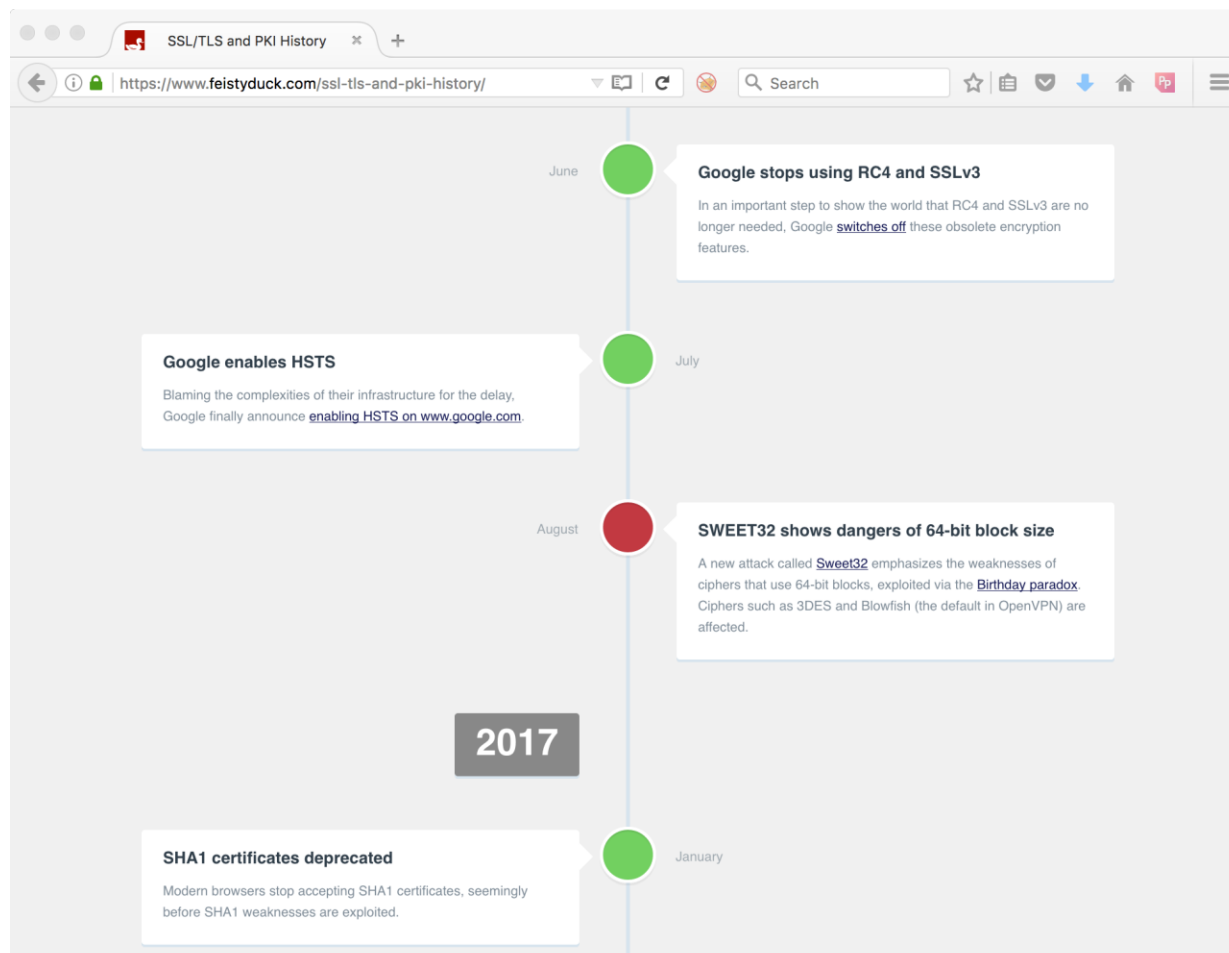
[Showing All]

- TLS 1.0
 - Todos
- TLS 1.1
 - No: IE 6-10 y Android 4.4.x
- TLS 1.2
 - << Idem >>
- Server Name Indication (SNI)
 - Todos

<http://caniuse.com/#search=TLS>

DEMO

Historia (de las vulnerabilidades) de SSL/TLS

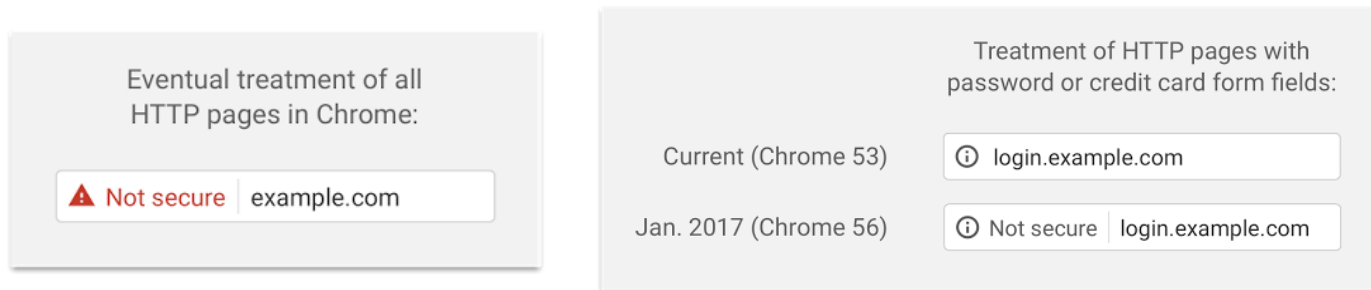


<https://www.feistyduck.com/ssl-tls-and-pki-history/>

TLS en 2016

- Enero 2016: Las CAs no emiten certificados firmados con SHA-1
- Enero 2016: Nuevos algoritmos EC
- Enero 2016: SLOTH
- Febrero 2016: Análisis del diseño de TLS 1.3 (+2 años desarrollo)
- Marzo 2016: Mejoras en la revocación de certificados
 - Firefox 45: OCSP Must Stable y Short-Lived certificates
- Marzo 2016: DROWN
- Junio – Julio 2016: Google habilita HSTS y elimina RC4 y SSLv3
- Agosto 2016: SWEET32

TLS en 2017 (1/2)



- **Enero 2017: Fin del soporte de certificados firmados con SHA-1**
 - Firefox 51: <https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/>
 - Edge & IE 11 (Feb 14, 2017): <https://blogs.windows.com/msedgedev/2016/11/18/countdown-to-sha-1-deprecation/>
 - Chrome 56: <https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html>
- **Enero 2017 (Chrome 56): HTTP - "Not secure"**
 - <https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html>
- **Enero 2017: Apple App Transport Security (ATS) en iOS**
- **Enero-Junio 2017: Actualización de los criterios de SSL Labs**
 - 3DES, RC4, FS, AEAD suites (TLS 1.3), SCSV, SHA-1, HSTS preload...
 - <https://blog.qualys.com/ssllabs/2016/11/16/announcing-ssl-labs-grading-changes-for-2017>

TLS en 2017 (2/2)

- Febrero 2017: Ratificación TLS 1.3 (Firefox 52)
 - <https://www.ietf.org/mail-archive/web/tls/current/msg21709.html>
- 30 junio 2017: Paypal sólo permitirá conexiones TLS 1.2 de otros sitios web (tiendas online)
 - <https://devblog.paypal.com/upcoming-security-changes-notice/>
 - <https://devblog.paypal.com/wp-content/uploads/2016/03/Foundation-for-June-2017-TLS-1.2-Upgrade-5.4.16.pdf>
- Octubre 2017: Chrome requerirá que todos los nuevos certificados sean registrados en Certificate Transparency (CT)
 - <https://groups.google.com/a/chromium.org/forum/#!topic/ct-policy/78N3SMcqUGw>
- Julio 2018: Fin del soporte de TLS 1.0 por PCI DSS (era para Jul'16)
 - Todos los sitios web que acepten pagos con tarjeta de crédito



Recomendaciones en la implementación de HTTPS

Errores de certificados



- Certificados raíz de la FNMT
 - <https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt>
- Solución (política y técnica)
 - Incluir la CA en los diferentes clientes HTTPS (navegadores web, sistemas operativos, etc....)

¿Predicando con el ejemplo?

- <https://www.dinosec.com>
 - Octubre 2016
 - HTTP solo (para pruebas): <http://www.raulsiles.com>
- TLSSLed (herramienta obsoleta...)
 - <https://www.dinosec.com/en/lab.html#TLSSLED>



Reto para diciembre de 2017...

Recomendaciones: Índice

- (Fecha y hora sincronizadas) - NTP
- Evitar contenidos mixtos: HTTPS y HTTP
- Validez del certificado digital
- Proteger las cookies y renegociación segura TLS
- Usar "nuevas" cabeceras HTTP(S) de seguridad
 - HSTS, CSP, HPKP, etc.
- Correcta implementación de TLS
 - Protocolos y algoritmos de cifrado e integridad
- Vinculación de certificados con dominios, CDNs, revocación...



Recomendaciones en la implementación de HTTPS (1/3)

Contenidos web

- Evitar contenidos mixtos: HTTPS y HTTP (multimedia, CSS, JS, etc.)
 - Proteger/Cifrar el proceso de autenticación... y el resto de la sesión
 - Utilizar URLs relativas
 - Redirigir (301 ó 302) todos los contenidos de HTTP a HTTPS
 - Mejor aún: Cerrar el puerto TCP/80 ☺ ¿Realmente?
 - <https://scotthelme.co.uk/why-closing-port-80-is-bad-for-security/>
 - Diferentes servidores/subdominios: www, sede, secure, portal, etc.
 - Comprobar que el dominio y todos los subdominios ("www") usan HTTPS
 - Spider (HTTP y HTTPS)
 - CSP...



Recomendaciones en la implementación de HTTPS (2/3)

Autenticación: Certificado digital

- Validez del certificado digital
 - Entidad (Subject o CN) - ¿Certificado comodín: *.dinosec.com?
 - Certificate Subject Alt(ernate) Names: www & dominio (dinosec.com)
 - CA de confianza (AC Raíz FNMT-RCM, FNMT Clase 2 CA, etc.)
 - Verificar todos los certificados intermedios en la cadena de confianza
 - Inválidos o ausentes
 - Longitud de la clave pública/privada:
 - RSA $\geq$ 2.048 bits (3.072 bits...) – 112 bits de seguridad (128 bits)
 - ECDSA $\geq$ 256 bits - 128 bits de seguridad
 - Algoritmo de firma del certificado: $\geq$ SHA-1 (SHA-256, SHA-384...)
 - Expiración (múltiples herramientas de monitorización...)

Recomendaciones en la implementación de HTTPS (3/3)

Cifrado

- Proteger las cookies
 - Propiedad "Secure" (y "HttpOnly", "domain" restrictivo, etc.)
 - https://www.owasp.org/index.php/Session_Management_Cheat_Sheet
- Deshabilitar renegociación TLS, o usar la versión segura (RFC 5746)
- Usar "nuevas" cabeceras HTTP(S) de seguridad...
 - HSTS
 - CSP
 - HPKP

Cifrado e integridad: Algoritmos (¿*Ciphers* y *CipherSuites*?) (1/3)

- Versiones del protocolo TLS: ≥ 1.2 (1.1, 1.2... y 1.3)
 - No SSL (2.0 ó 3.0) `SSLProtocol All -SSLv2 -SSLv3 -TLSv1.0 -TLSv1.1`
- Algoritmos robustos de cifrado y longitud de las claves
 - No NULL, ADH, *export ciphersuites*, RC4, 3DES, etc.
 - AES (Advanced Encryption Standard): Claves ≥ 128 bits (256 bits...)
 - AES-GCM (Galois/Counter Mode) 256 bits > AES-CBC (ej. BEAST)
 - Otros: <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>

```
SSLCipherSuite ECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLHonorCipherOrder on
```

Configuración HTTPS del servidor web

Cifrado e integridad: Algoritmos (¿*Ciphers* y *CipherSuites*?) (2/3)

- (P)FS: (Perfect) Forward Secrecy
 - (EC)DHE: (Elliptic Curve) Diffie-Hellman Ephemeral
 - Evitar intercambio de claves (key exchange) mediante RSA (no FS)
- Fortaleza del intercambio de claves (DHE): tamaño del pool de DH
 - DHE $\geq$ 2.048 bits (3.072 ó 4.096 bits)
 - ECDHE = 256 bits

```
$ openssl dhparam -out dhparams.pem 4096
```

- Añadir a la configuración del servidor web: Apache

```
SSLOpenSSLConfCmd DHParameters "/etc/ssl/certs/dhparams.pem"
```

Cifrado e integridad: Algoritmos (¿*Ciphers* y *CipherSuites*?) (3/3)

- No usar RC4 (desde 2013 y especialmente, desde 2015)
 - <https://www.rc4nomore.com> (prohibido en RFC 7465 – Feb 2015)
- Algoritmos robustos de integridad (*hashing*)
 - SHA2: SHA-256, SHA-384, SHA-512, etc.
- Deshabilitar compresión en TLS (ej. CRIME)

```
SSLCompression off
```

- Obtener un listado de CipherSuites mediante OpenSSL:

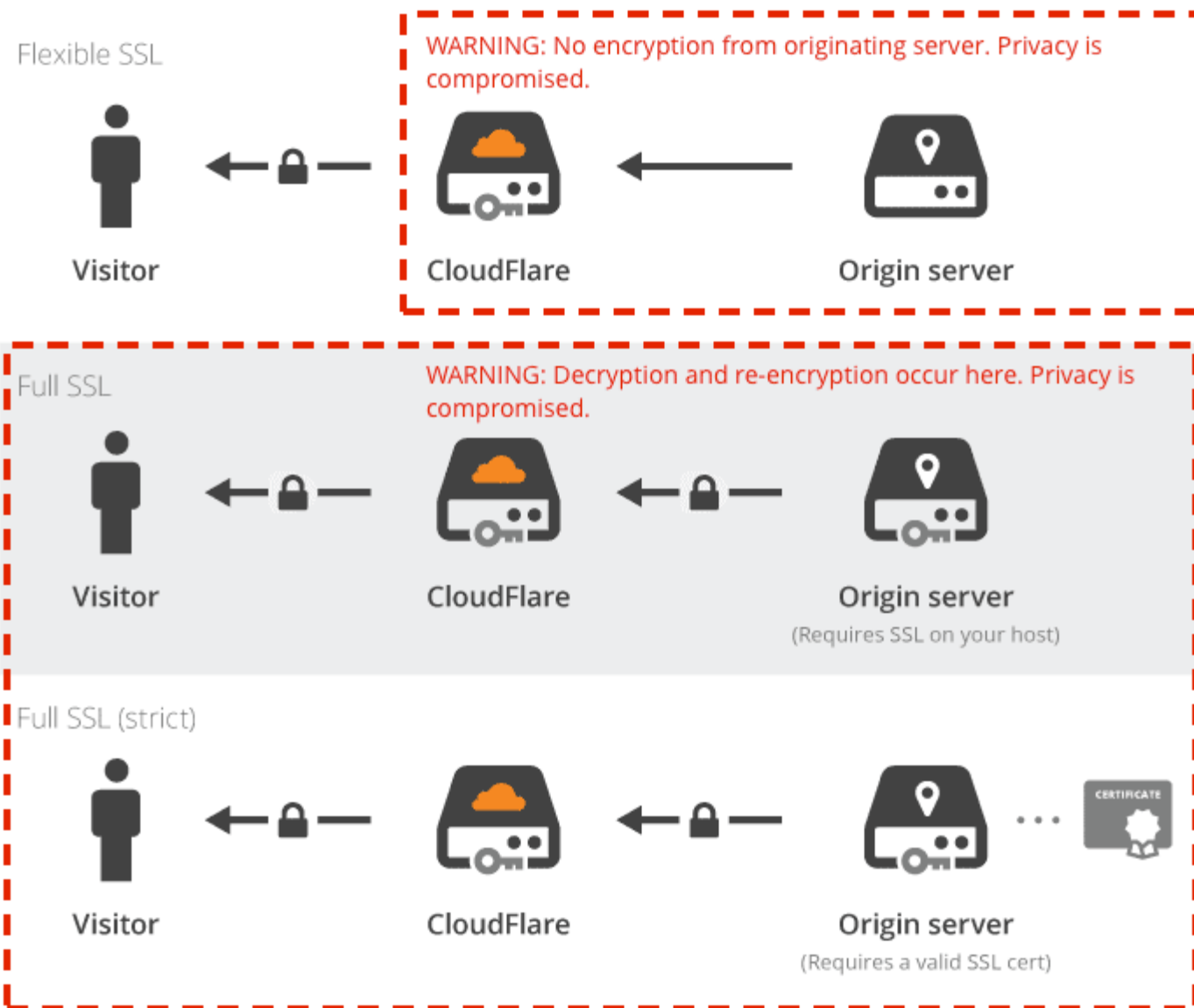
```
$ openssl ciphers  
HIGH:\!SSLv2:\!SSLv3:\!TLSv1:\!kRSA:\!kECDH:\!ADH:\!DSS:\!PSK:\!SRP:  
\!aNULL:\!eNULL:\!MD5:\!RC4:\!DES:\!3DES:\!EXPORT:\!LOW
```

Vinculación de certificados (o CAs) con dominios

- Certificate Transparency (Google)
 - <http://www.certificate-transparency.org> & <https://suricat.io>
 - <https://www.google.com/transparencyreport/https/ct/>
 - RFC 6962 (Jun 2013) - Experimental
 - <https://tools.ietf.org/html/rfc6962>
 - <https://www.entrust.com/ct-search/>
- Certification Authority Authorization (CAA)
 - DNS Resource Records (RR): "CAA" – CAs usadas por un dominio
 - RFC 6844 (Ene 2013): <https://tools.ietf.org/html/rfc6844>
 - CAA Record Generator: <https://ssllmate.com/labs/caa/>
- DANE: DNS-based Authentication of Named Entities
 - Vincular certificados con dominios a través de DNSSEC
 - RFC 6698 (Ago 2012) – TLSA: <https://tools.ietf.org/html/rfc6698>



As of Dec 13, 2016, 3:55:10 PM, there have been 171,956,668 entries made to the set of Certificate Transparency logs that Google monitors.

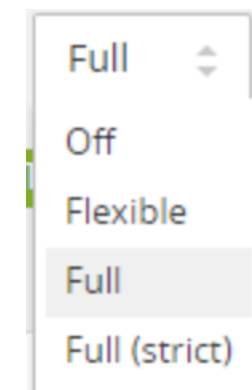


This modified image illustrates user privacy compromises.

Original Source Dec 2014: <https://www.cloudflare.com/images/ssl/ssl.png>

Content Delivery Networks (CDNs / Clouds)

- <https://www.troyhunt.com/cloudflare-ssl-and-unhealthy-security-absolutism/>
- <https://www.troyhunt.com/how-to-get-your-ssl-for-free-on-shared/>

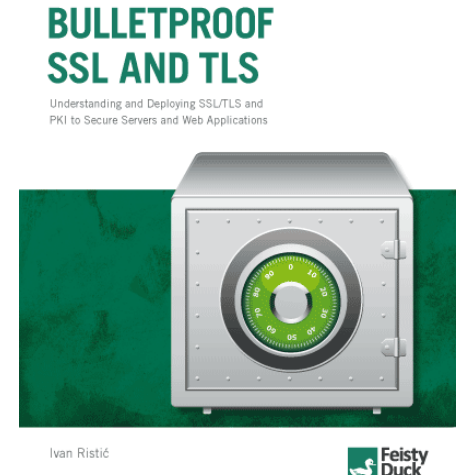


Revocación de certificados (más allá de las CRLs)

- OCSP: <http://tools.ietf.org/html/rfc6960>
- Certificados de corta vida: <https://blog.digicert.com/short-lived-certificates/>
- OCSP Stapling (prueba embebida en el propio intercambio TLS)
 - <https://tools.ietf.org/html/rfc6066> & <https://tools.ietf.org/html/rfc6961>
 - Acelerar la comprobación de la validez del certificado
 - Puede ser eliminada (soft fail – MitM o DoS). Solución:
 - Extensión certificado OCSP Must-Staple - <https://tools.ietf.org/html/rfc7633>
- CRLsets (Chrome): <http://dev.chromium.org/Home/chromium-security/crlsets>
 - <https://www.imperialviolet.org/2012/02/05/crlsets.html>
 - <https://www.imperialviolet.org/2014/04/19/revchecking.html>
- OneCRL (Firefox): <https://wiki.mozilla.org/CA:RevocationPlan>

Referencias TLS: Documentación

- "How to Deploy HTTPS Correctly" (EFF, Sep'16)
 - <https://www.eff.org/https-everywhere/deploying-https>
- "SSL/TLS Deployment Best Practices" (SSL Labs)
 - <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>
- "Enabling HTTPS on Your Servers"
 - <https://developers.google.com/web/fundamentals/security/encrypt-in-transit/enable-https>
- "Bulletproof SSL and TLS" (book)
 - <https://www.feistyduck.com/books/bulletproof-ssl-and-tls/>
- "OpenSSL Cookbook" (book)
 - <https://www.feistyduck.com/books/openssl-cookbook/>
- Bulletproof TLS Newsletter
 - <https://www.feistyduck.com/bulletproof-tls-newsletter/index.html>



Referencias TLS: Más documentación

- https://wiki.mozilla.org/Security/Server_Side_TLS
- https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
- <https://timtaubert.de/blog/2014/10/deploying-tls-the-hard-way/>
- <https://scotthelme.co.uk/still-think-you-dont-need-https/>
- https://raymii.org/s/tutorials/Strong_SSL_Security_On_Apache2.html
- <https://blog.cloudflare.com/tls-1-3-overview-and-q-and-a/>
- <https://github.com/tlswg/tls13-spec>
- <https://www.theguardian.com/info/developer-blog/2016/nov/29/the-guardian-has-moved-to-https>
- <https://speakerdeck.com/kwhite/https-and-tls-in-2016-security-practices-from-the-front-lines>
- "TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks". <https://tools.ietf.org/html/rfc7507>

Referencias TLS: Herramientas de configuración



- Cipherli.st: <https://cipherli.st>
 - Recomendación de configuraciones con algoritmos robustos
 - ¿Software viejo y obsoleto?
 - IE < 9, Android < 2.2 o Java < 6
 - CipherSuites más permisivas
 - Otros protocolos y servicios distintos a HTTP...
- Mozilla SSL Configuration Generator
 - <https://mozilla.github.io/server-side-tls/ssl-config-generator/>

Referencias TLS: Herramientas de comprobación (1/2)

- Monitorizar la validez de los certificados digitales (expiración)
 - Certificate Expiry Monitor (PHP): <https://certificatemonitor.org>
 - <https://github.com/RaymiiOrg/certificate-expiry-monitor>
 - Certmon (Python): <https://github.com/corelan/certmon>
 - ssl-cert-check (bash): <http://prefetch.net/articles/checkcertificate.html>
- Comprobar la configuración TLS del servidor
 - SSL Decoder (PHP): <https://ssldecoder.org> (<https://tls.so>)
 - <https://github.com/RaymiiOrg/ssl-decoder>
- OWASP DeepViolet TLS/SSL Scanner
 - https://www.owasp.org/index.php/OWASP_DeepViolet_TLS/SSL_Scanner

Referencias TLS: Herramientas de comprobación (2/2)

- OWASP O-Saft
 - <https://www.owasp.org/index.php/O-Saft>
- Evaluar la implementación TLS: ¿*Ciphers* y *CipherSuites*?
 - Nmap NSE script: ssl-enum-ciphers (actualizado)
 - <https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html>

```
$ nmap --script ssl-enum-ciphers -p 443 www.dinosec.com
```

- CipherScan (bash)
 - <https://github.com/mozilla/cipherscan>
- Mozilla TLS Observatory
 - <https://github.com/mozilla/tls-observatory>

Referencias TLS: Herramienta de comprobación de referencia



QUALYS® **SSL** LABS

- (Qualys) SSL Labs
 - Ivan Ristic
 - SSL Server Test: <https://www.ssllabs.com/ssltest/index.html>
 - <https://www.ssllabs.com/ssltest/analyze.html?d=www.dinosec.com&hideResults=on>
 - SSL Server Rating Guide:
https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf
 - SSL Client Test: <https://www.ssllabs.com/ssltest/viewMyClient.html>
 - Soporte de los navegadores web
 - <https://www.ssllabs.com/ssltest/clients.html>
 - SSL Threat Model
 - <https://www.ssllabs.com/projects/ssl-threat-model/index.html>



HSTS

HSTS

HTTP Strict Transport Security (HSTS o STS)

- RFC 6797 (Nov 2012)
 - <https://tools.ietf.org/html/rfc6797>
- Estándar "similar" a la extensión HTTPS Everywhere (EFF) o "https://"
 - <https://www.eff.org/https-everywhere>
 - Solución complementaria durante la "migración"
- Cabecera HTTP HSTS (a nivel del dominio)

"El navegador web puede hablar tanto HTTP como HTTPS contra cualquier sitio web"



```
Strict-Transport-Security: max-age=31536000 [; includeSubDomains]
[; preload]
```

- Deshabilita la posibilidad de ignorar las alertas o errores en la validación de certificados del navegador web por parte del usuario

TOFU: Trust On First Use

- Objetivo: Evitar ataques activos de SSLStrip (MitM) o capturas pasivas
- HSTS: El navegador web obedece al uso de HTTPS para un servidor web concreto durante el periodo indicado por el parámetro "max-age"
- Solución: Lista precargada para HSTS (HSTS Preload List)



Lista precargada para HSTS (HSTS Preload List)



- Solicitud, estado actual y elegibilidad (Chrome)
 - <https://hstspreload.appspot.com>
 - Usada por: Chrome, Firefox, Opera, Safari, IE 11 y Edge
 - Requisitos: certificado válido, redirección de HTTP a HTTPS, todos los subdominios por HTTPS (ej. "www"), y cabecera HSTS:
 - max-age >= 10886400 (18 semanas), includeSubDomains, y preload
 - Dominio (dinosec.com) y subdominios (*.dinosec.com, *.*.dinosec.com...)
- Estado actual de la lista precargada
 - Chrome: <https://www.chromium.org/hsts>
 - https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json
 - Firefox:
 - <https://dxr.mozilla.org/mozilla-central/source/security/manager/ssl/nsSTSPreloadList.inc>

Riesgos de HSTS: Lista precargada

- Posible DoS en el acceso a contenidos sólo disponibles por HTTP
- Verificar que todo el dominio y los subdominios usan HTTPS
- Añadir "Strict-Transport-Security", incluir "includeSubDomains" y comenzar con un valor de "max-age" pequeño
 - Incrementarlo progresivamente: 300 (5m), 604800 (1s), 2592000 (1m)
 - Monitorizar logs de acceso por HTTP
- Incrementar "max-age" a 2 años (63072000)
 - "Soportar HTTPS durante toda la vida" (en "*.dominio.com")
 - Recomendación: certificado comodín (*) o certificados para cada subdominio

Riesgos reales de HSTS: Lista precargada

- "(Be) sure that you can support HTTPS for the long term."
- ¿Eliminar un dominio de la lista precargada de HSTS? 😊
 - <https://hstspreload.appspot.com/#removal>
- "... but it'll take months to take effect." (¿en todos los navegadores?)
 - Ej. Cambio de proveedor de *hosting* sin soporte de HTTPS
 - "Remove website from HSTS list" (issue: 467486)
 - <https://bugs.chromium.org/p/chromium/issues/detail?id=467486>
 - "Allow dynamic HSTS knockout values (max-age=0) to override preload list"
 - <https://bugs.chromium.org/p/chromium/issues/detail?id=454055>

Can I use... HSTS?

[Showing All]

- Chrome 4
 - URL: `chrome://net-internals/#hsts`
- Firefox 4 (Firefox 17: HSTS preload list)
 - URL: <https://www.elevenpaths.com/es/labstools/pin-patrol-2/index.html>
 - SiteSecurityServiceState.txt
- Safari 7 (OS X Mavericks)
 - Fichero: `~/Library/Cookies/HSTS.plist` (lista precargada & dinámicos)
- IE11 (Win 7 & 8.1 + KB3058515 – June 2015)
- IE11 & Edge 12 (Win 10)
- Opera 12.1

<http://caniuse.com/#search=hsts>

DEMO

¿Quién está usando HSTS?

- Netcraft's SSL Survey (Marzo 2016)
 - **5%** (de todos los sitios web HTTPS)
- Uso incorrecto de HSTS
 - Un valor de "max-age=0" (para anular la política HSTS) sólo tendrá éxito si el cliente web vuelve a conectarse al servidor

<https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html>

Referencias HSTS

- <https://scotthelme.co.uk/hsts-the-missing-link-in-tls/>
- <https://scotthelme.co.uk/manually-enforcing-hsts-chrome/>
- <https://scotthelme.co.uk/hsts-preload-test/>
- <https://scotthelme.co.uk/hsts-cheat-sheet/>
- <https://www.troyhunt.com/understanding-http-strict-transport/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>
- https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet
- https://raymii.org/s/tutorials/HTTP_Strict_Transport_Security_for_Apache_NGINX_and_Lighttpd.html



CSP

Content Security Policy (CSP)

- Definir la política general de seguridad de los contenidos del sitio web
 - XSS, Clickjacking (X-Frame-Options), etc.
- Ejemplo: Restringir contenidos mixtos granularmente por tipo de contenido
 - No cubierto por HSTS

```
Content-Security-Policy[-Report-Only]: default-src https:; form-action  
https:; connect-src https: wss:; font-src https: data:; frame-src  
https:; img-src https: data:; media-src https:; object-src https:;  
script-src 'unsafe-inline' 'unsafe-eval' https:; style-src 'unsafe-  
inline' https:; [report-uri "<URL>"]
```

Preferiblemente crear una política CSP más completa...

CSP: Upgrade Insecure Requests (Tolerante)

- Evitar contenidos mixtos: HTTPS y HTTP
 - Indicarle al navegador web que actualice las referencias HTTP a HTTPS antes de obtenerlas
 - Facilitar la migración de todos los contenidos "http://" a "https://"
 - Progresivamente, ir modificando los contenidos (bases de datos, etc.)
- Cabecera HTTP CSP - Upgrade Insecure Requests (más tolerante)

```
Content-Security-Policy: upgrade-insecure-requests; default-src https;;  
Content-Security-Policy-Report-Only: default-src https;; report-uri  
"<URL>"
```

- Cabecera HTTP en los clientes web (indica preferencia y soporte)
 - <http://caniuse.com/#feat=upgradeinsecurerequests>

```
Upgrade-Insecure-Requests: 1
```

CSP: Block All Mixed Content (Intolerante)

- Evitar contenidos mixtos: HTTPS y HTTP
 - Bloquear la carga de contenidos mediante HTTP si la página ha sido obtenida mediante HTTPS
- Cabecera HTTP CSP - Block All Mixed Content (más radical)
 - Usar Upgrade Insecure Requests o Block All Mixed Content, no ambas
 - BAMC no aplica si existe UIR

```
Content-Security-Policy: block-all-mixed-content;
```

Referencias CSP

- CSP
 - https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
 - <https://scotthelme.co.uk/content-security-policy-an-introduction/>
 - <https://scotthelme.co.uk/migrating-from-http-to-https-ease-the-pain-with-csp-and-hsts/>
- Upgrade Insecure Requests & Block All Mixed Content
 - <https://w3c.github.io/webappsec-upgrade-insecure-requests/>
 - <https://w3c.github.io/webappsec-mixed-content/>
 - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy#Other_directives
 - <https://googlechrome.github.io/samples/csp-upgrade-insecure-requests/>
- Subresource Integrity (SRI) - Integración de contenidos de terceros (ej. CDN)
 - https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
 - <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/require-sri-for>



HPKP

HPKP

HTTP Public Key Pinning (HPKP o PKP)

- RFC 7469 (Abr 2015)
 - <https://tools.ietf.org/html/rfc7469>
- Cabecera HTTP HPKP

```
Public-Key-Pins: pin-sha256="<base64-A==>" ; pin-sha256="<base64-B==>" ;  
max-age=5184000 [; includeSubdomains][; report-uri="<URL>"]
```

- Elimina la confianza en las CAs (PKI) – ataques MitM
- Certificate Pinning empleado en las aplicaciones móviles (apps)
- Pruebas:

```
Public-Key-Pins-Report-Only: pin-sha256="..." ; report-uri="..."
```

 - PINs ignorados para CAs raíz importadas por el usuario (Chrome/Firefox)

"Cualquier CA "reconocida" puede emitir un certificado válido para cualquier sitio web"

Creación del PIN principal para HPKP

- Subject Public Key Information (SPKI) *fingerprint*, codificado en base64
 - pin-sha256
 - OpenSSL: A partir del fichero de certificado (CRT) o del sitio web o ...

```
$ openssl x509 -in dinosec.crt -pubkey -noout | openssl rsa -pubin -
outform der | openssl dgst -sha256 -binary | openssl enc -base64
nWyZlrCxEOvbXKMg2oVL822wc77tS6/r0+mYbnxNy1k=
$ openssl s_client -servername www.dinosec.com -connect
www.dinosec.com:443 | openssl x509 -pubkey -noout | openssl rsa -pubin
-outform der | openssl dgst -sha256 -binary | openssl enc -base64
```

- Múltiples PINs (mínimo dos: clave pública de producción y de *backup*)
 - Renovación de la clave pública del servidor tras un incidente de seguridad

Creación del PIN de *backup* para HPKP

- Crear la nueva clave, y la *Certificate Signing Request* (CSR) asociada

```
$ openssl genrsa -out dinosec_bak.key 2048  
$ openssl req -new -sha256 -key dinosec_bak.key -out dinosec_bak.csr
```

- pin-sha256 de *backup* (no debe estar en la cadena de confianza actual)
- OpenSSL: A partir del fichero de la clave o de la CSR... (como antes)

```
$ openssl rsa -in dinosec_bak.key -outform der -pubout | openssl dgst -  
sha256 -binary | openssl enc -base64  
fcLC/4L/wODZxineWZuO10HKTZGRgqMsaRfMy6ddwy0=  
$ openssl req -in dinosec_bak.csr -pubkey -noout | openssl rsa -pubin -  
outform der | openssl dgst -sha256 -binary | openssl enc -base64
```

- Convertir la nueva clave en un nuevo certificado firmado por la CA
 - Listo para ser puesto en producción en caso de ser necesario

HPKP Report-URI

Desarrollar código propio o ...

- Report URI: <https://report-uri.io> (Registrar cuenta)
 - Scott Helme
 - CSP & HPKP
- HPKP violation report: HTTP POST - JSON (múltiples campos)
 - <http://tools.ietf.org/html/rfc7469#section-3>
- HPKP Toolset: <https://scotthelme.co.uk/hpkp-toolset/>
 - <https://report-uri.io/home/tools>
 - Create your HPKP hash (URL): https://report-uri.io/home/pkp_hash
 - Fichero: https://report-uri.io/home/pubkey_hash
 - Analyse your HPKP policy: https://report-uri.io/home/pkp_analyse



TOFU: Trust On First Use

- Objetivo: Evitar ataques con certificados de confianza válidos (CAs) pero ilegítimos (no autorizados por la organización)
- HPKP: El navegador web acepta el primer PIN (la primera clave pública) que obtiene para un servidor concreto
- Solución: No hay "lista precargada" ($\approx$ HSTS)
 - Lista de PINs interna de Chrome/Firefox: "static_spki_hashes"



Can I use... HPKP?

[Showing All]

- Chrome 38 (Oct'14) ("...-Report-Only" desde Chrome 46)
 - URL: chrome://net-internals/#hsts (& hpkp)
- Firefox 35 (Ene'15) (sin soporte para "...-Report-Only" – Bug: 1091177)
 - URL: <https://www.elevenpaths.com/es/labstools/pin-patrol-2/index.html>
- Safari 10
- IE11
- Edge (En estudio...)
- Opera 25

<http://caniuse.com/#search=hpkp>

 DEMO

Riesgos de HPKP (1/2)

- DoS – Ej. (Mobile) Barclays Bank (Nov 2016)
 - <https://cabforum.org/pipermail/public/2016-November/008989.html>
- Comenzar con "Public-Key-Pins-Report-Only"
 - Monitorizar "report-uri"
 - Enviar "violation reports" a otro dominio (también se aplica HPKP)
 - Inicialmente sólo en un recurso concreto (evitar ∞ "violation reports")
- Cambiar a "Public-Key-Pins" y comenzar con un "max-age" pequeño
 - Incrementarlo progresivamente
 - Monitorizar "report-uri"
- "No" poner el PIN de la CA emisora
- HPKP no protege frente a la manipulación local de las CAs



Note: While the example below shows how to set a pin on a server certificate, it is recommended to place the pin on the intermediate certificate of the CA that issued the server certificate, to ease certificates renewals and rotations.



Riesgos de HPKP (2/2)

- Si se incluye el PIN de la CA (raíz o intermedia)
 - ¿Qué ocurre si la CA decide usar una cadena de confianza distinta para los nuevos certificados?
- Si se incluye un PIN de *backup* asociado a una nueva clave pública
 - ¿Qué ocurre si se pierde?
 - ¿Qué ocurre si no es válido para generar un nuevo certificado cuando es necesario hacer uso del mismo (ej. nueva vulnerabilidad tecnológica)?
- Let's Encrypt genera (por defecto) un nuevo par de claves cada vez que se renueva el certificado: ¡Cuidado con HPKP y los PINs!
 - <https://ithenrik.com/blog/posts/activating-http-public-key-pinning-hpkp-on-lets-encrypt>
- *RansomPKP*

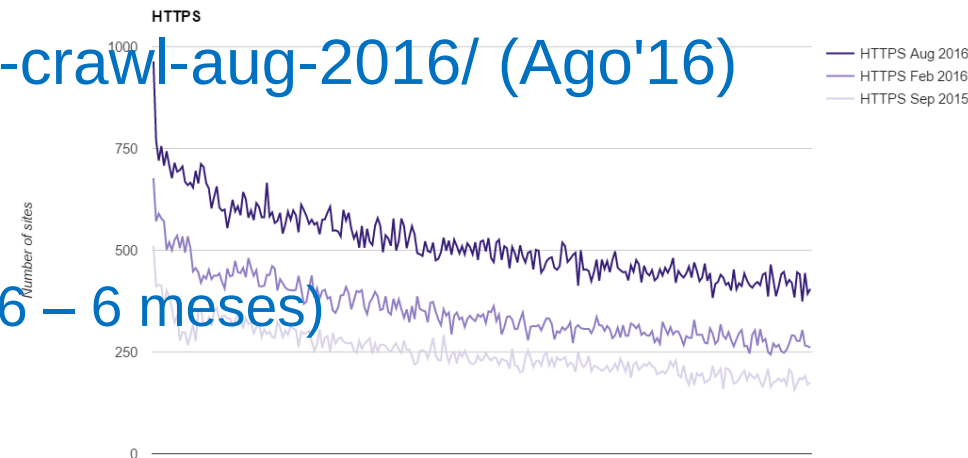
¿Quién está usando HPKP? (1/2)

- Netcraft's SSL Survey (Marzo 2016)
 - **0,09%** (< 4.100 sitios web; correctamente < 3.000 sitios web)
- Uso incorrecto de HPKP
 - Valor de "max-age" demasiado pequeño (segundos o minutos)
 - Utilización de un solo PIN ("pin-sha256") – 25%
 - Utilización de dos PINs ("pin-sha256"), pero ambos en la cadena de confianza actual (sin PIN de *backup*)
 - Sintaxis incorrecta de la cabecera HPKP
 - Políticas HPKP sobre HTTP (no HTTPS)
 - "report-uri" apuntando (HTTPS) al mismo sitio web que emplea HPKP

<https://news.netcraft.com/archives/2016/03/30/http-public-key-pinning-youre-doing-it-wrong.html>

¿Quién está usando HPKP? (2/2)

- Alexa Top 1 Million (Febrero 2016 & Agosto 2016)
 - <https://scotthelme.co.uk/security-headers-alexa-top-million/> (Feb'16)
 - HPKP: **249**
 - HSTS: 22.078
 - HTTPS: 88.199 (+42% desde agosto 2015 – 6 meses)
 - De un 6,7% a un 9,4%
 - <https://scotthelme.co.uk/alexa-top-1-million-crawl-aug-2016/> (Ago'16)
 - HPKP: **375**
 - HSTS: 29.908
 - HTTPS: 129.149 (+46% desde febrero 2016 – 6 meses)
 - De un 9,4% a un 13,7%



Referencias HPKP

- <https://scotthelme.co.uk/hpkp-http-public-key-pinning/>
- <https://scotthelme.co.uk/demonstrating-hpkp-validation-failures/>
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning
- <https://noncombatant.org/2015/05/01/about-http-public-key-pinning/>
- <https://developers.google.com/web/updates/2015/09/HPKP-reporting-with-chrome-46>
- <https://timtaubert.de/blog/2014/10/http-public-key-pinning-explained/>
- https://raymii.org/s/articles/HTTP_Public_Key_Pinning_Extension_HP KP.html
- <https://labs.detectify.com/2016/07/05/what-hpkp-is-but-isnt/>
- <https://news.netcraft.com/archives/2016/03/22/secure-websites-shun-http-public-key-pinning.html>
- <https://news.netcraft.com/archives/2016/03/30/http-public-key-pinning-youre-doing-it-wrong.html>
- <https://blog.qualys.com/ssllabs/2016/09/06/is-http-public-key-pinning-dead>
- <https://scotthelme.co.uk/using-security-features-to-do-bad-things/>
- TLS Server Identity Pinning w/ Tickets: <https://tools.ietf.org/html/draft-sheffer-tls-pinning-ticket-03>
- TACK: <http://tack.io>



Clientes HTTPS

Navegadores web: Tradicionales (¿y móviles?)

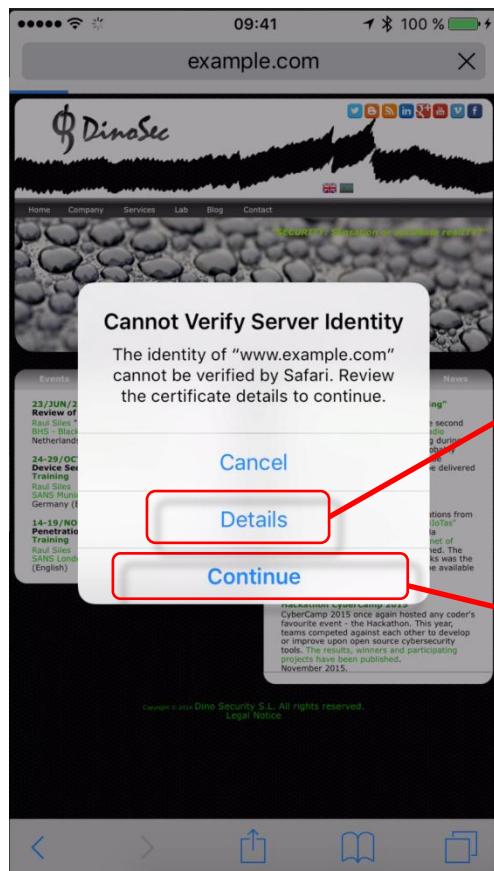
- "Informe Buenas Prácticas: CCN-CERT BP-06/16 Navegadores web"
 - Utilizar siempre un navegador web actualizado
 - Soporte para nuevas cabeceras HTTP de seguridad
 - Hacer uso de HTTPS: HSTS y HTTPS Everywhere
 - Revisar cuidadosamente alertas o errores en la validación de certificados
 - "Certificate Pinning" (frente a ataques MitM)
 - ...

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-buenas-practicas-bp/1801-ccn-cert-bp-06-16-navegadores-web/file.html>

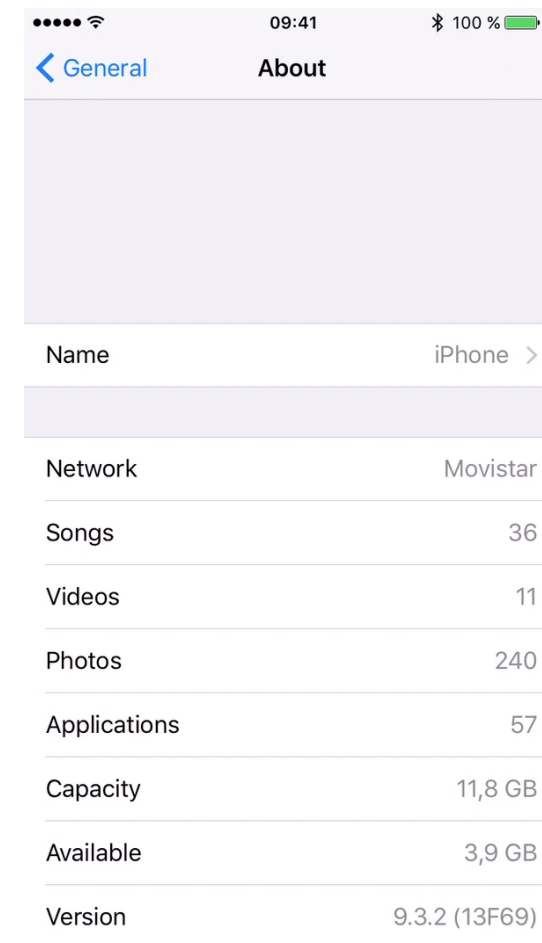
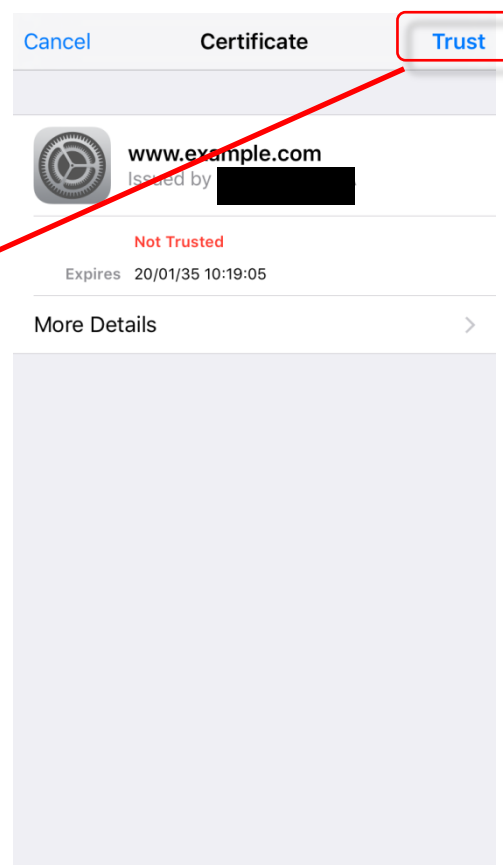


Navegadores web: Móviles

- iOS: Mobile Safari – Gestión de certificados en iOS



The double button
of
mass destruction!!





Aplicaciones Móviles (Apps): Android

- Android 6.x (M): Manifest
 - `android:usesCleartextTraffic [ = true ]`
 - Por defecto permite tráfico sin cifrar (HTTP)
 - <http://android-developers.blogspot.com.es/2016/04/protecting-against-unintentional.html>
- Android 7.x (N): Manifest + `res/xml/network_security_config.xml`
 - Network Security Configuration
 - Definir CAs y escenarios de confianza
 - Certificate pinning
 - Hacer sólo uso de HTTPS
 - <https://developer.android.com/preview/features/security-config.html>



Aplicaciones Móviles (Apps): iOS

- Apple App Transport Security (ATS) introducido en iOS 9 (2015)
- Junio 2016: WWDC 2016 - Session 706: "What's New in Security"
 - *"Today, I'm proud to say that at the end of 2016, App Transport Security (ATS) is becoming a requirement for App Store apps"*
 - Apple's head of security engineering and architecture, Ivan Krstic
 - Requisitos: TLS 1.2, Forward Secrecy,
 - Mínimos: RSA 2.048 bits o ECC 256 bits y SHA-256
- Enero 2017: ATS obligatorio
 - Proceso de revisión estricto para permitir excepciones ATS
 - <https://forums.developer.apple.com/thread/48979>





Conclusiones

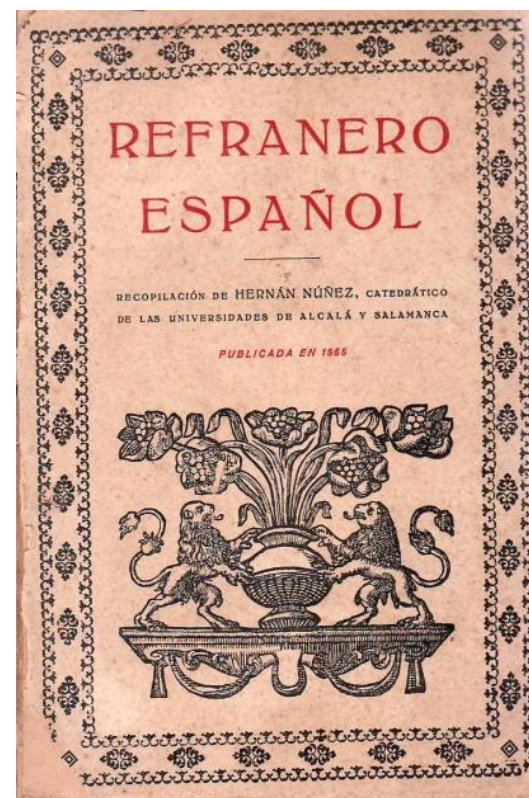
Ponerlo más difícil...



El refranero español

Y dónde uno dice cifrar, dice autentificar, etc. ("HTTPSear")

“No dejes para
mañana lo que
puedas **cifrar**
hoy...”



Estrategia para "HTTPSear" las organizaciones en 2017

- Designar una persona dedicada a "HTTPSear" la organización en 2017
 - ¿Os parece mucho? ¿Cuánta gente tenéis en seguridad física...?
- Empezar por...
 - Aplicaciones y servicios web (principales y secundarios)
 - Empezar al menos por los externos (y continuar con los internos)
 - Aplicaciones móviles (apps)
 - Clientes/Navegadores web (tradicionales y móviles)
 - Internet of Things (IoT)...
- Identificar la implementación de TLS (y versión) de todos los servicios
 - Tipo de servidor & OpenSSL, BoringSSL, LibreSSL, BearSSL, picotls, Microsoft SSL/TLS, etc.

Gestión de incidentes y monitorización

¿Qué aprendimos de vulnerabilidades pasadas como...?

- ... Heartbleed
 - Actualización urgente de la implementación TLS
 - Renovación urgente de todos los certificados digitales
- Nuevas vulnerabilidades de diseño o implementación
 - Modificación "urgente" de los algoritmos de cifrado e integridad
- HPKP
 - Sustitución urgente de la clave (PIN) y el certificado digital asociado
- Diseñar y/o adaptar los mecanismos de monitorización
 - Cortafuegos, WAF, IDS, IPS, etc.
 - TLS 1.3: Fin de RSA (!FS) en el intercambio de claves (¿descifrado?)



Cabeceras HTTP y otras tecnologías de seguridad

- Security Headers: Otras cabeceras HTTP de seguridad
 - <https://securityheaders.io>
 - Scott Helme
 - Content-Security-Policy, X-Content-Type-Options, X-Frame-Options y X-XSS-Protection + Strict-Transport-Security, Public-Key-Pins
 - Scores: <https://scotthel.me/stsh>
- Hardenize: Implementación de los últimos estándares de seguridad
 - <https://www.hardenize.com> (alpha)
 - Ivan Ristic & Scott Helme (et. al.)

securityheaders.io



¡Muchas gracias!

¿Preguntas?



Raúl Siles

Fundador & Analista de Seguridad

raul@dinosec.com



www.dinosec.com

[@dinosec](https://twitter.com/dinosec)

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

