Certificate Pinning

¿Tenemos el c...ertificado roto?

SEGU.INFO
SEGURIDAD DE LA INFORMACION

Lic. Cristian Borghello, CISSP – CCSK – MVP
www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

OWASP LATAM 2015
LATIN AMERICA TOUR

Sobre Cristian Borghello

- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (Certified Information Systems Security Professional) desde 2008
- Microsoft MVP Security (Most Valuable Professional) desde 2010
- CCSK (Certificate of Cloud Security Knowledge) desde 2014
- Creador y Director de Segu-Info
- Consultor independiente en Seguridad de la Información

Línea de tiempo

07/1988 X.509 1.0

06/1991 PGP 1.0

05/ 1995 PGP 2.6.2i

02/1995 SSL 2.0

12/1998 OpenSSL

05/2008
RFC 5280

X.509 v3

01/1999 TLS 1.0

GPG 1.0

999 OpenSSH

08/2000 PGP 6.5.8

GPG

```
root@kali:/pentest/cert/gpg# gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software
```

```
root@kali:/pentest/cert/gpg# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   1024R/A07B732A 2014-10-14
uid                  Cristian Borghello <info@segu-info.com.ar>
sub   1024R/13533FE3 2014-10-14

root@kali:/pentest/cert/gpg# gpg -r A07B732A -e secreto.txt
```

```
kali:/pentest/cert/gpg# hexdump -C secreto.txt.gpg
000  84 8c 03 77 a4 c0 82 13  53 3f e3 01 03 fc 0f af  |...w....S?......|
```

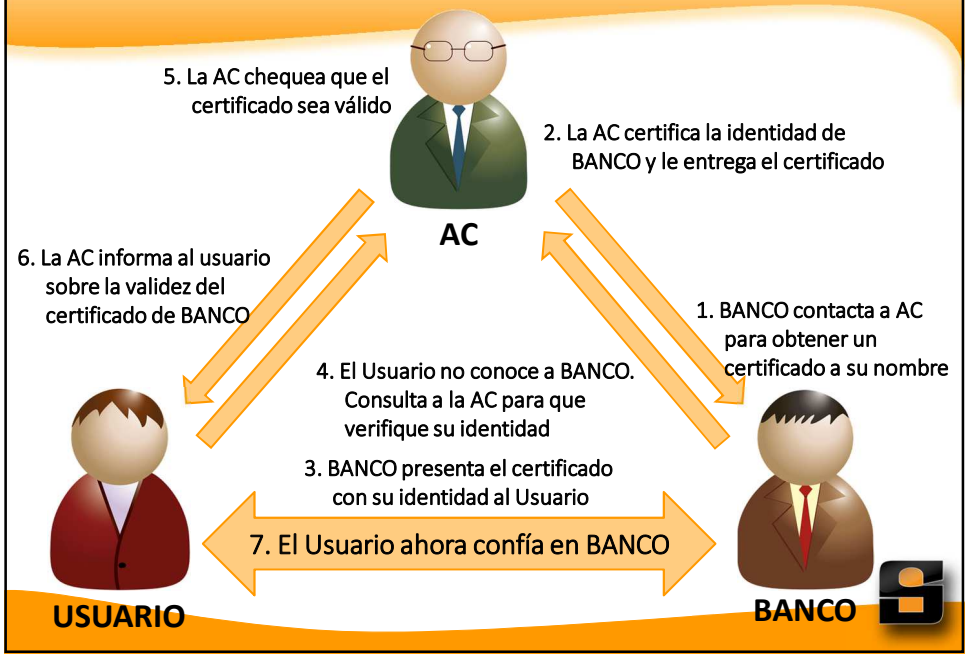
```
root@kali:/pentest/cert/gpg# gpg -d secreto.txt.gpg

You need a passphrase to unlock the secret key for
user: "Cristian Borghello <info@segu-info.com.ar>"
1024-bit RSA key, ID 13533FE3, created 2014-10-14 (main key ID A07B732A)

gpg: encrypted with 1024-bit RSA key, ID 13533FE3, created 2014-10-14
      "Cristian Borghello <info@segu-info.com.ar>"
```

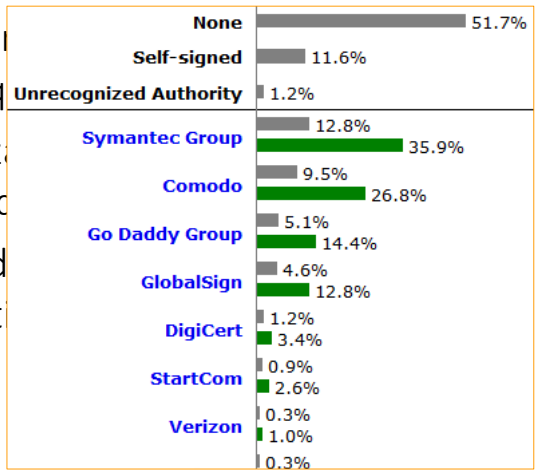
```
w/367sEqVl0mojXYEPapf9GouB5VXbqwKOOXGvvuZCzz0i8vgv4lPhew47jsWFtT
U41s
=GhzT
-----END PGP MESSAGE-----
```

Autoridad de Certificación



Autoridad de Certificación

- Organismos encar
  Digitales de cualq
- Entidades autoriz
  generan certificac
- En cada certificad
  (*issuer*) como ent
  certificado



http://w3techs.com/technologies/overview/ssl_certificate/all

¿Confianza?

¿Cómo saber si el certificado descargado es real y no se ha generado de forma fraudulenta?

- Verificando la Autoridad de Certificación (*issuer*) y los certificados involucrados en la cadena
- Si un certificado se ha firmado por una Autoridad de Certificación de confianza se establece una cadena de confianza
- Esta información está almacenada en los navegadores

Confianza del Emisor

- Los campos del emisor (*issuer*) pueden parecer útiles para identificar la entidad pero…
- Pueden ser establecidos a gusto, por lo que **no suponen ninguna garantía** de procedencia y autenticidad del Certificado Digital

fail

Confianza del Emisor

```
root@kali:/pentest/cert# openssl req -new -newkey rsa:2048 -nodes -keyout servido
r.key -out servidor.csr
Generating a 2048 bit RSA private key
.....................................................+++
.......................................+++
writing new private key to 'servidor.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
-----
Country Name (2 letter code) [AU]:AR
State or Province Name (full name) [Some-State]:Bs As
Locality Name (eg, city) []:Bs As
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Segu-Info
Organizational Unit Name (eg, section) []:Bla bla
Common Name (e.g. server FQDN or YOUR name) []:bla bla bla
```

cert_override.txt

```
# PSM Certificate Override Settings file
# This is a generated file!  Do not edit.
www.securecoding.cert.org:443   OID.2.16.840.1.101.3.4.2.1
0D:07:EB:57:48:1B:E7:D0:A7:A4:E7:4B:51:C9:EF:43:92:75:9D:95:2C:FD:2A:8A:04:DA:4F:60:
9A:3E:F4:3A U   AAAAAAAAAAAAAAAQAAAAmUeTPsM1MraGV0NiU6B/j2kwgZYxCzAJBgNVBAYTAkdC
MRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAOBgNVBAcTB1NhbGZvcmQx
GjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMTwwOgYDVQQDEzNDT01PRE8gU1NB
IE9yZ2FuaXphdGlvbiBWYWxpZGF0aW9uIFNlY3VyZSBTZXJ2ZXIgQ0E=
```

https://dev.mozilla.jp/localmdc/localmdc_822.html

Cadena de confianza jerárquico

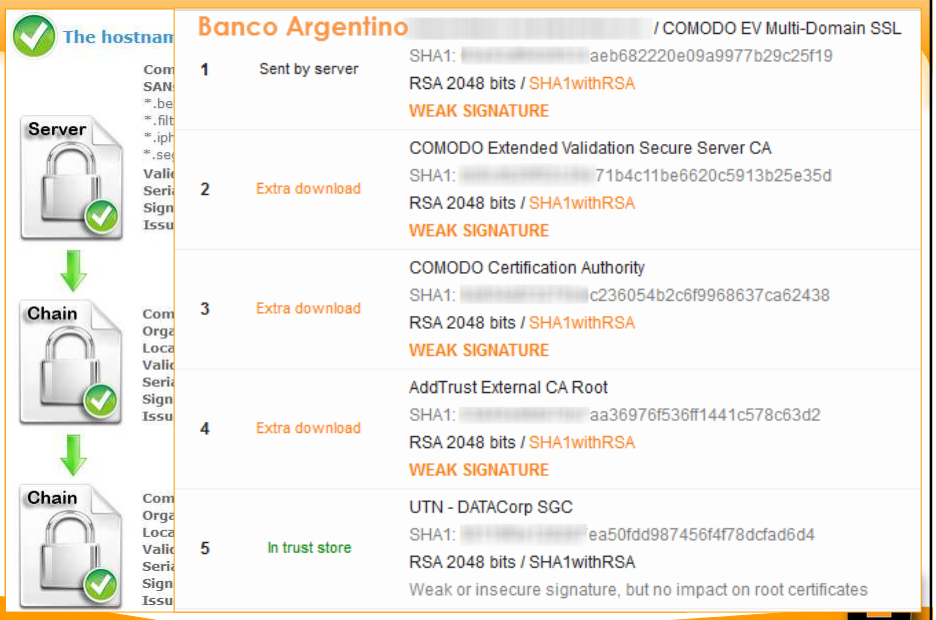
Jerarquía de Certificados

- Builtin Object Token:Equifax Secure CA
  - GeoTrust Global CA
    - Google Internet Authority G2
      - *.blogger.com

Jerarquía de Certificados

- GTE CyberTrust Global Root
  - Baltimore CyberTrust Root
    - DigiCert High Assurance EV Root CA
      - DigiCert High Assurance CA-3

Cadena de confianza jerárquico



¿Entidades de confianza?

VeriSign Secured

03/2001: emitió dos certificados a alguien que se hizo pasar por personal de Microsoft

03/2011: uno de sus *partners* fue comprometido y se firmaron certificados sin la correspondiente verificación

C·O·M·O·D·O AUTHENTIC SITE SECURED BY SSL

DigiNotar Internet Trust Services

fail

09/2011: s[illegible] su seguridad y se ge[illegible] certificados falsos

01/2013: emitió dos certificados de CA subordinada y esta uno para *.google.com

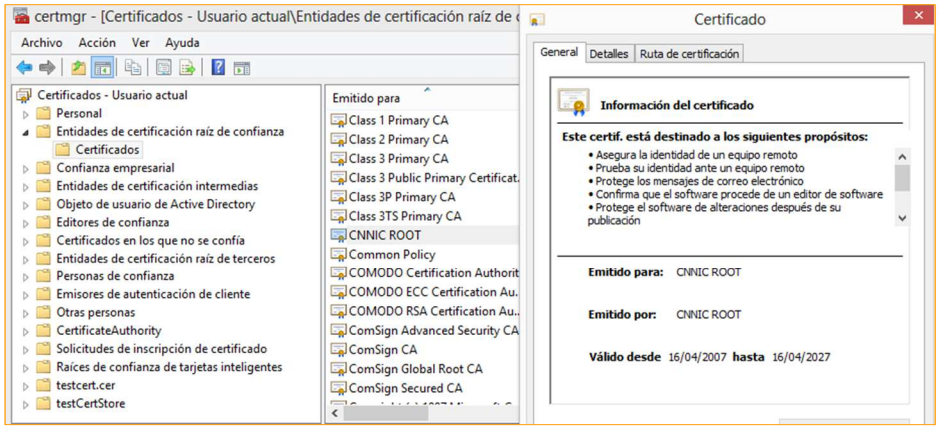
TURKTRUST

Emitieron un certificado para **live.fi** (MS), a través de [illegible] administración mal configurado

03/2015

MCS Holdings (China) [illegible] certificados falsos en nombre de Google

¿Entidades de confianza?



Vulnerabilidades (IV)

- 2011 BEAST
- 2012 CRIME
- 2013
  - BREACH
  - Lucky13
- 2014
  - HeartBleed
  - POODLE
  - ShellShock
- 2015
  - Freak
  - Bar Mitzvah

http://resources.infosecinstitute.com/beast-vs-crime-attack/
https://community.qualys.com/blogs/securitylabs/2011/10/17/mitigating-the-beast-attack-on-tls
https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls
http://www.isg.rhul.ac.uk/tls/Lucky13.html
https://community.qualys.com/blogs/securitylabs/2013/08/07/defending-against-the-breach-attack
http://blog.segu-info.com.ar/2014/09/faq-de-shellshock-exploit-rce-ddos.html
http://blog.segu-info.com.ar/2015/03/bar-mitzvah-attack-otro-ataques-rc4.html

CRL y OSCP

- Las CA utilizan dos protocolos para ofrecer a los mecanismos de validación y revocación de certificados:
  - CRL (*Certificate Revocation List*)
  - OCSP (*Online Certificate Status Protocol*)

CRL (Certificate Revocation List)

- Para validar un certificado, se descarga la lista CRL actualizada del repositorio de la CA, se verifica la validez de la firma, y se comprueba el identificador del certificado
- Si el certificado se encuentra en la CRL (está revocado), no es aceptado como válido
- La CRL se publica periódicamente y almacena localmente
- Si se emplea una versión obsoleta de CRL se podría considerar válido un certificado que ya no lo es
- **Nota:** MS además usa *Certificate Trust List (CTL)*

http://support2.microsoft.com/kb/931125/en-us

CRL (Certificate Revocation List)

Verificación del certificado revocado de **Malayan Banking**, el mayor banco y grupo financiero de Malasia

```
root@kali:/pentest/cert# wget http://SVRIntl-G3-crl.verisign.com/SVRIntlG3.crl
root@kali:/pentest/cert# openssl x509 -in maybank.crt -noout -serial
serial=14394B794CEBA750CE1648189AF06049
root@kali:/pentest/cert# nano maybank.crt
root@kali:/pentest/cert# grep "14 39 4B 79" SVRIntlG3.txt
131455     16:         INTEGER 14 39 4B 79 4C EB A7 50 CE 16 48 18 9A F0 60 49
```

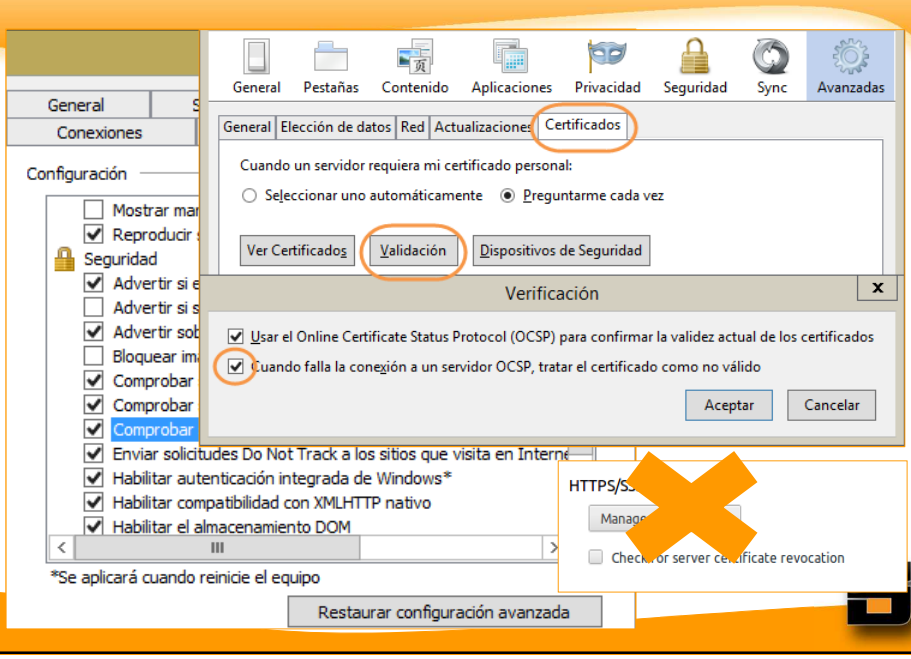
http://toolbar.netcraft.com/site_report?url=https://emdm.maybank.com.my

OSCP (Online Certificate Status Protocol)

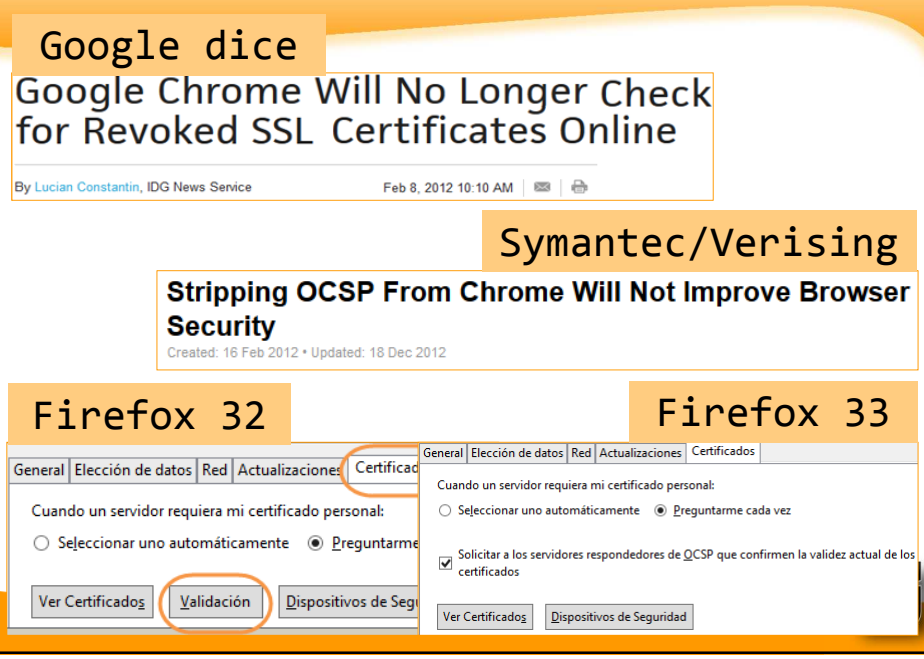
- OCSP (RFC 2560) elimina la necesidad de que los clientes tengan que obtener y procesar las CRL, pero requiere conexión permanente con el *"OCSP Responder"*
- Se realiza una petición con el identificador del certificado que se requiere validar

http://randomoracle.wordpress.com/2009/07/31/ocsp-this-fail-brought-to-you-by-the-number-three/

OSCP en los navegadores



Estado actual de CRL y OCSP



HSTS (HTTP Strict Transport Security)

- HSTS (RFC 6797) es una política por la cual el servidor indica al navegador que sólo deben interactuar a través de HTTPS
- La política HSTS se comunica a través del campo HTTP *"Strict-Transport-Security" y se* especifica un período de tiempo
- La cabecera HSTS sólo se debe enviar a través de HTTPS y no cuando se utiliza HTTP *(mmm...)*

http://tools.ietf.org/html/rfc6797
https://crypto.stanford.edu/forcehttps/
https://hstspreload.appspot.com/

Funcionamiento de HSTS

1. La primera vez se realiza una petición HTTPS
2. Luego, el browser realiza una petición HTTP al servidor (podría ser HTTPS)
3. Si el servidor devuelve HSTS, se redirecciona a HTTPS:// durante el tiempo especificado
4. Si el certificado es "confiable" se continúa
5. Si la seguridad de la conexión no se puede asegurar, se informa al usuario y no se permite el ingresa al sitio

Nota: En [1], se podría utilizar HTTPS EveryWhere para garantizar siempre el ingreso vía HTTPS

Campo HSTS

```
GET / HTTP/1.1
Host: www.segu-info.com.ar:443
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
Accept-Encoding: gzip,deflate
Accept-Language: es-ES,es;q=0.8
Cookie: __cfduid=dde14f2971adc59a5b7f033c2c1382d651412441031951; __utmt=1;
__utmb=221750938.6.10.1413229937; __utmc=221750938; __utmz=221750938.141244
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML,

HTTP/1.1 200 OK
age: 0
cf-ray: 178e1ad0ad550880-IAD
content-encoding: gzip
content-type: text/html;charset=UTF-8
date: Mon, 13 Oct 2014 19:57:11 GMT
server: cloudflare-nginx
set-cookie2: WS_Tracker=af02bbcb.505531d50df1a; path=/
status: 200 OK
strict-transport-security: max-age=16070400; includeSubdomains; preload
vary: Accept-Encoding,User-Agent
version: HTTP/1.1
```

Certificate Pinning

- **Pinning** es el proceso de asociar un Host con su respectivo certificado X.509 y/o su Clave Pública
- **Pinned"** → asociar certificado o Clave Pública
- Se asocia un certificado digital a un dominio concreto
- Como en SSH, cada Host se identifica a través de su PK
- El Pinning elimina la "confianza en el otro": una aplicación "pineada" no necesita confiar en un tercero (se vuelve a confiar en los pares)
- El pineo se agrega en el primer encuentro entre el cliente y el servidor

https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
https://www.owasp.org/index.php/Pinning_Cheat_Sheet
https://tools.ietf.org/html/draft-ietf-websec-key-pinning

```
root@kali:/pentest/cert# openssl x509 -in GeoTrust.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 144470 (0x23456)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA
        Validity
            Not Before: May 21 04:00:00 2002 GMT
            Not After : May 21 04:00:00 2022 GMT
        Subject: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:da:cc:18:63:30:fd:f4:17:23:1a:56:7e:5b:df:
                    3c:6c:38:e4:71:b7:78:91:d4:bc:a1:d8:4c:f8:a8:
                    43:b6:03:e9:4d:21:07:08:88:da:58:2f:66:39:29:
                    bd:05:78:8b:9d:38:e8:05:b7:6a:7e:71:a4:e6:c4:
                    60:a6:b0:ef:80:e4:89:28:0f:9e:25:d6:ed:83:f3:
                    ad:a6:91:c7:98:c9:42:18:35:14:9d:ad:98:46:92:
                    2e:4f:ca:f1:87:43:c1:16:95:57:2d:50:ef:89:2d:
                    80:7a:57:ad:f2:ee:5f:6b:d2:00:8d:b9:14:f8:14:
                    15:35:d9:c0:46:a3:7b:72:c8:91:bf:c9:55:2b:cd:
                    d0:97:3e:9c:26:64:cc:df:ce:83:19:71:ca:4e:e6:
                    d4:d5:7b:a9:19:cd:55:de:c8:ec:d2:5e:38:53:e5:
                    5c:4f:8c:2d:fe:50:23:36:fc:66:e6:cb:8e:a4:39:
                    19:00:b7:95:02:39:91:0b:0e:fe:38:2e:d1:1d:05:
                    9a:f6:4d:3e:6f:0f:07:1d:af:2c:1e:8f:60:39:e2:
                    fa:36:53:13:39:d4:5e:26:2b:db:3d:a8:14:bd:32:
                    eb:18:03:28:52:04:71:e5:ab:33:3d:e1:38:bb:07:
                    36:84:62:9c:79:ea:16:30:f4:5f:c0:2b:e8:71:6b:
                    e4:f9
                Exponent: 65537 (0x10001)
    pin-sha1=base64(SHA1(SubjectPublicKeyInfo))
    pin-sha256=base64(SHA256(SubjectPublicKeyInfo))
```

Pinning en el código fuente *(Hardcoded)*

https://src.chromium.org/svn/branches/1312/src/net/base/transport_security_state_static.h

```
static const char kSPKIHash_GeoTrustGlobal[] =
  "sha1/wHqYaI2J+6sFZAwRfap9ZbjKzE4=";
```

A

Mozilla Foundation (US) | https://mxr.mozilla.org/mozilla-central/source/security/manager/boot/src/StaticHPKPins.h

```
155 static const char kGTE_CyberTrust_Global_RootFingerprint[] =
156   "EGn6R6CqT4z3ERscrqNl7q7RC//zJmDe9uBhS/rnCHU=";
157
158 /* GeoTrust Global CA */
159 static const char kGeoTrust_Global_CAFingerprint[] =
160   "h6801m+z8v3zbgkRHpq6L29Esgfzhj89C1SyUCOQmqU=";
161
```

B

```
root@kali:/pentest/cert# python http_pins.py GeoTrust.crt
GeoTrust.crt:
* SPKI fingerprint (sha256): 87:af:34:d6:6f:b3:f2:fd:f3:6e:0
7:f3:86:3f:3d:0b:54:b2:50:23:90:9a:a5
* SPKI fingerprint (sha1): c0:7a:98:68:8d:89:fb:ab:05:64:0c:

Public-Key-Pins: max-age=600; pin-sha256="h6801m+z8v3zbgkRHp
; pin-sha1="wHqYaI2J+6sFZAwRfap9ZbjKzE4="
```

B

A

http://src.chromium.org/viewvc/chrome/trunk/src/net/http/transport_security_state_static.json

Probar Pinning en Chrome

chrome://net-internals/#hsts

HSTS capturing events (715)

Query domain

Input a domain name to query the current HSTS set:

Domain: google.com Query

Found:

domain: google.com
static_upgrade_mode: OPPORTUNISTIC
static_sts_include_subdomains: true
static_pkp_include_subdomains: true
static_sts_observed: 1412136506
static_pkp_observed: 1412136506
static_spki_hashes: sha1/vq7OyjSnqOco9nyMCDGdy77eijM=,sha1/Q9rWMO5T+KmAym79hfRqo3mQ4Oo=
dynamic_upgrade_mode: UNKNOWN

```
root@kali:/pentest/cert# python http_pins.py GiaG2.crt
GiaG2.crt:
* SPKI fingerprint (sha256): ec:72:29:69:cb:64:20:0a:b6:63:8f:
9:a6:48:56:61:04:2a:10:61:c4:61:27:76
* SPKI fingerprint (sha1): 43:da:d6:30:ee:53:f8:a9:80:ca:6e:fd

Public-Key-Pins: max-age=600; pin-sha256="7HIpactkIAq2Y49orFOO
; pin-sha1="Q9rWMO5T+KmAym79hfRqo3mQ4Oo="
```

https://src.chromium.org/chrome/trunk/src/net/http/transport_security_state_static.certs

```
GeoTrustGlobal
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSq
MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwY
aWZpY2F0ZSBBdXRob3JpdHkwHhcNMDI
WjBCMQswCQYDVQQGEwJVUzEWMBQGA1U
AxMSR2VvVHJ1c3QgR2xvYmFsIENBMII
CgKCAQEA2swYYzD99BcjGlZ+W988bDj
OSm9BXiLnTjoBbdqfnGk5sRgprDvgOS
T8rxh0PBFpVXLVDviS2Aelet8u5fa9I
JmTM386DGXHKTubU1XupGc1V3sjs014
Cw7+OC7RHQWa9k0+bw8HHa8sHo9gOeI
PeE4uwc2hGKceeoWMPRfwCvocWvk+QI
aPkr0rKV10fYIyAQTzOYkJ/UMB0GA1U
TjAPBgNVHRMBAf8EBTADAQH/MA4GA1U
```

```
root@kali:/pentest/cert# openssl x509 -in GeoTrustGlobalCA.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1227750 (0x12bbe6)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Equifax, OU=Equifax Secure Certificate Au
        Validity
            Not Before: May 21 04:00:00 2002 GMT
            Not After : Aug 21 04:00:00 2018 GMT
        Subject: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwYDVQQLEyRFcXVpZmF4IFNlY3VyZSBDZXJ0
aWZpY2F0ZSBBdXRob3JpdHkwHhcNMDIwNTIxMDQwMDAwWhcNMTgwODIxMDQwMDAw
WjBCMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNR2VvVHJlc3QgSW5iLjEbMBkGA1UE
```

https://chromium.googlesource.com/chromium/src/+/b4efad77d9b3a5a49b398052fbf43d51b906aea1/net/http/transport_security_state_stati

```
1381. { "name": "mountainmusicpromotions.com", "include_subdomains": true, "mode": "force
1382. { "name": "newstarnootropics.com", "include_subdomains": true, "mode": "force-https
1383. { "name": "onedot.nl", "include_subdomains": true, "mode": "force-https" },
1384. { "name": "powerplannerapp.com", "include_subdomains": true, "mode": "force-https"
1385. { "name": "ru-sprachstudio.ch", "include_subdomains": true, "mode": "force-https"
1386. { "name": "segu-info.com.ar", "include_subdomains": true, "mode": "force-https" },
1387. { "name": "slattery.co", "include_subdomains": true, "mode": "force-https" },
```

```
AHbhEm5OSxYShjAGsoEIz/AIx8dxfmbuwu3UOx//8PDITtZDOLC5MH0Y0FWDomrL
NhGc6Ehmo21/uBPUR/6LWlxz/K7ZGzIZOKuXNBSqltLroxwUCEm2u+WR74M26x1W
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
```

Public Key Pinning dinámico (HTTP)

- Nueva cabecera HTTP (*HPKP Header*) que permite a un servidor indicar cuáles son sus "certificados habituales" y su tiempo de validez
- Permite al dueño de un sitio declarar qué certificados le son propios
- Si se produce un ataque MitM y/o suplantación de certificados, el navegador avisa de que no se corresponde con el indicado por el servidor
- Aún no totalmente soportado por los *browsers*

https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21

Public Key Pinning dinámico (HTTP)

```
D:\>curl -k -i https://projects.dm.id.lv/s/pkp-testresult.html
HTTP/1.1 301 Moved Permanently
Date: Tue, 28 Oct 2014 19:28:26 GMT
Server: nginx
X-Content-Type-Options: nosniff
Vary: Accept-Encoding,Cookie,User-Agent
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: private, must-revalidate, max-age=0
Last-Modified: Tue, 28 Oct 2014 19:28:27 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
Public-Key-Pins: pin-sha256="8MfHQC9XAUF/XBmQ/mZ8S/XEc5aSYzOljOEHTj870+s="; pin-
sha256="tpFbv65QoYvcWNVl7gAEd1FAWWn/pjL8Fo2+f1pTrC8="; pin-sha256="WKbBsAclTiyDM
7EEJ5yUmrWmp9DxWM/hG+D+wcCLA24="; pin-sha256="nxpEakAMgSw92zkssp A8LdZyrdW/MGGr70
VfcIT7DBU="; max-age=31536000; includeSubDomains
Location: https://projects.dm.id.lv/s/pkp-testresult.html
Keep-Alive: timeout=30
```

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: segu-info.com.ar
Date: Sat, 01 Nov 2014 21:29:16 GMT
Content-Type: text/html;charset=UTF-8
Connection: keep-alive
Set-Cookie2: WS_Tracker=d0b1da3c.506d297f8bb9b; path=/
Strict-Transport-Security: max-age=60; includeSubdomains; preload
Public-Key-Pins: pin-sha256="CkyQ1Y4SwcNCm19Iy/8M1LYAFLsQtGwKeNN9ahvKsXA=";
Vary: Accept-Encoding,User-Agent
X-Varnish: 710102182
Age: 0
```

https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21

¿Quién pinea?

- **Chrome:** de forma nativa pinea desde su código fuente *(hardcoded)* y HPKP
- **Firefox:** a partir de su v32 pinea desde su código fuente y HPKP
- **IE:** pinea a través de EMET
- **Spartan (Windows 10):** nativo
- **Opera:** soportado desde la v26
- **Safari:** soportado desde OS X 10.9 y iOS 7

http://blogs.msdn.com/b/ie/archive/2015/02/16/http-strict-transport-security-comes-to-internet-explorer.aspx
https://www.veracode.com/blog/2014/03/security-headers-on-the-top-1000000-websites-march-2014-report/

Ejemplos de Pinning

https://pinningtest.appspot.com/

Ejemplos de Pinning

Firefox

https://www.google.com.ar/

Esta conexión no es de confianza

Ha solicitado a Firefox que conecte de forma segura a **www.google.com.ar**, pero no podemos confirmar que su conexión sea segura.

Normalmente, cuando se trata de conectar de forma segura, los sitios presentan un identificación

Firefox | about:config

Buscar: security.cert_pinning

Nombre Opción	Estado	Tipo	Valor
security.cert_pinning.enforcement_level	predeterminado	integer	1

How to use pinning

Starting with FF 32, it's on by default, so you don't have to do anything. The pinning level is enf

- 0. Pinning disabled
- 1. Allow User MITM (pinning not enforced if the trust anchor is a user inserted CA, default)
- 2. Strict. Pinning is always enforced.
- 3. Enforce test mode.

Ejemplos de Pinning

Internet Explorer - EMET

Certificate Trust Configuratior

Export | Add Website | Remove Website

File | Add / Remove

Protected Websites | Pinning Rules

Find | Clear

Active	Website	Pin Rule
☑	google.com	GoogleCA
☑	login.live.com	MSLiveCA

EMET 5.0

EMET detected that the SSL certificate for **"www.google.com.ar"** is not trusted by the rule **"GoogleCA"** associated with the domain **"www.google.com.ar"**

http://www.microsoft.com/en-us/download/details.aspx?id=43714

Otras propuestas y "soluciones" (I)

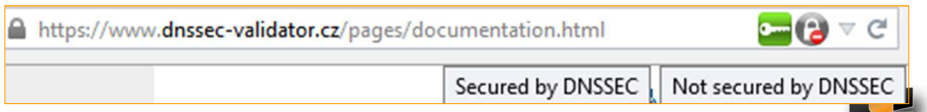
- Certificate Transparency (SCT): *framework* en desarrollo que permitiría tener un "log" público donde cada CA debe registrar los certificados emitidos para realizarle auditorías periódicas
- El propietario de un sitio puede consultar periódicamente qué certificados hay en circulación
  http://tools.ietf.org/html/rfc6962
  http://www.links.org/files/CertificateTransparencyVersion2.1a.pdf
  http://www.certificate-transparency.org/original-proposal

Otras propuestas y "soluciones" (II)

- Convergence: proyecto de Moxie (2011) que pretende sustituir las CA a través de un anillo de claves público llamados "notarios"
  http://convergence.io/
- TACK: proyecto de Moxie (2013) que pretende crear una extensión a TLS para permitir el registro de la cadena de certificación a nivel de conexión, sin CAs
  http://tack.io/draft.html

Otras propuestas y “soluciones” (III)

- DANE/TLSA: vincula TLS a dominios específicos. Se realizan modificaciones al protocolo DNS para vincular DNSSEC a los certificados y a los nombres de dominio
  http://tools.ietf.org/html/rfc6698
  http://dane.verisignlabs.com/ http://www.dnssec-validator.cz/
  https://www.huque.com/bin/gen_tlsa
  http://blog.huque.com/2012/10/dnssec-and-certificates.htm
  https://github.com/shuque/tlsa_rdata



Registro DNS TLSA

1. Generar registro DNS TLSA

```
openssl x509 -in huque.crt -outform DER | openssl sha256
(stdin) = 0013BEF11B875A58F3B0B1D7A0D439A608277F...
```

2. Actualizar registro DNS (nsupdate)

3. Consultar registro DNS TLSA

```
root@kali:# dig +dnssec +noall +answer +multi _443._tcp.www.huque.com. TLSA
_443._tcp.www.huque.com. 5 IN TLSA 3 0 1 (
                                0013BEF11B875A58F3B0B1D7A0D439A608277F58433B
                                BB12245B2A28B398C281 )
```

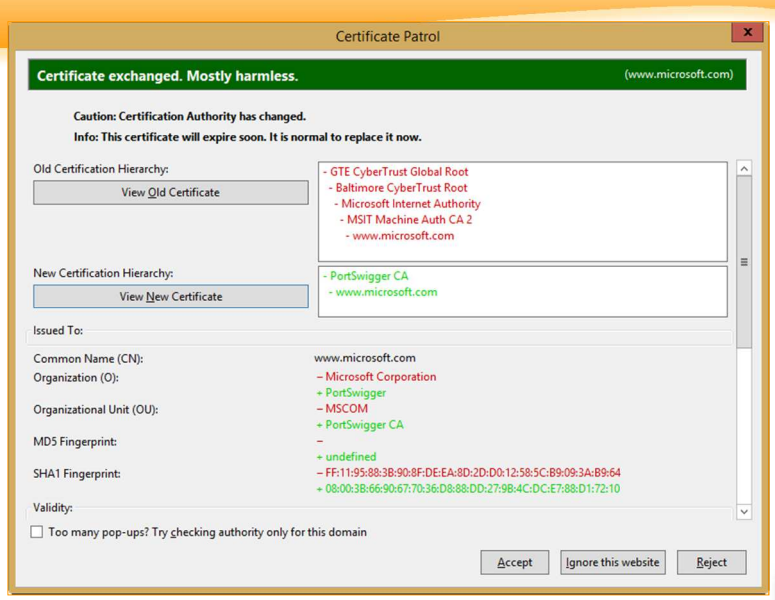
```
root@kali:/pentest/cert# dig +dnssec +noall +answer +multi type52 _443._tcp.good.d
ane.verisignlabs.com TLSA
;; Warning, extra type option
_443._tcp.good.dane.verisignlabs.com. 5 IN TLSA 3 0 1 (
                                0332AA2D58B3E0544B65656438937068BA44CE2F1446
                                9C4F50C9CC6933C808D3 )
root@kali:/pentest/cert# dig +dnssec +noall +answer +multi type52 _443._tcp.bad-ha
sh.dane.verisignlabs.com. TLSA
;; Warning, extra type option
_443._tcp.bad-hash.dane.verisignlabs.com. 5 IN TLSA 3 0 1 (
                                9999999999999999999999999999999999999999999999
                                9999999999999999999999 )
```

http://blog.huque.com/2012/10/dnssec-and-certificates.html

Otras propuestas y “soluciones” (IV)

- **SSLCOP:** herramienta que permite bloquear CAs que no son de interés debido a su procedencia geográfica
  http://www.securitybydefault.com/2012/03/sslcop-10.html
- **Certificate Patrol:** extensión que verifica cualquier modificación de la cadena de certificación
  https://addons.mozilla.org/en-US/firefox/addon/certificate-patrol/

Certificate Patrol



https://addons.mozilla.org/en-US/firefox/addon/certificate-patrol/

Conclusiones

- Las cadenas de certificación no son confiables
- Cada empresa crear su propia “solución” no compatible
- Cada una de las “soluciones” es vulnerable
- No se brinda un mensaje claro al usuario sobre lo que es “seguro”
- Es necesario un gran cambio, que además sea compatible con lo existente y fácil de entender