CLOUDFLARE

SHA-1 → SHA-2 TLS Migrations and new standards

Felipe Tribaldos

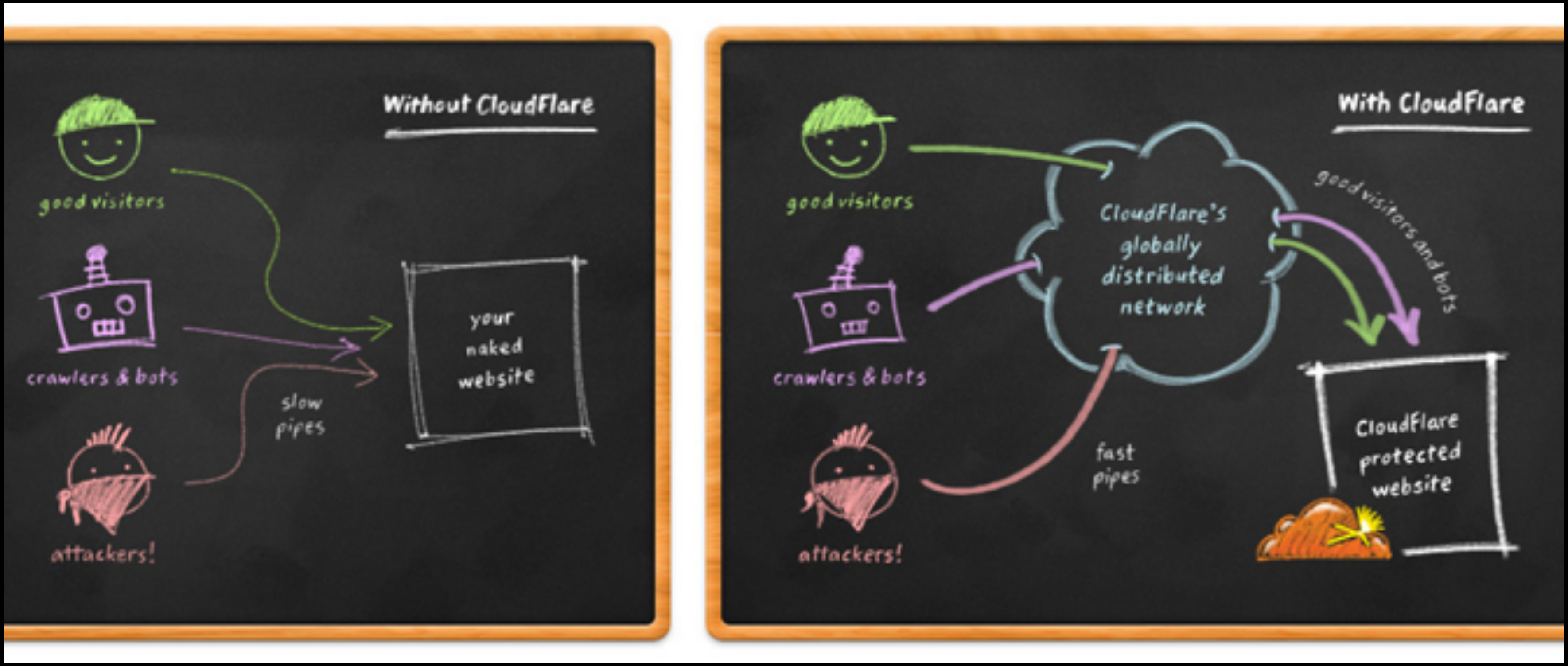
felipe@cloudflare.com

GTER 40
GTS 26
10 E 11 DE DEZEMBRO

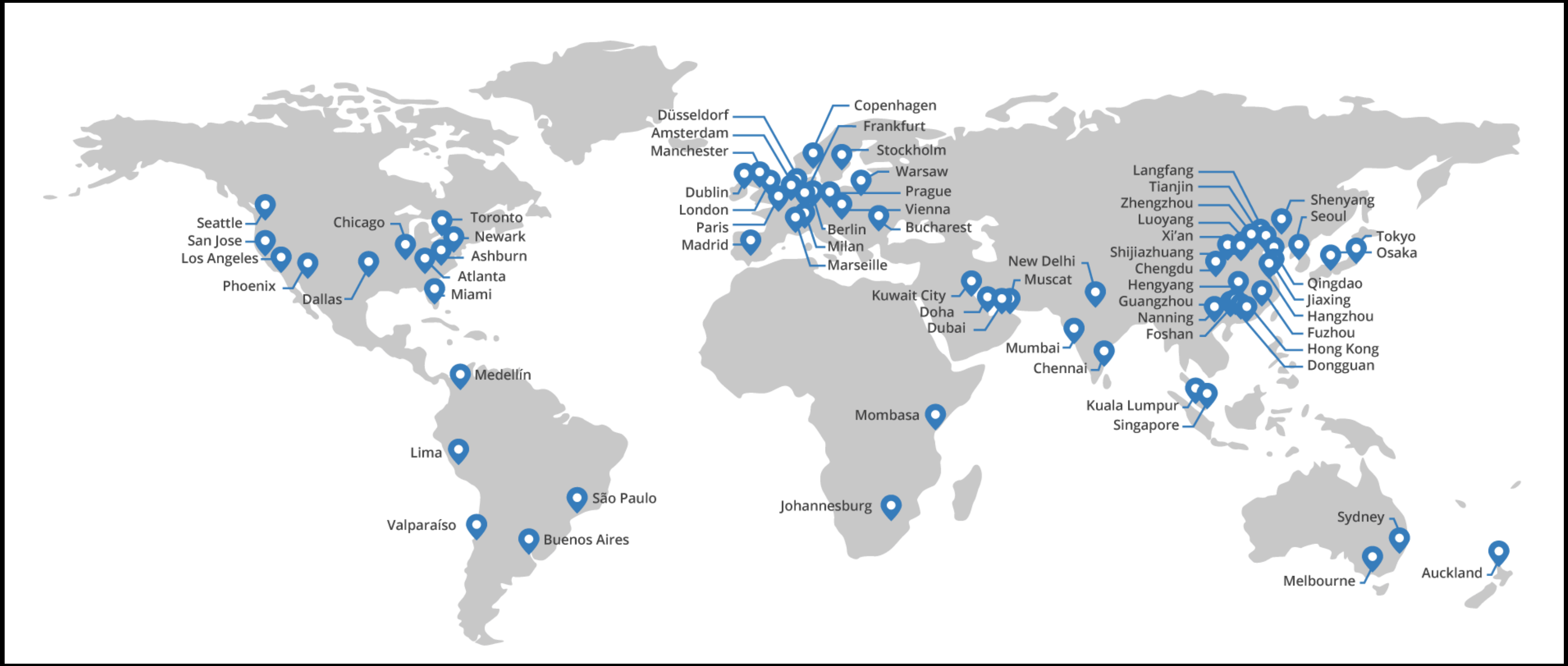
Outline

1. Intro on CloudFlare
2. Brief review of terminology
3. Overview of the problem
4. Research on Brazil Sites and Financial Sector
5. CloudFlare’s Approach

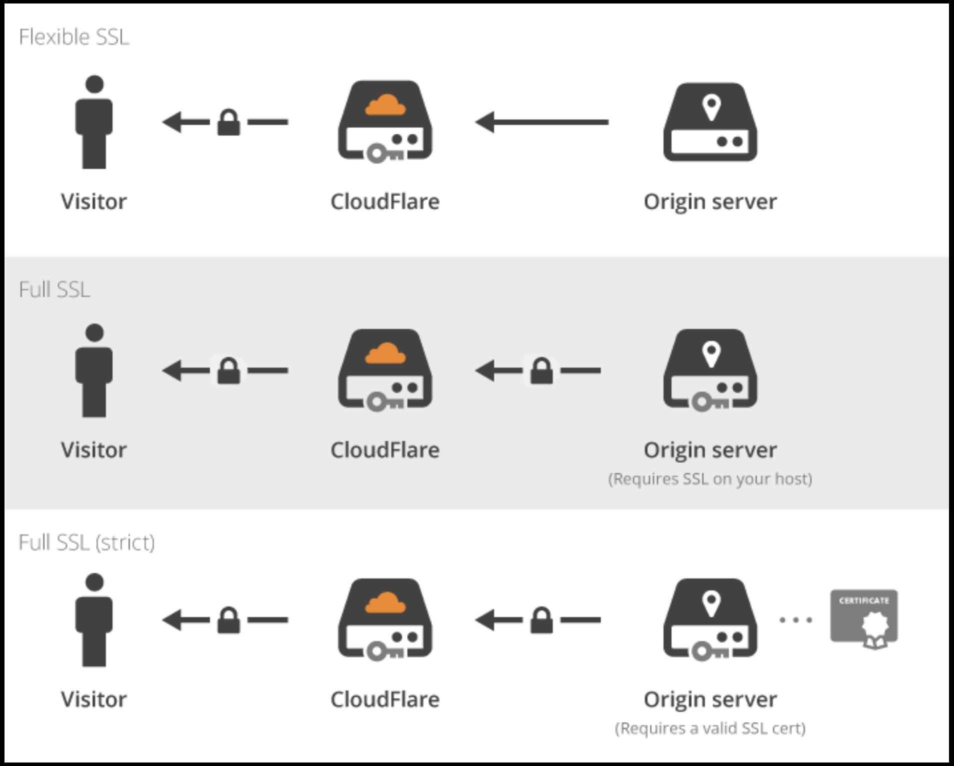
Who are we ?


Without CloudFlare
good visitors
crawlers & bots
attackers!
slow pipes
your naked website
With CloudFlare
good visitors
crawlers & bots
attackers!
CloudFlare's globally distributed network
good visitors and bots
fast pipes
CloudFlare protected website

CloudFlare Global Anycast Network



CloudFlare SSL



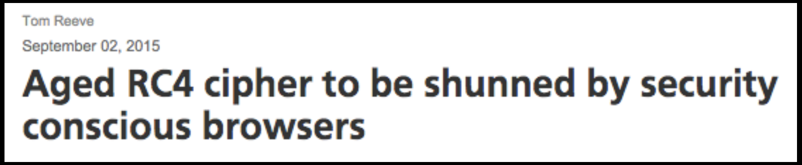
CloudFlare Universal SSL

- In October 2014 CloudFlare Introduced Universal SSL
- Offering SSL Certificates to all customers
- SNI Certificates for Free and Pro Levels
- SAN and Dedicated Certificates for Enterprises
- Over 2M sites covered by Universal SSL

SHA-1 deprecation

Background on the issue

Recent TLS Related News

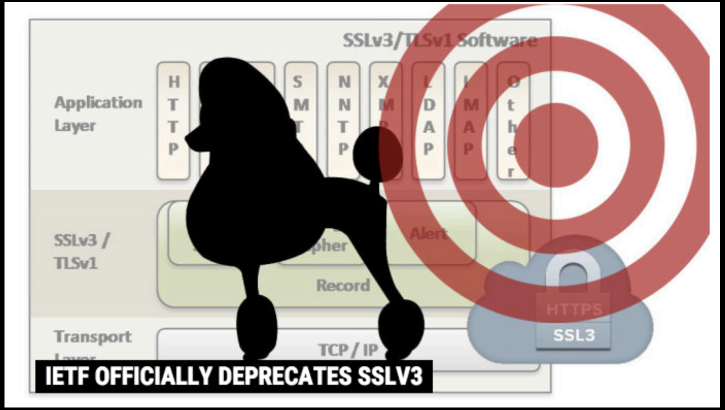


Tom Reeve

September 02, 2015

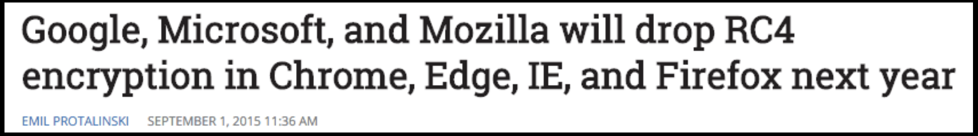
Aged RC4 cipher to be shunned by security conscious browsers

SHA-1 Freestart Collision
Oct. 8, 2015



IETF OFFICIALLY DEPRECATES SSLV3

RFC 7568 Deprecating Secure Sockets Layer Version 3.0



Google, Microsoft, and Mozilla will drop RC4 encryption in Chrome, Edge, IE, and Firefox next year

EMIL PROTALINSKI SEPTEMBER 1, 2015 11:36 AM

A quick primer on certificates and signatures

What is a certificate? X509? Hash function? Signature?

Certificates, X509, and signatures

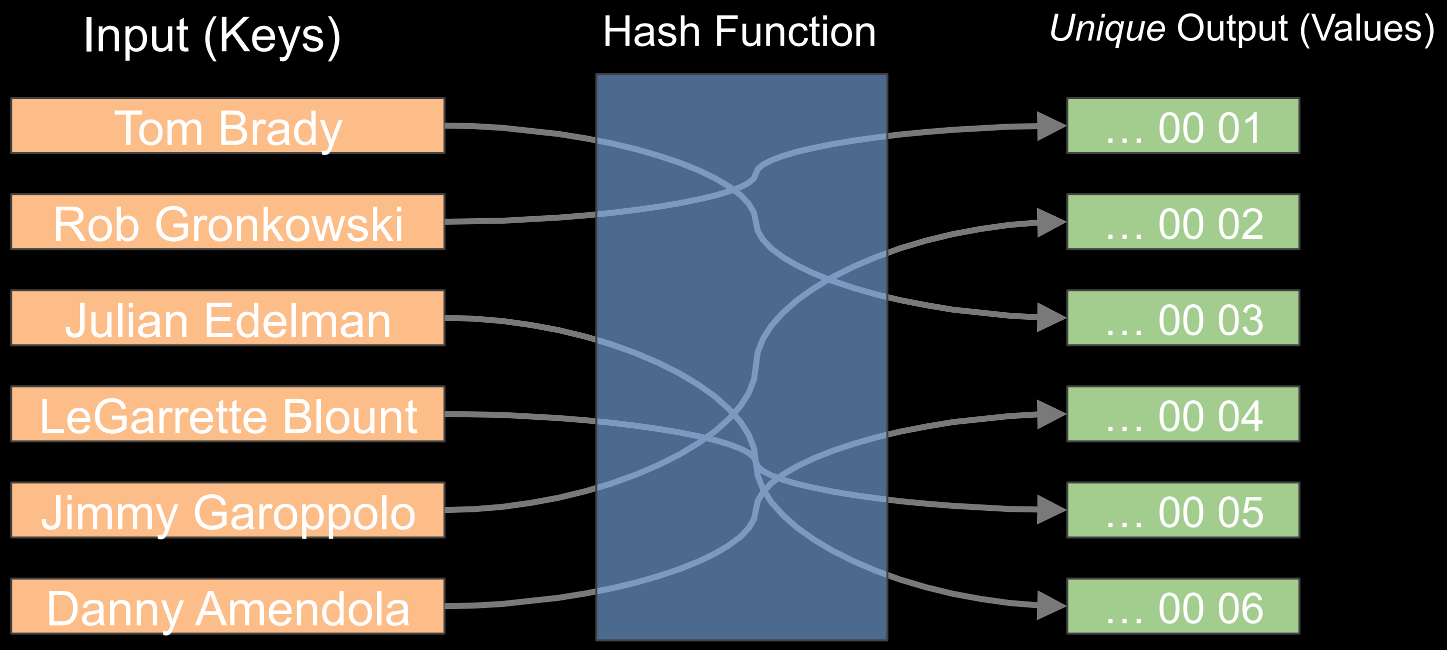
1. **Certificates** are used to *establish* HTTPS sessions between browsers and servers
2. Certificates are distributed to browser in a standardized data structure called “**X509**” that contains other (identifying) information
3. Certificate authorities attest – to varying degree – that the site is who it says it is; they do this by **signing** a **hash** of the X509 structure

X509 (v3) Structure - Fields w/Example Data

Field	Example Data
Version Number	3
Serial Number	4710875
Signature Algorithm (ID)	**SHA-1** with RSA Enc.
Issuer Name	COMODO CA Limited
Validity Period - Not Before - Not After	Not Before 2015/01/04 Not After: 2015/12/31
Subject Name	O=CloudFlare, Inc. ...
Subject Public Key Information - Public Key Algorithm - Subject Public Key	rsaEncryption Mod: 00 DE B2 06 B3 F9 … Exp: 65537 (0x10001)

Field	Example Data
Issuer Unique Identifier (opt.)	
Subject Unique Identifier (opt.)	
Extensions (opt.)	Subject Alternative Name(s) DNS.1 cloudflare.com DNS.2 www.cloudflare.com CRL Distribution Points http://crl.comodoca.com/… OCSP Protocol http://ocsp.coododa.com/…
Certificate Signature Algorithm	**sha1WithRSAEncryption**
Certificate Signature	**256 bytes**: 5E 5E 66 56 68 ...

Hash function



Input (Keys)

Hash Function

Unique Output (Values)

Tom Brady

Rob Gronkowski

Julian Edelman

LeGarrette Blount

Jimmy Garoppolo

Danny Amendola

… 00 01

… 00 02

… 00 03

… 00 04

… 00 05

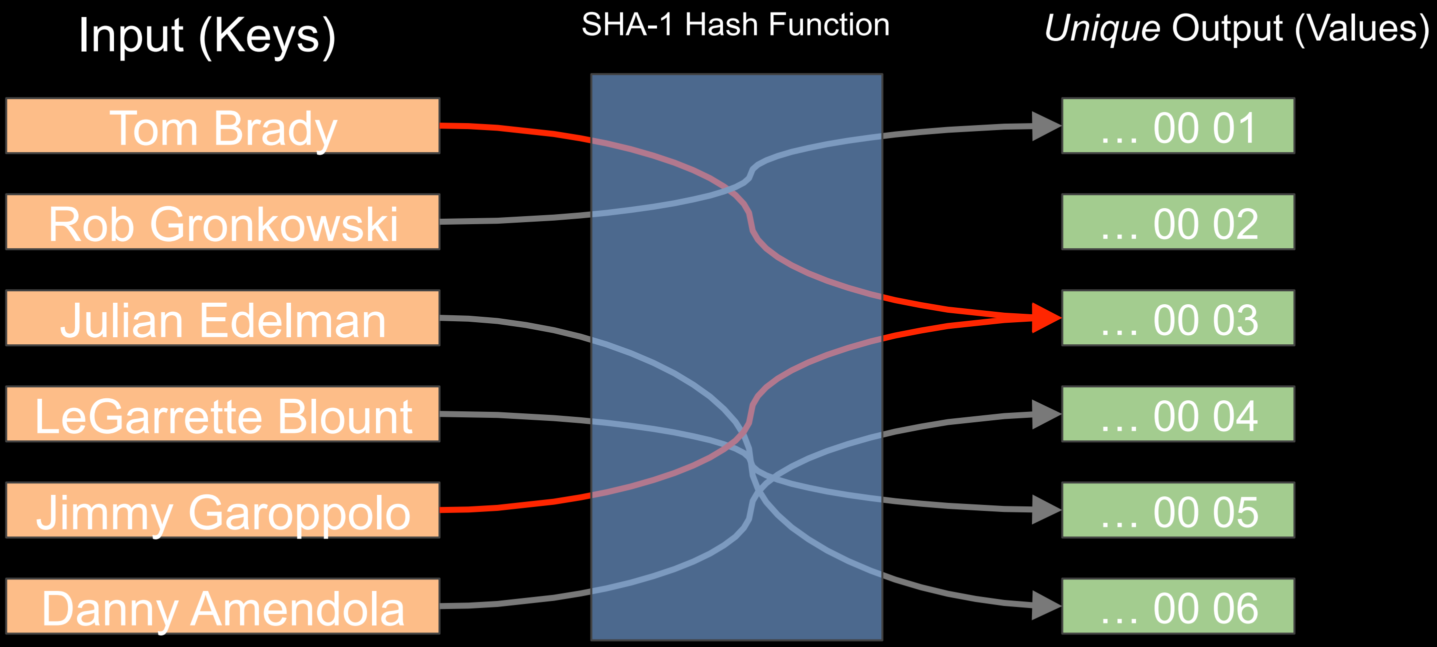
… 00 06

What if someone could re-use signatures?

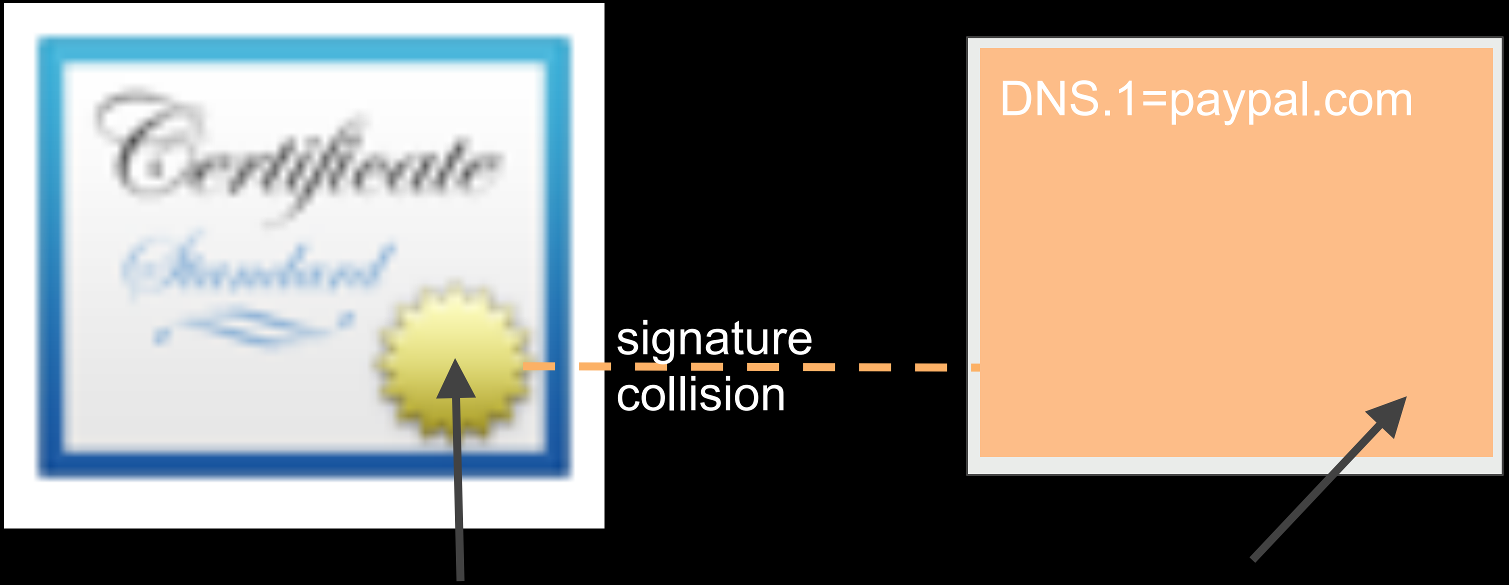
1. Signatures indicate to the browser whether or not they should **trust** the signature presented

2. What if this signature could be “steamed off” like the seal on a letter and then re-used?

Hash function (with collisions)



Producing a (signature) hash collision



Seal (signature) issued by Comodo attesting to the validity of the information contained in the certificate.

Attacker can craft X509 container such that it generates the same signature, i.e., they produce a “[hash] collision”.

Cost of inducing collision

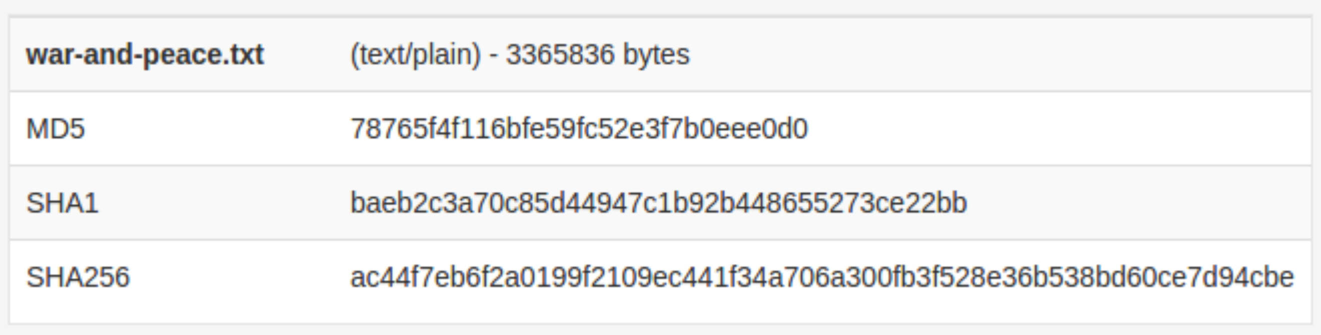
Year	Estimated Cost
2012	$2,700,000
2015	$700,000
2018	$173,000
2021	$43,000

Recent Paper on “freestart” Collision lowers these estimates

Source: Bruce Schneier

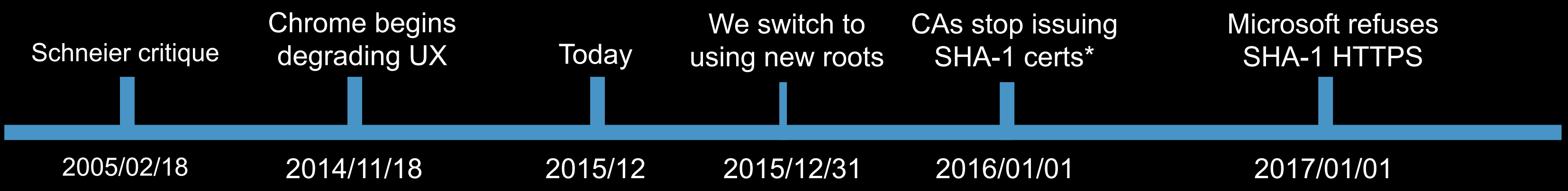
Improved hash function

Hash	Output (bits)	Possibilities
SHA-1	160	2^160 = 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976
SHA-256	256	2^256 = 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936



war-and-peace.txt	(text/plain) - 3365836 bytes
MD5	78765f4f116bfe59fc52e3f7b0eee0d0
SHA1	baeb2c3a70c85d44947c1b92b448655273ce22bb
SHA256	ac44f7eb6f2a0199f2109ec441f34a706a300fb3f528e36b538bd60ce7d94cbe

Timeline of events



Schneier critique
2005/02/18

Chrome begins degrading UX
2014/11/18

Today
2015/12

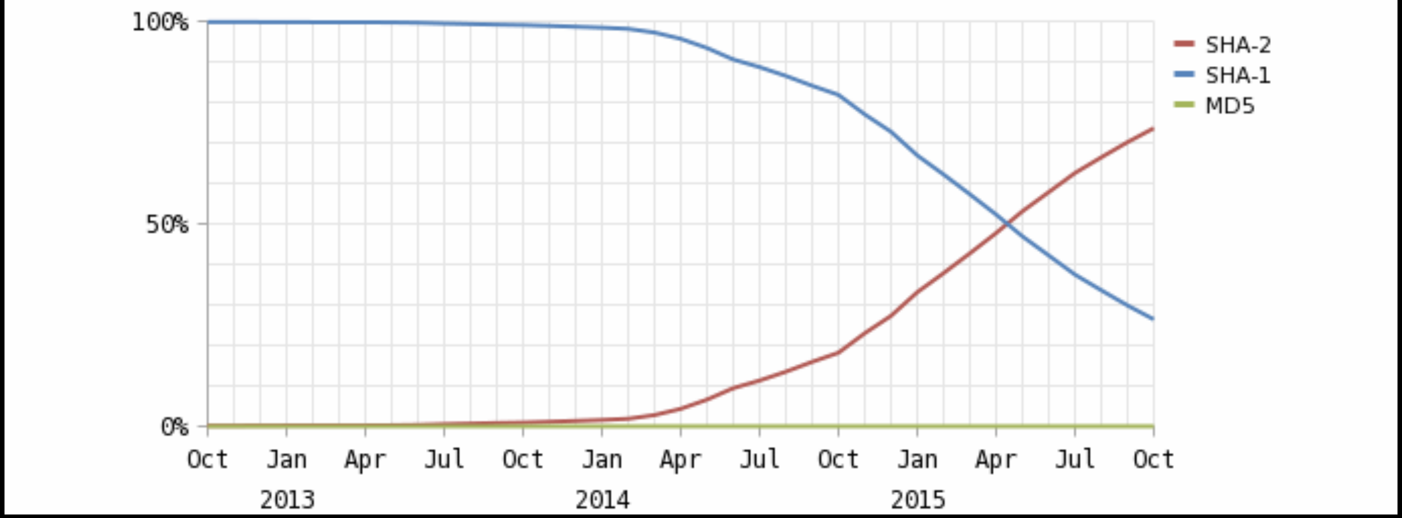
We switch to using new roots
2015/12/31

CAs stop issuing SHA-1 certs*
2016/01/01

Microsoft refuses SHA-1 HTTPS
2017/01/01

* Proposal for LV (Legacy Verified) Certificates

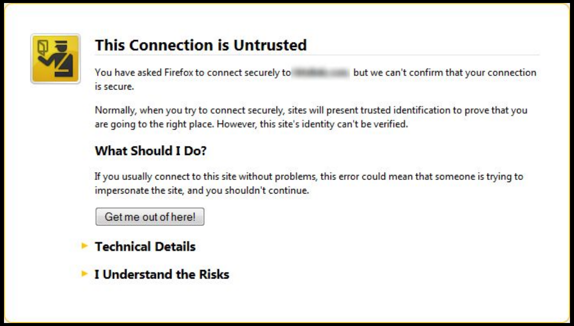
SHA-2 Adoption



Source: *SHA-1 vs SHA-2 (source: Netcraft SSL Survey October 2015)*

January 1, 2016

- Internet Explorer
  - Block June 2016
- Mozilla
  - Untrusted warning Certs Issued - until July 2016
  - Reject afterwards
- Chrome
  - SHA-1 issued in 2016
  - SHA-1 Certs expiration >2016



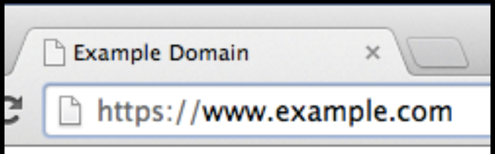
This Connection is Untrusted

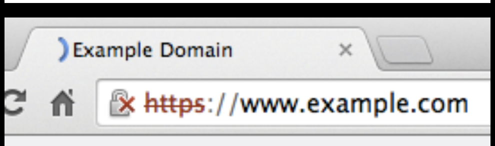
You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

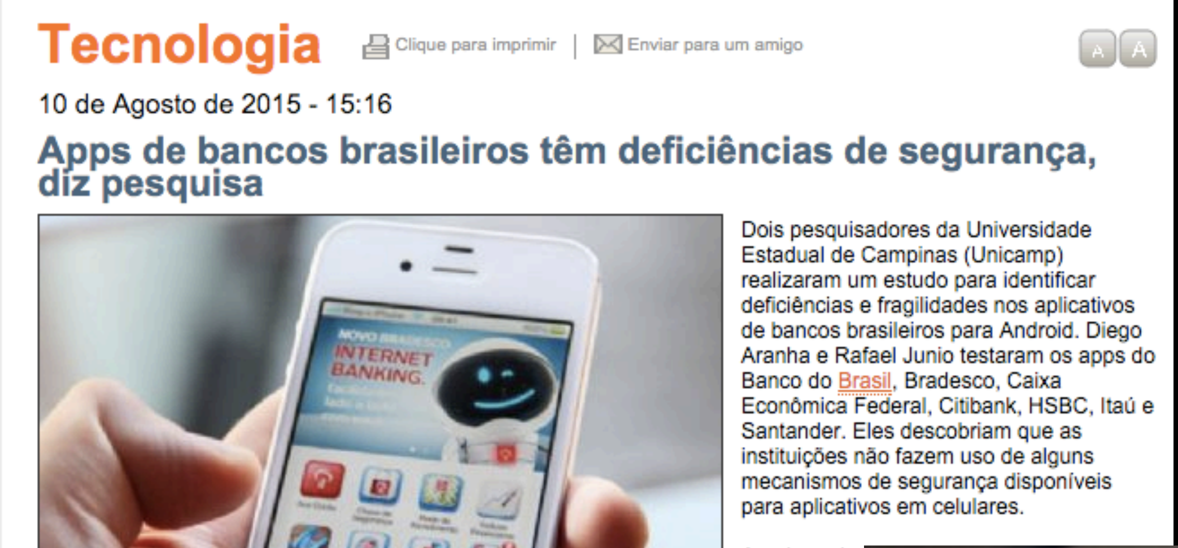
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.





Research on Brazil Sites and Financial Sector

Many Sites with Outdated Standards

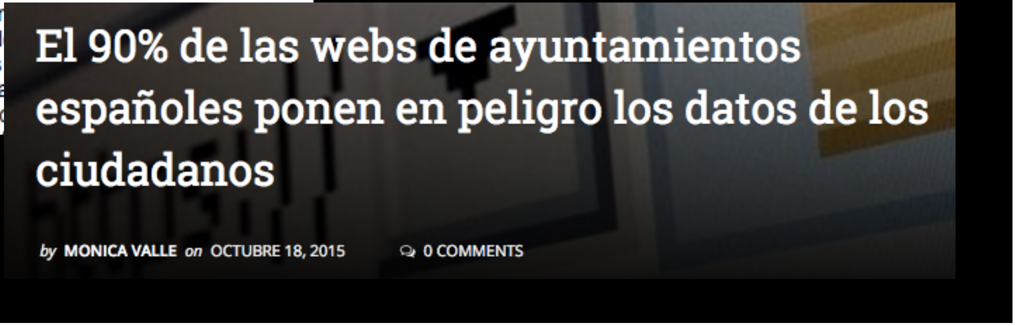


10 de Agosto de 2015 - 15:16

Apps de bancos brasileiros têm deficiências de segurança, diz pesquisa

Dois pesquisadores da Universidade Estadual de Campinas (Unicamp) realizaram um estudo para identificar deficiências e fragilidades nos aplicativos de bancos brasileiros para Android. Diego Aranha e Rafael Junio testaram os apps do Banco do Brasil, Bradesco, Caixa Econômica Federal, Citibank, HSBC, Itaú e Santander. Eles descobriam que as instituições não fazem uso de alguns mecanismos de segurança disponíveis para aplicativos em celulares.

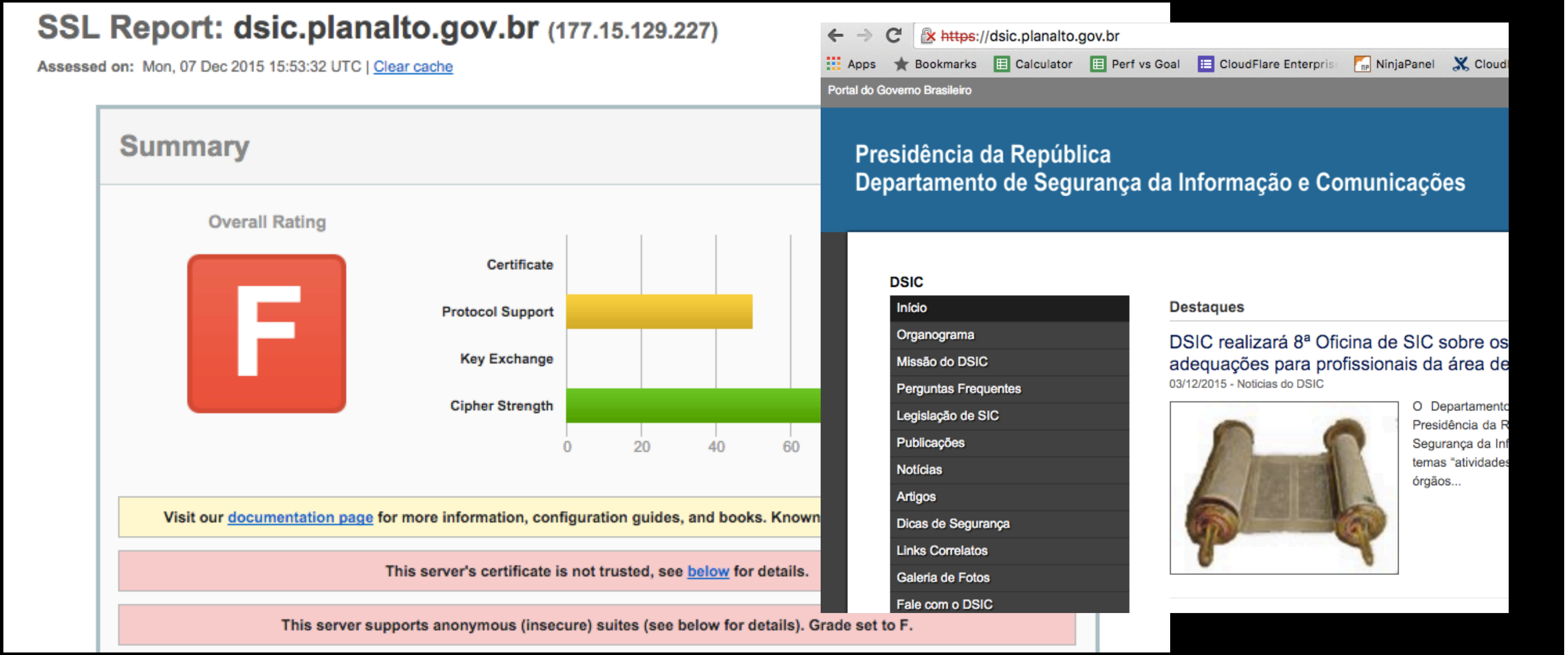
Aranha e Jur
ferramenta d
identificar as
bancos na ca
dados e desc



El 90% de las webs de ayuntamientos españoles ponen en peligro los datos de los ciudadanos

by MONICA VALLE *on* OCTUBRE 18, 2015 0 COMMENTS

Brazilian Government Website



SSL Report: dsic.planalto.gov.br (177.15.129.227)

Assessed on: Mon, 07 Dec 2015 15:53:32 UTC | Clear cache

Summary

Overall Rating

F

Visit our documentation page for more information, configuration guides, and books. Known

This server's certificate is not trusted, see below for details.

This server supports anonymous (insecure) suites (see below for details). Grade set to F.

Portal do Governo Brasileiro

Presidência da República
Departamento de Segurança da Informação e Comunicações

DSIC

- Início
- Organograma
- Missão do DSIC
- Perguntas Frequentes
- Legislação de SIC
- Publicações
- Notícias
- Artigos
- Dicas de Segurança
- Links Correlatos
- Galeria de Fotos
- Fale com o DSIC

Destaques

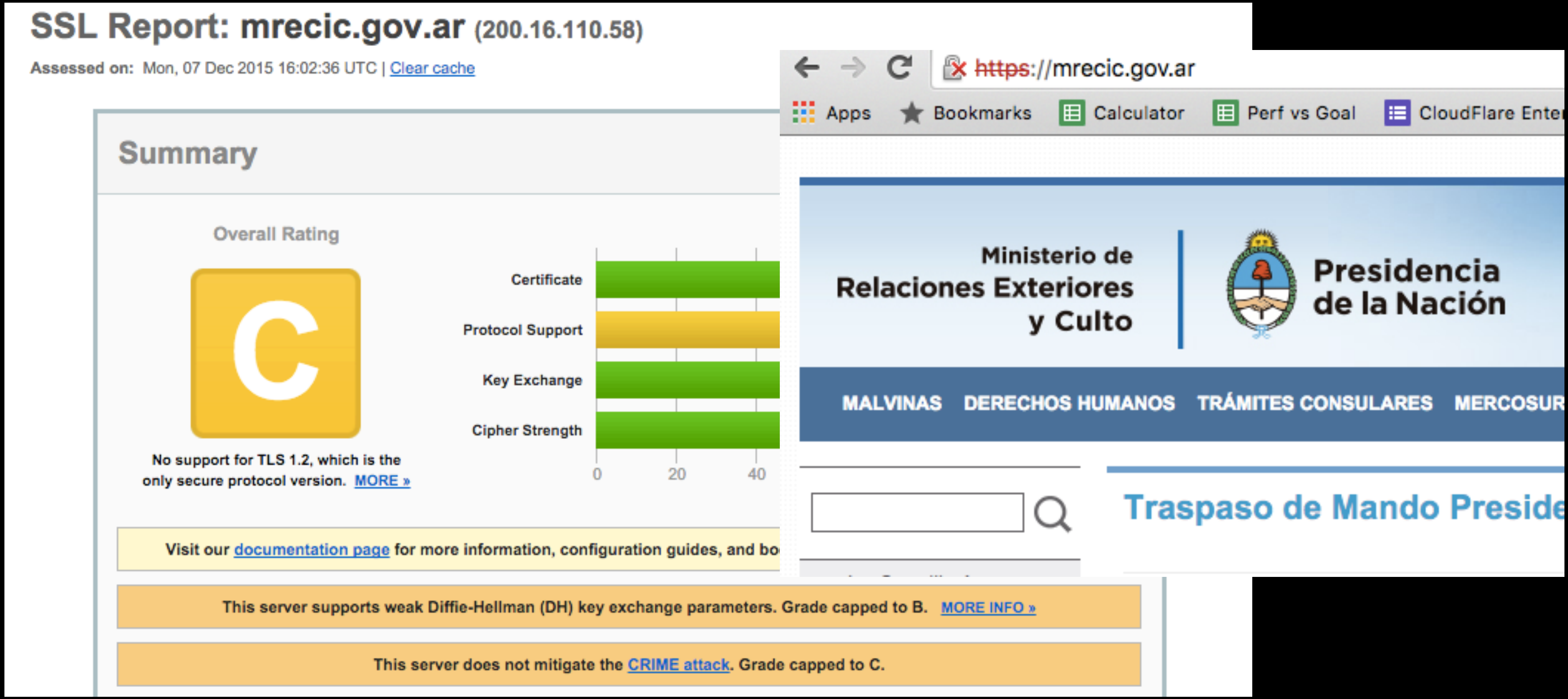
DSIC realizará 8ª Oficina de SIC sobre os
adequações para profissionais da área de

03/12/2015 - Notícias do DSIC

O Departamento
Presidência da R
Segurança da Inf
temas "atividades
órgãos...

https://www.ssllabs.com/ssltest/analyze.html?d=dsic.planalto.gov.br

Argentina Government Website



SSL Report: mrecic.gov.ar (200.16.110.58)

Assessed on: Mon, 07 Dec 2015 16:02:36 UTC | Clear cache

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »

Visit our documentation page for more information, configuration guides, and bo

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server does not mitigate the CRIME attack. Grade capped to C.

https://www.ssllabs.com/ssltest/analyze.html?d=mrecic.gov.ar

Research on .BR (in Alexa 1M)

- 18,749 .BR Domains in (Alexa 1M 1.8%)
- 10,130 TLS Configured (54%)

NO SSL	8619	46%
SHA-1 Only	2135	11.4%
SHA-2 Only	7787	41%
SHA-2 w/ SHA-1 Fallback	208	1.1%

- What about the Banks…...

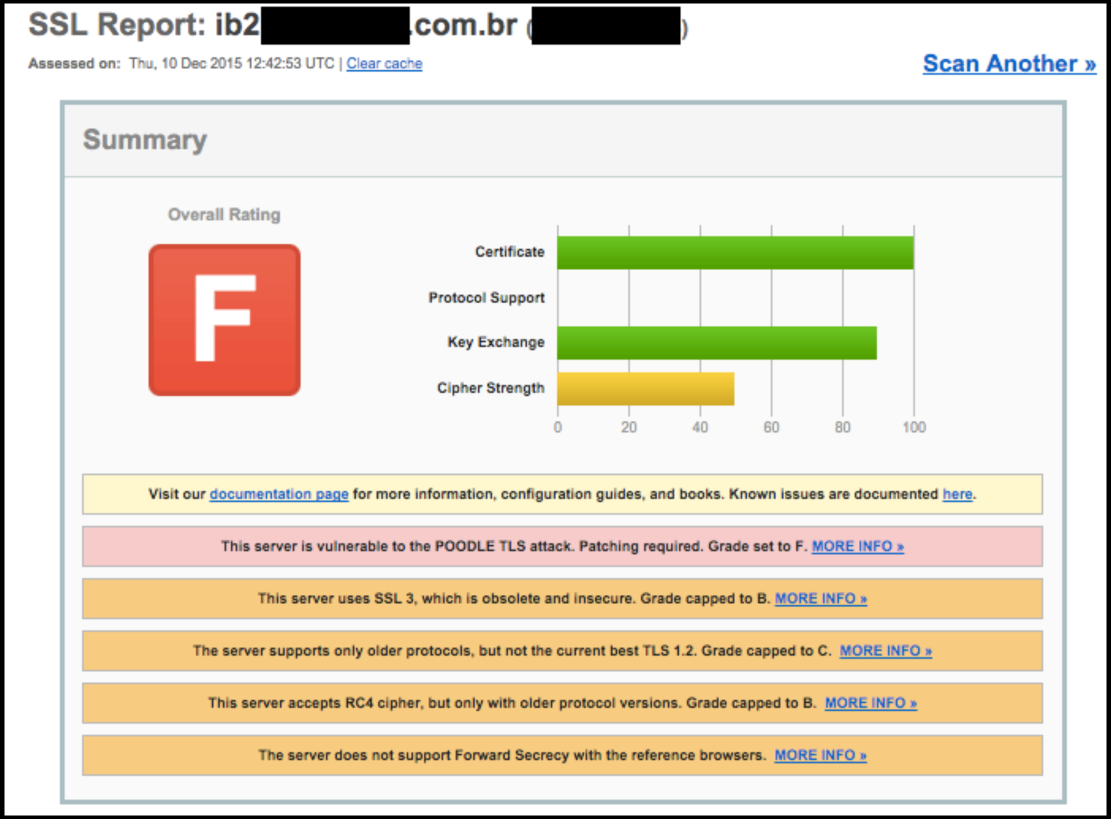
Source: Alexa 1M List

Banks in Brazil

- FEBRABAN - Federação Brasileira de Bancos – 114 Banks Listed
- Scanned Main Website (www) on Dec. 4th (May not include E-banking sites)

NO SSL	**49**	**43%**
SHA-1 Only	15	13%
SHA-2 Only	44	38%
SHA-2 w/ SHA-1 Fallback	6	5.3%

Brazilian Financial Website



SSL Report: ib2[redacted].com.br ([redacted])

Assessed on: Thu, 10 Dec 2015 12:42:53 UTC | Clear cache

Scan Another »

Summary

Overall Rating

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE TLS attack. Patching required. Grade set to F. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Challenges for Website owners

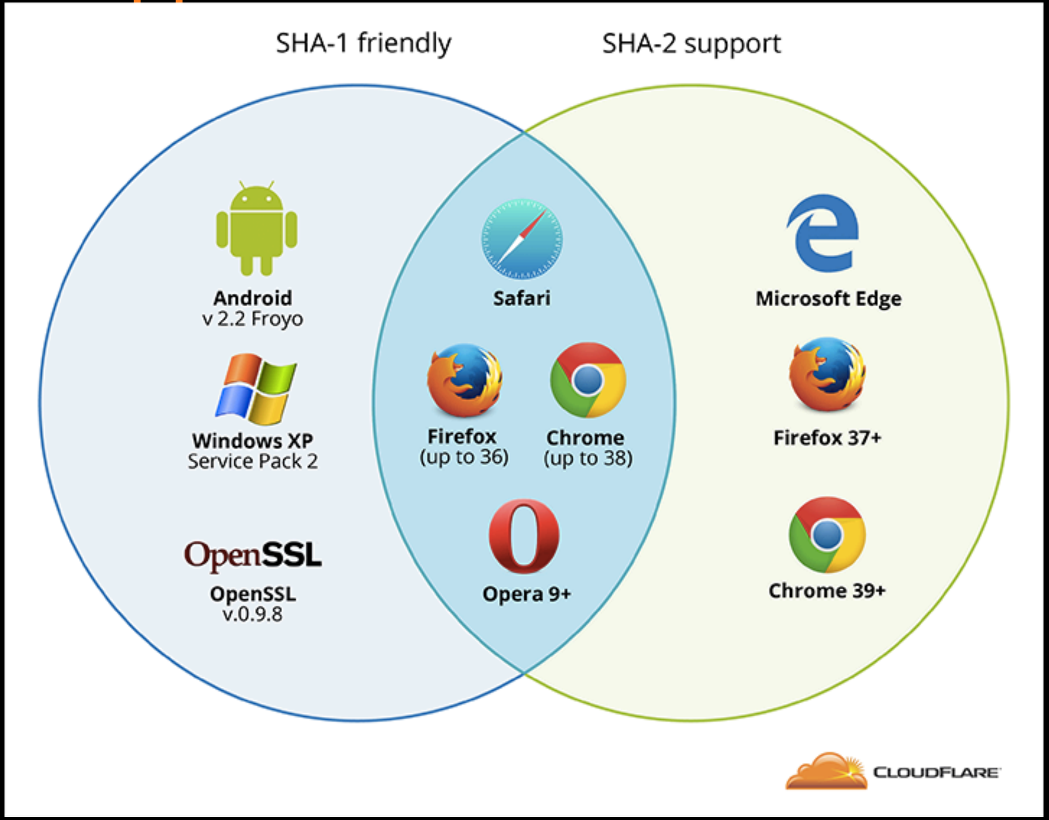
- Outdated Infrastructure and software
  - Front End Web Server Infrastructure, Back Ends
  - SSL Termination Equipment (Balancers, Proxies, etc).
- Complacency (False Sense of Security).
- Fear of Changes - Compatibility

CloudFlare Approach

CloudFlare SHA-2 Migration

- Major Challenge due to the large number of customer certificates deployed.
- Needed to make a migration that was seamless to end customers.
- Needed to insure backward compatibility with SHA-1 Clients
- SHA2 % Error
    - US - 0.68%
    - Brazil - 1.67%
    - Global - 1.4%
- Base needed for deployment of HTTP/2

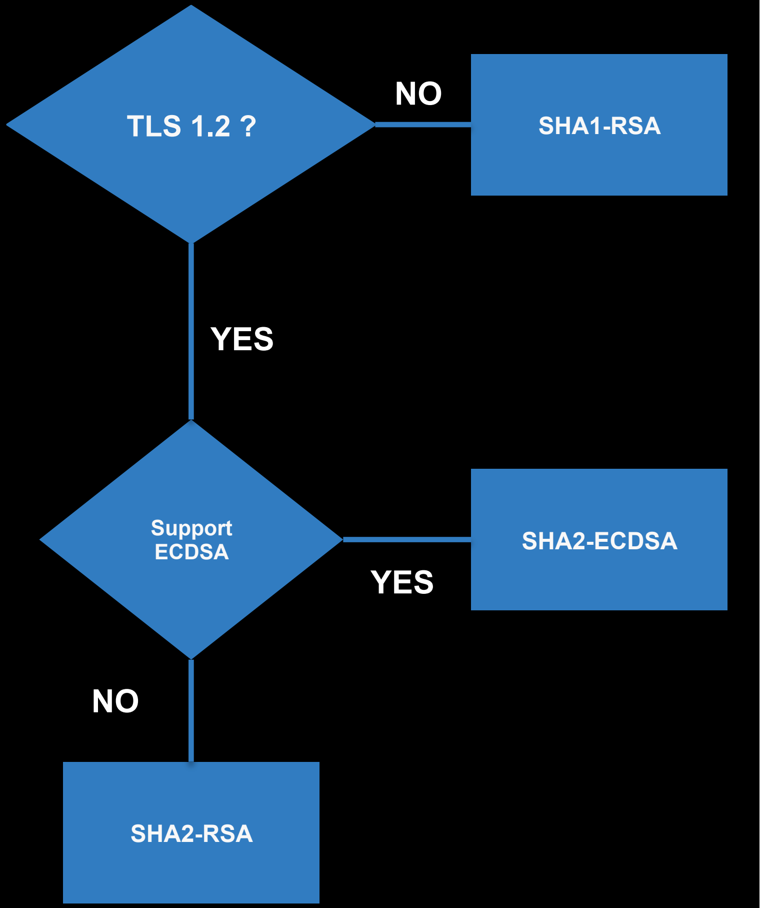
Support for SHA-2



- Difficulty in upgrading older clients
- Embedded Systems
    - Android, Kiosks, Digital Signage, POS

CloudFlare Approach

- Supports 3 certificates simultaneously
  - Interoperable with SNI and SAN Certificates
- SHA-2 ECDSA, SHA-2 RSA and SHA-1 RSA Fallback
- The best certificate is chosen based on a decision tree
- “Lazy Loading” of Certificates
- Deployed in Open_ssl and NGINX



TLS 1.2 ?

NO

SHA1-RSA

YES

Support ECDSA

YES

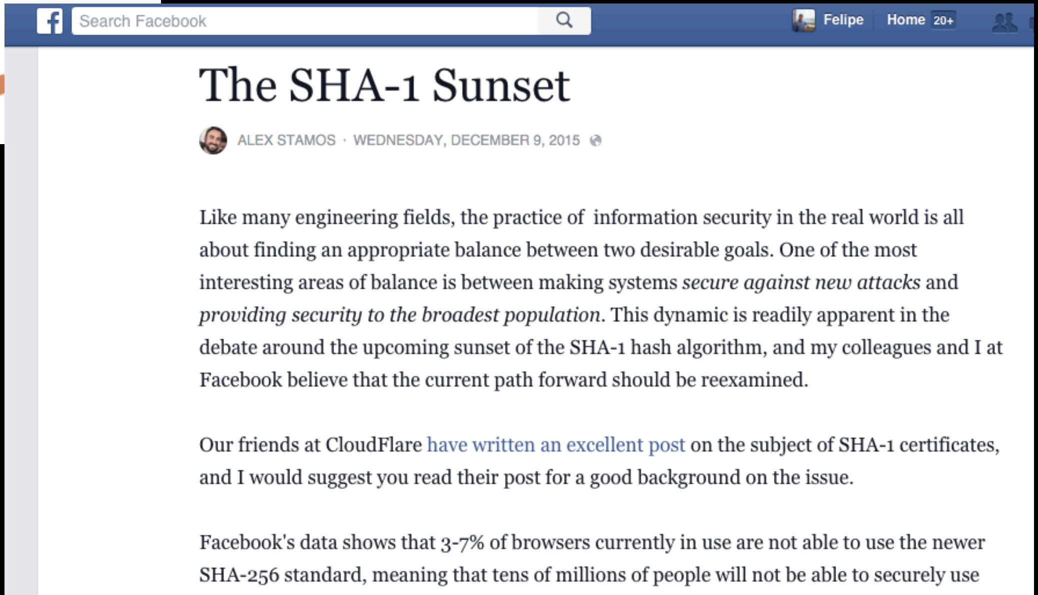
SHA2-ECDSA

NO

SHA2-RSA

Who else is doing this

Facebook and Alibaba



The SHA-1 Sunset

ALEX STAMOS · WEDNESDAY, DECEMBER 9, 2015

Like many engineering fields, the practice of information security in the real world is all about finding an appropriate balance between two desirable goals. One of the most interesting areas of balance is between making systems *secure against new attacks* and *providing security to the broadest population*. This dynamic is readily apparent in the debate around the upcoming sunset of the SHA-1 hash algorithm, and my colleagues and I at Facebook believe that the current path forward should be reexamined.

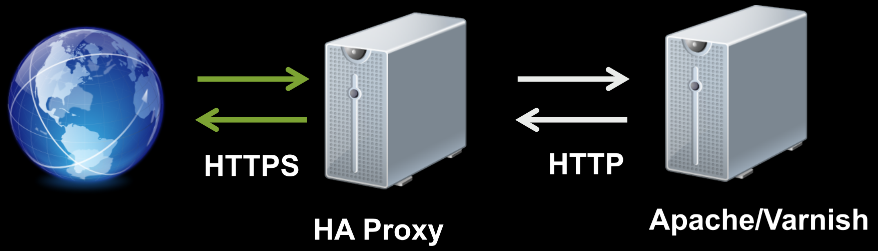
Our friends at CloudFlare have written an excellent post on the subject of SHA-1 certificates, and I would suggest you read their post for a good background on the issue.

Facebook's data shows that 3-7% of browsers currently in use are not able to use the newer SHA-256 standard, meaning that tens of millions of people will not be able to securely use

Can I build this ?

In the Lab

- Build your own Security Proxy
  - Useful for forcing HTTPS and avoiding mixed content messages.
  - Certificate Switching (Facebook Open sourced certificate switching)
  - How to get A+ Rating on ssllabs.com: Forward Secrecy, Session Tickets, HSTS



  - Guide: http://arstechnica.com/information-technology/2015/05/web-served-how-to-make-your-site-all-https-all-the-time-for-everyone/

Further Reading

- CloudFlare Blog: https://blog.cloudflare.com/sha-1-deprecation-no-browser-left-behind/
- Facebook Article: https://www.facebook.com/notes/alex-stamos/the-sha-1-sunset/10153782990367929
- Netcraft: http://news.netcraft.com/archives/2015/10/19/one-million-ssl-certificates-still-using-insecure-sha-1-algorithm.html
- Qualys: https://community.qualys.com/blogs/securitylabs/2014/09/09/sha1-deprecation-what-you-need-to-know
- CA/Browser Forum: https://cabforum.org/

Obrigado

Felipe Tribaldos
felipe@cloudflare.com
Twitter: @ftribaldos

CLOUDFLARE