Cutting your TLS baggage

Jan Schaumann
A really boring talk.
I really like boring.
I really like boring.

I’m so boring, even BoringSSL is too exciting for me.
23 years old
“There are two types of companies: those that have been hacked and those that don't know it yet.”

— every #infosec nerd, smugly

No, seriously, that includes yours.

— this guy, jaded
$ units
You have: a huge infrastructure with lots of baggage
You want: a unified ingress serving platform
  * lots of work across tons of teams
    
/ 0

Floating point exception (core dumped)
$
You have: an HTTPS service

You want: to accept end-user traffic from the internet
- keep up with changing requirements
- implement critical updates across all systems in <24h
- run latest stable release of supported software
- implement non-critical updates within <3 months
Be f*ckin explicit about general things.
Be f*ckin explicit about general things.

(Common sense ain’t.)
$ units
You have: ...uhm, good question
^C
$
Weird things we found:

- certificates with a **Not Before** date set prior to the Unix epoch (00:00:00, January 1st, 1970)
- certificates with a **Not Before** date set in 2023
- certificates with a **Not Before** date set to "110204212630-1200"
- certificates with a **Not After** date set in 1902
- certificates expiring 10 years in the future
- certificates expiring in 2100
- certificates expiring in the year 4752
- self-signed certificates galore
- various properties having stood up their own CAs
- key length of 512
- certificates with an MD5 signature
- publicly used certificates that expired -15 years
- cipher suites using a NULL encryption cipher
- cipher suites using a NULL authentication cipher
- cipher suites offering export ciphers
- 14 different versions of OpenSSL
- systems vulnerable to Heartbleed, POODLE, Logjam, FREAK, DROWN, and $SILLYNAME
- certificates with ~200 SANs
- certificates without either a CN or a SAN
- certificates with a CN of "*"
Any sufficiently large infrastructure is indistinguishable from the internet.
One in a million is next Tuesday every couple of minutes.
The lowest common denominator will always drag you down.
The lowest common denominator internet of unpatchable crap will always drag you down.
IoT is when “smart” means “dumb”.

https://www.philips.com/a-w/mobile-privacy-notice/smart-shaver-app.html
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

ECDSA missing - coming soon!
ChaCha20/Poly1305 missing - coming soon!

Prefer GCM over CBC
Prefer faster “good enough” over slower, stronger.

Prefer Forward Secrecy
Lowest common denominator is low...

https://github.com/jschauma/cipherdiff
You have: an x509 certificate
You want: to accept end-user traffic from the internet
- be issued by approved CA
- have Certificate Transparency
- RSA keys >= 2048; ECDSA >= 256
- misc. CN/SAN restrictions
- validity <= 6 months

O'Reilly Security 2017
$ certdiff -s www.google.com
1563eeb632a619c2 'www.google.com' (leaf): Incomplete chain or unknown root!
1563eeb632a619c2 'www.google.com' (leaf): 5N (www.google.com) not in list of app
proved domains (brightroll.com, flickr.com, flurry.com, tumblr.com, yahoo.com, yimg.com).
1563eeb632a619c2 'www.google.com' (leaf): no valid pin nor root serial found.
12b0e6 'GeoTrust Global CA' (intermediate): invalid signature algorithm (SHA1-RS
A not in [SHA256-RSA])

$ certdiff -s www.yahoo.com
ct = true
cabundle = ~/work/ssl_ca_bundle/yahoo_certificate_bundle.pem
domains = brightroll.com, flickr.com, flurry.com, tumblr.com, yahoo.com, yimg.co
m
keyLength = 2048
maxValidity = 190
maxSANs = 100
maxWildcards = 60

pins = sha256/2fR4ALxyl4f HadT5kA7y4FB/GLJLuNAZCqY=, sha256/2oALgLKofTmeZ
v0Zi1y/1Sg7979jPMx8bVeA6DH4o/q8=, sha256/Gtk3r1efLBrSb0G3hmVmd9ad6xWf/06eCm
r5M=, sha256/I/Lt/z7ek2CVanmD8tCvj5EqXsl20aThE0H2BqB6T/o=, sha256/JcBqUG53MjU0i6
brnxv3x3Fz9kOJxkqPBXGGv7jN8FQ=, sha256/VscWumuteCOHvVIAarO DxzVVeS7fF6xuxv6ve
s4=, sha256/UZJDJsnp1+4M5x9cbdbfLB779y5YRBeV6Z6rBMLIL104=, sha256/Wd8xe/qfT	Wq3yLF
Nd31pajqQHzh2ZNNLuvZmzNkpvw, sha256/WoLVrY1OvNa9xhaBciRSC7XhjLiyS9yW6G01ud4P8
8=, sha256/cAajgjWl7GTSaIEZ7YIMxEl0O5oJc870v0exWf72QM=, sha256/do1nbtzEBzELx/91
OE022e60Z0/NOnbV6SS2kH4A3E7a=, sha256/i7wTqTvh0ioIruIFFR4kMnBqr52rdiVPL/s2u/CY
=, sha256/1duNwFmk0TyZw3se/XV+Xcbj01LluW09QPa6A4yUwpu4M=, sha256/lnsMT7/09/384sJF
nrrPsFp3awJ3+Z2byPqWzGloahI=, sha256/256/rmIKq3eEpVdm-u/kocwzQMo1bk4TyHLibYi54E=
, sha256/1uwZtwOQxxcBxRqcntw+u/KYFkivkQaezL0WYEZ3anJc=

sigAlgs = SHA256-RSA
If it hurts, do it more often.

https://www.martinfowler.com/bliki/FrequencyReducesDifficulty.html
#Infosec Minimum Viable Protection

1. What even is an infosec?

2. Script Kiddies

3. Motivated, goals driven

4. Relentless, creative, targeted

5. Privileged, powerful, targeted, evil.

O'Reilly Security 2017
1) get buy-in from exec.
0) get pwned
1) get buy-in from exec.

https://www.netmeister.org/blog/crazy-like-a-fox.html
0) get pwned
1) get buy-in from exec.
2) incremental changes
Perfect is the enemy of the good.

"Eh, good enough." is the enemy of actually good.
0) get pwned
1) get buy-in from exec.
2) incremental changes
3) sell something
CAN'T SOMEONE ELSE DO IT?
Patience, young skywalker.
0) get pwned
1) get buy-in from exec.
2) incremental changes
3) sell something
4) profit
SSL Report: login.yahoo.com (98.136.189.41)

Summary

Overall Rating

A+

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

- Static Public Key Pinning observed for this server.
- HTTP Strict Transport Security (HSTS) with long duration deployed on this server.
- DNS Certification Authority Authorization (CAA) Policy found for this domain.
0) get pwned
1) get buy-in from exec.
2) incremental changes
3) sell something
4) profit
0) get pwned
1) get buy-in from exec.
2) incremental changes
3) sell something
4) profit goto 2
“We fight for the user.

We must do better today that we did yesterday, and better tomorrow than we did today.”

— Chris Nims, CISO / Chief Paranoid at Oath
Things to come:

- ECDSA
- Expect-CT
- OpenSSL 1.1 (ChaCha20/Poly1305)
- OCSP Must-Staple
- shorter validity
- apply to all Oath brands
Effecting change

Fake it 'till you make it.

O'Reilly Security 2017
Effecting change
Chokepoints and defaults are your secret weapon.
Effecting change

First: fix the future.
Effecting change

Lead by example, but offer autonomy.
Effecting change

Know what might break before you hit ‘go’.
Effecting change

Transparency goes a long way.

O’Reilly Security 2017

@jschauma
How to be boring:

Incremental changes.
Always move forward.
Lead by example, be transparent.
Encourage autonomy.

We can’t reach 100% security,
but we can always improve.
Credits

Apache Traffic Server
Google Chrome Team
Mozilla Observatory
SSL Labs
Yahoo Edge Team

(Yahoo/Oath/All) Paranoids

O’Reilly Security 2017