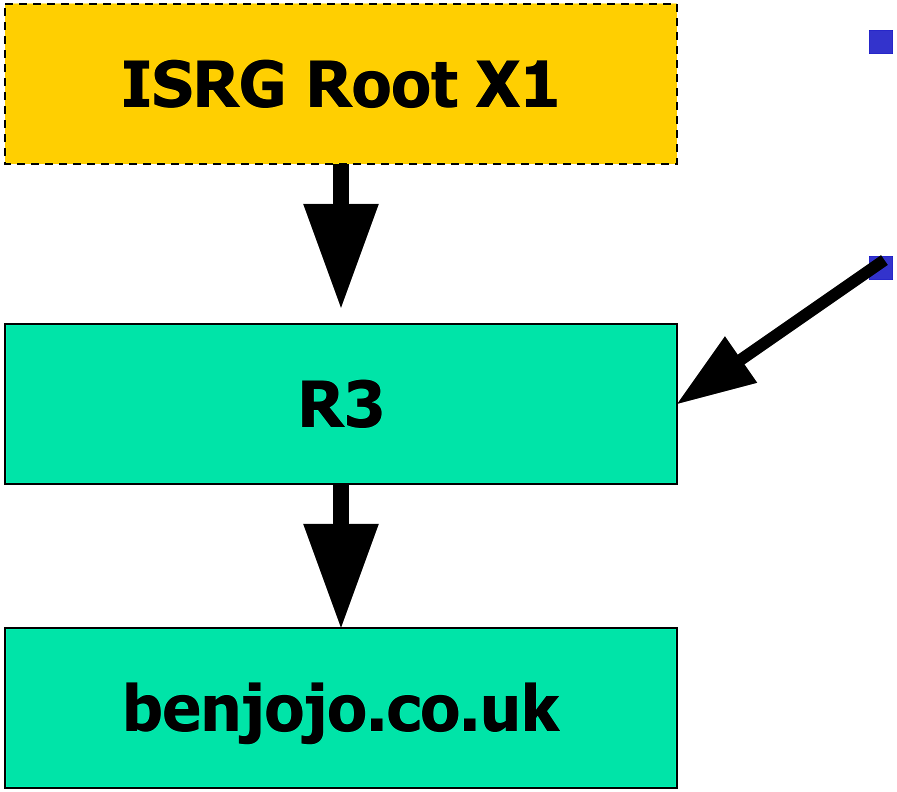
Browsers biggest TLS mistake

37C3 Lightning Talk

Benjojo / Ben Cartwright-Cox

A good TLS server



- Sends you a certificate chain
- The top of the certificate chain is signed by a Root CA installed in the software

A bad TLS server

- Just sends you the certificate with their domain/SAN/Name on it.
- This does not work… Unless it does?

benjojo.co.uk

Why this happens

- Most ACME and similar clients give you back 3 files
  - The “Full Chain” (You want this)
  - The Private Key (You want this)
  - The Certificate (Some software wants this, but 99% chance you do not want this file)
- People use the wrong certificate file

But this works anyway!

- Chrome and Firefox have mitigations to “fix” this from being a issue
  - Likely Safari does too but I don’t like to test on Safari because it’s a pain
- However the way that Chrome and Firefox go about it are different
  - Both methods give back bad vibes in terms of purity

Firefox (and friends)

- Ships with a huge list of known intermediate chains that the browser will try and use to make a chain ‘work’
- Behavior is consistent, does need constant updates to ensure it works well (since intermediates change over time)

Chrome (and friends)

- When a chain comes up that does not reach a Root CA, the browser looks at all of the other TLS Cert chains it’s seen, and tries to “make them fit”.
- This means a “cold start” chrome **does not** behave the same way as a chrome that was running for 4 hours browsing the web

Can we talk about how insane that is?

- Chrome’s TLS validation varies based on if you just started the browser, vs have been using it for a few hours

I don't like this!

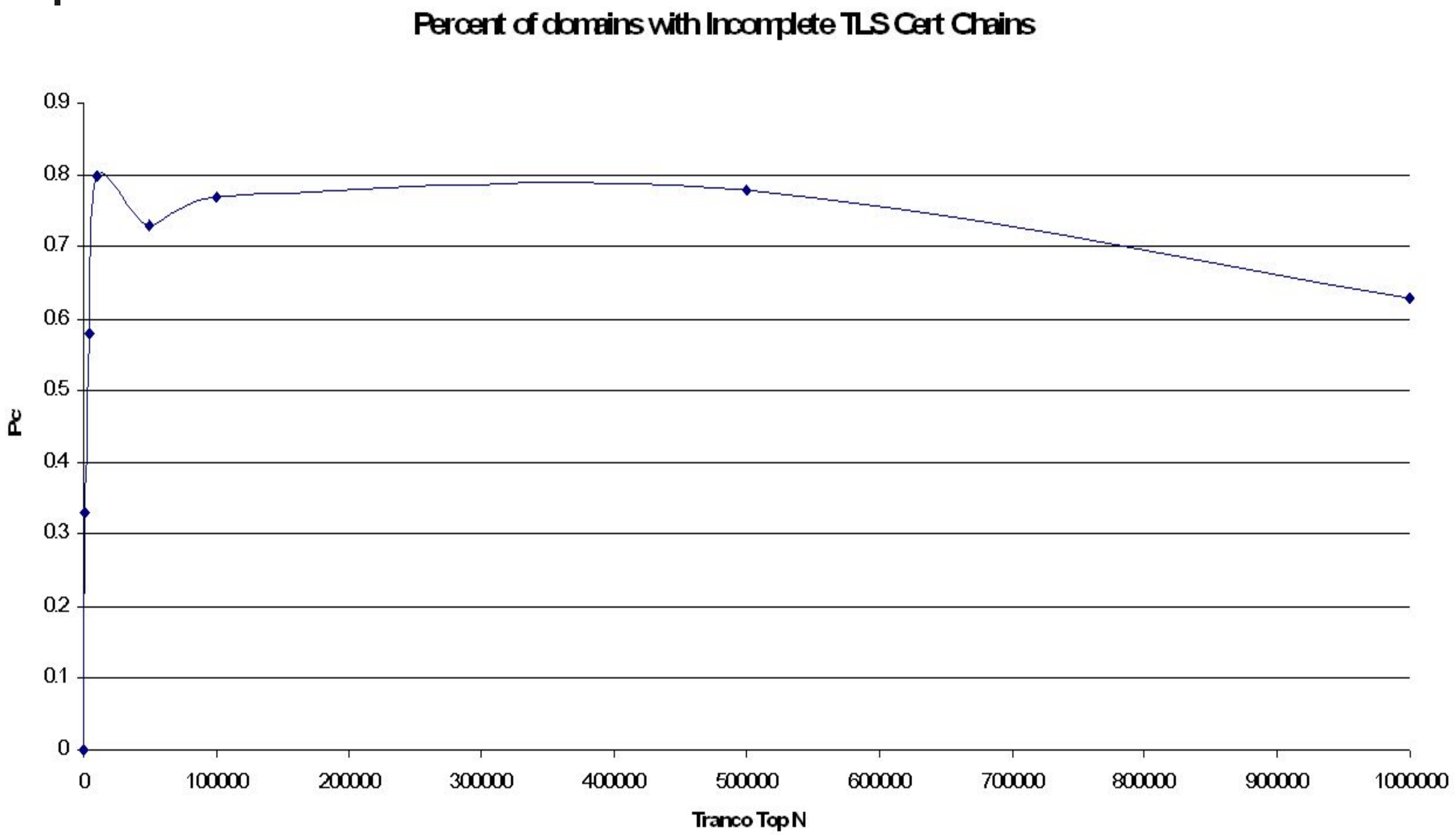
How often is this happening?

- There is a Go library that mimics the Firefox behaviour
-
- We can test the Tranco 1 Million (*A successor to the Alexa 1M list*) and compare how many more work over TLS with said go library

Terrible Hack

Range	% Broken In Range	Cumulative Broken	Broken In Range (Between Last DP)
10	**0%**	0	0
100	**0%**	0	0
1000	**0.33%**	3	3
5000	**0.58%**	26	23
10000	**0.8%**	66	40
50000	**0.73%**	359	293
100000	**0.77%**	745	386
500000	**0.78%**	3851	3106
1000000	**0.63%**	7005	3154

Terrible Hack



Terrible Hack

- Notable examples of failures
  - playstation.com (who sends the leaf cert twice)
  - bt.com
  - (house|hhs|virginia|fdic).gov / disa.mil
- A large % of the domains who have messed up cert chains are government sites

Did we really have to do this?

- There are now TLS sites that are mostly only reachable in browsers because browsers are the only place where this hack happens consistently
  - Though that might be considered a bonus by some
- Why did we open pandora's X509 box?

See the broken domain list!

https://docs.google.com/spreadsheets/d/1rbPDQQHNPR4JdWnl_DLxoHyjj8ykWuRemtLaoB4I9_4/edit?usp=sharing
<- Or scan the QR code

That’s all folks

You can always find me on fediverse (or email) at:

@benjojo@benjojo.co.uk