SSL/TLS and Certificates

Let's get some of the basics down!

What's involved?

- We want to make sure the traffic accessing our website is encrypted
- We need to enable HTTPS
- HTTPS requires a certificate to enable TLS

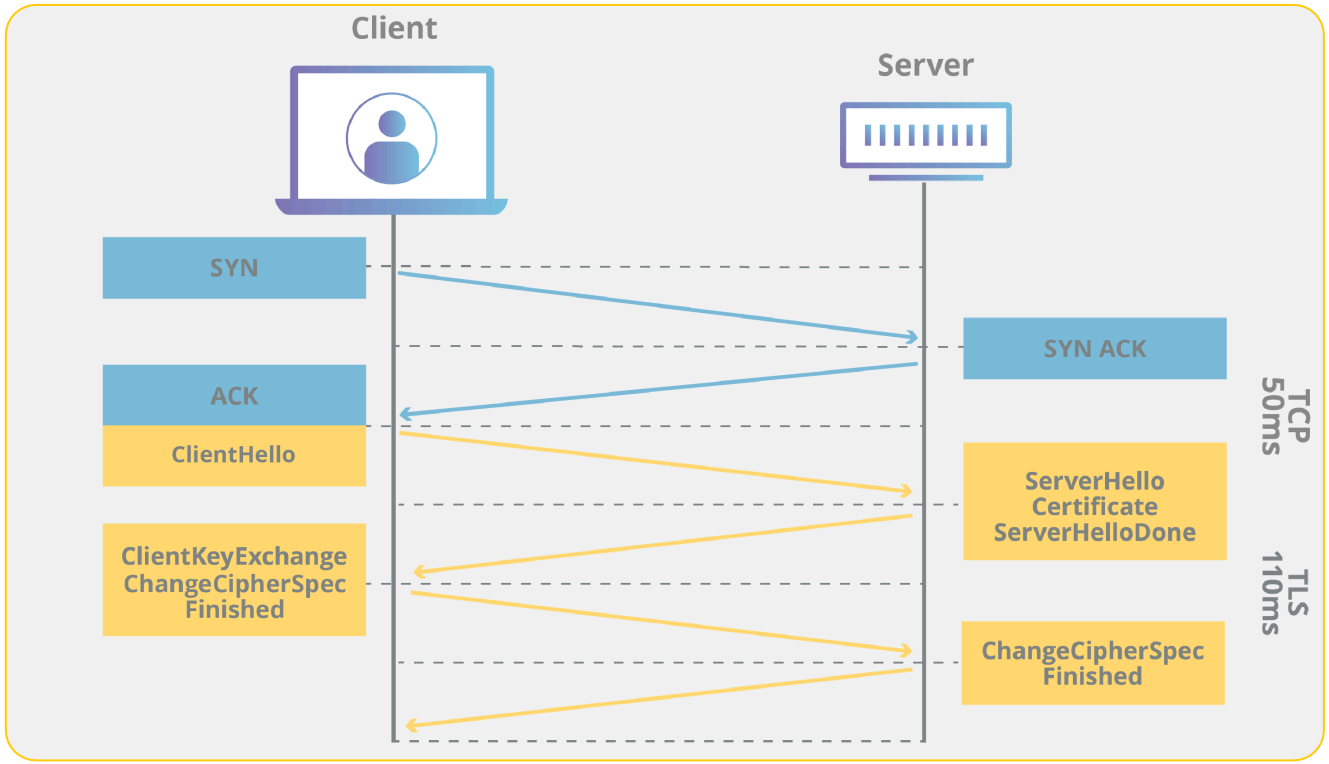
You might hear 'SSL' and 'TLS' used interchangeably. We use TLS now, but some people still say SSL 🤷‍♀️

Let's get a bit more detailed….

- Without TLS, your HTTP traffic could be intercepted and read in a 'MITM' attack
- Certificates provides data encryption when interacting with a website
- Certificates use public and private keys for encryption
- Pub and Priv keys work together, and used alone aren't used for decryption
- Certificate Authorities ensure a Pub key provided from a server's certificate is legit

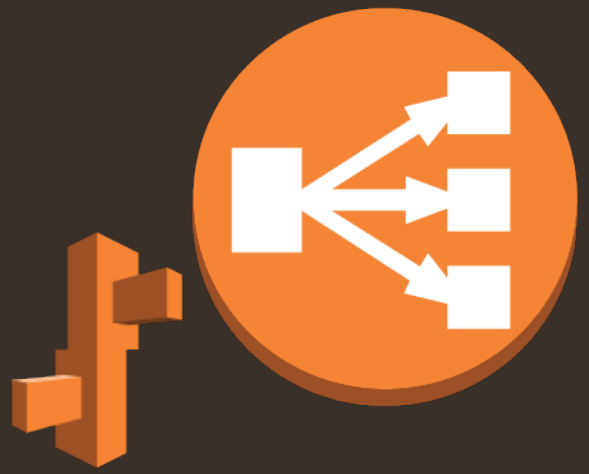
The Handshake

"TLS is an encryption protocol designed to secure Internet communications. A TLS handshake is the process that kicks off a communication session that uses TLS encryption. During a TLS handshake, the two communicating sides exchange messages to acknowledge each other, verify each other, establish the encryption algorithms they will use, and agree on session keys. TLS handshakes are a foundational part of how HTTPS works."

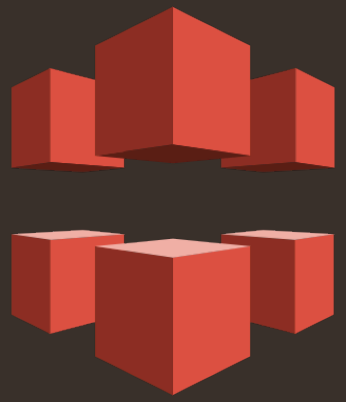


https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

What can have a cert?



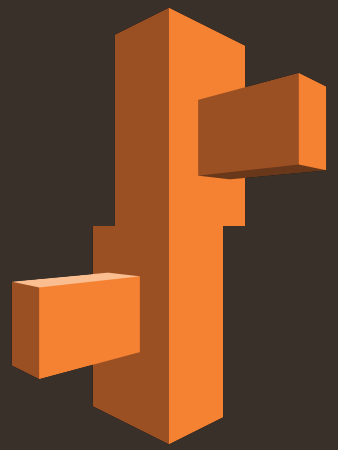
AWS Load Balancers
(and Elastic Beanstalk)



Cloudfront

API Gateway

What are we looking at today?



Route 53 Domain

AWS Certificate Manager

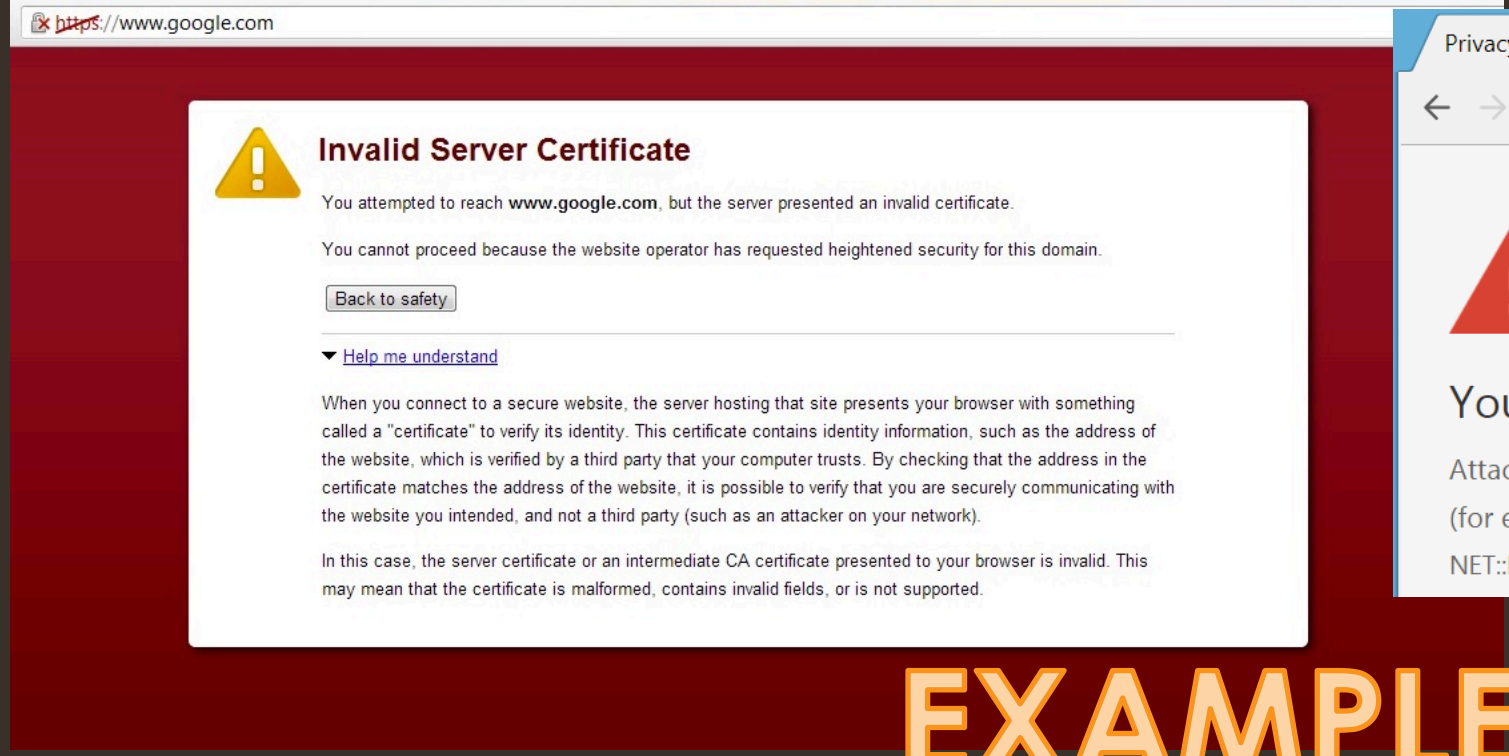
Load Balancer

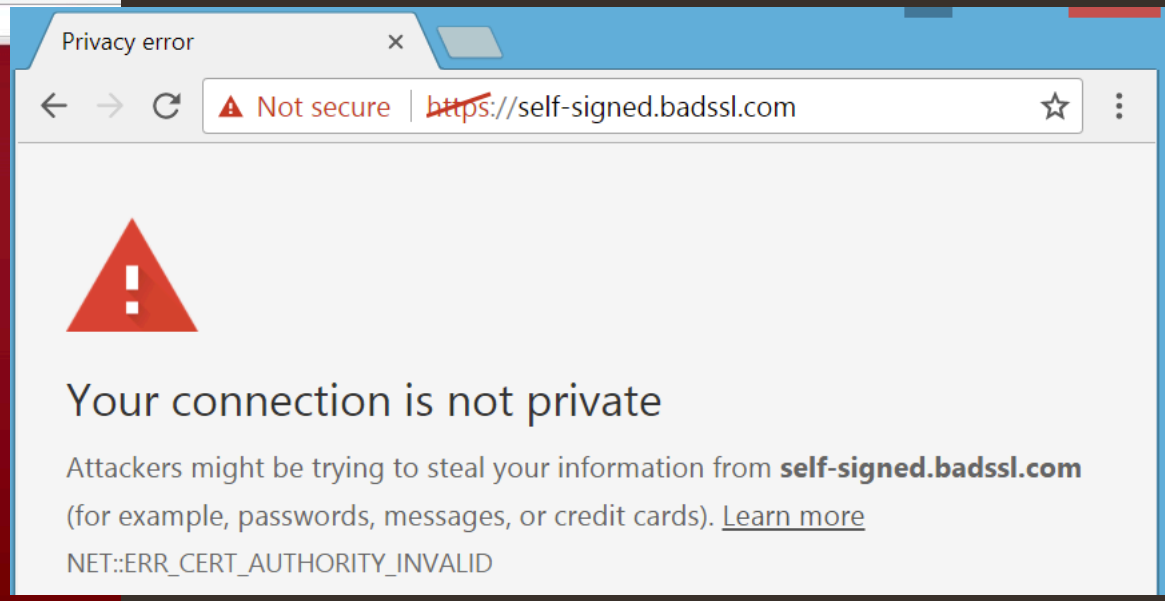
Certificate Expiry

- Certificates do require renewal
- If the certificate is associated with some AWS resources it can be auto-renewed

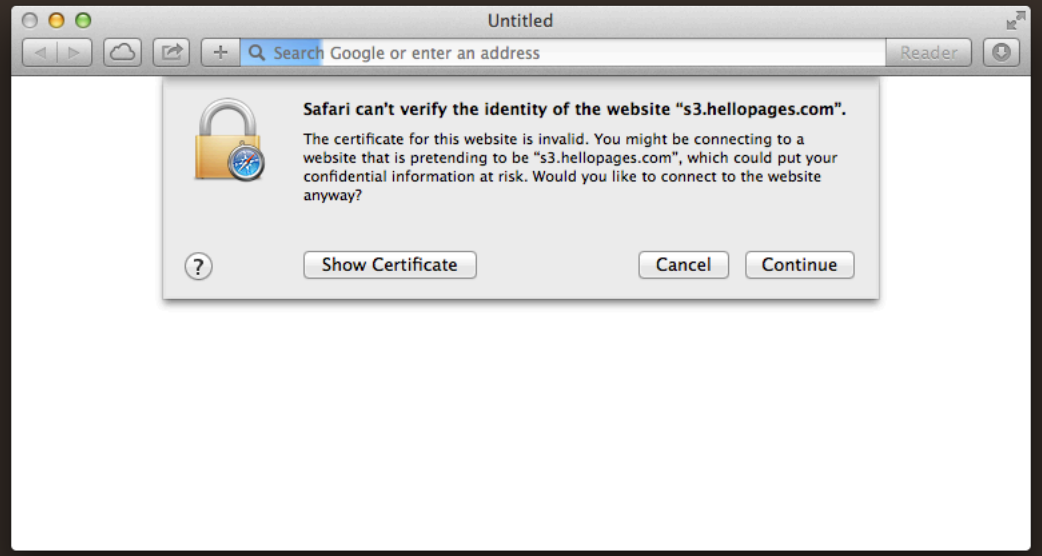
- Certificate expiry may be an indication of a broader cultural issue related to security

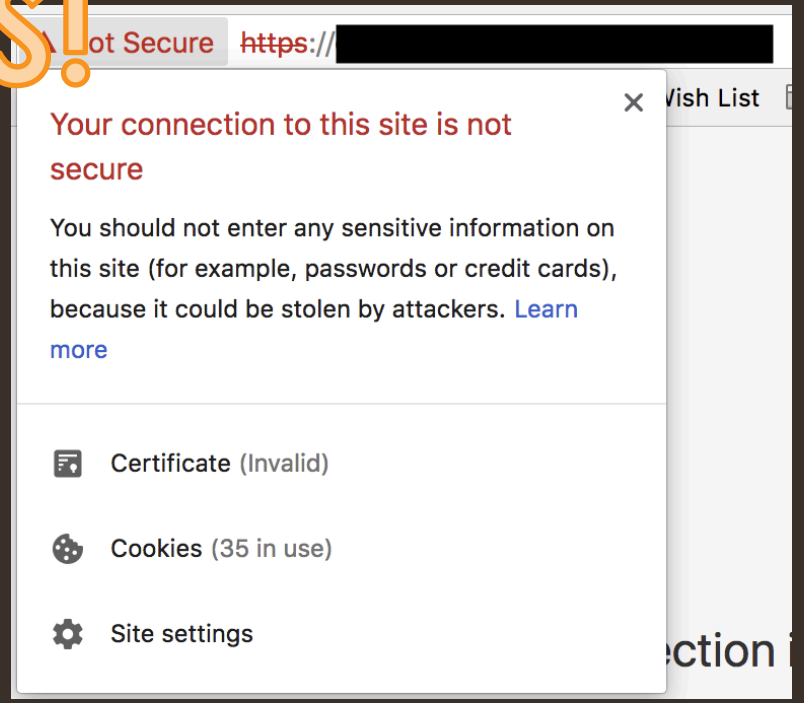
- It doesn't look good for that company!


https://www.google.com
Invalid Server Certificate
You attempted to reach www.google.com, but the server presented an invalid certificate.
You cannot proceed because the website operator has requested heightened security for this domain.
Back to safety
Help me understand
When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).
In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. This may mean that the certificate is malformed, contains invalid fields, or is not supported.


Privacy error
Not secure
https://self-signed.badssl.com
Your connection is not private
Attackers might be trying to steal your information from self-signed.badssl.com (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID

EXAMPLES!


Untitled
Search Google or enter an address
Reader
Safari can't verify the identity of the website "s3.hellopages.com".
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "s3.hellopages.com", which could put your confidential information at risk. Would you like to connect to the website anyway?
Show Certificate
Cancel
Continue


ot Secure
https://[redacted]
Wish List
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
Certificate (Invalid)
Cookies (35 in use)
Site settings

Bug Bounty Example

- Ubiquiti (50days expired): https://hackerone.com/reports/220615