Cryptography - SSL

Network Security Workshop

25-27 April 2017

Bali Indonesia

Issue Date: [31-12-2015]

Revision: [V.1]

APNIC

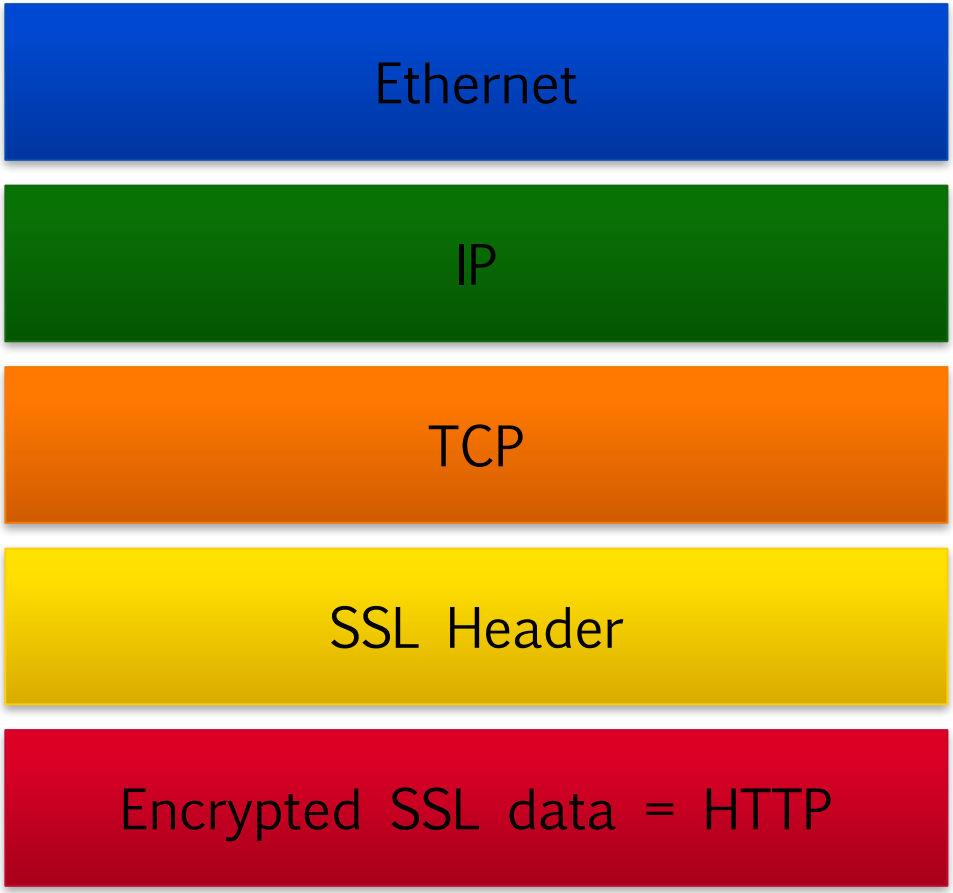
History

- Secure Sockets Layer was developed by Netscape in 1994 as a protocol which permitted persistent and secure transactions.
- In 1997 an Open Source version of Netscape's patented version was created, which is now OpenSSL.
- In 1999 the existing protocol was extended by a version now known as Transport Layer Security (TLS).
- By convention, the term "SSL" is used even when technically the TLS protocol is being used.

TLS/SSL : What it does

- Encryption
- Integrity
- Authentication

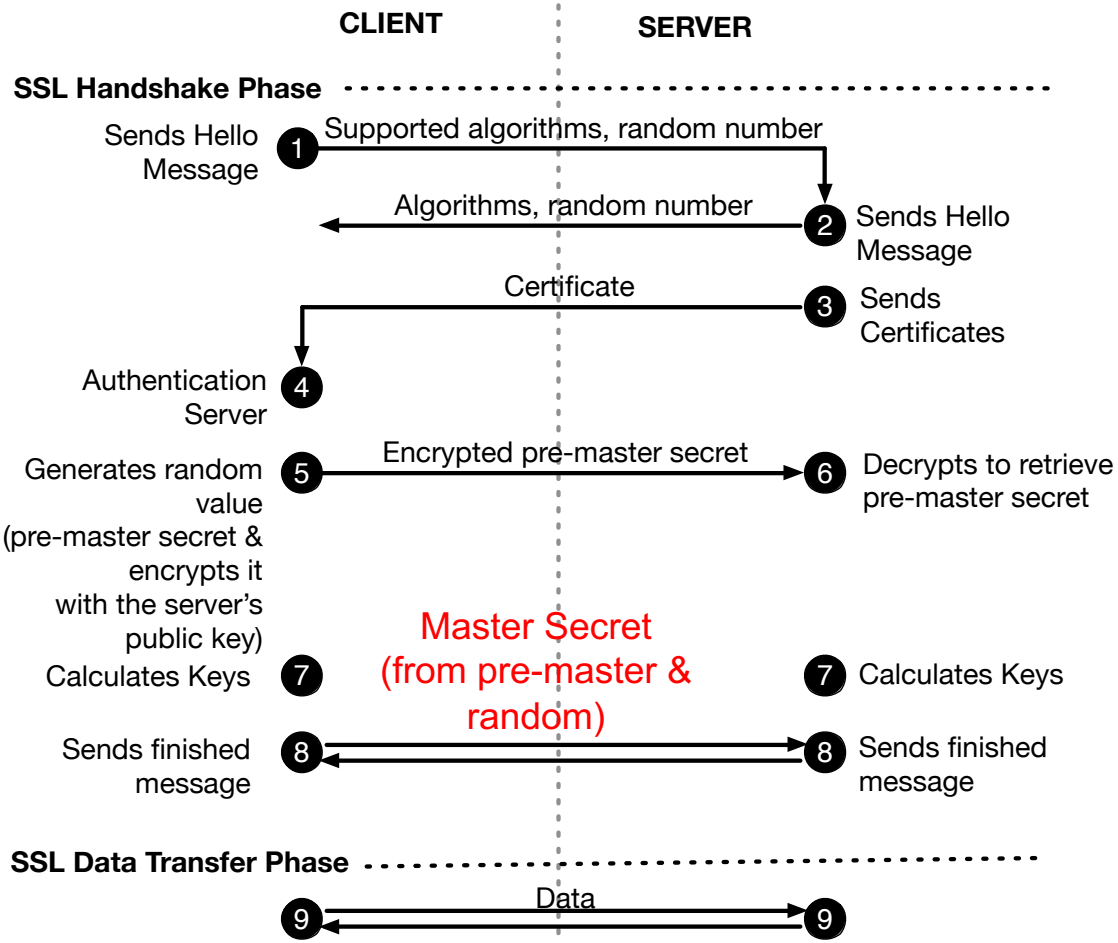
Location of SSL Protocol & TCP Ports



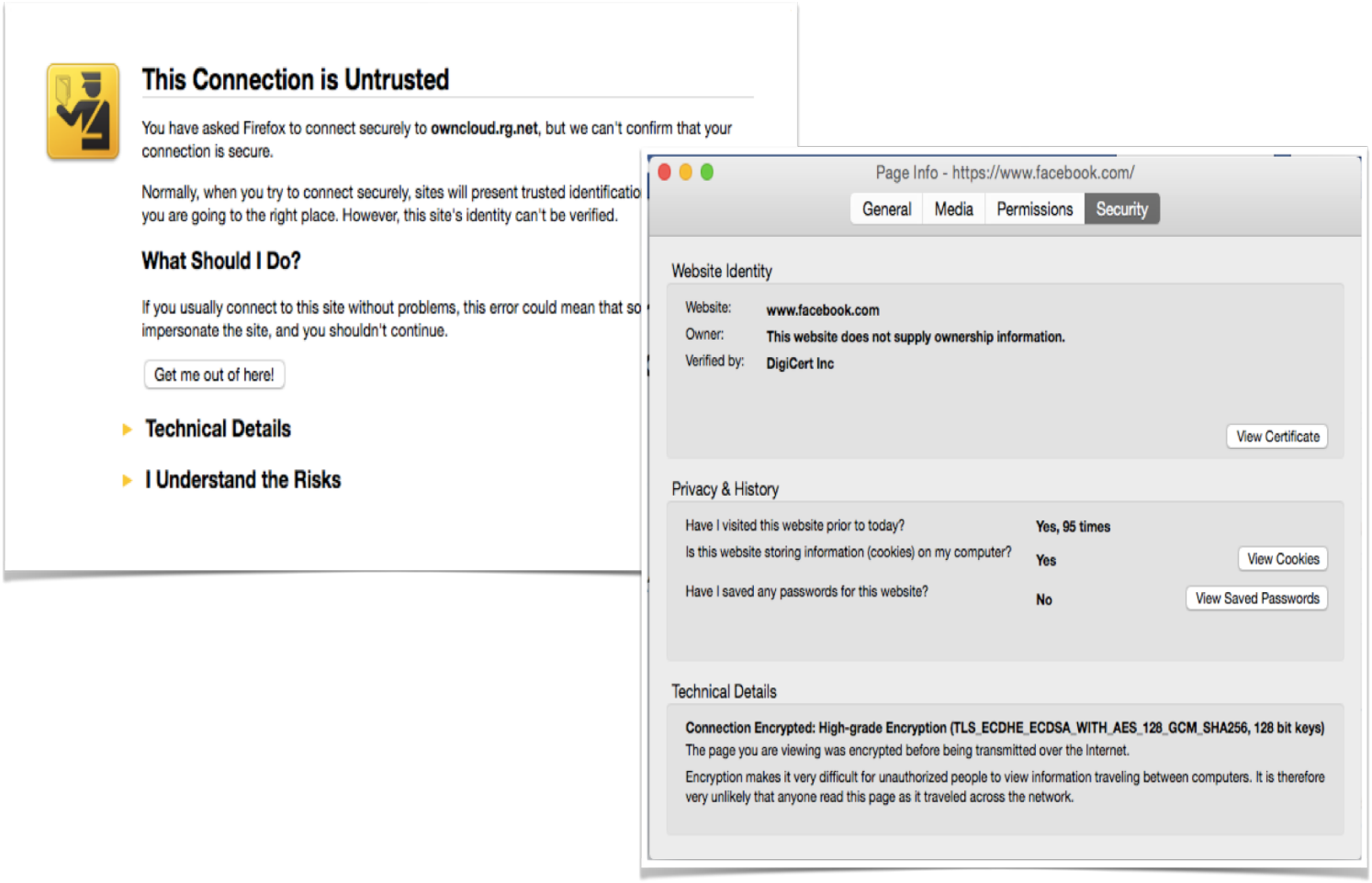
SSL Operations

- Application calls SSL connect routines to set up channel.
- Public Key cryptography is used during handshake to authenticate parties and exchange session key.
- Symmetric Key cryptography (using session key) is used to encrypt data.

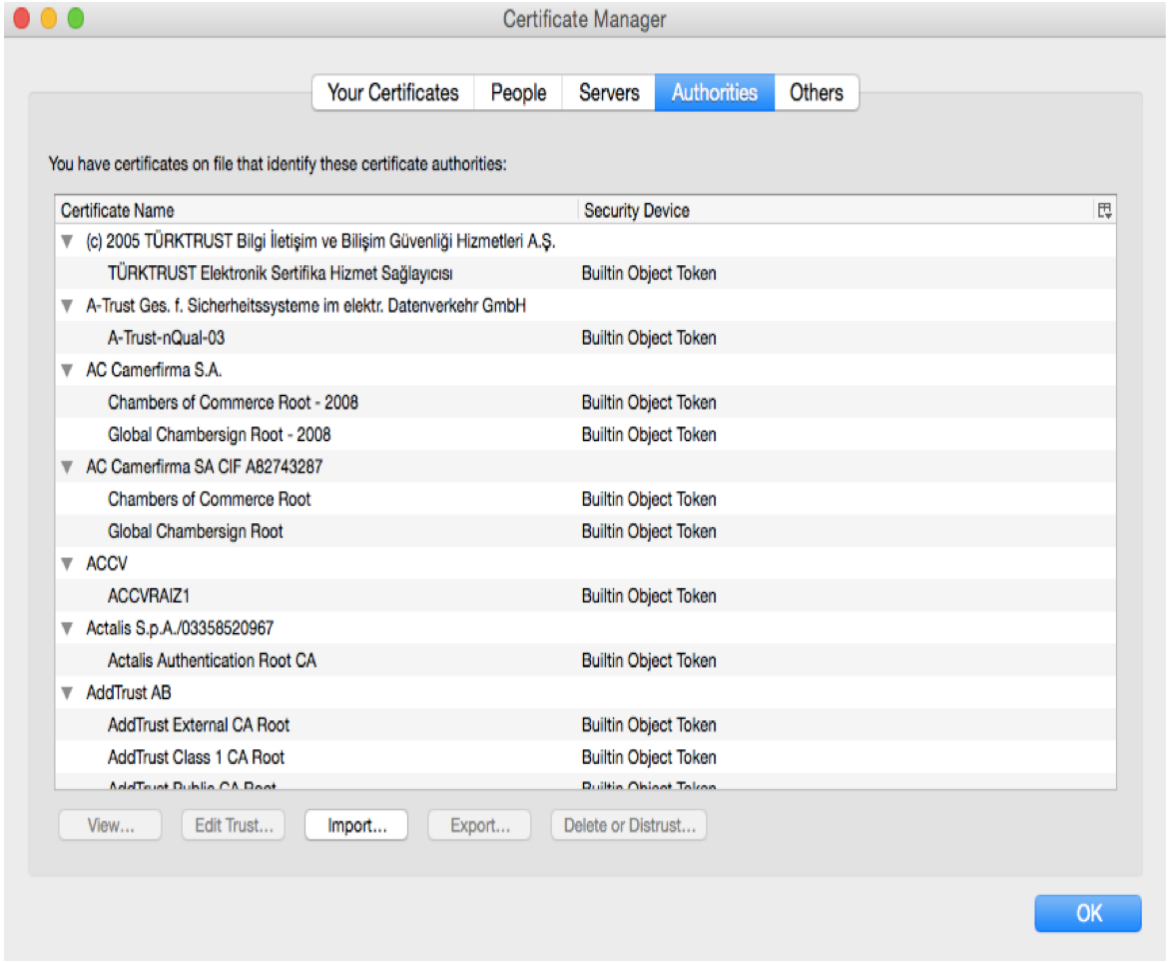
How SSL Works



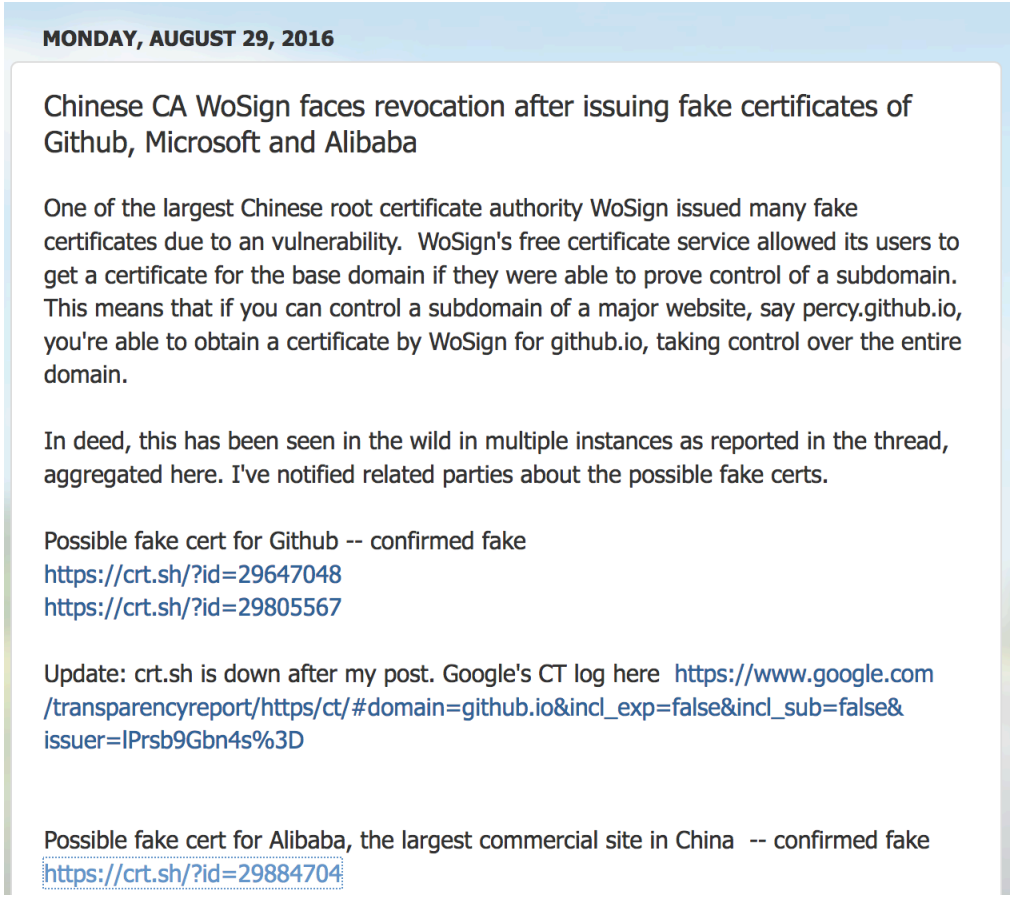
Trusted vs Non Trusted Certificate



Certificate Authority



Chinese CA WoSign faces revocation after issuing fake certificates of Github, Microsoft and Alibaba



MONDAY, AUGUST 29, 2016

Chinese CA WoSign faces revocation after issuing fake certificates of Github, Microsoft and Alibaba

One of the largest Chinese root certificate authority WoSign issued many fake certificates due to an vulnerability. WoSign's free certificate service allowed its users to get a certificate for the base domain if they were able to prove control of a subdomain. This means that if you can control a subdomain of a major website, say percy.github.io, you're able to obtain a certificate by WoSign for github.io, taking control over the entire domain.

In deed, this has been seen in the wild in multiple instances as reported in the thread, aggregated here. I've notified related parties about the possible fake certs.

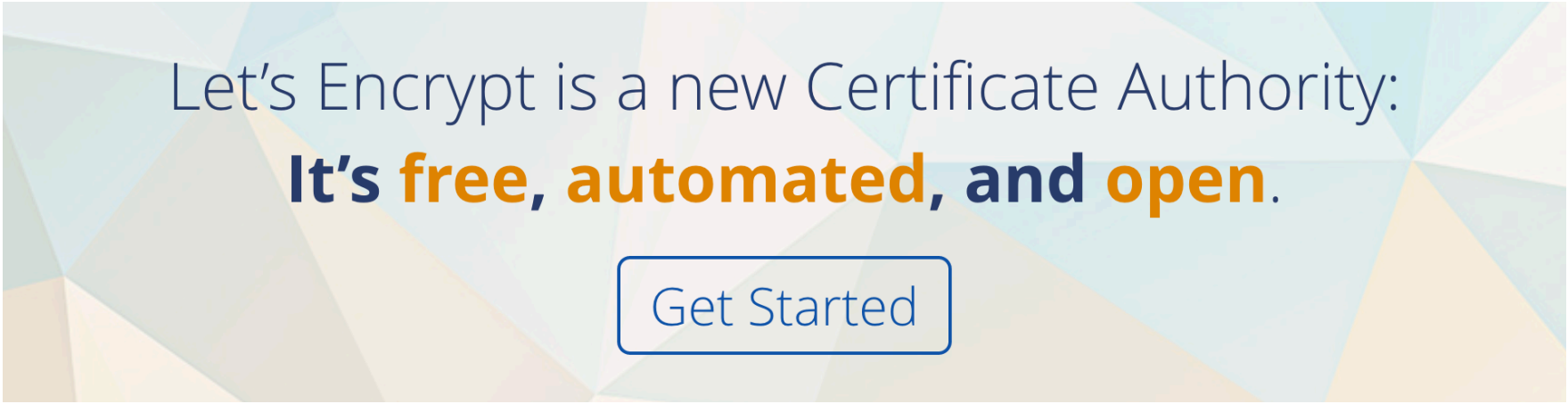
Possible fake cert for Github -- confirmed fake
https://crt.sh/?id=29647048
https://crt.sh/?id=29805567

Update: crt.sh is down after my post. Google's CT log here https://www.google.com/transparencyreport/https/ct/#domain=github.io&incl_exp=false&incl_sub=false&issuer=IPrsb9Gbn4s%3D

Possible fake cert for Alibaba, the largest commercial site in China -- confirmed fake
https://crt.sh/?id=29884704

https://groups.google.com/forum/m/#!topic/mozilla.dev.security.policy/k9PBmyLCi8I/discussion

Introducing Let'sEncrypt



https://letsencrypt.org/

Introducing Let'sEncrypt

- Which browsers and operating systems support Let's Encrypt
  - https://community.letsencrypt.org/t/which-browsers-and-operating-systems-support-lets-encrypt/4394
- Check your browser
  - https://wiki.apnictraining.net

LAB