SECURITY

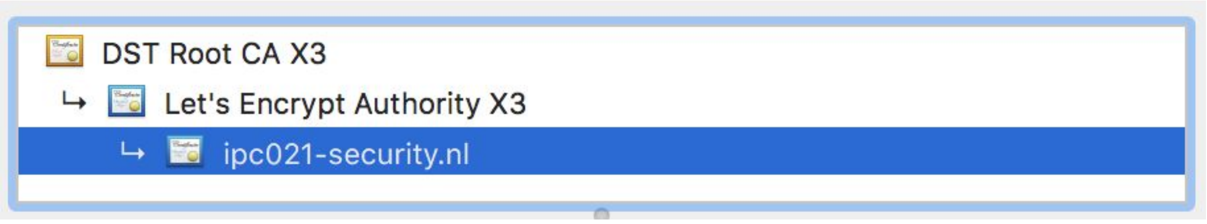
Assignment 11, Monday, December 12, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Exercise 1

A. Let’s encrypt

B. 

DST Root CA X3
↳ Let's Encrypt Authority X3
↳ ipc021-security.nl

C. Expires: Wednesday, 10 January 2018 at 10:52:37 Central European Standard Time

D. PKCS #1 SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

E. The certificate is for the wrong domain. The certificate is only valid for the subdomain: “notthefirstsubdomain.ipc021-security.nl”

F. The error given in the browser reads as:

firstsubdomain.ipc021-security.nl uses an invalid security certificate. The certificate is only valid for notthefirstsubdomain.ipc021-security.nl Error code: SSL_ERROR_BAD_CERT_DOMAIN

For example this makes the user of the browser prone to MITM attacks. To prevent this from happening, the browser notifies the user of this problem.

G. Method 2: Physical exchange
Method 3: Web of trust
Method 4: TOFU

H. Method 2: The main downside is that all cryptography requires trust in devices! You cannot quickly exchange certs as you have to go meet each other.
Method 3: When you have a new key, you have to let a couple of friends sign it before you can actually use it.

Method 4: Dangers of a MITM make that you have to secure your own machine very well which could make it less usable.

I. The content of this page was not encrypted when it was sent from the server. This makes it possible for an eavesdropper to see the content (partially) that was sent. This is caused by a javascript file with the name: somescript.js in the block: "`<script src="http://yetanothersubdomain.ipc021-security.nl/somescript.js"></script>`" which is sent over http instead of a secure https connection.

Exercise 2

The data for this exercise is sent by email to the required adres. To be sure nothing went wrong, we sent the following message:

The names and properties of the keys are below each other

Carlo Jessurun s1013793
Key ID: B518E909
Fingerprint:
4C86 13D5 AD13 67EF F7E6=C2=A0 E4E7 D42A 66FF B518 E909

Signed the Keys with the following ID:
Tony: 37ECF14A
Heda:=C2=A0 1B94DC58

Tony Lopar s1013792
Key ID: 37ECF14A
Fingerprint:
01A0 6822 1F2F 1C39 DDE5 F74E 79FF 4F6C 37EC F14A

Signed the Keys with the following ID:
Carlo: B518E909
Heda:=C2=A0 1B94DC58
Anass: B7910D5C