INSA Lyon Télécommunications

4TC-CSC Cryptographie et Sécurité des Communications
Semester 1, 2024

TD TD : Public Key Infrastructure for the Web

Background

This exercise sheet takes a closer look at public key certificates. You will occasionally be asked to visit various web sites. Please use Chrome in the first instance, although you are welcome to also test these out using other browsers.

Exercise 1: Public key certificate basics

Public key certificates are crucial to supporting the security of any application using public key cryptography.

QUESTION 1

What is the purpose of a public key certificate?

It is time to look at a public key certificate.

Visit `https://www.insa-lyon.fr/`.

We are going to use this example across several exercises, so do not close it at the end of Exercise 1.

Click on the padlock icon.

QUESTION 2

(a) Is the public key certificate currently valid, and what does this actually mean?

(b) Click on "Learn more" after the mention "Connection is secure".

What is Google's definition of a certificate? To what extent do you think the certificate actually does any of these things?

(c) Click on the "Certificate is valid" link. Who is this certificate issued to?

(d) Who issued this certificate? In other words, which CA?

Visit the website of the CA and take a few moments to look around and see what services they offer.

cont/...

QUESTION 3

What is your opinion about this CA? Do you trust them to do a good job? Explain the opinion that you have about them.

Go to the webpage of the CA. Go to their Services. Find the ones related to Security, and then to Trusted Certificate Services (TCS). Finally, find the WIKI page.

QUESTION 4

- Who is the TCS partner?
- Again, what is your opinion about this CA?

QUESTION 5

(a) The full Common Name (CN) of the CA is GEANT OV RSA CA 4. What does OV mean? What does RSA suggest? What does 4 refer to?

(b) What disclaimers are made here about the extent to which you can rely on a certificate? Do you think these are reasonable?

Exercise 2: Public key certificate contents

We now take a more detailed look at a public key certificate.

Return to the Certificate information (if not still open, select padlock then select Certificate). Click on the Details tab.

You can now see links to all the details of the public key certificate, which is essentially a data structure containing everything you might need to know about the certificate. Clicking each entry on the list should reveal more information. The next series of questions explore different aspects of the certificate contents.

Optionally, you might want to use the Export option to export the certificate (just go with default settings to do so). The next tasks may be easier when the certificate is stored locally but up to you.

QUESTION 6

(a) The Version field should display V3. What does this mean?

(b) For which websites can this public key be used?

(c) How long is this certificate valid for?

cont/...

(d) What cryptographic algorithms did the CA use to digitally sign this certificate?

(e) What is the INSA Lyon's public key? Check the value of the modulus.

(f) What two primes did INSA Lyon use to generate this public key?

(g) The public key parameters (Public Exponent) are 01 00 01, what does this mean?

(h) Where would you go to find out if INSA Lyon's private key was compromised last week (assuming that someone has realised this!)?

The next questions relate to the SCT List field. Google searches may help!

QUESTION 7

(a) What does SCT stand for?

(b) What is the purpose of the SCT?

(c) How much does an SCT cost?

Let's consider the usage of the public key.

QUESTION 8

(a) What two actions are you allowed to use this public key for?

(b) Why do you think "encrypting data" is not one of the permitted uses?

The certificate thumbprint (also called fingerprint) contains a hash of all the data in the certificate (the hash is computed over all certificate data and its signature.). This is mainly used as a quick means of checking whether two certificates are the same.

QUESTION 9

(a) What hash function was used to compute this thumbprint? You may need Google to find that out!

(b) Why is the thumbprint not actually included in the certificate (rather, your browser has computed it when you asked to inspect the certificate details)?

We have looked at most of the fields of the certificate here. However, there is one **absolutely vital** field of a public key certificate that we have not looked at!

cont/...

QUESTION 10

(a) What is missing?

(b) What is its value?

Exercise 3: Public key certificate paths

It is time to look at the certificate path.

Return to the basic Certificate information (if not still open, select padlock then select "Certificate is valid") or your downloaded copy of the Certificate. Look at the Certificate Hierarchy.

The certificate for INSA Lyon's public key is at the bottom of a "chain" of three certificates.

It is time to find out about the CA that issued INSA Lyon's certificate. Select the next certificate in the chain above `www.insa-lyon.fr` *and view the certificate.*

QUESTION 11

(a) What is the name of the CA which signed INSA Lyon's certificate?

(b) Is this CA's public key longer (offering better security) than INSA Lyon's public key? Explain why or why not.

(c) Is this CA's public key valid for longer that INSA Lyon's public key? Explain why or why not.

(d) What can this CA's public key be used for?

Now we inspect the root certificate.

Select the top certificate in the chain.

QUESTION 12

(a) Who signed the certificate of the CA that signed INSA Lyon's certificate?

(b) What cryptographic algorithms did the root CA use to digitally sign the certificate that it issued? What do you notice?

(c) Who signed the certificate of the CA that signed the certificate of the CA that signed UC's certificate?

The answer to the last question is of course "nobody", it is installed in your browser! But we should better check this.

Navigate to `chrome://settings`*. Under Privacy and Security, click Security and then click Manage Certificates. Select Authorities.*

cont/...

QUESTION 13

There are several root CAs from INSA Lyon's certificate provider on this list. Which is the correct one?

Exercise 4: Issuing public key certificates

Public key certificates bind identities to public keys, and CAs are the organisations trusted to do this binding. So how do they do it?

Sectigo currently operates 4 modern root certificates, including the USERTrust RSA Certification Authority that we have found. Go to the Sectigo webpage. Find the Certification Practices Statement (CPS) document and read Section 3.2.2.

QUESTION 14

What general techniques does the CA use to determine whether an applicant organisation for a certificate is who they claim to be? Just extract the main techniques from a high level read.

Now we see what is required if an **individual** (like you or me!) applies for a certificate.

Navigate to Section 3.2.3.

QUESTION 15

What does the CA use this time to determine whether a human applicant for a certificate is who they claim to be?

For some types of certificate (but not all), it is wise/necessary for the CA to check that the public key certificate applicant actually knows the corresponding private key (a process sometimes called demonstrating **proof of possession**).

QUESTION 16

(a) If a proof of possession is NOT done, what might an attacker do, and what attack could they perform as a result?

(b) How does this CA conduct proof of possession checks?

Exercise 5: Invalid public key certificates

To finish, we see what happens when a certificate is invalid.

Navigate to `https://expired.badssl.com/`.

There is nothing special about this website, I found it when web searching for invalid certificates!

cont/...

QUESTION 17

How does Chrome warn you that something is wrong?

Click on the warning in the address bar. Click on the Certificate link.

Navigate to `https://www.ssllabs.com/analyze.html?d=expired.badssl.com/` *to get more information about the above website.*

QUESTION 18

(a) What is the problem with the public key certificate?

(b) What would you advise a visitor to this web site to do next?

(c) Which CA issued this certificate?

The CA that issues this certificate is very interesting and represents a relatively new initiative.

Visit the website of the CA that issued this certificate and take a look around the site.

QUESTION 19

(a) Why was this CA established and what makes it different to the CA that we looked at earlier?

(b) How long do certificates issued by this CA last and why has the CA chosen this relatively short timeframe?