Security

Assignment 11, Wednesday, December 2, 2015

Handing in your answers: the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Brinda or Joost).

Deadline: Thursday, December 10, 24:00 (midnight) sharp!

Goals: After completing these exercises successfully you should be able to

- analyse relations among certificate within a certificate chain;
- examine and evaluate certificates on the web;
- use GnuPG to send signed and encrypted email.

Marks: You can score a total of 100 points.

1. **(20 points)** Let C_X^Y be (ad hoc) notation for a public-key certificate[1] of X, signed by Y. Consider a system that consists of the agents P, Q, R, S and only the following three certificates

   $$C_Q^P, \;\; C_R^P, \;\; C_S^R.$$

   Assume further that everybody knows his own key pair and also P's public key.

   Explain briefly which certificates (and thus: which public keys) are needed by both agents S and Q in order to securely perform the following tasks.

   (a) S sends a confidential message to Q.

   (b) S sends a signed message to Q, and Q verifies this message.

2. **(30 points)** Now let us see how PKI certificates look in practice. In this exercise you have to find out details about the public-key certificate of the ABN AMRO's web site (`https://www.abnamro.nl/`).

   (a) What is the root certificate authority (CA) of this certificate? Is this certificate still valid in 2018?

   (b) How long is the certificate chain? Describe the whole chain.

   (c) When does the ABN AMRO certificate expire?

   (d) How did the CA sign ABN AMRO's public key? Specify the hashing and signature scheme.

   (e) How many bits are the public key and the signature?

   (f) What are the last 8 bits of ABN's public key and of the signature?

[1] In this exercise, a certificate C_X^Y simply contains the public key of X and the signature of Y on it. For a more detailed discussion, see Wikipedia: `http://en.wikipedia.org/wiki/Public_key_certificate`

(g) Can you deduce from this certificate, how the client's browser authenticates itself to the ABN AMRO's web server?

(h) You probably found the fingerprints at the bottom of the certificate. What do these fingerprints account for?

(i) Why do you think there are two types of fingerprints?

3. **(50 points)** In this question we ask you to use PGP (Pretty Good Privacy) which allows you to send and receive encrypted and/or signed e-mails. To do this, you need to create your own PGP-identity which is basically your e-mail address and public key signed with your private key. For this purpose we recommend the combination of *Thunderbird*[2] with the extension *Enigmail*[3] which uses *GnuPG*[4]. The latter is an open-source implementation of the OpenPGP standard (RFC4880).

   (a) Find out how PGP works by performing the following steps (additional information is available in the Enigmail Quick Start Guide[5]):

      i. Generate a PGP-identity, and submit it to the public key server `pgp.mit.edu`. This can either be done by using the command line or by using *Enigmail*.

      ii. Sign the key of at least one other student, and convince at least one other student to sign your key. Remember to upload the signed public keys to the key server to make your signature public.

      iii. Refresh the public key information from the key server to verify that the keys have been signed. Note that there might be some delay between your upload and actual publication.

   (b) Now you have a PGP-identity you can use it to e-mail securely. Send an **encrypted** and (digitally) **signed** e-mail with the subject "Assignment 11" using the e-mail address and key ID according to your TA group.

   Note: While a 32-bit key ID is nice and short to communicate to people, it is not a secure way to uniquely identify keys. In fact, 32-bit keys are very easy to spoof. When in doubt, always check the 128-bit fingerprint. For more information about this, including software that can brute force key IDs, see `https://evil32.com`. If you feel like giving it a try, please do not push the spoofed key to the key servers. This may lead to confusing situations, as not all clients handle this properly..

TA group	E-mail	Key ID
Brinda	`rick.erkens@student.ru.nl`	`A1FF87A4`
Joost	`koenvaningen@student.ru.nl`	`BD3145B4`

Key ID	Fingerprint
`A1FF87A4`	`569A 2549 2A5C F153 56D0 8A6C D5C9 9405 A1FF 87A4`
`BD3145B4`	`C906 2318 A5AC BFF5 07D8 B2E5 35EC 2CD6 BD31 45B4`

   The message should contain: your **name**, your **S-number**, your public **key ID**, your **key fingerprint** and the **key ID(s)** of the key(s) you signed. If you are doing this exercise in pairs, it is still advisable to set up keys individually.

   It is a good idea to first send this to another student, using her/his public key, and see whether it works!

   Note: The solutions to the other two exercises should still be submitted via Blackboard!

[2] `http://www.getthunderbird.com/`
[3] `http://enigmail.mozdev.org/download/` or `https://addons.mozilla.org/thunderbird/addon/enigmail/`
[4] `http://www.gnupg.org/download/`
[5] `http://enigmail.mozdev.org/documentation/quickstart.php.html`