Security

Assignment 11, Friday, December 8, 2017

Handing in your answers:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Bart or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, December 18, 09:00 sharp!

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

- identify characteristics and problems of real-world certificate use
- use PGP to send and receive encrypted email

Marks: You can score a total of 100 points.

1. **(50 points)** In this question, we look at PKI certificates in practice. First, we look at the certificate used for `https://ipc021-security.nl`.

   Note: recent versions of Google Chrome made it a bit more tricky to find certificate information. Look for the 'Security' tab in the 'Developer tools' (listed under 'More tools'). In most other browsers, clicking the padlock icon in front of the URL is a good place to start.

   (a) Who signed this certificate?

   (b) Which certificates exist in the entire chain?

   (c) When does this certificate expire?

   (d) What hash function and signature algorithm were used to create the signature?

   Now look at the certificate used for `https://firstsubdomain.ipc021-security.nl`.

   (e) Your browser rejects this certificate (at least, it should!). What is wrong with the certificate?

   Now look at the certificate used for `https://anothersubdomain.ipc021-security.nl`.

   (f) Again, your browser should not accept this certificate. Why not? Be specific!

   (g) Some people do actually use certificates like this in practice (in particular, when they do not want to use or support the CA system). There are three other common ways to establish some 'trust' in public keys. List these three methods.

   (h) For each of these methods, describe what its disadvantages are (in terms of usability and/or security) compared to each other or the CA system.

   Now look at the page available at `https://yetanothersubdomain.ipc021-security.nl`.

   (i) Most of this page looks just fine. However, depending on your browser setting, you should get a warning indicator, or some of the content might even be missing. Explain what the problem is on this page.

2. **(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 essentially comes down to a signature on the combination of e-mail address and a public key). For this purpose we recommend the combination of *Thunderbird*[1] with the extension *Enigmail*[2] which uses *GnuPG*[3]. The latter is an open-source implementation of the OpenPGP standard. Feel free to use alternatives (such as the *GPG Suite*[4] for Mail on macOS), but note that we may not be familiar enough with other tools to answer questions.

   (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 one of the standard public key servers (such as `pgp.surfnet.nl` or `pgp.mit.edu`).

      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, especially when synchronizing between different key servers.

   (b) Now that you have a PGP identity, you can use it to e-mail securely.

      i. Retrieve the key matching the fingerprint listed below from your favorite key server (or from the exercise website).

Key ID	**Fingerprint**
E827 F020	24E4 1AAC 01D3 A53A 163A FC56 90DB 16C0 E827 F020

      ii. Send an **encrypted** and digitally **signed** e-mail to `ipc021-security@cs.ru.nl`, including "Assignment 11" in the subject line. The message should contain: your **name**, your **student number**, your public **key ID**, your **key fingerprint** and the **key ID(s)** of the key(s) you signed.

   Note: If you are doing this exercise in pairs, it is advisable to set up keys individually (so that you both have a key), but please send us **one** email containing both fingerprints.

   It is a good idea to first send an email to another student (using their public key!) to test if it all works.

   Note: The solutions to exercise 1 should still be submitted as a PDF via Blackboard!

   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 full 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 can actually deal with this attack..

[1] `http://www.getthunderbird.com/`

[2] `http://enigmail.mozdev.org/download/` or `https://addons.mozilla.org/thunderbird/addon/enigmail/`

[3] `http://www.gnupg.org/download/`

[4] `https://gpgtools.org/`

[5] `http://enigmail.mozdev.org/documentation/quickstart.php.html`