Assessed Coursework 2 - Certificates

Hamish Taylor

This assessed coursework is for 4th year BSc students taking F20CN and MSc students taking F21CN. It is worth 20% of the overall course mark for Computer Network Security. It is one of two pieces of assessed coursework for this course.

Plagiarism

I have uploaded a set of slides, entitled "Academic Misconduct" with more details on plagiarism and other forms of academic misconduct as well as a few tips on how to avoid them. You can find the slides in the same folder as this description. Notable things to take into consideration:

- Coursework reports must be written in your own words and any code in your coursework must be your own code. If some text or code in the coursework has been taken from other sources, these sources must be properly referenced.
- Failure to reference work that has been obtained from other sources or to copy the words and/or code of another student is plagiarism and if detected, this will be reported to the School's Discipline Committee. If a student is found guilty of plagiarism, the penalty could involve voiding the course.
- Students must never give hard or soft copies of their coursework reports or code to another student. Students must always refuse any request from another student for a copy of their report and/or code.
- Sharing a coursework report and/or code with another student is collusion, and if detected, this will be reported to the School's Discipline Committee. If found guilty of collusion, the penalty could involve voiding the course.
- And remember: the consequences of taking unacceptable short cuts in coursework are much worse than getting a bad mark (or even no marks) on a piece of coursework. There has been one case this year where a student was awarded on Ordinary degree (rather than an Honours degree) because of the sanction imposed by the University's Discipline Committee. The offence was plagiarism of coursework.

Further information on academic misconduct can be found in: https://www.hw.ac.uk/students/doc/discguidelines.pdf

Your coursework submissions will be automatically checked for plagiarism.

Late Submission

As per our new coursework submission regulations, no individual extensions can be granted. Late submission by up to 5 days will receive a penalty of -30%. Note that a 1-day late submission receives the same penalty as 4-days late one. After that, no submission will be allowed. If you have mitigating circumstances, contact the AAO for an MC form immediately.

Tasks Description

This coursework is an exercise in creating and using X.509 and PGP certificates. It involves developing a Java Rich Internet Application or RIA (web start application or applet) that can be securely used to sign messages digitally. The work should be done in pairs. However, pairs of students also have to join together with other pairs to form a wider group of people who are prepared to sign each other's certificates. Students finding it difficult to find partners and groups should contact me by e-mail. I will endeavour to put them in touch with other such individuals.

Each pair should perform the following tasks:

- Create self-signed PGP certificates and private keys for each of them.
- Create a self-signed X.509 certificate and private key for the pair.
- Form a larger group with the rest of the class and do group activities (see below)
- Get their local CA to sign their X.509 certificate.
- Write RIA to create file signatures with either of their PGP private keys.
- Sign RIA with private key corresponding to the pair's X.509 certificate.
- Set-up sensible security to run the RIA.
- Demonstrate their RIA works correctly by the due date (see below).
- Submit a written report describing their work by the due date (see below).

X.509 certificates should have a sensible X.500 name. PGP certificates should have sensible identifiers of their owner and include at least an e-mail address and a small photograph of them. Students should exercise due diligence in key parties when signing each other's PGP certificates. The RIA should enable a user to select a message in the local file system, select a user (one of the pair) and input their passphrase to access their private key in a private keyring in the local file system and create a digital signature of the message with that key in a second local file.

The wider group and CA should:

- Create a private key and X.509 certificate for a local certificate authority.
- Exercise due diligence in using key to sign member pair's certificates.
- Hold a key party for members to sign each other's OpenPGP certificates.

The local CA should be given a suitable X.500 name and have a self-signed X.509 certificate created for it. It may be appropriate to take steps to ensure that this certificate has the basic constraint extension set on it to identify it as a CA certificate.

Setting up security for their RIA will require the Java Control Panel import their group CA certificate as a trusted signatory of certificates. It may also require setting permissions in the JVM's Java policy file. Its location can be found by running the Java console and listing its deployment properties. The advanced settings of the Java Control Panel can make the Java console show itself.

The demonstration that their RIA works should:

- Launch the RIA (web start application or applet) using a web browser.
- Enforce security on the signed code via Java security policies.
- Show code creates a signature for a message with group member's private key.

- Prove that the message's signature can be verified using the signer's PGP public key.

The written report should:

- Succinctly describe your work - what they and group did and what they produced.
- List certificates, JNLP/HTML, policy file, manifest attributes and code along with a brief account of how it works.
- 4th year only: briefly explain the extent to which security has been achieved or not
- MSc only: critically discuss the proposed security solution in terms of its security policy, threat model and a risk assessment of how well the deployed security measures mitigate threats

Groups may be composed of 4th year BSc and MSc students. In such cases, the more detailed security analysis must be supplied. Marks will be given based on each pair's demonstration and their written project submissions. Pair members may also elect to be individually assessed. If so they must state so in their written submissions, include a mutually agreed account of who did what on their group work, and supply separate security analyses at the appropriate level.

You will demonstrate your work during the lab session of Monday the 12th of November. The written coursework must be submitted as a single PDF file (report+code) to the course on Vision by midnight on Monday 12th November at 18:00GST by only one member of each group, i.e., only one submission per group. Separate PDFs for report and code can be joined using the Linux utility pdftk or the Windows utility PDFArchitect from PDFCreator. E-mail or hard copy coursework submissions are NOT acceptable. No individual extensions will be given. Submissions that are late by up to 5 working days will be assessed at a 30% penalty. After that no submissions will be allowed.

The marks given for this project will consider conformity to the specification and how well and to what level it was achieved in the report writing, the programs produced and the overall scope of what was essayed. High marks (70%+) will only be awarded to those who have successfully attempted something reasonably challenging and written it up appropriately.