**Assessed Coursework for Hamish Taylor**

This assessed coursework is for 4th and 5th year undergraduates (BSc, MEng) and MSc students taking F20CN or F21CN. Third year undergraduates taking this course do quite different assessed coursework. Fourth year students are only required to do a lesser security analysis, while MSc and MEng 5th years must do a fuller security analysis. The difference is detailed below. The coursework is worth 20% of the overall course mark for *Computer Network Security*.

This coursework is an exercise in creating and using X.509 and PGP certificates. It involves developing an 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 wider groups of people who are prepared to sign each other's certificates.

These wider groups have two purposes

•

to form a local certificate authority that signs pairs' X.509 certificates

•

to hold a key party for members to sign each other's OpenPGP 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. The local CA should be given a suitable X.500 name and have a self-signed X.509 certificate created for it. It should exercise due diligence before signing member's X.509 certificates by a means like that described in lecture 8 slides 3 and 4.

Each pair should perform the following tasks

•

create self-signed PGP certificates for each of the pair

•

create a self-signed X.509 certificate for the pair

•

form a wider group of fellow students and carry out the group activities

•

write applet to create file signatures with either of their PGP private keys

•

sign applet with private key corresponding to the pair's X.509 certificate

•

set up sensible security for their web browser to run the applet

•

demonstrate their applet 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 applet 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.

Setting up security for their web browser will require use of a browser that allows the user to import their group CA certificate as a trusted signatory of certificates. For example Internet Explorer on Windows allows any self-signed X.509 certificate to be imported as a Trusted Root Certificate Authority. Setting up security also requires setting the right permissions in the browser's java policy file. In the department that file has the following Windows NT and Unix file names for browsers running under Windows NT:

  H:\.windows\_settings\Application Data\Sun\Java\Deployment\security\java.policy  
  ~/.windows\_settings/Application Data/Sun/Java/Deployment/security/java.policy

Browsers running under Unix often look for a user's java policy file for the Java plugin called ".java.policy" in their home directory.

The demonstration that their applet works should

•

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 project - what they and group did and what they produced

•

list their certificates 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/MEng(5) -*

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 both 4th year and MSc or 5th year MEng 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 elect to be individually assessed. In that case they must state so in their written submissions and also include in it a mutually agreed account of who did what on their group work. Separate security analyses by named authors at the appropriate level must be supplied in such cases.

The project must be demonstrated to the assessor before Friday 17.15 on 28th November 2014 at the latest. The written coursework must be submitted to the coursework box by 3-30pm on Friday 28th November. Late submissions are liable to be penalised at the standard school rate unless permission to submit late is granted before the due date.

The marks given for this project will take into account 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.

Hamish Taylor   
H.Taylor@hw.ac.uk

© [Hamish Taylor](mailto:H.Taylor@hw.ac.uk) 2014

XHTML 5