# Exercise 3, Security models, X.509 and PKI

T-110.4200/6 course staff

deadline Friday 09.10.2009 23:55

## 1 Security models

Aim: Students review a few concrete examples of security models.

Answer the associated Quiz in Moodle.

## 2 X.509

To pass this excercise you must complete the following script and answer questions at Moodle.

From somewhere inside the TKK network, connect with *ssh(1)* to the server winnie.cs.hut.fi. The username is your student ID and password is the password you cracked for moodle at the first exercise round.

The machine winnie is supposed to serve as an intermediate X server. On it you can start Firefox (use -X when connecting with ssh).

Go to the website `https://honeypot.cs.hut.fi`. Click on the picture of the lock and view the certificate.

Now, go to the website `https://hunnypot.cs.hut.fi:8443`. What happens? Why? Examine the site's certificate. Your first reaction might be to distrust the site, but don't browse off just yet. Remember the weird fingerprints that that the lecturer had in his slides that covered X509 and PKI? Go retrieve it and compare it to the fingerprint strings. Only one of the two is correct. Which one?

What IP do the servers hunnypot and honeypot have? Why is this a funny IP for a web server?