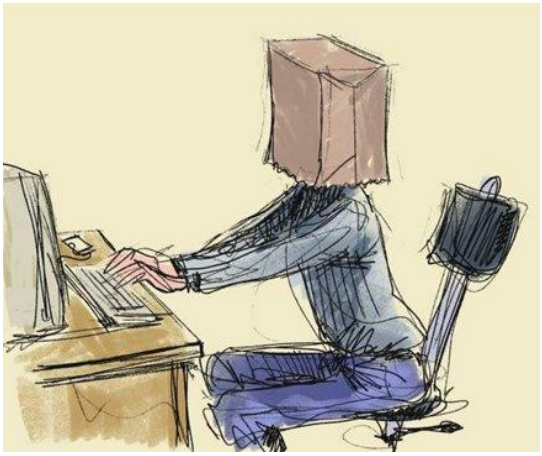
Project Description:

Privacy Enhanced Access Control

Application Scenario



Access control mechanisms are generally based on the authenticated identity of the principal (*the subject*) who request some form of access to a resource (*the object*). This means that the access control mechanism has complete knowledge about users' utilisation of resources in the system, e.g., the access control mechanism on Campusnet may know when a student downloaded a project description, whether the student consults the different handouts and how often the student looks for updates on course web-pages.

In order to enhance the privacy of students at DTU, you are requested to investigate cryptographic means to build an access control mechanism for Campusnet that balances the privacy of students against the legitimate need to ensure that only authorised users are granted access to protected Campusnet resources. Some resources should be accessible to all DTU students (study handbooks, course databases, etc.), some should only be accessible only to students on a particular course (handouts) and some should only be accessible to identified students (student hand-ins). This pilot project is supposed to develop an access control mechanism that can guarantee different degrees of privacy depending on the requested resource; this mean that you only need to consider a subset of the resources accessible through Campusnet.

Project Definition

Design, and evaluate a privacy enhanced access control mechanism for a selected set of resources accessible through Campusnet. Issues that *must* be investigated are:

- Closed loop authorisation, where servers issue "tickets" (cookies or encrypted capabilities) to authorised subjects.
- Open loop authorisation, where a certificate authority issues non identifying certificates (blinded attribute certificates, authorization certificates) to students who then employ these certificates to authenticate themselves towards the Campusnet.
- The degree of privacy that can be guaranteed for different classes of Campusnet resources.
- Threat model; you should explicitly state what threats your access control mechanism has been designed to handle, both with respect to the protected resources and the privacy of students.
- Security: Make sure that your system protects against the security issues raised in the threat model, and clearly document the threats that you do not protect against.