CS5430: System Security Programming Project (Spring 2025)

MEng Project Option

MEng students who are enrolled in CS5430 have the option to extend the course project into an MEng project. The extensions will add the following security functionality to the key-value store that is already being used for the class. Both of the following extensions are required.
- 2-factor authentication.
- Multi-level security (MLS) mandatory access control or role-based access control (RBAC).

Since this is an MEng project, the problem statement is somewhat open-ended and there is considerable flexibility, allowing student(s) to decide what will be built and how. Thus, this MEng project would be an opportunity to put into practice what you are learning in the class.

An MEng student can work alone on the extension or together with any group of 2 or 3 other students who are enrolled for MEng project credit.

To enroll in this option, submit to the course instructor for approval a short contract that gives the following information.

- The names of all students in the group building this project. All should plan to enroll for 3 credits of MEng project credit.

- A schedule for the implementation of 2-factor authentication, as follows.

  o A date, that is a Monday and is March 17 or later, when the group will meet with the course staff to review the proposed functionality and its design. Plan to make a 10-minute ppt presentation. Plan to give enough details so that the course staff is convinced you know what you will be building and it will work. Be prepared to give citations to the documentation that inspired the design.

  o A date at least 3 weeks later but before May 6, where the group will present a running implementation and give a demo.

- A schedule for the implementation of MLS or RBAC authorization, as follows.

  o A date, that is a Monday and is April 7 or later when the group will meet with the course staff to review the proposed functionality and its design. Plan to make a 10-minute ppt presentation. Plan to give enough details so that the course staff is convinced you know what you will be building and it will work. Be prepared to give citations to the documentation that inspired the design.

  o Some date at least 3 weeks later but before May 6, where the group will present the final implementation and give a demo.

Notes on 2-Factor Authentication.

A minimal scheme would involve implementing a 2FA-server process that runs concurrently with the existing key-value store. The user would communicate with this 2FA-server process using the keyboard and console. There would be no direct electronic communication between the 2FA-server and the key-value store server or between the 2FA-server and the key-value store client.

A more ambitious scheme would be to build or use an existing app that runs on an external device, like a cell phone or a separate laptop. You also might consider supporting time-based one-time password (TOTP), interfacing with Duo, or using some other commercially supported 2FA scheme.

Notes on MLS Authorization.

The authorization could be for values, or it could be for values and for keys. MLS could assign fixed labels, or the labels could change as objects are used in different ways. Support could be provided for confidentiality, integrity, or both.

Notes on RBAC

There are a wide variety of RBAC schemes in the literature. Different forms of inheritance can be supported, for example. The authorization could be for values, or it could be for values and for keys.