SYSC4907 Sensor Based Access Control Project Update

Craig Shorrocks
100887781

Jessica Morris
100882290

Richard Perryman
100887250

December 9, 2016

Supervisors: Shikharesh Majumdar and Chung-Horng Lung

1 Abstract

This report outlines the work that has been done so far on the Sensor Based Access Control System (SBACS). There are three main components to the system: the hardware and software that manages the lock units, the server which stores information about the system, and the software that handles user interactions with the server and lock units.

At this time, most of the work on the lock unit technology as well as the server has been completed. The majority of the remaining work to be done is on the access points, in particular, a web application to run administrative or user tasks has only been planned.

Aside from this missing element, we are mostly on track compared to our schedule from our initial proposal. We are in the middle of preliminary integration testing, and intend to have the system fully functional by the end of December. From there, we can work on refining the design of the system, testing the system, and handling the other course requirements like the final report.

2 Hardware

At this point in time, the main lock process running on the Raspberry Pi is able to receive authentication tokens of variable size, process them, and send them to the server to request access. It can then process the server's response, and grant or deny access as necessary. On startup, the main process will verify that it can reach the server, verify that it has at least one authentication module connected, and then enter a polling loop to wait for tokens from authentication modules. If a combination of tokens is required, the authentication process can time out. The tokens are cleared from memory after an access request has been sent, and after the timeout.

The NFC authentication module has been fully developed, and can receive the 256-byte NFC authentication token from an Android phone, and forward it to the main process. Due to the limitations of the PN532 NFC shield, the token is built from data across several messages received from the Android phone; however, this means that the module itself is more accomodating to changes, should we decide to change the size of an NFC token.

The work remaining to fully complete the hardware component is to refactor the authentication module code to create a "AuthenticationModule" abstract class. Since the mechanism for sending data to the main process is the same across all authentication modules, but the manner in which a module receives data from the user is unique to the module, refactoring the code will facilitate the development of new authentication modules for the system. In addition to this, video streaming from the IR camera attached to the Pi to a user's mobile phone still needs to be implemented.

3 Server

The server handles the maintenance of users, locks, and means of authentication. The server connects with the database to store and retrieve the information as it is needed. The server currently is able to handle and respond to a variety of accessor and mutator types of requests to view and modify the user, lock, and authentication information. There is also functionality to verify that the provided authenticators are allowed to open a given lock. Overall, the server portion of the project is largely functional and on schedule.

The one part of the server that is not yet implemented is logging in by users, for the phone application and web portal. This would restrict access and modification of the information stored in the database to users that are supposed to have those rights. This functionality is the one of the last steps to completing the work on the server, and should be finished by the beginning of the next school term.

4 Access Points

There were meant to be two main access points to the SBACS system: a phone application as well as a web portal. Both systems allow users to manage their various identities and the locks that they associate them with. Both also expose administrative capabilities for service providers. The phone application also had to provide a way for NFC to be used with locks associated with the user.

The phone application currently does not authenticate users, but otherwise can perform all of the required actions. The authentication implementation needs to be worked on in conjunction with the server adding the notion of sessions or something similar. The web application currently doesn't exist, but should largely mimic the phone application in design.

5 Conclusion