Security for Classroom Learning Partner

by

Karin Iancu

Submitted to the Department of Electrical Engineering and Computer Science
in Partial Fulfillment of the Requirements for the Degree of
Master of Engineering in Electrical Engineering and Computer Science
at the Massachusetts Institute of Technology

September 2006

Copyright 2006 Massachusetts Institute of Technology

All rights reserved.

Author

Department of Electrical Engineering and Computer Science
September 8, 2006

Certified by

Kimberle Koile, Ph.D.
Research Scientist, CSAIL
Thesis Supervisor

Certified by

Howard E. Shrobe, Ph.D.
Principal Research Scientist, CSAIL
Thesis Co-Supervisor

Accepted by

Arthur C. Smith, Ph.D.
Professor of Electrical Engineering
Chairman, Department Committee on Graduate Theses
Security for Classroom Learning Partner

by

Karin Iancu

Submitted to the
Department of Electrical Engineering and Computer Science

September 8, 2006

In Partial Fulfillment of the Requirements for the Degree of
Master of Engineering in Electrical Engineering and Computer Science

ABSTRACT

This MENG thesis implements a security system for a classroom presentation system called the Classroom Learning Partner (CLP). The goal of the security system is to prevent cheating on electronic quizzes. CLP is a system that uses Tablet PCs in the classroom to enhance learning and encourage interaction between the instructor and students. The instructor creates exercises which are displayed on slides on the students’ Tablet PCs. The students complete the exercises and submit them to the instructor and to a central database. The security implementation makes it possible to extend this framework for electronic quiz administration. This thesis discusses current cheating prevention methodologies and extends them to account for electronic quiz-taking scenarios. The basis of the security system is SQL Server authentication for authentication to a central database, and SSL for encryption of network traffic.

Thesis Supervisor: Kimberle Koile, Ph.D.  
Title: Research Scientist,CSAIL

Thesis Co-Supervisor: Howard E. Shrobe, Ph.D.  
Title: Principal Research Scientist,CSAIL
Acknowledgements

First, I would like to thank my thesis supervisors, Dr. Kimberle Koile and Dr. Howard Shrobe. I thank Dr. Koile for suggesting this project and for all her help along the way. Her enthusiasm for the project is contagious and she has been a wonderful mentor. I thank Dr. Shrobe for his guidance and ideas and for knowing hot to point me in the right direction.

I would like to thank the 1.00 Professors George Kocur, Steven Lerman, and Judson Harward for funding my Masters education and giving me the opportunity to be a Teaching Assistant for the course. Being a Teaching Assistant and discussing the project with the Professors helped to shape parts of this thesis.

I owe much thanks to the members of the CLP group for creating CLP and assisting me with various parts of this thesis. I would especially like to thank Adam Rogal for his help with the networking components of the project and his knowledge of Windows infrastructure, Kah Seng Tay for his help with the database components, Kevin Chevalier for helping me integrate with CLP, and Capen Low for implementing the login GUI.

I would like to thank my family for all their love and support. I thank my parents for paving the way for me to get where I am: I thank them for raising me to appreciate science and education, for teaching me determination and confidence, and for making it possible for me to come to MIT to pursue my education. I would also like to thank my grandparents for their love and understanding; for their phone calls, and for sending me back to school with good food to nourish me while I pursued my education. Finally, I would like to thank my new husband, Josh, for his support, patience, and encouragement, for his discussions about the project, for putting up with me when I was stressed the last year, for picking me up on the late nights, and for taking over wedding planning when I had too much work to do.
1 Introduction

The goal of this project is to implement a security infrastructure for an educational technology, Classroom Learning Partner (CLP) in order to administer quizzes electronically during class. The main goal is to help ensure the validity of the quizzes by preventing cheating. The CLP infrastructure prevents cheating in two ways: by enforcing authentication to the system and by encryption of network traffic.

There are a number of system components that contribute to the security of CLP. It is crucial that each component of the system and all traffic between each component be protected, so that an unauthorized party cannot access and modify private data. This protection is achieved by requiring authentication to each component, and by encrypting traffic. The system uses SQL Server authentication and SSL for encryption. Denial of service and nonrepudiation are not addressed.

This project is valuable, not only because of the benefit for deployments planned for the academic year 2006-2007, but also because of the potential for future enhancements and developments, such as automated quiz grading.
2 Classroom Learning Partner

Classroom Learning Partner (CLP) is a system being developed with the goal of improving student learning in the classroom. It will allow for increased interaction between the instructor and students. [Koile and Singer, 2006a] and [Koile and Singer, 2006b] show that students who used this system did better in an introductory computer science class than students who did not use the system.

Classroom Learning Partner employs Tablet PCs to provide the instructor with immediate feedback from students working exercises in-class and wirelessly submitting anonymous answers to the instructor. The system allows the instructor to create questions that are displayed on slides on the students’ Tablet PCs. The students’ answers are submitted to a database, where an aggregator then combines them into equivalence classes. The aggregated answers are sent to the instructor, who can use them to assess the students’ understanding of the material presented thus far and pace the class accordingly [Koile and Shrobe, 2005] & [Koile and Singer, 2006b].
2.1 CLP System Architecture

The system is currently being developed by the CLP group, headed by Dr. Kimberle Koile, at the MIT Computer Science and Artificial Intelligence Laboratory. It consists of the following main components:

- Instructor Authoring Tool (IAT),\(^1\) which helps the instructor create slides and exercises.
- Ink Interpreter, which interprets the student’s handwritten answers by producing semantic representations. [Rbeiz, 2006]
- Aggregator, which groups the student answers into equivalence classes using the semantic representations produced by the interpreter. [Smith, 2006]

\(^1\)The current version of the Instructor Authoring Tool was implemented by CLP group members Kevin Chevalier, Capen Low, Michel Rbeiz, and Kenneth Wu. [Chen, 2006] describes an earlier implementation.
The following diagram illustrates the architecture of the system.

![CLP Architecture Diagram]

Figure 1: Steps 1-8 represent the process of using Classroom Learning Partner

1. Before class, the instructor creates a PowerPoint presentation and a set of exercise objects using the CLP authoring tool. The exercise information is both embedded in the slides and stored as a separate object in the database.
2. Prior to class, the instructor retrieves the presentation from the database. The instructor also may store the presentation on his or her tablet and use the central database for archival.
3. Presentation slides are broadcast to student machines or students' machines automatically load them from a file server or the central database.
4. When a slide containing an exercise is displayed, each student enters ink answer, which is interpreted on his or her machine.
5. Each student's ink answer is submitted to the database.
6. Aggregator retrieves the interpreted ink answers, aggregates them, and produces summary data.
7. Summary data is stored in the database.
8. Summary data is displayed on the instructor's machine.
2.2 Current Implementation

The first version of Classroom Learning Partner is functioning and has been deployed in the classroom. The following is a description of a classroom scenario.

- The student walks into class, picks up tablet, and logs in with MIT username and password
- The tablet connects to MIT to authenticate (using Kerberos user name and password), gets a ticket and user name
- CLP on the tablet logs student into Windows system as “student” user name
- A script on the tablet creates a link to the student’s MIT directory, configures services for the MIT user name, adds an entry to the database (database CLPRecords, table TabletRecords) with user name and time of log in, and starts up CLP. The entry serves as a mapping between student and machine names. Figure 2 shows an example of the table in the database.

---

2 Student answers to in-class exercises are still anonymous. The instructor is unaware of the mapping between student and machine names. The information is used only by an educational assessment expert when investigating student performance.
Figure 2

- **CLP on the tablet** downloads slides from the instructor’s website automatically (because storing the slides on a file server proved to be the fastest).

- **The student** clicks connect

- **The tablet** connects to the virtual classroom set up by CLP for wireless communication
• *The student* views slides

• *The instructor* displays a slide containing an exercise

• The exercise slide shows up on each student’s *tablet*. Figure 3 shows an example of a slide that is displayed on the tablet during a class.

**Figure 3**

• *The student* works the exercise, writing an answer in digital ink with a tablet stylus pen in the answer box provided (Figure 4) and presses submit
The following expressions evaluate to values of what type?

\[
\begin{align*}
&\text{evaluating to type } \text{num, num, num } \rightarrow \text{num} \\
&\text{evaluating to type } \text{boolean } \rightarrow \text{string} \\
&\text{evaluating to type } \text{number}
\end{align*}
\]

Figure 4

- **CLP on the tablet** collects the ink and passes it to the ink interpreter

- **The ink interpreter** returns a semantic representation of the ink

- **CLP on the tablet** creates student answer object, transfers student answer object to database (database IAT, table Answers and table StudentAnswers) over TCP and transfers answer to instructor over RTP

- **The instructor** gets student answers

- When the **aggregator** is running on the instructor machine, the instructor does not get all the student answers, but rather only the representative ones released by the aggregator.

See figure 5 for a diagram illustrating the above scenario.
3 Quiz-taking Issues

The purpose of this MENG thesis is to design the security for CLP so that it can be used to administer quizzes electronically in class. CLP already provides the instructor with the framework to create and distribute exercises electronically in class, so quiz administration is a natural addition. When designing the security system, it is important to look at the current quiz-taking model and expand upon it for the electronic quiz-taking scenario.

Electronic quiz-taking offers numerous advantages over conventional quiz-taking methodologies. Certain tasks, such as distribution, collection, and scoring of quizzes, could be automated when a quiz is administered electronically [Dyreson, 1996]. This functionality would allow the instructor more time to focus on improving student learning and less time on quiz administration. Another advantage with electronic quiz administration is that it would be easy to collect statistics from the quiz [Dyreson, 1996]. The statistics could be used to determine student improvement in the class as well as overall class performance on a particular question or style of question. Finally, electronic quizzes could facilitate testing specifically in computer science classes by allowing students to write code in the same environment that they use for homework and projects.

While electronic quiz-taking does offer some advantages over conventional quiz-taking, it is not without its costs. Electronic quiz-taking provides increased opportunities for students to cheat, and students may cheat in more creative ways that are harder for instructors to detect.
3.1 Problem: Cheating/Benefits?

According to Davis [Davis, 1993], between 40 and 70 percent of college students have cheated at some point. Evidence suggests that if students are given the opportunity to cheat, they will take it [Bushweller, 1999]. Cheating is dishonest and prevents the cheating student from understanding the material to his full potential. Therefore, it is very important for teachers to do all that they can to prevent cheating. While there are many forms of cheating, this thesis focuses on how to prevent cheating on in-class quizzes.

3.1.1 Conventional quiz-taking

The traditional classroom quiz-taking scenario involves students taking a quiz on paper while the instructor or other proctor watches to make sure that no student is cheating. The following is a list of ways in which students may cheat:

a) Access the answers dishonestly during the quiz
   a. Copy off of another student
   b. Bring a source to copy from
      i. Cheat sheet
      ii. Writing on hand
      iii. Electronic device that contains the answers
   c. Communicate with a source outside of the classroom
b) Change either answer or score after the quiz [Bushweller, 1999]
c) Access quiz questions before the quiz [Bushweller, 1999]
   a. Break in to location where quiz is stored and steal a copy of the quiz
   b. Break the seal on a section of the quiz ahead of time [Bushweller, 1999]
c. Pass quiz questions of a standardized quiz to students in a later time zone
d. Give questions to students in a later class
d) Impersonate a student in the class and take the quiz in his place

3.1.2 Electronic quiz-taking

The electronic quiz-taking scenario involves students taking a quiz on an electronic device that may or may not have the capability to connect to the internet or other devices that students are using. For our purposes, each student will take the quiz on an individual electronic device. The devices have some sort of network connectivity through which the students obtain quiz questions, prove their identity, and submit quiz answers. Cheating in the electronic quiz-taking scenario is fundamentally the same as in the conventional scenario, however there are new opportunities for students to revise and expand upon conventional cheating methodologies.

Let’s revisit the ways that students cheat and examine how technology affects the scenarios.

a) Access the answers dishonestly during the quiz
   a. In addition to the conventional cheating methods described above, students also have the following possibilities of cheating at their disposal
      i. A student may attempt to access the quiz answers from a database or instructor’s machine where they are stored, or another student’s machine after he answers the questions.
      ii. A student may attempt to use the device that the quiz is being taken on to communicate with other students in or out of the class.
      iii. A student may try to view another student’s answers over the network traffic.
b) Change either answer or score after the quiz [Bushweller, 1999]
   a. There are potentially more ways a student can do this in the electronic scenario.

c) Access quiz questions before the quiz [Bushweller, 1999]
   a. There are more ways to do this in the electronic scenario, one of which is to eavesdrop on the network when the instructor submits/reads the exercises and answers to/from the database.

d) Have a friend impersonate a student in the class and take the quiz in his place
   a. This method might be easier to do in the electronic case since some electronic quiz-taking scenarios may not require that the student be present in a classroom.

### 3.2 Solution

There are a number of solutions to prevent cheating. We look at some of the conventional methods and discuss how they can be applied to the electronic scenario.

#### 3.2.1 Conventional solutions

Teachers have developed methods to counter cheating. The methods are not all foolproof, and each has its own advantages and disadvantages. The following is a list of some of the methods.

a) Be alert during the quiz to make sure that students are not copying off of or communicating with each other or using a cheat sheet or other device to get the answers.

b) Keep backup records of the quiz and the scores.
   a. Photocopy each student's quiz after the exam to make sure that they do not change their incorrect answers after the quizzes are returned.
b. Keep backup copies of the grade book so that if a student steals it and modifies some grades, it will be easier to catch and fix the changes.

c) Ensure that the quizzes and quiz questions are secure before the exam and change the quiz questions when another class is taking the same quiz later in the day.

a. Teachers can prevent students from breaking in to a room where a quiz is being stored by making sure that it is locked securely and that all people with access to the room can be trusted to restrict access from unauthorized people.

b. When a student broke the seal of the essay question on an ETS administered test, ETS later wrapped the questions in cellophane to deter students from opening it since there is a greater risk of getting caught [Bushwell, 1999].

c. In order to prevent students from divulging quiz questions to other students who are taking the quiz at a later time, instructors should change the questions.

d) Quizzes should be proctored by an instructor who is familiar with the students in order to prevent a student from impersonating a peer and taking the quiz in his place. An alternative to this is to require all students to bring their id to the quiz and use it as an authentication mechanism.

Many of these methods rely on students’ fear of getting caught. That is, they will not prevent cheating, but will make it likely that the student will get caught if he does cheat. In most cases, the possibility of getting caught is enough to prevent cheating altogether.

3.2.2 Electronic Solutions

While electronic quiz-taking introduces new ways in which students can cheat, it also provides the instructors with new ways to detect and prevent cheating. Most of the
cheating situations that are introduced by the electronic quiz-taking scenario can be prevented with a good authentication and encryption system.

The following describes how the instructors can enhance the methods to prevent cheating with technology.

a) In addition to watching students in class to make sure that they are not copying off of one another or a cheat sheet, ensure that all network traffic is encrypted so that students cannot eavesdrop on the network traffic and view each other’s submissions.

b) Since all submissions are stored electronically, it is easier to store backup copies.

c) A good authentication system will help prevent students from obtaining the exam ahead of time. As an additional measure, instructors may set up a system to determine if a break in has occurred.

d) Quizzes should be proctored by an instructor who is familiar with the students in order to prevent a student from impersonating a peer and taking the quiz in his place. An alternative to this is to require all students to bring their id to the quiz and use it as an authentication mechanism.
4 Preventing Cheating with CLP: Security System Architecture

In order to use CLP to administer quizzes in class, the system must be fortified to prevent cheating. The most important things to consider are data privacy and integrity, so that only authorized users can access and participate in the quiz. These two properties are achieved via authentication and encryption.

4.1 Authentication

In order to access any component of the system, it is necessary to authenticate to it. The component then grants access based on the particular user’s permissions. It is necessary to employ a good authentication mechanism to ensure that the parties with access cannot be impersonated. It is also necessary to have a strong system to set up permissions, so that an impersonator cannot modify the access list (either by adding a new name or by changing some existing permissions).

A good authentication system will prevent the following scenarios:

- A student accesses the instructor’s computer to view the questions and/or answers before class.
- A student accesses the database to view the questions and/or answers before class.
- A student accesses the instructor’s computer during class to view the answers.
- A student accesses the database during class to view the answers.
- A student accesses another student’s computer during class to view his answers.
- A student accesses the database during class to view another student’s answers.
- A student from another class accesses the database to view the questions before his own class.

4.2 Encryption

All traffic in the system must be encrypted. This encryption is necessary in order to prevent eavesdroppers from obtaining information to which they are not entitled.

The following transmissions must be encrypted:

a) Instructor sends exercises and answers to the database.
   - The instructor does this task in preparation for the class, so if a student could view this traffic, he would have access to the exercise questions and answers before class.

b) Instructor reads exercises and answers from the database.
   - If this traffic is viewed, it is the same scenario as above.

c) Instructor broadcasts slides to the students.
   - Whether or not to encrypt this step is a design decision. The benefit of encrypting this information is that it prevents students in other classes from viewing the exercises.

d) Students submit answers to the database.
   - This task prevents cheating that is equivalent to looking at another student’s paper in a traditional quiz setting. In a non-quiz setting, it could make some students feel more comfortable to know that other students cannot see their answers.
e) Instructor reads student answers from the database (either individually or in aggregated form).

- If this traffic is viewed, it is the same scenario as above.

The following figure illustrates the above scenarios.

Figure 6
4.3 Outside Scope

Nonrepudiation is not addressed in the implementation of the system. Nonrepudiation is a way to ensure that a message was sent and received. This would be a way to prevent a student from claiming that he did not receive a quiz question.

This system does not protect against a denial of service attack. A denial of service attack floods a system so that it can no longer function. A student might attempt this attack if he decides he would rather not take the quiz that day. Neither of these issues has been addressed.

The quiz-taking scenario addressed in this thesis requires that the quiz is administered with the students in the classroom. It is necessary to consider addition scenarios in order to secure a quiz that is taken from a remote location.
5 Design Choices and Implementation

As mentioned earlier, this MENG thesis implements a security system for CLP that consists of authentication and encryption. The following is a description of the sequence when CLP is used for quiz administration:

1. The instructor or database administrator creates a new password for the student account in the database. (see appendix for instructions on how to do this, or should I put instructions somewhere else?).

2. The student walks in to class and picks up a tablet from the front of the classroom. Note that the tablets are in the control of the instructor between classes, so she can control the tablet settings and what programs are installed before class.

3. The student logs in to the tablet with his MIT Athena user name and password.

4. The tablet connects to MIT and logs the student in to Athena via the Kerberos system.

5. Once the MIT Athena credentials are verified, the student is logged in to Windows under the user name “student”. All students will be logged in to the tablet as “student”.

6. Next, a script runs which adds an entry to the database (database CLPRecords, table TabletRecords) with the user name, tablet name, and time of log in of the student and starts up CLP.

7. At this point, the slides are downloaded onto the tablet.
8. The student starts up CLP and connects to the classroom. When prompted for a password, the student enters the password assigned by the instructor.

9. The student takes the quiz by viewing the quiz questions on the slides and answering them in an answer box provided. Once the student is satisfied with his answer, he presses submit. This causes the student’s identity to be checked and if it is verified, the answer is encrypted with SSL and submitted to the database. The student can resubmit his answer as many times as he would like. The instructor should instantiate a policy of how to deal with multiple submissions. One reasonable policy is to only look at the latest submission. This is similar to conventional quiz-taking, where a student may cross out or erase his answer, so the instructor only sees the latest one.

10. The instructor or database administrator should change the student password immediately after class so that no student can log in again.

The password should be changed at the end of class so that students cannot submit new answers after class. As long as the students are only allowed to insert answers, changing the password is not a critical issue: if the students don’t have the ability to delete, and a timestamp is submitted with each insert, the instructor will see when an answer was submitted and can disregard answers submitted after the quiz ended.
5.1 Authentication

Students authenticate to the database using SQL Server authentication. Currently, anyone with an MIT account can log in to a CLP tablet during class with his Athena user name and password. When CLP starts up, a login prompt appears that asks the user for his user name and password. This information is saved in the CLP code and used to authenticate the student when he submits an answer to the database.

SQL Authentication versus Windows Authentication

In general, it is recommended to use Windows authentication over SQL authentication when authenticating to an MS SQL Server 2000 database since Windows authentication has many of the security considerations built in and automatically configured. However, Windows authentication is not possible for the current classroom architecture, since each student does not have a distinct Windows account that he is logged in to.

One disadvantage of using SQL Server authentication is that the password travels over the network in clear text. It must be encrypted so that no one can eavesdrop on the network packets and see the password. We use SSL to encrypt the password and solve this problem. This encryption does not add any overhead over using Windows authentication since even Windows authentication still necessitates encryption of all other network traffic.
Student Database Accounts

It is important to ensure that each user connects to the database with an account that has the fewest privileges necessary for him to accomplish what he needs. Each student will log in to the database with a password supplied at the beginning of class. The student’s account will only have the capability to insert into the database and not to read or delete entries.

The student account should be created and maintained by the instructor, teaching assistant, or other administrator who would normally have access to student records. As mentioned earlier, in the current implementation, there is one student account with which every student logs in. Students are distinguished from each other by mapping their Athena user name to their tablet name and storing that information in another table in the database. This is done with a script that automatically runs on the tablet when the students log in. It is a bit awkward to have the students’ identifying information in a separate database, so it might be beneficial to create an individual database account for each student in the class.
5.2 Encryption

All communications with the SQL Server are encrypted with SSL\(^3\). This encryption prevents an unauthorized person from viewing network traffic. A server certificate\(^4\) is installed on the computer on which the SQL Server database resides, and the database is set up to only allow encrypted connections. Whenever a client connects to the SQL Server, the connection and all traffic between the client and server will be encrypted with SSL.

SQL Server 2000 supports both SSL and IPSec for encryption. In order to use IPSec, all client machines must have a static IP address. It is also necessary to configure every machine in the network to use IPSec. SSL does not have this administrative overhead. The only setup necessary for SSL encryption is on the server machine, thus making it easy to add new client machines to the system.

\(^3\)See [ ] for a description of how SSL works.

\(^4\)The server certificate is obtained from the CSAIL Certificate Authority.
5.3 Vulnerabilities

The system specification requires that the instructor change the student password immediately after class. This means that if a student finishes the quiz early and leaves class, the password that was given in class will still be valid. The student may try to access the database remotely and add a new submission before the instructor changes the password. In order to do this, the student would need to know on which machine the SQL Server is running, which database and table on the SQL Server contains the student’s quiz submissions, and how to access the table and insert new entries. It is unlikely that the student would obtain all this information. However, it is important to note that if he does, the system could be compromised. An important and not difficult addition to the system would be a mechanism for having the system automatically change the password after all students have logged in.

When a student first logs in to the tablet, a script runs that does two things: it mounts the user’s Athena directory on the tablet (as a new device) and inserts an entry, which pairs student user names with machine id, into the TabletRecords table in the CLPRecords database on the SQL Server. A student may try to cheat by accessing files in his or her Athena directory. It is important, therefore, that the part of the script that mounts the student’s Athena directory be removed. Note that access to the directory may not be a problem if the quiz is open notes, depending on the instructor’s wishes. The other potential vulnerability in the script is that it needs to access the database to insert the mapping between the student user name and machine name. The script uses its own
account, but the user name and password is displayed in the script. If the students know where the script is located on the computer, they could look at it to obtain the user name and password and use that to insert a new entry into the table that maps their user name to a different machine. The script account only has permission to insert new entries and not to delete or read entries, so that helps to prevent further unauthorized access.

In the current system configuration, students can still access the internet during class, and therefore, potentially communicate with each other or other students outside of class to cheat. This communication can be prevented easily with a firewall that is set up to only allow the necessary connections. Another option is to leave the system as is and monitor the network traffic to make sure that students are not communicating with each other. This approach is similar to the current cheating prevention model at MIT, since although there is no way to guarantee that the students will be honest, the fear of getting caught is usually enough to prevent cheating, and MIT does have an academic honesty policy in place to which students are expected to adhere.

All of the above vulnerabilities are easily addressed and will be considered in the next version of the system.
6 Testing

The system was tested in a mock classroom setting with one instructor and 2 student tablets. The “quiz” is stored on the Desktop of the tablet. Each student logs in to CLP with the given username and password and loads the quiz from the Desktop. The students submit their answers by pressing the submit button in CLP. The quiz testing was done twice: once with encryption disabled and once with it enabled.

Figure 7 shows the TabletRecords table in the CLPRecords database, which contains the mapping from a student’s computer name to his Kerberos name.

![Table of TabletRecords](Image)

Figure 7

---

3 It was also tested with more than 2 student tablets, however for simplicity of the documentation, I discuss a scenario with 2 student tablets.
Figure 8 shows the ink student submissions.

![Ink Submissions](image)

As you can see, the student using CLP16 wrote “test student” and the student using CLP10 wrote “test karin”. These exercises were submitted in an unencrypted session. Figures 9 and 10 show the submissions in the database. The StudentAnswers table in the IAT database (figure 9) shows that the student using CLP16 has submitted an answer, which is identified by the AnswerID 233 and the student using CLP10 has submitted an answer identified by AnswerID 234.

![Database Submission](image)

The AnswerIDs 233 and 234 and the semantic representations that correspond to their ink answer can be found in the Answers table in the IAT database (figure 10).
Figure 10
The same thing was done with encryption enabled. Figures 11 and 12 show the tables in the encrypted session. The student answers can be seen in the database in figure 10 in AnswerIDs 239 and 240.

![Figure 11](image)

Notice that there is no difference in how the answers are stored in the database in the encrypted and unencrypted versions. We must examine the network traffic in order to see the difference.

The following two network traces show the unencrypted traffic when the Athena name to tablet name mapping is made in the database. Notice how easy it is to see that the database name is CLPRecords. Also notice how the SQL statement
"INSERT INTO TabletRecords VALUES ("CLP10","karin",GETDATE())" is visible in the second trace.

```
| 0000 | 00 0f b0 71 61 67 00 12 3f 53 02 ce 08 00 45 00 | ...qag.?S....E. |
| 0010 | 01 b1 05 63 40 00 80 06 be 69 80 1e 1a 47 80 1e | ...@...I..G. |
| 0020 | 1a f7 05 90 f0 82 1b 9c f4 49 eb b1 b7 ab 50 18 | ............I...P. |
| 0030 | 33 37 1e 00 00 04 01 01 89 00 33 01 00 e3 23 | 37.........3....# |
| 0040 | 00 01 0a 43 00 4c 00 50 00 52 00 65 00 63 00 6f | ...C.L.P.R.e.c.o |
| 0050 | 00 72 00 64 00 73 00 06 6d 00 61 00 73 00 74 00 | ...r.d.s.m.a.s.t. |
| 0060 | 65 00 72 00 ab 6e 00 45 16 00 00 02 00 29 00 43 | e.r.n.e.....).C |
| 0070 | 00 68 00 61 00 6e 00 67 00 65 00 64 00 20 00 64 | h.a.n.g.e.d.d |
| 0080 | 00 61 00 74 00 61 00 62 00 61 00 73 00 65 00 20 | .a.t.a.b.a.s.e. |
| 0090 | 00 63 00 6f 00 6e 00 74 00 65 00 78 00 74 00 20 | .c.o.|'CLP.R.e.c.o.r.d.s.'|
| 00a0 | 00 74 00 6f 00 20 00 27 00 43 00 4c 00 50 00 52 | M.A.N.D.A.L. |
| 00b0 | 00 65 00 63 00 6f 00 72 00 64 00 73 00 27 00 2e | ...U.S...e.n.g |
| 00c0 | 00 08 41 00 4d 00 41 00 4e 00 44 00 41 00 43 00 | ...l.l.sh...I.o. |
| 00d0 | 03 00 00 00 00 00 e3 08 00 07 05 09 04 00 00 34 | S............4. |
| 00e0 | e3 17 00 02 0a 75 00 73 00 5f 00 65 00 6e 00 67 | ...U.S...e.n.g |
| 00f0 | 00 6c 00 69 00 73 00 68 00 00 ab 6a 00 47 16 00 | ...l.l.sh...I.o. |
| 0100 | 00 01 00 27 00 43 00 66 00 61 00 6e 00 67 00 65 | ...C.h.a.n.g.e |
| 0110 | 00 64 00 20 00 6c 00 61 00 66 00 67 00 75 00 61 |...d..l.a.n.g.u.a |
| 0120 | 00 67 00 65 00 20 00 00 73 00 65 00 74 00 74 00 | ...r.e...s.e.t.t.i |
| 0130 | 00 6e 00 67 00 20 00 74 00 66 00 20 00 70 00 73 | ...h.t.o..u.s |
| 0140 | 00 5f 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 | ...e.n.g.l.l.sh |
| 0150 | 00 2e 00 08 41 00 4d 00 41 00 4e 00 44 00 41 00 | ...A.M.A.N.D.A. |
| 0160 | 43 00 53 00 00 00 00 ad 36 00 01 71 00 00 01 16 | C.S.S......6.q. |
| 0170 | 4d 00 69 00 63 00 72 00 6f 00 73 00 66 00 66 00 | M.i.c.r.o.s.o.f.t |
| 0180 | 74 00 20 00 53 00 51 00 4c 00 20 00 53 00 65 00 | .t..S.Q.L..s.e. |
| 0190 | 72 00 76 00 65 00 72 00 00 00 00 00 00 08 00 7f | r.v.e.r. ........... |
| 01a0 | 63 13 00 04 04 34 00 30 00 39 00 36 00 04 34 00 | ................4.0.9.6.4. |
| 01b0 | 30 00 39 00 36 00 f0 00 00 00 00 00 00 00 00 00 00 09.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.6.
The same situation holds with the student submissions to the database. In the next two examples, the SQL statement is sent in clear text, and in the last two, it is encrypted.
We have thus verified that the network traffic corresponding to student responses is encrypted. Such encryption substantially decreases the likelihood of students being able to acquire other students’ submitted responses.
7 Future work

There are a number of projects that would be interesting extensions of the system described in this thesis.

One obvious extension is remote quiz-taking. This thesis only addresses quizzes that are taken in the classroom. In a remote electronic quiz-taking scenario, the quiz is posted online, and the students take it from any location outside of the classroom. This type of quiz is an electronic version of a take-home exam. Our encryption method works just as well for the remote scenario as for the in-class scenario and probably would not need to be changed. The remote scenario has the same fundamental cheating concerns as the classroom version, but also presents additional opportunities for cheating. The method of student authentication we used for the in-class scenario, i.e. student logon with a quiz-specific password, may not be appropriate in the remote scenario. Providing a password at quiz start time would be possible if students started the quiz at the same time. An encrypted message containing the password could be sent to all logged in students, for example. In addition, if the remote quiz is to be taken at a certain time by all students, database access can be disabled until the time of the quiz. If it is acceptable that the students take the quiz at any time, they can be given a password in advance and a timer can be implemented that would track when a student logs in and forces the student to log out after a certain amount of time has passed. Note that this method has the potential for more cheating than requiring a designated start time, since one student can take the quiz first and disclose the questions to another student.
Another issue to consider with remote quiz-taking is how to ensure that only students registered for the class log in to the tablets. One method would be to run a script on the tablet that would check the student user name against a list of registered students. As each class is likely to have such a list of students stored in the central database, adding this functionality would be quite easy.

Another addition to the system would be to extend the aggregator to help detect cheating. It could use its similarity metrics and clustering methods to find entries that are similar and unusual [Smith, 2006]. The clustering would be enhanced by providing functionality that would allow the system to automatically detect the location of tablets and provide the aggregator with that information. In this way, the aggregator could also check answer similarity for students sitting near each other.

An addition that would make quiz administration more efficient is the automated grading of the quizzes once they are submitted to the database.

It would be interesting to analyze the behavior of the system when it is up and running. Shrobe discusses a system that performs “Computational Vulnerability Analysis” to adaptively determine what vulnerabilities are present in a system [Shrobe, 2002]. This system can be used in CLP to help determine if the system has been compromised, for example by students’ unauthorized access to the database.
One of the most interesting extensions would be to integrate handwriting recognition with the authentication. "Distinctive Touch" [Kleek, 2004] is a system that was developed to authenticate users by what the developers call a passdoodle, which is a handwritten "doodle" drawn by the user in digital ink which acts as a user name and password. Distinctive touch enhances handwriting recognition so that it would be appropriate to authenticate a user. In addition to identifying the sketch, Distinctive Touch also looks at stroke order and the speed that the sketch is drawn.
8 Summary and Contributions

This thesis analyzes the security risks associated with using CLP to electronically administer a quiz in class, implements an infrastructure which reduces those risks, and lays the groundwork for future enhancements. The system which is implemented can be used to authenticate students to the database and to ensure that the database network traffic is not readable by unauthorized individuals. We discuss the vulnerabilities in the current implementation and ways to increase the trust in the system, as well as a number of projects to expand the system.
References


