

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

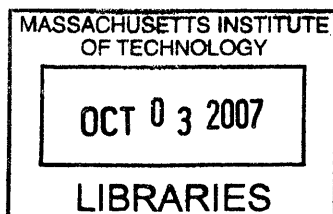
All rights reserved.

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



BARKER

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 how 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	5
2	CLASSROOM LEARNING PARTNER	6
2.1	CLP System Architecture	7
2.2	Current Implementation	9
3	QUIZ-TAKING ISSUES	14
3.1	Problem: Cheating/Benefits?	15
3.1.1	Conventional quiz-taking	15
3.1.2	Electronic quiz-taking	16
3.2	Solution	17
3.2.1	Conventional solutions	17
3.2.2	Electronic Solutions	18
4	PREVENTING CHEATING WITH CLP: SECURITY SYSTEM ARCHITECTURE.....	20
4.1	Authentication	20
4.2	Encryption	21
4.3	Outside Scope	23
5	DESIGN CHOICES AND IMPLEMENTATION.....	24
5.1	Authentication	26
	SQL Authentication versus Windows Authentication	26
	Student Database Accounts	27
5.2	Encryption	28
5.3	Vulnerabilities	29
6	TESTING	31
7	FUTURE WORK.....	39
8	SUMMARY AND CONTRIBUTIONS.....	42
	REFERENCES	43

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 20006-2007, 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.

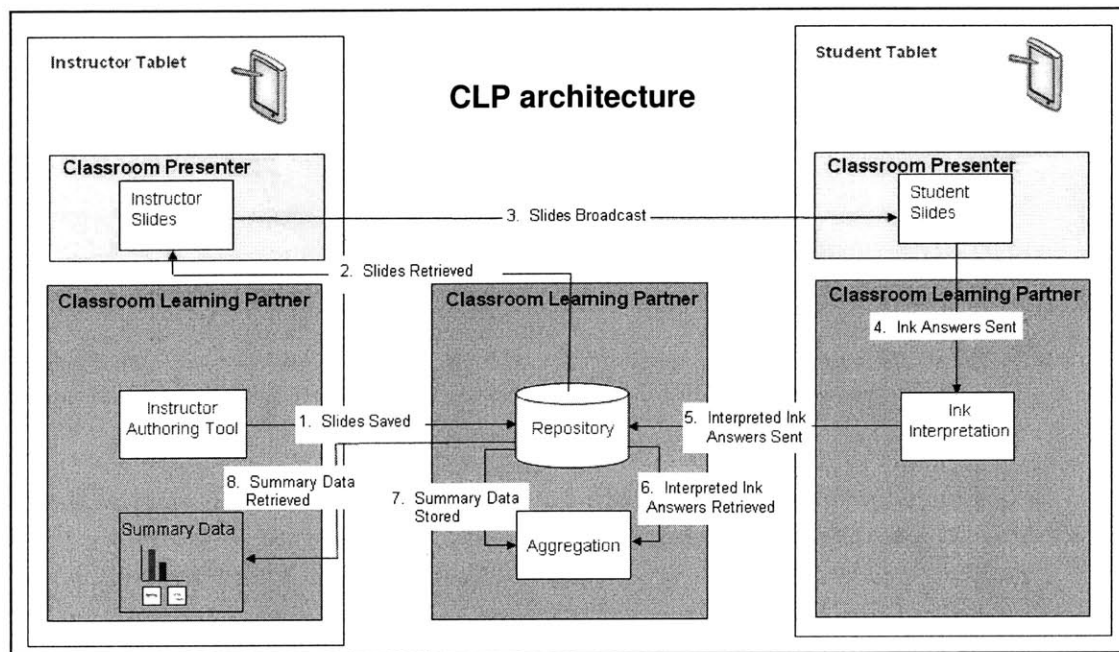


Figure 1: Steps 1-8 represent the process of using Classroom Learning Partner

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 names²

Figure 2 shows an example of the table in the database.

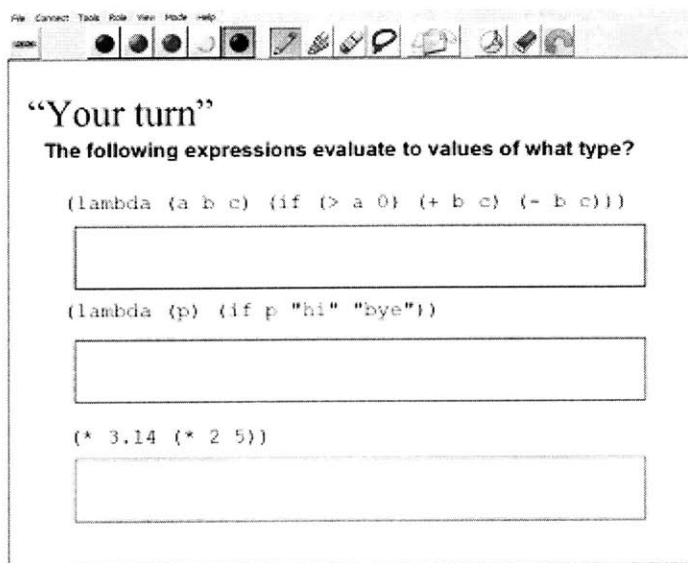
² Student answers to in-class exercises are still anonymous. The instructor is unaware of the mapping between student and machine names. The information is used only by an educational assessment expert when investigating student performance.

ComputerName	KerberosName	LoginTime
AC10	kn...iley	3/22/2006 1:08:50
CLP10		3/15/2006 1:08:29
AC10		3/15/2006 1:08:34
CLP4		3/15/2006 1:08:37
CLP3	...iley	3/15/2006 1:08:45
CLP16	...vd	3/15/2006 1:08:46
AC7	...eng	3/15/2006 1:08:51
CLP7		3/15/2006 1:09:05
CLP8	...stev	3/15/2006 1:09:07
AC9	...n	3/15/2006 1:09:20
CLP18		3/15/2006 1:09:39
CLP2	...m	3/15/2006 1:09:41
AC8	...n	3/15/2006 1:09:59
CLP6	...	3/15/2006 1:10:02
CLP13	...rd	3/15/2006 1:10:29
CLP9		3/15/2006 1:10:35
CLP11	...n	3/15/2006 1:10:52
CLP14	...rd	3/15/2006 1:10:53
CLP17	...e	3/15/2006 1:11:52
CLP12	...rfj	3/15/2006 1:12:57
CLP5	...y	3/15/2006 1:13:02
CLP15		3/15/2006 1:37:40
CLP14	...rd	3/15/2006 1:47:28
CLP6	...iley	3/17/2006 1:10:14
AC10	...eng	3/17/2006 1:10:28
CLP3	...n	3/17/2006 1:10:41
CLP10	...n	3/17/2006 1:10:41
CLP8	...e	3/17/2006 1:10:48
CLP12	...rfj	3/17/2006 1:10:49
CLP9		3/17/2006 1:10:54
AC9		3/17/2006 1:11:04
CLP4	...vd	3/17/2006 1:11:04
AC8	...stev	3/17/2006 1:11:08
CLP16	...n	3/17/2006 1:11:24
CLP14	...ent	3/17/2006 1:13:02
CLP16		3/22/2006 1:08:59

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.



The screenshot shows a tablet interface with a menu bar at the top containing icons for file, connect, tools, role, view, mode, and help. Below the menu bar is a slide titled "Your turn" with the question: "The following expressions evaluate to values of what type?". There are three code snippets, each followed by a text input box for the answer:

```
(lambda (a b c) (if (> a 0) (+ b c) (- b c)))
```

```
(lambda (p) (if p "hi" "bye"))
```

```
(* 3.14 (* 2 5))
```

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

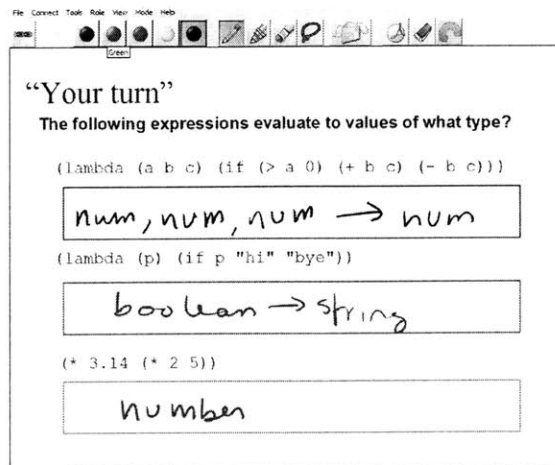


Figure 4

- *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.

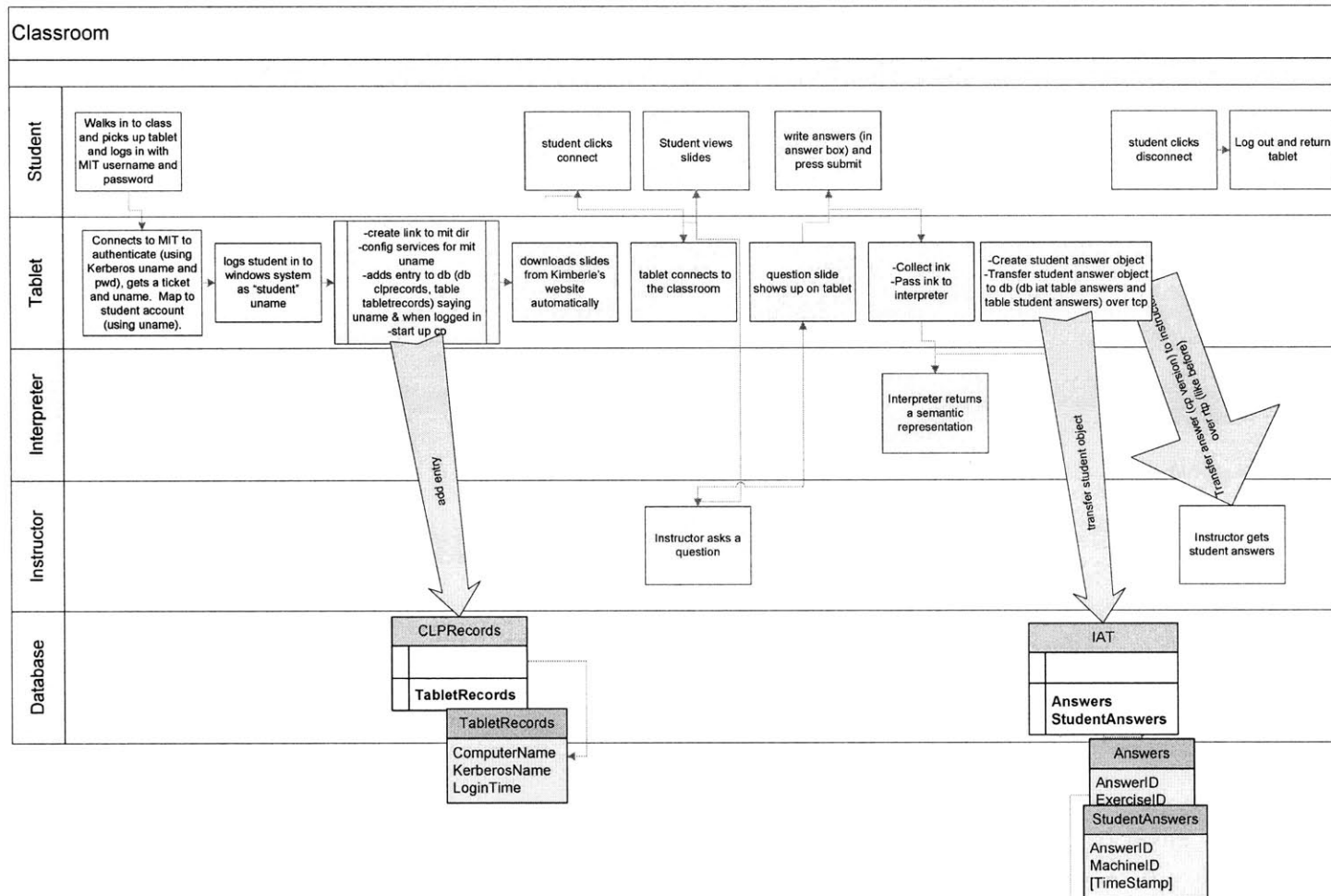


Figure 5

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 [Bushweller, 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.

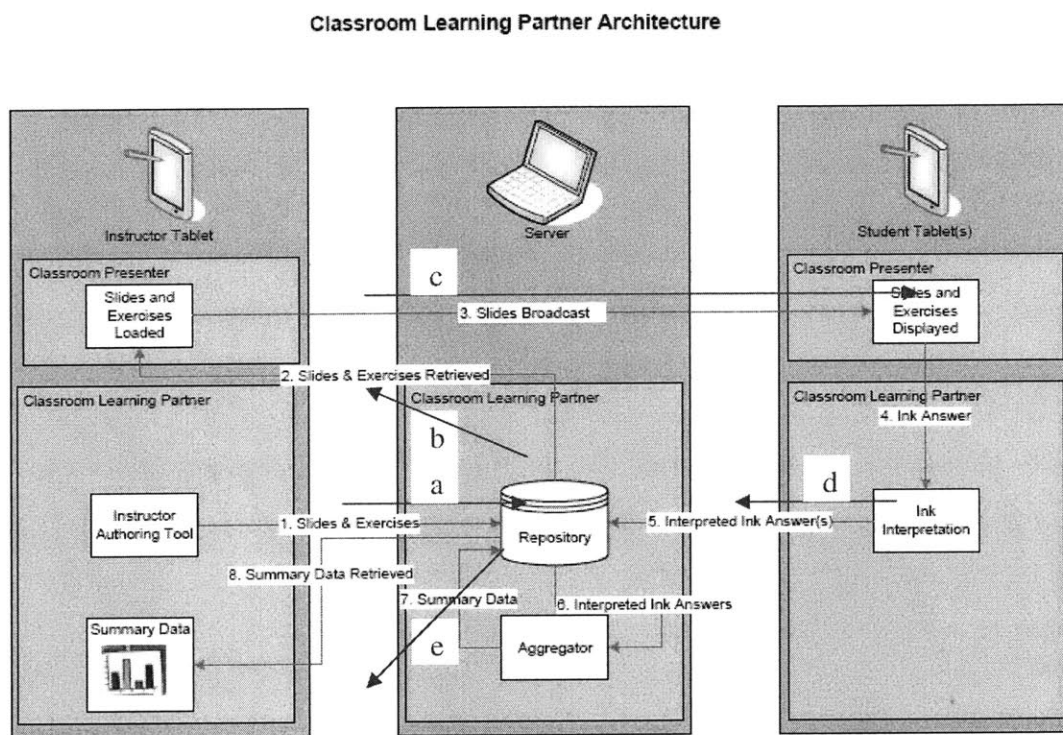


Figure 6

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 additional 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 SSL³. This encryption prevents an unauthorized person from viewing network traffic. A server certificate⁴ 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.

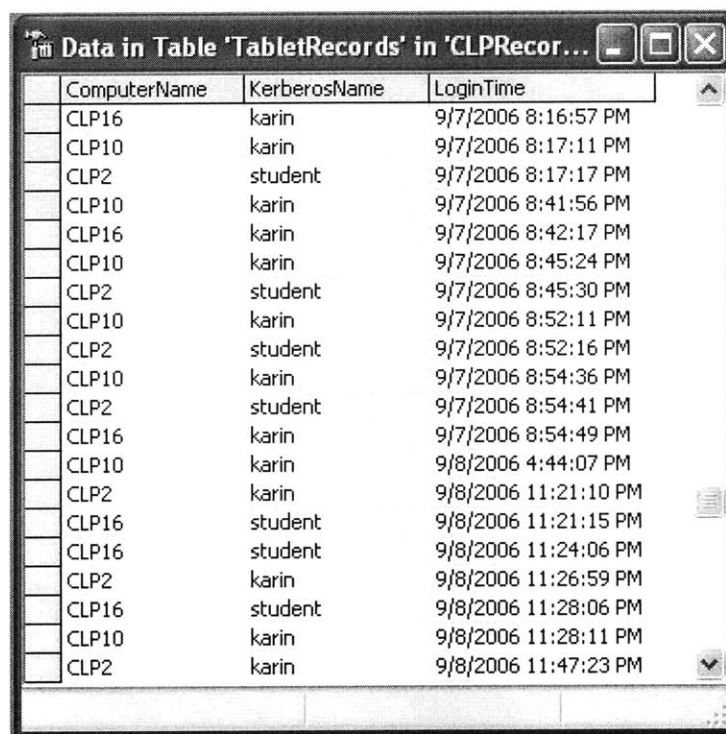
In the current system configuration, students can still access the internet during class, and therefore, potentially communicate with each other or other students outside of class to cheat. This communication can be prevented easily with a firewall that is set up to only allow the necessary connections. 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 tablets⁵. 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.



ComputerName	KerberosName	LoginTime
CLP16	karin	9/7/2006 8:16:57 PM
CLP10	karin	9/7/2006 8:17:11 PM
CLP2	student	9/7/2006 8:17:17 PM
CLP10	karin	9/7/2006 8:41:56 PM
CLP16	karin	9/7/2006 8:42:17 PM
CLP10	karin	9/7/2006 8:45:24 PM
CLP2	student	9/7/2006 8:45:30 PM
CLP10	karin	9/7/2006 8:52:11 PM
CLP2	student	9/7/2006 8:52:16 PM
CLP10	karin	9/7/2006 8:54:36 PM
CLP2	student	9/7/2006 8:54:41 PM
CLP16	karin	9/7/2006 8:54:49 PM
CLP10	karin	9/8/2006 4:44:07 PM
CLP2	karin	9/8/2006 11:21:10 PM
CLP16	student	9/8/2006 11:21:15 PM
CLP16	student	9/8/2006 11:24:06 PM
CLP2	karin	9/8/2006 11:26:59 PM
CLP16	student	9/8/2006 11:28:06 PM
CLP10	karin	9/8/2006 11:28:11 PM
CLP2	karin	9/8/2006 11:47:23 PM

Figure 7

⁵ 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.

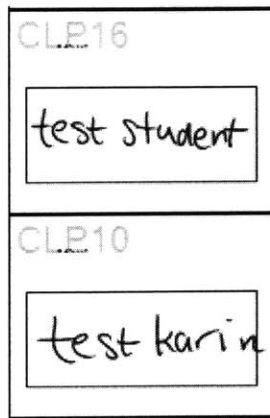


Figure 8

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.

AnswerID	MachineID	SessionID	TimeStamp
233	CLP16	142	9/8/2006 11:30:25
234	CLP10	142	9/8/2006 11:30:35

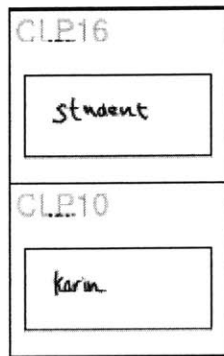
Figure 9

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).

AnswerID	ExerciseID	BoxIndex	Ink	SemanticRep
222	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">hi</Chunk></Answer>
223	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">to</Chunk></Answer>
224	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">you</Chunk></Answer>
225	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">hi</Chunk></Answer>
226	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">Ni</Chunk></Answer>
227	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">to</Chunk></Answer>
228	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">you</Chunk></Answer>
229	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">hi student</Chunk></Answer>
230	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">hi Karin</Chunk></Answer>
231	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">hi student</Chunk></Answer>
232	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">hi student</Chunk></Answer>
233	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">test student</Chunk></Answer>
234	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">test Karin</Chunk></Answer>
235	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">123</Chunk></Answer>
236	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">123756</Chunk></Answer>
237	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">(112)</Chunk></Answer>
238	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">(434)</Chunk></Answer>
239	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">student</Chunk></Answer>
240	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">Karin</Chunk></Answer>
241	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">123</Chunk></Answer>
242	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Strong">456</Chunk></Answer>
243	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">#12</Chunk></Answer>
244	4	0	<Binary>	<Answer Type="STRING"><Chunk Type="STRING" Confidence="Poor">(5*34)</Chunk></Answer>

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.



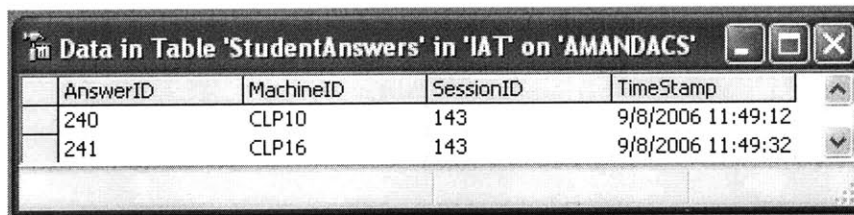
CLP16

student

CLP10

karin

Figure 11



AnswerID	MachineID	SessionID	TimeStamp
240	CLP10	143	9/8/2006 11:49:12
241	CLP16	143	9/8/2006 11:49:32

Figure 12

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 ...c@....i...G..
0020 1a f7 05 99 f0 82 1b 9c f4 49 eb b1 b7 ab 50 18 .....I....P.
0030 fd 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.r.d.s..
00a0 00 74 00 6f 00 20 00 27 00 43 00 4c 00 50 00 52 (.o..'.C.L.P.R
00b0 00 65 00 63 00 6f 00 72 00 64 00 73 00 27 00 2e e.c.o.r.d.s.'.
00c0 00 08 41 00 4d 00 41 00 4e 00 44 00 41 00 43 00 ..A.M.A.N.D.A.C.
00d0 53 00 00 00 00 e3 08 00 07 05 09 04 d0 00 34 00 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.i.s.h...j.G..
0100 00 01 00 27 00 43 00 68 00 61 00 6e 00 67 00 65 ...'.C.h.a.n.g.e
0110 00 64 00 20 00 6c 00 61 00 6e 00 67 00 75 00 61 .d..l.a.n.g.u.a
0120 00 67 00 65 00 20 00 73 00 65 00 74 00 74 00 69 .g.e..s.e.t.t.i
0130 00 6e 00 67 00 20 00 74 00 6f 00 20 00 75 00 73 .n.g..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.i.s.h
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.....6..q....
0170 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 M.i.c.r.o.s.o.f.
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 08 00 07 f7 r.v.e.r.....
01a0 e3 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 fd 00 00 00 00 00 00 00 00 00 0.9.6.....

0000 00 12 3f 53 02 ce 00 0f b0 71 61 67 08 00 45 00 ..?S.....qag..E.
0010 00 aa 02 47 40 00 7f 06 c3 8c 80 1e 1a f7 80 1e ...G@.....
0020 1a 47 f0 82 05 99 eb b1 b7 ab 1b 9c f5 d2 50 18 .G..'......P.
0030 42 b4 f3 9e 00 00 01 01 00 82 00 00 01 00 49 00 B.....1.
0040 4e 00 53 00 45 00 52 00 54 00 20 00 49 00 4e 00 N.S.E.R.T..I.N.
0050 54 00 4f 00 20 00 54 00 61 00 62 00 6c 00 65 00 T.O..T.a.b.l.e.
0060 74 00 52 00 65 00 63 00 6f 00 72 00 64 00 73 00 t.R.e.c.o.r.d.s.
0070 20 00 56 00 41 00 4c 00 55 00 45 00 53 00 20 00 .V.A.L.U.E.S..
0080 28 00 27 00 43 00 4c 00 50 00 31 00 30 00 27 00 (.'.C.L.P.1.0.'.
0090 2c 00 27 00 6b 00 61 00 72 00 69 00 6e 00 27 00 ,..'.k.a.r.i.n.'.
00a0 2c 00 20 00 47 00 45 00 54 00 44 00 41 00 54 00 ..'.G.E.T.D.A.T.
00b0 45 00 28 00 29 00 29 00 E.(.).).

```

Now look at the network trace when it is encrypted and notice how it is unreadable without the key.

```

0000 00 0f b0 71 61 67 00 12 3f 53 02 ce 08 00 45 00 ...qag..?S....E.
0010 01 c6 08 4f 40 00 80 06 bb 68 80 1e 1a 47 80 1e ...o@....h...G..
0020 1a f7 05 99 f0 9e 79 89 c0 00 fa 21 26 50 50 18 .....y....!&PP..
0030 fd 35 37 33 00 00 17 03 01 01 99 0a 36 99 7c 29 .573.....6.|)
0040 58 b2 30 ba 39 6c bf 8f 27 03 38 7e 2e c6 e7 de x.0.9l...'.8~....
0050 9b 5f 8c c1 c3 44 e5 da 85 b0 b7 25 3d 66 60 7a ...D....%=f`z
0060 3b 25 41 34 d8 27 9a 5b 99 7e 12 f6 30 42 86 16 ;%A4.'.[.~..0B..
0070 da 4a 5a c4 be 42 70 9f ce 9e 5d 12 d6 12 7a 35 .JZ..Bp....]...z5
0080 c8 36 a2 e0 d3 ca c8 b2 2b 1a cd e5 c1 10 ba 0b .6.....+.....
0090 60 bb 01 af 50 dc c6 db 02 0a 5b 64 df ef 24 06 ...P.....[d.$..
00a0 25 01 1b d9 fa 45 fe e8 91 07 ea 15 8d 21 e8 e5 %....E.....!...
00b0 99 28 fa 97 a2 99 66 8d 4e 68 57 c4 33 2c ce ae ...f.Nhw.3,...
00c0 d3 a6 b3 43 f7 09 1b 5f 6d fc f1 8f b5 88 98 f3 ...C...m.....
00d0 28 62 38 9a 2b 0b aa c1 ef be 9f f2 f9 f6 c3 23 (b8.+.....#
00e0 d9 e9 f1 37 c6 3a 63 78 fe 6f c2 87 95 a9 a7 be ...7.:cx.o.....
00f0 cd 86 b7 af cf 42 f5 f1 29 40 9a 5d af a0 02 a9 .....B..)@.]....
0100 67 3b b8 19 31 fc 87 31 75 25 9f 86 1b 32 41 9c g;..1..1u%...2A.
0110 4e 05 67 c8 49 f3 3e 68 2e 08 62 d4 f0 b2 30 e5 N.g.I.>h..b...0.
0120 9f 8e 2d 6b 3c 3f 99 45 22 30 cd 86 c1 25 f2 19 ..-k<?.E"0...%.
0130 48 c1 1d ea cc 92 4f e6 30 44 74 2c 71 00 b9 52 H...O.Odt,q..R
0140 ca 02 55 44 66 f4 a6 df a9 da f4 0a c1 06 fc 54 ..Udf.....T
0150 21 23 64 9b 6d e5 cb 87 96 a9 85 a9 81 ec 71 79 !#d.m.....qy
0160 1e 1a 85 50 3b e6 f5 6e cc 4b b2 bb 84 19 c1 e2 ...P;...n.K.....
0170 67 f8 65 7f 89 d5 c8 2d 74 a8 ec e2 7c a0 a1 bd g.e....-t...|...
0180 3f 44 eb dc 1b c5 dc b0 f1 e8 6f 5f 78 a7 0d 79 ?D.....o_x..y
0190 0c 3c 38 e0 f2 b1 0b 9b 8f 91 81 70 77 65 0b 4a .<8.....pwe.J
01a0 dd ed 46 b4 60 c9 eb 6b 63 95 18 c8 03 d4 58 53 ..F...kc.....X5
01b0 e9 3e fc 1a 3a 99 93 46 7d cd b9 27 15 e3 3b 1a .>.....F}...'...;
01c0 57 9d 58 b9 7c 18 ea e1 26 7e 8a c3 a8 4b 68 7c w.X.|...&~....Kh|
01d0 ef b5 f2 e2 .....

```

```

0000 00 12 3f 53 02 ce 00 0f b0 71 61 67 08 00 45 00 ..?S.....qag..E.
0010 00 bd 23 5d 40 00 7f 06 a2 63 80 1e 1a f7 80 1e ...#]@....C.....
0020 1a 47 f0 9e 05 99 fa 21 26 50 79 89 c1 9e 50 18 .G.....!&Py...P.
0030 42 9f 3c 7b 00 00 17 03 01 00 90 51 f8 80 b3 b4 B.<{.....Q.....
0040 33 36 d7 b4 43 e0 c5 a4 8a ff ef 33 af 32 7a 86 36..e.....s.2z.
0050 ed 02 6b 9d 7b 08 f3 6d ba 24 0f 81 54 2e bc ac ...k.{..m.$..T...
0060 a5 04 3f 85 aa 56 02 6b 0d 76 c5 c9 17 99 4a 50 ...?.v.k.v.....JP
0070 27 51 fa 72 fa 9b 72 13 35 2d fb 32 96 f9 ff 63 'Q.r..r.5-.2...c
0080 94 f4 48 d2 c9 48 c7 42 b0 37 fc 85 f1 12 64 a6 ..H..H.B.7....d.
0090 91 29 1d 7f b3 31 46 33 47 45 1f 38 47 23 ec 74 .)....1F3GE.8G#.t
00a0 7c eb 36 20 0b cc 05 70 e3 2f 32 4b b6 9c d3 17 |.6...p./2K....
00b0 fc 7d 90 4f f5 11 f4 b3 76 ad 42 a3 e9 05 9d 35 .}.O....v.B....5
00c0 96 96 21 41 99 0a 63 c7 69 7d f4 ..!A..c.i}.

```

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.

0000	00	12	3f	53	02	ce	00	0f	b0	71	61	67	08	00	45	00	..?S.....qag..E.
0010	01	eb	05	21	40	00	7f	06	bf	71	80	1e	1a	f7	80	1e	...!@.....q.....
0020	1a	47	f0	87	05	99	8d	99	82	49	ef	ea	7c	55	50	18	.G.....I.. UP.
0030	41	03	49	79	00	00	03	01	01	c3	00	00	01	00	ff	ff	A.Iy.....
0040	0a	00	02	00	00	00	e7	58	00	09	04	d0	00	34	58	00X....4X.
0050	49	00	4e	00	53	00	45	00	52	00	54	00	20	00	49	00	I.N.S.E.R.T..I.
0060	4e	00	54	00	4f	00	20	00	41	00	6e	00	73	00	77	00	N.T.O..A.n.s.w.
0070	65	00	72	00	73	00	20	00	56	00	41	00	4c	00	55	00	e.r.s..V.A.L.U.
0080	45	00	53	00	20	00	28	00	40	00	31	00	2c	00	20	00	E.S..(.@.1.,..
0090	40	00	32	00	2c	00	20	00	40	00	33	00	2c	00	20	00	@.2.,..@.3.,..
00a0	40	00	34	00	29	00	3b	00	00	00	e7	5a	00	09	04	d0	@.4.);....Z....
00b0	00	34	5a	00	40	00	31	00	20	00	69	00	6e	00	74	00	.4Z.@.1..i.n.t.
00c0	2c	00	40	00	32	00	20	00	69	00	6e	00	74	00	2c	00	,@.2..i.n.t.,..
00d0	40	00	33	00	20	00	76	00	61	00	72	00	62	00	69	00	@.3..v.a.r.b.i.
00e0	6e	00	61	00	72	00	79	00	28	00	32	00	29	00	2c	00	n.a.r.y.(.2.),..
00f0	40	00	34	00	20	00	6e	00	76	00	61	00	72	00	63	00	@.4..n.v.a.r.c.c.
0100	68	00	61	00	72	00	28	00	39	00	30	00	29	00	02	40	h.a.r.(.9.0.).@
0110	00	31	00	00	26	04	04	00	00	00	02	40	00	32	00		.1..&.....@.2.
0120	00	26	04	04	00	00	00	02	40	00	33	00	00	a5	02		.&.....@.3....
0130	00	02	00	00	00	02	40	00	34	00	00	e7	b4	00	09	04@.4.....
0140	d0	00	34	b4	00	3c	00	41	00	6e	00	73	00	77	00	65	..4..<.A.n.s.w.e
0150	00	72	00	20	00	54	00	79	00	70	00	65	00	3d	00	22	.r..T.y.p.e.=."
0160	00	53	00	54	00	52	00	49	00	4e	00	47	00	22	00	3e	.S.T.R.I.N.G.">
0170	00	3c	00	43	00	68	00	75	00	6e	00	6b	00	20	00	54	<.C.h.u.n.k..T
0180	00	79	00	70	00	65	00	3d	00	22	00	53	00	54	00	52	.y.p.e.=."S.T.R
0190	00	49	00	4e	00	47	00	22	00	20	00	43	00	6f	00	6e	I.N.G."..C.o.n
01a0	00	66	00	69	00	64	00	65	00	6e	00	63	00	65	00	3d	.f.i.d.e.n.c.e.=
01b0	00	22	00	50	00	6f	00	6f	00	72	00	22	00	3e	00	74	..P.o.o.r.">.t
01c0	00	65	00	73	00	74	00	20	00	73	00	74	00	75	00	64	.e.s.t..s.t.u.d
01d0	00	65	00	6e	00	74	00	3c	00	2f	00	43	00	68	00	75	.e.n.t.<./C.h.u
01e0	00	6e	00	6b	00	3e	00	3c	00	2f	00	41	00	6e	00	73	.n.h.>.<./A.n.s
01f0	00	77	00	65	00	72	00	3e	00								.w.e.r.>.

0000	00	12	3f	53	02	ce	00	0f	b0	71	61	67	08	00	45	00	..?S.....qag..E.
0010	01	2e	05	23	40	00	7f	06	c0	2c	80	1e	1a	f7	80	1e	...#@.....
0020	1a	47	f0	87	05	99	8d	99	84	54	ef	ea	7c	98	50	18	.G.....T.. P.
0030	40	c0	b3	47	00	00	03	01	01	06	00	00	01	00	ff	ff	@..G.....
0040	0a	00	02	00	00	00	e7	74	00	09	04	d0	00	34	74	00t....4t.
0050	49	00	4e	00	53	00	45	00	52	00	54	00	20	00	49	00	I.N.S.E.R.T..I.
0060	4e	00	54	00	4f	00	20	00	53	00	74	00	75	00	64	00	N.T.O..S.t.u.d.
0070	65	00	6e	00	74	00	41	00	6e	00	73	00	77	00	65	00	e.n.t.A.n.s.w.e.
0080	72	00	73	00	20	00	56	00	41	00	4c	00	55	00	45	00	r.s..V.A.L.U.E.
0090	53	00	20	00	28	00	40	00	31	00	2c	00	20	00	40	00	S..(.@.1.,..@.
00a0	32	00	2c	00	20	00	40	00	33	00	2c	00	20	00	47	00	2.,..@.3.,..G
00b0	45	00	54	00	44	00	41	00	54	00	45	00	28	00	29	00	E.T.D.A.T.E.(.)
00c0	29	00	3b	00	00	00	e7	38	00	09	04	d0	00	34	38	00);....8....48.
00d0	40	00	31	00	20	00	69	00	6e	00	74	00	2c	00	40	00	@.1..i.n.t.,@
00e0	32	00	20	00	6e	00	76	00	61	00	72	00	63	00	68	00	2..n.v.a.r.c.h.
00f0	61	00	72	00	28	00	35	00	29	00	2c	00	40	00	33	00	a.r.(.5.),..@.3.
0100	20	00	69	00	6e	00	74	00	02	40	00	31	00	00	26	04	.i.n.t..@.1..@.
0110	04	e9	00	00	00	02	40	00	32	00	00	e7	0a	00	09	04@.2.....
0120	d0	00	34	0a	00	43	00	4c	00	50	00	31	00	36	00	02	..4..C.L.P.1.6..
0130	40	00	33	00	00	26	04	04	8e	00	00	00					@.3..&.....

0000	00	12	3f	53	02	ce	00	0f	b0	71	61	67	08	00	45	00	..?S.....qag..E.
0010	01	f6	0c	35	40	00	7f	06	b8	52	80	1e	1a	f7	80	1e	...5@.....R.....
0020	1a	47	f0	b4	05	99	8c	3a	0b	93	ac	dd	7d	07	50	18	.G.....}.P.
0030	40	9a	a0	9b	00	00	17	03	01	01	c9	51	46	94	4a	00	@.....QF.J.
0040	29	ec	34	d2	3b	b9	e5	8a	15	59	94	a4	c0	14	d6	cc).4.;...Y.....
0050	30	5b	a1	08	9d	d2	37	45	f7	bb	48	59	3f	97	48	07	0[...7E...HY?.H.
0060	cf	61	a0	df	77	45	4e	f2	90	98	29	b7	c1	02	e8	58	...WEN...).X
0070	ef	d1	e2	97	00	25	2c	d7	f2	b0	3d	38	62	35	8a	58	...%,...=8p5.X
0080	c2	de	8f	63	c8	94	5a	8e	60	0d	5f	22	4a	fc	c8	48	...c..Z...".J..H
0090	41	8f	cd	d7	6a	1d	0a	b6	e6	96	61	07	13	36	80	ee	A...j.....a...6..
00a0	dd	ce	a1	ad	94	56	3e	3e	d8	ac	cc	d1	4d	84	89	89V>>...M...
00b0	88	6c	f6	f5	9b	dd	85	31	af	72	e8	95	9c	2a	73	bd	.J.....1.r...*s.
00c0	e8	90	d4	8f	cc	9c	b1	4f	18	e1	f3	78	b6	3a	0f	c10...x...:
00d0	66	49	54	2b	f5	d4	10	de	f0	2f	f3	cd	54	75	86	82	IT+...../.Tu...
00e0	21	80	61	50	e4	55	b1	b8	f8	ad	5a	3e	59	b3	a6	43	.aP.U.....Z>Y..C
00f0	a7	80	28	e1	46	6b	3a	8e	37	bf	18	9b	d0	f2	da	b1	..(.Fk:.7.....
0100	00	79	51	8b	33	4b	da	2b	26	b3	02	68	bb	e7	b5	5f	.yQ.3K.+&..h....
0110	32	92	2a	3e	e8	b6	37	66	40	5c	74	e2	ed	11	37	d5	2.*>...7f@t...7.
0120	9d	9d	cc	7e	bc	bd	8d	56	55	23	5f	20	2f	ab	21	56VU#.../..v
0130	4f	9c	78	90	c4	e0	f5	30	7c	ad	f8	7e	a5	e1	16	a1	O.x....0 ...~....
0140	c7	31	cd	7c	2b	72	d6	ff	60	11	4c	be	75	e5	dd	ab	.1. +r...L.u....
0150	86	33	fa	76	29	42	ec	02	e0	7d	41	b6	ad	5b	4d	54	.3.v)B...}A..[MT
0160	fc	80	03	bc	a1	48	0e	1d	ac	bd	30	2e	6e	3f	ae	43H....0.n?.C
0170	d6	d8	a3	a9	18	29	98	fd	da	8e	7f	48	3c	05	c1	fd).H<...
0180	cf	6b	77	8c	5c	f9	39	9d	64	39	09	78	57	55	5e	51	.kw.\.9.d9.xwuAQ
0190	36	3d	08	e9	25	47	90	52	b1	ea	6b	3b	3e	ee	3a	88	6=.%G.R..k;>...:
01a0	05	25	0e	e0	c2	2a	1e	85	3b	eb	06	8c	cb	cf	03	24	;%...*.;;...\$
01b0	e3	e7	59	b3	ee	eb	1b	47	73	e4	09	e6	98	df	36	3c	..Y....Gs.....6x
01c0	36	db	d7	03	59	2f	cd	48	aa	89	ba	f3	96	c8	a4	7a	6...Y/.H.....Z
01d0	c4	40	fd	4d	53	7a	87	8c	71	3f	c2	81	0b	9f	8a	f1	.@.MSZ...q?.....
01e0	47	82	bd	d7	3a	19	0c	93	ff	e8	57	f1	28	2c	97	12	G.....w.(...
01f0	26	87	88	15	a8	dd	82	7c	e3	69	82	4b	dd	e2	44	e6	&..... .i.K..D.
0200	fe	e5	26	0a													...&.

0000	00	12	3f	53	02	ce	00	0f	b0	71	61	67	08	00	45	00	..?S.....qag..E.
0010	01	43	0c	37	40	00	7f	06	b9	03	80	1e	1a	f7	80	1e	.C.7@.....P....
0020	1a	47	f0	b4	05	99	8c	3a	0d	be	ac	dd	7d	74	50	18	.G.....}tP.
0030	40	2d	a1	e6	00	00	17	03	01	01	16	e3	9c	a2	9a	ee	@-.....P....
0040	86	b0	a3	0f	63	d4	66	bf	13	d1	28	bc	78	f7	f1	c4c.f...(.x....
0050	d9	84	ce	3c	13	de	7e	87	e9	34	07	b0	0e	15	1c	0a<...4.....
0060	2b	d2	a9	64	1d	fe	87	02	af	32	ca	ca	25	ab	c3	34	+...d...2...%.4
0070	5c	45	5b	52	cd	37	ac	99	e0	47	fb	b8	ef	45	7e	15	\E[R.7...G...E~.
0080	96	2e	22	6e	d7	47	1e	c9	08	73	13	2e	75	1e	a8	9b	...n.G...s..u...:
0090	aa	54	91	74	1a	49	65	28	27	82	fd	04	e7	1a	94	f3	.T.t.Ie('.....
00a0	44	53	02	7e	58	60	e7	84	2c	c2	3c	70	8d	af	13	53	PS.~X'.....<p...s
00b0	f4	4d	1d	18	dc	dd	ce	98	36	a9	ab	71	c1	5a	d4	ea	.M.....6...q.Z..
00c0	68	41	12	89	72	c9	82	25	db	82	47	52	1c	64	e6	f4	hA...r...%.GR.d..
00d0	b9	20	4f	a7	5a	15	12	d9	3b	d1	0b	3f	80	fa	28	6b	...O.Z...;.?.(k
00e0	b3	10	e2	59	bf	13	47	ee	63	1c	a2	ca	b0	c3	36	90	...Y..G.C.....6.
00f0	91	75	9e	66	a4	82	43	eb	84	c1	e7	80	d6	63	f7	d6	.u.f..C.....C..
0100	e1	f7	13	14	6e	d8	22	3d	75	67	fb	00	7d	c4	f2	e4n."=ug..}...
0110	22	92	ac	3d	7e	1a	ff	e1	fe	66	8e	9a	0e	d3	25	8b	...==...f....%
0120	75	17	f6	ed	41	3c	9c	4b	9c	3a	b7	94	e4	6a	38	44	u...A<.K.:...j80
0130	ef	59	8e	9a	75	0f	47	b7	4f	c5	58	53	b1	9d	87	86	.Y...u.G.O.XS....
0140	8c	46	c4	af	89	98	5d	f8	92	fe	ae	51	e7	21	d3	8c	.F...].Q...!
0150	cb																.

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

[Bushweller, 1999] Bushweller, Kevin. "Generation of Cheaters," The American School Board Journal, April, 1999.

[Chen, 2006] Chen, Jessica. "Instructor Authoring Tool: A Step Toward Promoting Dynamic Lecture-Style Classrooms." M.Eng. Thesis, MIT Department of Electrical Engineering and Computer Science, February 2006.

[Davis, 1993] Davis, Barbara Gross. *Tools for Teaching*. San Francisco, California.: Jossey-Bass Publishers, 1993.

[Dyreson, 1996] Dyreson, Curtis E. " An Experiment in Classroom Management Using the World-Wide," *Proceedings of the Second Australian Conference on the World-Wide Web (AusWeb '96)*, Gold Coast, QLD, July 1996.

[Kleek, 2004] Kleek, Max Van. (2004) "distinctive touch." Mas.622j final project.

[Kleek, Varenhorst, and Rudolph] Kleek, Max Van and Varenhorst, Christopher and Rudolph, Larry. "Lightweight Identification for Enabling Personalization on Public Displays." MIT CSAIL.

[Koile and Shrobe, 2005] Koile, K. and Shrobe, H.E. (2005) "The Classroom Learning Partner: Promoting Meaningful Instructor-Student Interactions in Large Classes." MIT CSAIL TR.

[Koile and Singer, 2005] Koile, K. and Singer, D., "Educational Assessment for the Classroom Learning Partner", Massachusetts Institute of Technology, 2005.

[Koile and Singer, 2006a] Koile, K. and Singer, D., *Development of a Tablet-PC-based System to Increase Instructor-Student Classroom Interactions and Student Learning*, To appear in *The Impact of Pen-based Technology on Education; Vignettes, Evaluations, and Future Directions*. Berque, D., Gray, J., and Reed, R. (editors). Purdue University Press, 2006.

[Koile and Singer, 2006b] Koile, K. and Singer, D., "Improving Learning in CS1 with Tablet-PC-based In-Class Assessment", Submitted to ICER 2006 (Second International Computing Education Research Workshop), September 9-10, 2006, University of Kent, Canterbury, UK.

[Lewis, 2004] Lewis, Morris. *SQL Server Security Distilled*. Apress: 2 edition, 2004.

[Rbeiz, 2006] Rbeiz, Michel. *Semantic Representation of Digital Ink in the Classroom Learning Partner*. M.Eng. Thesis, MIT Department of Electrical Engineering and Computer Science, 2006.

[Shrobe, 2002] Shrobe, H.E. "Computational Vulnerability Analysis for Information Survivability," *AI Magazine*, vol. 23, issue 4, Winter, 2002, 81-94.

[Smith, 2006] Smith, Amanda. *Aggregation of Student Answers in a Classroom Setting*. M.Eng. Thesis, MIT Department of Electrical Engineering and Computer Science, 2006.

[Wolfman, 2004] Wolfman, Steve. *Understanding and Promoting Interaction in the Classroom*. Ph.D. Defense, July 28, 2004.