DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.033—Computer System Engineering Handout 23—April 13, 1995

Design Project #2: ELECTRONIC SHOPPING AT MIT

Introduction

MIT is going through a reengineering phase, which includes redesigning some information technologies (I/T). (Please see the attached article published in Tech Talk on MIT's reengineering effort.) Professor James Bruce, who heads the I/T reengineering task force, has heard about some radical new ideas (such as electronic shopping) while attending the latest Computer Society International Conference, and he is intending to make an electronic shopping mall be part of MIT's reengineering plan. In particular, he is wondering whether a payment switch (the heart of an electronic shopping system) could be deployed at MIT with the help of the Kerberos authentication mechanisms, since secure authentication is an important part of any kind of electronic shopping. Professor Bruce has heard that 6.033 students are well versed in Kerberos and the necessary security and systems issues that are involved in setting up an on-line electronic shopping mall.

Your Assignment

Your task is to write a 10 to 12-page report that proposes a design for an MIT electronic shopping mall, evaluates the feasibility of the idea, discusses the important issues, and gives recommendations. In particular, your report should focus on the payment switch for the electronic shopping mall. As is typical of most real world assignments, a good portion of the problem is defining the problem, as the initial definition of the problem seems to start with many muddled, disconnected ideas. Your general approach should be to first collect, read, and review any appropriate documentation, find the important issues, work out a design, identify the important design decisions, and write a clear, concise, coherent report. For important design issues, be sure to explain your reasoning and possible alternatives. Be sure to include step by step descriptions of what occurs when a buyer uses the system to purchase a copy of the 6.033 course notes, adds $100 to a meal card, and orders the 6.001 textbook.

You can assume that Professor Bruce is the primary audience for your report, so you need to go into some technical depth, especially with regards to security measures. You should provide sufficient background for Professor Bruce to be able to evaluate your report; you can assume that he has read the Kerberos paper some time in the past and understands the Athena infrastructure and computer systems issues at a 6.033 level. Your report should contain enough detail so that he can evaluate whether your design addresses all the requirements and whether your design won't cause too many downstream surprises. Professor Bruce asked the 6.033 staff to forward the best projects for possible input to the design for the real system.

The MIT Electronic Shopping Mall

The electronic shop will be open only to members of the MIT community (i.e., MIT Kerberos principals). The three initial products to be offered are:

- Course notes, which when purchased will give the buyer access to an on-line copy of the notes.
- Meal plan upgrades, which will add money to a meal plan account.
- Textbooks, which when purchased will be delivered via interdepartmental mail.

Your design should be general enough so that the electronic shop can be expanded to deliver other products. You may even like to suggest new products that the electronic shopping mall should offer.

The three methods of payment which are to be supported are:

1. A charge to a Bursar's account.
2. A debit on an MIT card account.
3. A charge to a national credit card (e.g., VISA).

The Interface to the MIT Electronic Shopping Mall

The user interface will be a Web browser. Buyers should be able to visit an on-line store via the URL "http://www.online_shop.mit.edu" and view information about the various items available for purchase. When a buyer decides he wants to buy something, that item is put into an electronic shopping cart. When the buyer is finished browsing and wishes to make the purchase, he or she fills out an on-line form, which specifies the method of payment, credit card number and card expiration date (for credit card purchases), delivery address (for textbooks), and any other necessary information.

Desirable Properties for the MIT Electronic Shopping Mall

- Sensitive data must be kept secure; it should not be transmitted in clear text over the net and should not be accessible to unauthorized parties.
- The server must always authenticate the clients on all purchases.
- Clients should have an option of authenticating the server.
- Clients should have the ability to anonymously browse and place items in a shopping cart (i.e. authentication should occur only when a purchase is made).
- The system should never charge a buyer for products that will not be delivered.
- The system should never deliver products that have not been paid for.
- The system should be appropriately reliable, available, and efficient.

You may identify other desirable properties; make sure to mention those explicitly and why you included them. Part of the design project is to identify the relevant issues for each design goal. For example, for security it is necessary to identify what kinds of data must be kept secure and the kinds of threats the system must defend against.

Hints

A large part of this project will consist of designing a server for the electronic store, accessible via the Web, that can meet the design goals. Another important issue deals with the necessary client software and how Web browsers may need to be modified to interact with the electronic store.

You should go into a reasonable level of technical depth for important design issues that are essential for the system to work properly. For example, it is not enough to simply say “HTTP needs to be modified to provide secure authentication and encryption”. Instead, you need to explain how this will be accomplished and what the protocols are.

The level of detail you should go into is different for this design project than for the first design project. We are not asking you to patch up an existing web browser and bugs in the Web naming scheme, but instead we asking for a design that extends one level “higher.”

You will probably want to take advantage of MIT’s existing Kerberos infrastructure for authentication. An important part of the design is figuring out how client Web software and the electronic store Web server can use Kerberos for authentication. In addition, you may want to incorporate the idea of a payment switch as discussed in Gifford’s paper (the attached article from Open Market Systems).

You need not worry about details of interfacing with the Bursar’s account computers, the meal card office’s computers, or outside financial institutions. You can assume that the necessary software and hardware will be available to the server.

Overall, you should look for opportunities to make use of ideas learned in 6.033 in many areas: control of complexity, client/server organization, networking, naming, cryptography, authentication and authorization, storage systems, fault-tolerance, social concerns and risks of technology, privacy, etc.

Getting Started

As a starting point, you should use the Kerberos paper (reading #29) and the attached article from Open Market Systems (which also contains references to other electronic payment switches). You might also want to check out the following URLs for some companies currently involved in on-line commerce (many others exist):

1. Open Market Systems (http://www.openmarket.com)
2. NetMarket (http://www.netmarket.com)
3. CDNow (http://www.cdnow.com)

You probably also should read about transactions, assigned for the week of 5/1, as background research for this project.

Logistics

You are to work in teams of three students. All the members of a given team must have the same recitation instructor. We have enclosed a **registration form** for your team to be submitted in recitation on **Thursday, April 20**.

Schedule: Your report is due in recitation Thursday, May 4.

6.033 REGISTRATION FORM FOR DESIGN PROJECT II

Please fill out this form and return it in recitation on Thursday, April 20.

The name of my recitation instructor is:

The members of my team for design project II are:

1.

Name:

Email address

2.

Name:

Email address

3.

Name:

Email address:

The Tech Talk------- I/T transformation is next... (3/25/95)

News Office/TechTalk

3/22/95 Tech Talk

I/T transformation is next on reengineering agenda

By Alice C. Waugh

News Office

Information technology will play a crucial role in enabling MIT's reengineering efforts to succeed, and to that end, information technology staff throughout MIT must begin working together in new ways, senior officers said in an announcement last week. An Institute-wide search to fill positions on a new I/T Leadership Team is the next step in transforming work to implement, operate and help people use information technology.

The announcement of a new framework for I/T work was made on March 15 by William R. Dickson, senior vice president and chair of the Reengineering Steering Committee. J. David Litster, vice president and dean for research, outlined elements of the new framework, based on work by the I/T Transformation Team. Professor Litster is the team's sponsor. James D. Bruce, vice president for information systems and reengineering program manager, described how the transition to the new framework will be launched.

Present for the announcement were staff from Information Systems, as well as information technology staff from other offices such as Admissions, the Alumni/ae Association, the Comptroller's Accounting Office and the Libraries. These included programmers, systems analysts, system operators, project managers, consultants, trainers and production coordinators.

The new framework for I/T addresses a major challenge, Professor Litster explained. While staff continue to run current systems, they must implement and help people use several systems needed for reengineering, such as the new SAP R3 financial package, a new appointments application and a data warehouse. This is a substantial addition to the I/T workload. "The guiding principle for administrative I/T is a partnership committed to a shared I/T mission: Great Systems Fast, where `great' is defined by the customer," Professor Litster said. At the same time, the Institute is committed to pursuing continued excellence in academic computing, Professor Bruce emphasized.

I/T Transformation will affect all staff and managers in central offices who do I/T work, Mr. Dickson said. Although long-term predictions can't be made, there are no plans for I/T staff reductions for at least the next year or two. However, during this period, some existing I/T jobs will be eliminated and some new I/T positions added.

The first staffing change is the creation of a new I/T Leadership Team, said Professor Bruce, who will head this team in his role as vice president for information systems. Posts on the new team include five I/T process leaders, up to three I/T competency group leaders and two I/T practice leaders, one each for office and academic computing. The academic computing post is currently held by Gregory Jackson and will not change. Professor Bruce announced that, as the present IS work migrates to the new I/T framework, other IS director positions associated with that work will be eliminated.

The Institute-wide search for the new positions begins immediately, and applications are due April 3 to Ken Hewitt, MIT Personnel Officer. Job descriptions and application instructions are available on the World Wide Web at <http://whodunit.mit.edu/itlt/jobdesc.html>.

The new I/T Leadership Team will coordinate the I/T transformation and lead ongoing activities in the new framework. Teams will be the center of the action, accountable for results and with the resources and authority to achieve them. Three dimensions of the framework support the teams: improving work processes, developing skills and focusing on customers.

The process leaders will coordinate the five major phases of I/T work, wherever it occurs: I/T Discovery (choosing what work needs to be done and how to do it), I/T Delivery (designing and furnishing the results to the customer), I/T Integration (maintaining a cohesive I/T infrastructure incorporating each new product or service), I/T Service (installing new services and keeping them running), and I/T Support (helping the MIT community acquire, access and use information technology).

Competency groups will act as conduits for sharing skills throughout the Institute's I/T community. Although group members will not have offices together, they will meet periodically and communicate electronically, "to promote learning, to coordinate appraisal and to share expertise. We believe, as we look across all of IS and beyond that across I/T, that we can learn a tremendous amount from each other," Professor Bruce said.

Leaders of I/T practices will focus on ensuring that MIT's I/T resources serve the needs of specific constituents, e.g., for academic computing and for office computing. These leaders will act as liaisons between I/T and constituents, promoting deeper understanding of constituents' needs and priorities.

In the new framework, individuals may be on one or several teams, they may be a member of one and a leader of another, and they may work on more than one process. "I realize this sounds more complicated than the way we think about work today, but it's a way of organizing ourselves so we can literally be more efficient in delivering results to the community," Professor Bruce said.

As I/T staff continue to support current systems and simultaneously implement new ones, there will be a greater emphasis on performance and flexibility. "In the future, we must achieve even greater results in less time, we must each have a more complete set of skills, and we must couple our work more closely with our customers' needs," he said.

Further information about the I/T transformation will be available through group meetings and other forums. Those with questions or suggestions may e-mail them to <trans-it@mit.edu> (for attribution) or anonymously to the Institute-wide reengineering mailbox at <workout@mit.edu>, indicating "Attn: I/T Transformation."