

**Ensuring Anonymity and Privacy
in an Online Mental Health Community**

by

Hsias Y. Leung

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

May 24, 2002

[June 2002]

Copyright 2002 Hsias Y. Leung. All rights reserved.

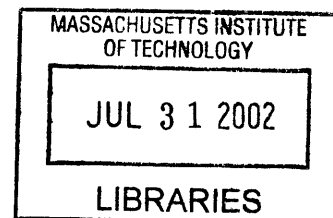
The author hereby grants to M.I.T. permission to reproduce and
distribute publicly paper and electronic copies of this thesis
and to grant others the right to do so.

Author _____
Department of Electrical Engineering and Computer Science
May 24, 2002

Certified by _____
Hal Abelson
Class of 1922 Professor, Mac Vicar Teaching Fellow
Thesis Supervisor

Accepted by _____
Arthur C. Smith
Chairman, Department Committee on Graduate Theses

BARKER



Ensuring Anonymity and Privacy in an Online Mental Health Community
by
Hsias Y. Leung

Submitted to the
Department of Electrical Engineering and Computer Science

May 24, 2002

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

Abstract

The design and development of an online mental health community, specifically the myCare web application, is aimed at providing users with anonymous and private communication and information resources. The formation of the system's requirements takes in to account the different services and components that the application will need to support. In examining previous research in the area of anonymity and privacy, we can determine the possible technologies that are available in building such an application. The design and implementation of the myCare application provides a framework of supporting multiple mental health topics, communication possibilities, and different user roles. Pseudonymous logins, moderated message boards, and instantaneous messaging between users and trained peer counselors are examples of functionality implemented to provide a protected way for users to communicate. The software architecture and implementation is discussed, along with future work and deployment criteria. An evaluation of the design is provided, verifying that myCare ensures more user anonymity and privacy than current systems. Finally, we suggest protocols and technical privacy disclaimers that can be used as a basis to form more stringent operational rules when the myCare software application is deployed by trained personnel.

Thesis Supervisor: Hal Abelson

Title: Class of 1922 Professor, Mac Vicar Teaching Fellow

Contents

1	Introduction	7
1.1	Purpose	7
1.2	Project Overview	7
1.3	Organization of Thesis	8
2	Usage Scenarios	10
2.1	Overview	10
2.2	Anonymous User	10
2.3	Pseudonymous User	15
2.4	Counselor	16
2.5	Administrator	19
2.6	Risks	19
3	Functional Requirements	21
3.1	Types of Users	21
3.1.1	General Requirements	21
3.1.2	Visitors	22
3.1.3	Regular Users	23
3.1.4	Counselors	24
3.1.5	Administrators	24
3.1.6	Summary of Types of Users	25
3.2	Features	25
3.2.1	General Requirements	25
3.2.2	Possible Features	26
3.2.3	Supported Features	27
3.2.4	Degree of Protection Summary	32
4	Research Topics	33
4.1	Overview	33
4.2	Terminology	33
4.3	Related Work and Technologies	35
4.3.1	Overview	35
4.3.2	Anonymity and Pseudonymity	35
4.3.3	Privacy	37

4.3.4	Security	38
5	Design	40
5.1	Logins	41
5.1.1	Logging In	41
5.1.2	Creating User Accounts	42
5.1.3	Administrators and Counselors	42
5.1.4	Design Considerations	43
5.2	Moderated Message Boards	44
5.2.1	General Message Structure	44
5.2.2	Message Creation	44
5.2.3	Message Moderation	45
5.2.4	Viewing Messages	45
5.2.5	Design Considerations	45
5.3	Instantaneous Messaging	46
5.4	Service and Component Infrastructure	47
5.5	Personal Configuration and Profiles Infrastructure	47
6	Software Architecture and Implementation	48
6.1	Overview	48
6.2	Software Architecture	50
6.2.1	myCare Web Application (.NET)	50
6.2.2	myCare Instantaneous Messaging	51
6.3	Database	53
7	Evaluation of the Design	55
7.1	Case Study 1: American Online, Inc.	55
7.2	Case Study 2: Medical Record Privacy	57
8	Deployment Notes and Issues	58
8.1	Deployment and Training	58
8.2	Operating Protocols	59
8.2.1	Administrator Accounts	59
8.2.2	Message Board Approval	60
8.2.3	Instantaneous Messaging	60
8.2.4	Personal Configurations	60

8.2.5 Administrator and Counselor General Usage61

8.3 Technical Privacy Policy62

9 Future Work62

9.1 Services and Components62

9.2 Personal Profiles62

9.3 User Interface Improvements63

10 Conclusions64

Bibliography66

Chapter 1

Introduction

1.1 Purpose

The last five years have seen a strong increase in demand for mental health services at MIT and across the country. In the year 2000, the MIT Medical Mental Health Service saw approximately 50% more students than in 1995 and an approximately 69% percent increase in student psychiatric hospitalizations, reflecting a growing number of students with serious mental health conditions. [12]

According to the MIT Mental Health Task Force Report from the end of 2001, there is a growing need for mental health resources and services for the MIT community, particularly students. It is a goal of the MIT Mental Health Task Force to increase late-night services, counseling support services, and promote awareness of mental health issues. Thus, the myCare project was formed as a student initiated effort to build an online community that provides resources concerning mental health issues and facilitates communication between students and trained peer counselors. A group of trained administrators and peer counselors will deploy the myCare web application, following a stringent set of operating protocols and privacy policies. Through strict definition and enforcement of anonymity and privacy practices, students can use the myCare system to share information or discuss mental health topics with trained peer counselors in a confidential manner.

1.2 Project Overview

In the design, development, and deployment of online mental health communities, there is great need to provide user anonymity and privacy while enabling

appropriate communication between different parties. The myCare project was created to develop and deploy a non-threatening online community to provide resources and communication media for students. By examining previous anonymity and privacy research, we are able to design the myCare mental health web application. Main features of the application include pseudonymous logins supporting different user roles, moderated message boards, and anonymous instantaneous messaging.

Possible technologies in existing anonymity and privacy research are discussed to provide background and potential solutions in designing the myCare application. The system is designed in such a way that communication is as secure as possible and any identifiable information is not persisted within the system. There are two main components of the myCare system: (1) a Microsoft .NET web application, providing most of the functionality for the myCare mental health web application, and (2) a Java server and applet implementation which provides instantaneous messaging functionality. The myCare system design is evaluated against other models, ensuring an adequate degree of protection for users. Along with suggested protocols and technological privacy policies, the application can be deployed with specially trained peer counselors and administrators to form an anonymous and private online mental health community.

1.3 Organization of Thesis

In Chapter 2, we describe usage scenarios for different user roles, intended purposes, available functionality, and possible risks. Chapter 3 enumerates the functional requirements of the myCare mental health web application. Chapter 4 is a listing and discussion of previous research topics in anonymity and security that were considered in the design of the myCare application. The design of the system, including alternatives, is discussed in Chapter 5, and the software architecture and

implementation is described in Chapter 6. In Chapter 7, the design of the myCare system is evaluated against two case studies. In Chapter 8, suggested protocols and technological privacy policies are given. In Chapter 9, we provide a listing of future work. Finally, conclusions are drawn in Chapter 10.

Chapter 2

Usage Scenarios

2.1 Overview

This section contains possible usage scenarios for different types of users. The different user roles in the myCare online mental health community have associated access controls and responsibilities. Examples of the intended usage purposes are discussed along with appropriate features and risks.

2.2 Anonymous User

A dormitory student, Amy, is having some problems dealing with cold Boston weather and the dreary atmosphere at MIT. While she is doing well in school, Amy simply wants to find out how other students might be dealing with the depressing winters. So, hearing about the new anonymous and private myCare mental health community available to MIT students, Amy decides to login to the myCare site. Upon bringing up the myCare webpage, she sees possible actions as seen in Figure 2.1: logging in to the site, instantaneous messaging, and a variety of services.

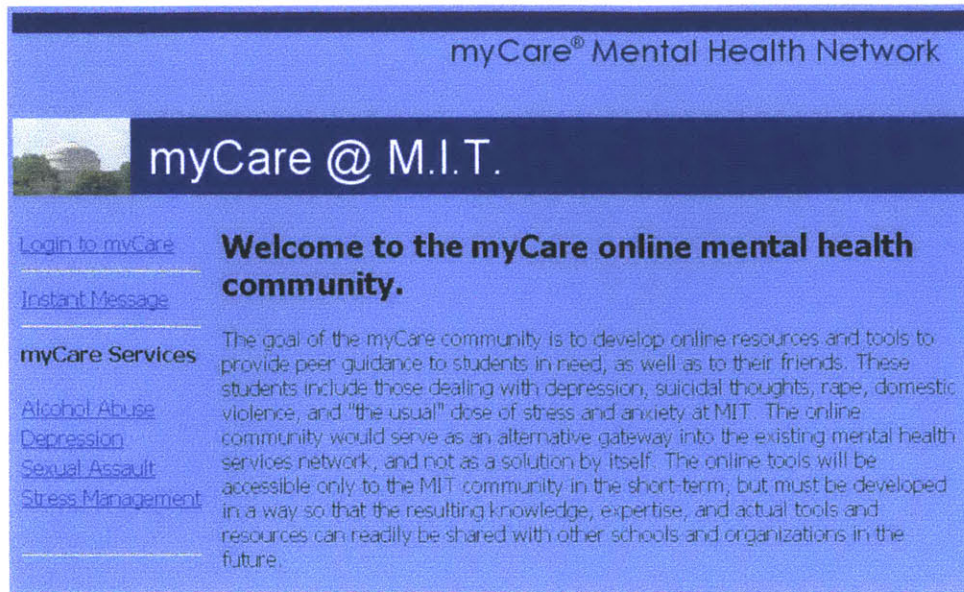


Figure 2.1: Initial entrance to the myCare website.

She decides that “Depression” is the appropriate topic of interest, so, she clicks on the “Depression” topic. Upon clicking on that topic, a summary page appears and new actions are available. However, Amy wants to know the opinion of other students, and chooses the “Message Board” option, as shown in Figure 2.2.

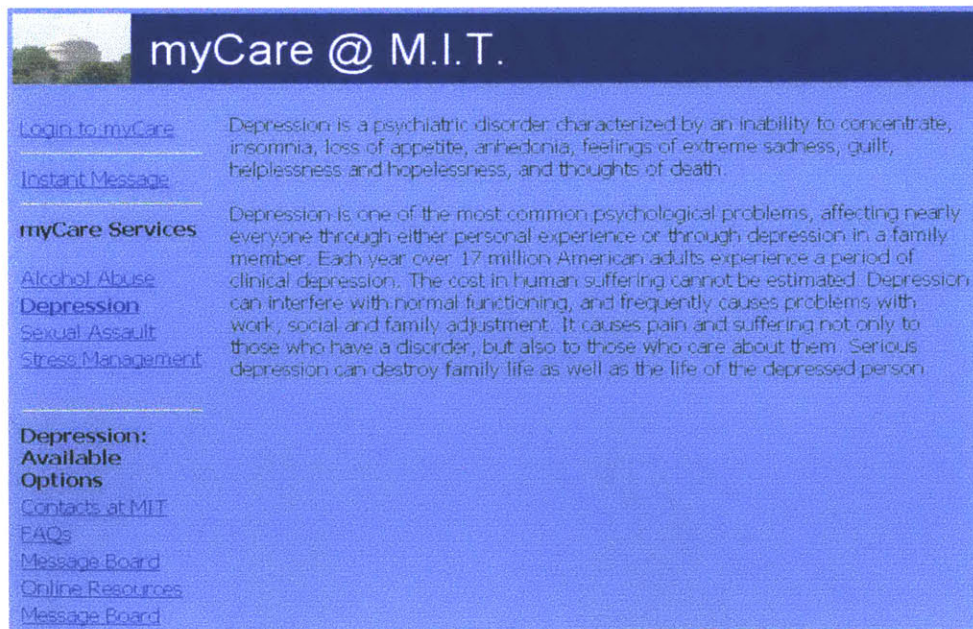


Figure 2.2: The site after an anonymous user chooses the “Depression” service.

She learns that this is a moderated message board, in Figure 2.3, where messages must be approved by trained moderators before being posted to the general public. She can also click on a link to take her to tips for adding messages. Figure 2.4 shows the message details after clicking on the subject of a message.

Depression: Moderated Message Board

Click on "Add New Message" to post a new message. Once a moderator has viewed your message as appropriate for the message board, it will be approved and publically viewable.

[Add New Message](#) [Tips for Adding a Message](#)

Date Posted	Subject	Posted By	Replies
02/12/2002 4:56pm	Welcome to the Depression Message Board!	Counsel_123	-
02/13/2002 2:12am	Prescriptions for anti-depressants at MIT Medical?	Anonymous	4
02/13/2002 10:30am	Opinion on psychiatrists at MIT Med.	BlueCat444	2
02/14/2002 10:00pm	Depressing dorm...	Anonymous	2
02/14/2002 10:20pm	Thoughts on classrooms and depression...	RedLyon222	-
02/15/2002 1:00pm	Coping with new roommates.	Anonymous	2
02/16/2002	New term blues	Anonymous	-

Figure 2.3: Depression Moderated Message Board Summary

Depression: Message Detail

[Add New Message](#) [Reply to this Message](#)

Subject: [Depressing dorm...](#)
Date: 02/14/2002 10:00pm
Posted by: Anonymous
Responses:
[Re: Depressing dorm...](#)
[Re: Depressing dorm...](#)

Body:
 I find dorms to be rather depressing places. I don't get along with most people on my floor. But, I have friends in other dorms. We try to go out to places other than the dorm for hanging out. What do people think about dorms? I don't know exactly why dorms are depressing--anyone have any ideas?

Figure 2.4: Depression Message Detail

After reading a handful of messages, Amy decides to post her own—with subject “Activities to combat depression during winter.” She enters the body of her message and submits the message, as in Figure 2.5.

The screenshot shows a web interface with a blue background. On the left is a navigation menu with links: 'Login to myCare', 'Instant Message', 'myCare Services', 'Alcohol Abuse', 'Depression', 'Sexual Assault', 'Stress Management', 'Depression: Available Options', 'Contacts at MIT', 'FAQs', 'Message Board', 'Online Resources', and 'Message Board'. The main content area is titled 'Depression: Add New Message'. It contains a 'Subject:' label above a text input field containing 'Activities to combat depression in winter.'. Below that is a 'Body:' label above a larger text area containing the message text: 'I'm not used to the Boston winter months, and find it dreary and depressing here. Do other people feel the same way? Anyone have suggestions of things to do around MIT to combat depression during the winter?'. At the bottom of the form is a 'Save Message' button.

Figure 2.5: Adding New Message.

She is notified that her message will be posted to the general public as soon as a moderator approves the message. When Amy checks the site the next day, her message has been posted, along with two replies written by BlueCat444 and Counsel_123, which she can read.

A few days later, Amy learns that her father has taken ill. All of her friends are studying for exams, and she does not want to disturb them. Amy decides to use the anonymous instantaneous messaging option on the myCare website. When she clicks on the “Instantaneous Messaging” link, a Java applet appears, shown in Figure 2.6, where she requests a session with a peer counselor. She tells the peer counselor of

the problems she is having in terms of the weather, dorm life, academics, and of her father being ill as the last straw. The two users discuss the issues at hand, and the peer counselor provides suggestions of how to deal with her problems. Amy, feeling satisfied that there is a knowledgeable and comforting resource to speak to finally ends the instantaneous messaging session, and closes her browser.

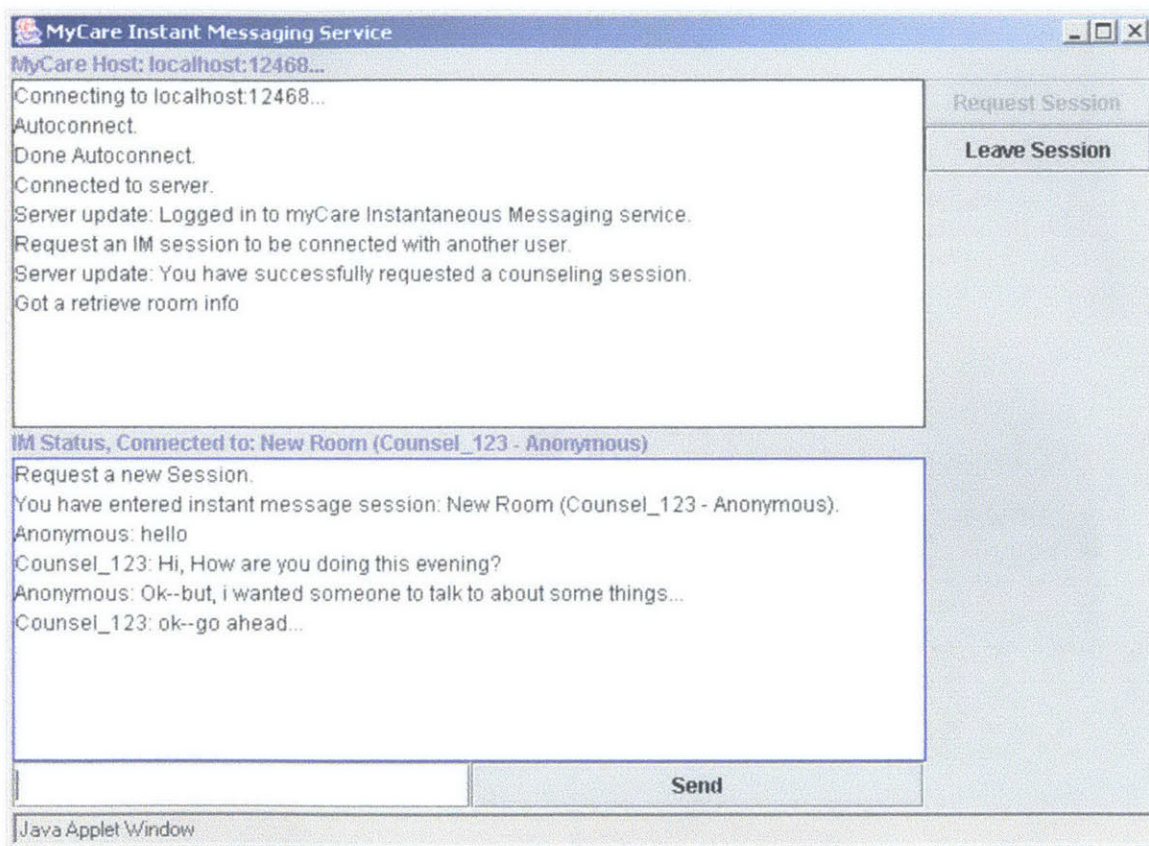


Figure 2.6: myCare Java Instant Messaging Applet.

What would the difference be if Amy were not an MIT student? Or, if Amy was a malicious web user who wanted to post obscenities on the website? And while she may not provide identifiable information about herself, what if she were to provide private information about others? Possibly, Amy could be involved in criminal activity, and law enforcement agencies would want to records of the messages and instantaneous

messaging communication she has had with peer counselors. What information monitoring and traffic analysis is possible in examining Amy’s communication to the myCare web application? It is also that Amy’s problems are not simple and is in danger of harming herself—so, should anonymity and privacy be broken in such a case?

2.3 Pseudonymous User

Bob, known as BlueCat444, the replier to Amy’s message concerning depression at MIT, uses the myCare online community often. Having taken some psychology classes, Bob has an interest in certain mental health topics, and has decided to create a pseudonymous login to build a reputation for himself. Figure 2.7 shows how Bob created a new user account for the pseudonym “BlueCat444”.

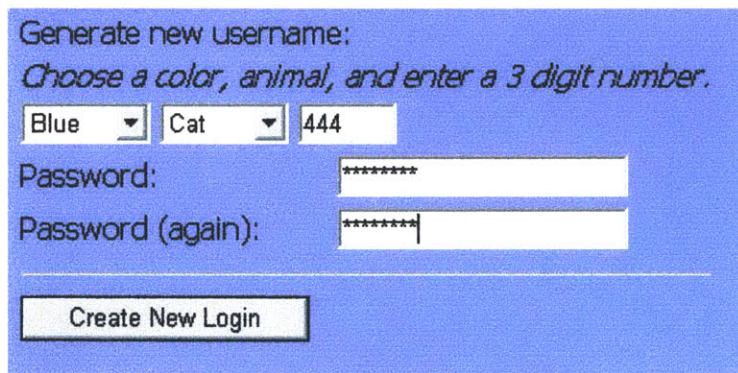


Figure 2.7: New user account.

Also, with configuration features provided, he can be notified of any new messages in the services he is most interested in (being depression and alcohol abuse), as in Figure 2.8.



Figure 2.8: User Profile for BlueCat444.

Other users, like Amy, may start looking for BlueCat444's responses to those messages if he has similar experiences and insights. On more than one occasion, BlueCat44 has spoken to a counselor that remembers his postings and other instantaneous messaging sessions, so meaningful counseling relationships have been built up between BlueCat44 and other users of the myCare application.

With a pseudonym, however, there is more chance of putting together distributed pieces of information to learn the true identity of BlueCat44. Furthermore, all of the risks involved in being an anonymous user of the system also apply for being a pseudonymous user.

2.4 Counselor

A myCare counselor is a student who learns the operating protocols of the application. One such counselor, Cindy, logs on the myCare application with her pseudonymous login, Counsel_123. Cindy begins viewing the new messages that need approval on the depression message board. Figure 2.9 shows the counselor view of the

depression message summary. The “Needs Approval” box is checked, notifying that the counselor that Amy’s new anonymous message needs to be viewed and approved.

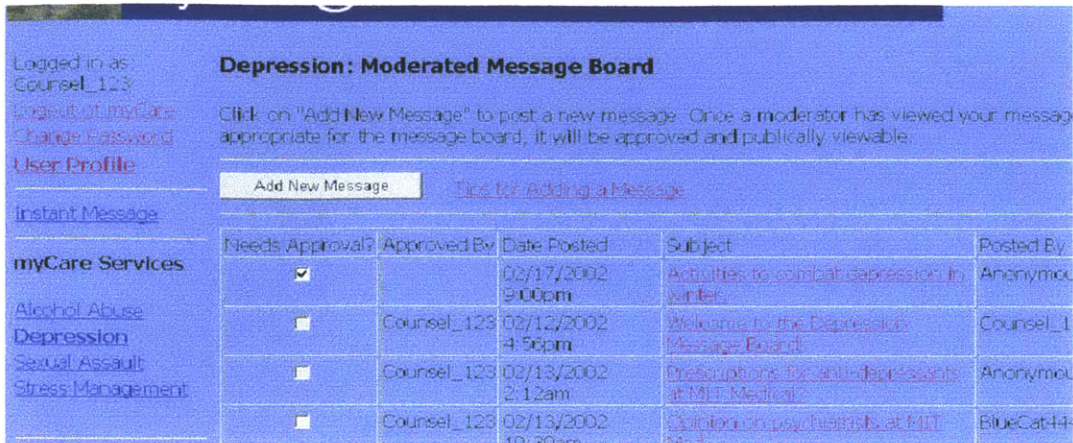


Figure 2.9: Counselor view of Depression Message Board.

She reads the message, and seeing that the anonymous user is asking for suggestions for how to cope with the dark Boston weather. Cindy clicks on the subject of the message, as in Figure 2.9, and approves the message, allowing all web site visitors to read and reply to a message. Cindy also chooses to reply to the message, giving her own suggestions of activities and resources around MIT. Her message is automatically in “approved” and available for the public to view, see Figure 2.10.

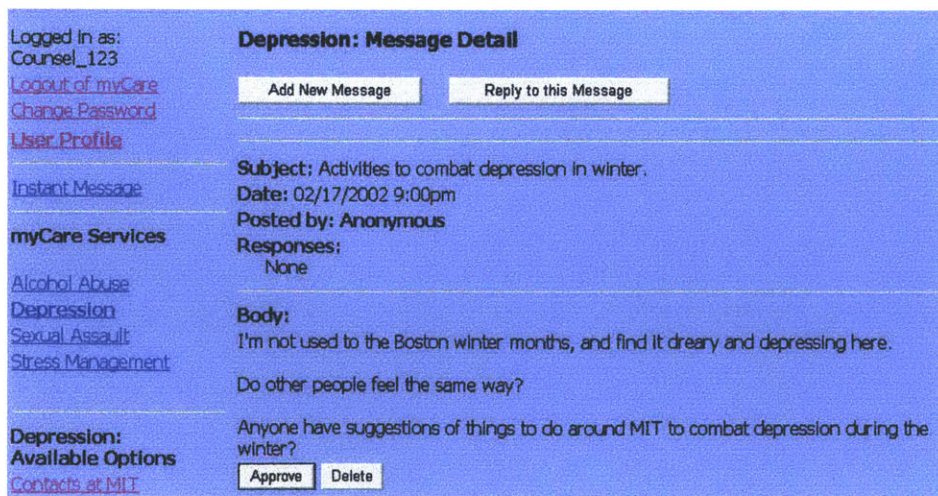


Figure 2.10: Counselor view of message details.

During the next session, Counsel_123 clicks on the instantaneous messaging functionality and is connected to user BlueCat444, who often talks about general mental health issues, coping with academics at MIT, and problems that his or her friends have.

Figure 2.11 shows the instantaneous messaging applet from the counselor's view.

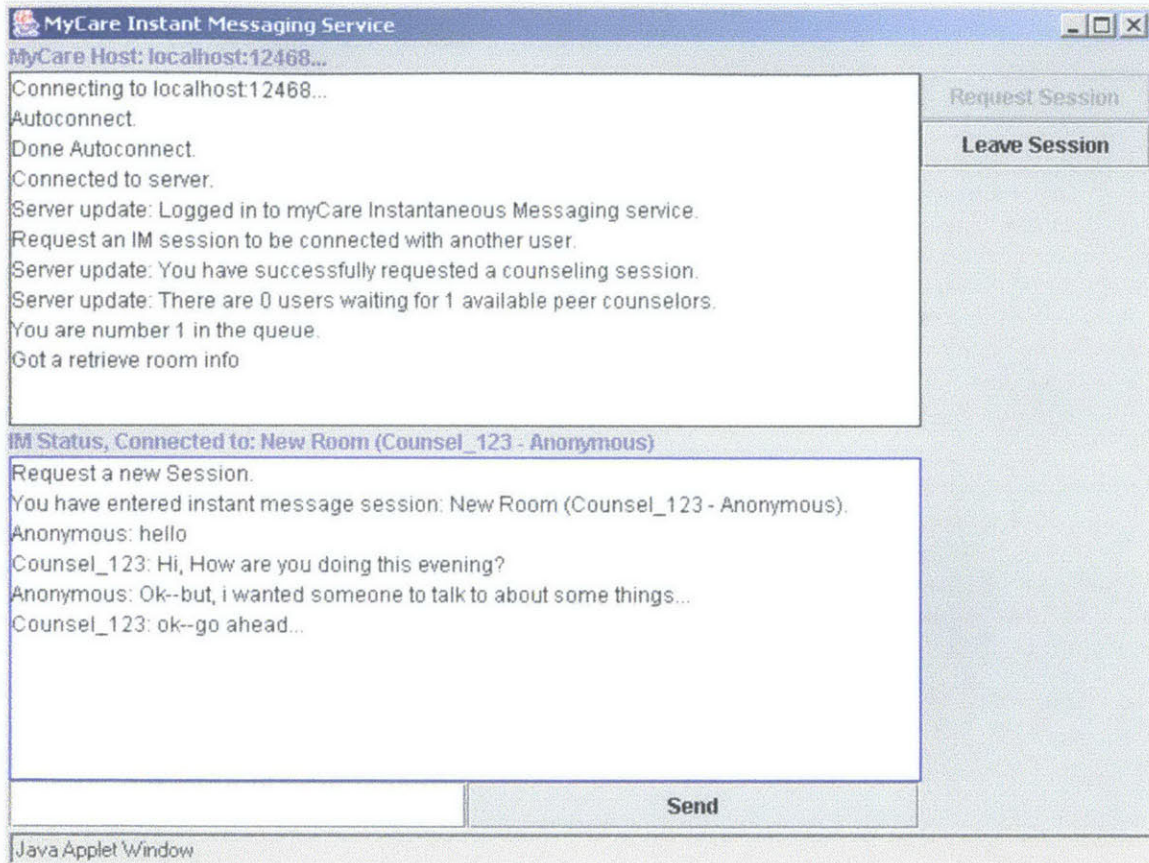


Figure 2.11: Counselor view of myCare instantaneous messaging applet.

While counselors must be trained, they will be known to other counselors and administrators of the system. However, regular users should not be able to learn the true identity of a counselor, since that is a risk of exposing counselor's privacy. Abuse is still possible from the counselor's end as well. What if they start logging their instantaneous messaging sessions or keep records of inappropriate messages that were deleted from the application?

2.5 Administrator

One of the myCare administrators, Dave, working with other administrators, has trained two new counselors, and it is his responsibility to create counselor accounts for them. So, he logs in to the myCare application and chooses to create two new counselor accounts, shown in Figure 2.12.. He emails the new counselors with their new account information, asking them to login and change their password at their next opportunity.

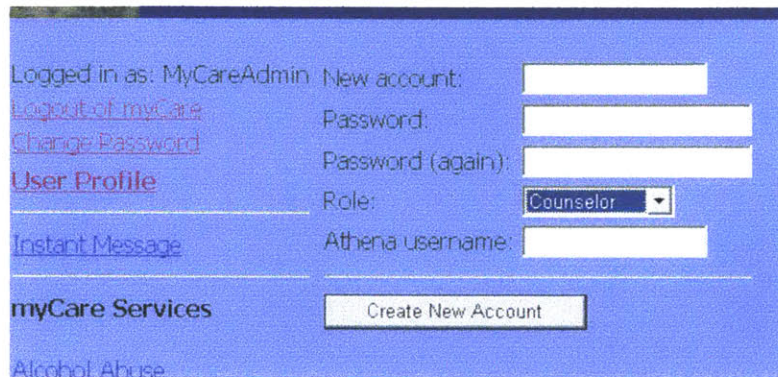
The image shows a screenshot of a web application interface for creating a new account. The background is blue. On the left side, there are several links: "Logged in as: MyCareAdmin", "Logout of myCare", "Change Password", "User Profile", "Instant Message", "myCare Services", and "Alcohol Abuse". On the right side, there is a form with the following fields: "New account:" (text input), "Password:" (password input), "Password (again):" (password input), "Role:" (dropdown menu with "Counselor" selected), and "Athena username:" (text input). Below the form is a button labeled "Create New Account".

Figure 2.12: Administrator account creator.

Administrators have all of the capabilities of counselors and more, so there are also risks involved of inadequately trained administrators.

2.6 Risks

From the common usages, we can see the risks concerning:

- Maintaining anonymity or pseudonymity and privacy
- Maintaining counselor and administrator privacy from regular web site users
- Abuse to the system by all types of users

- Mandatory request from a third party (law enforcement agency) for information stored within the system
- Inadequate training of counselors and administrators that leads to system abuse or loss of privacy

All of these threats will be addressed in the design and implementation of the myCare web application.

Chapter 3

Functional Requirements

This is a listing of the functional requirements of the myCare mental health web application. In conjunction with a team of trained administrators and counselors, the software application is the technological basis of the myCare online mental health community, which will be a non-threatening source of information and anonymous communication for MIT students.

The functional requirements begin with providing functionality to support different types of users (Section 3.1). Section 3.2 enumerates the features of the web application, specifically, what features are available to users and responsibilities associated with certain user roles. Section 3.3 summarizes the types of information stored in the myCare web application and the degrees of protection needed.

3.1 Types of Users

3.1.1 General Requirements

The general requirements of the system necessitate that the regular users of the web application must be anonymous or pseudonymous. Trained counselors and administrators must have adequate credentials and authentication upon logging in. (The training of counselors and administrators is discussed in Chapter 8.)

3.1.2 Visitors

Visitors to the online community may be web users inside or outside of the MIT community. Most of these users will browse the website for informative content. However, if visitors would like to participate in message boards, they must be logged in from an MIT IP address. If they are in a severe crisis, they may be able to instantaneously message any counselors. However, if counselors at anytime determine that the visitor is not an MIT affiliated person, the counselor may stop or continue communication at their discretion or as protocol directs. Visitors may also request a pseudonymous login name if logged in from an MIT IP address.

Upon visiting the site, visitors may:

Available Action	Protection	Caveats
Browse information content	None	None
Read Messages	None	None
Add/Reply Messages	Anonymous & Private	MIT IP Address
IM Counselors	Anonymous & Private	None
Request Login	Anonymous & Private	MIT IP Address

3.1.3 Regular Users

Regular users to the myCare mental health community will be MIT students seeking information or communication about any mental health topics. These users have an associated pseudonymous login and potentially a personal profile to enhance their experience on the website in terms of usability. Regular users can participate in all forms of communication, even if not within the MIT computing system. Another benefit of a pseudonymous login is the ability to establish a working relationship with a counselor or other individuals in the community via message boards.

While logged in, a regular user may:

Available Action	Protection	Caveats
Browse information content	None	None
Read Messages	None	None
Add/Reply Messages	Anonymous & Private	None
IM Counselors	Anonymous & Private	None
Add/Update Profile	Anonymous & Private	None

3.1.4 Counselors

A counselor is a trained student peer who is held to stringent operating protocols and has a background in assisting with mental health concerns. As a part of the myCare mental health application, it is the job of a counselor to read and approve messages for public view. Also, a counselor participates in instantaneous messaging with regular users of the system. A counselor's login must be authenticated, and his/her real identity is hidden to regular users within the myCare community.

While logged in, a counselor may:

Available Action	Protection	Caveats
Browse information content	None	None
Read Messages	None	None
Add/Reply Messages	Anonymous & Private	None
IM Regular Users	Anonymous & Private	None
Approve Messages	Anonymous & Private	None
Maintain Information Content	None	None

3.1.5 Administrators

An administrator is a trained technical site administrator, who is also familiar with the operating protocols of the myCare mental health community. It is the administrator's responsibility to maintain the different mental health topics that are offered at any given time. Also, the administrator is able to create or delete counselor accounts. If a user in the community abuses the services, the administrator may also delete those accounts.

Administrators must be authenticated before entering the web application.

Administrators have the ability to perform all actions the counselors do, but may not wish to do so on that account.

While logged in, an administrator may:

Available Action	Protection	Caveats
Browse information content	None	None
Read Messages	None	None
Add/Reply Messages	Anonymous & Private	None
IM Regular Users	Anonymous & Private	None
Approve Messages	Anonymous & Private	None
Maintain Information Content	None	None
Create Counselor Accounts	None	None
Delete Accounts	None	None
Create Topics/Services	None	None

3.1.6 Summary of Types of Users

Types of Users:

User	Authentication	Login
Visitor	None	None
Regular User	None	Pseudonymous
Counselor	Yes	Pseudonymous to Regular Users
Administrator	Yes	Pseudonymous to Regular Users

3.2 Features

The purpose of the myCare mental health community is to provide a non-threatening web resource for MIT students in a variety of mental health topics. The web application will provide anonymous and private communication between the different types of users discussed in the previous sections. The mental health topics of myCare may include: suicide, depression, sexual assault, alcohol and substance abuse, and stress management.

3.2.1 General Requirements

In terms of communication, all information passed between parties must be anonymous, private, and secure. No personally identifying information, such as names, phone numbers, addresses, etc., will be stored in the myCare system. The server will not log any information, such as connection statistics, IP addresses, usage statistics, or communication logs. For instance, if a message is posted to the moderated message board and contains the name and phone number of a student, the moderator will delete that message since it contains identifying information. Subsequently, the message will be deleted from the database entirely. In the case of instantaneous messaging, the server will not display the IP addresses of the user to a peer counselor or log any communication between users. So, the myCare application will be careful in striving to store as little information about particular users as possible.

3.2.2 Possible Features

The following is a listing of possible features that may be supported in the myCare web application. These are features that are found in a wide variety of web sites and applications:

- Informative content, possibilities include:
 - General Information
 - FAQs
 - Contact Information for resources at MIT
 - Online resources and publications
- Different user roles to support:
 - Visitors
 - Regular users
 - Counselors
 - Administrators
- Pseudonymous Logins
 - Non-identifying usernames
 - Risks involve being able to associate true identity with pseudonym
- Message Boards, dangers include:
 - Users posting identifying information about themselves or others.
 - Abuse through inappropriate or slanderous messages.
- Instantaneous Messaging (peer to peer-counselor)
 - Possible traffic analysis attacks
 - Possible dangers include logging of instantaneous messaging sessions: by the server or an inadequately trained counselor
- Chat rooms (among peers and counselors)
 - Same dangers as instantaneous messaging
 - Less control over regular user interaction and abuse
- Email counseling
 - Already pseudonym remailers that support this functionality (see Section 4.3.2)
- Journals
 - Highly personal and identifying information
- Personal Profiles (site settings, customization, interests)

- Possibility of user identification by inference (see Section 4.3.3)
- User to peer-counselor matching services and user to professional counseling matching services (MIT medical)
 - Possibility of user identification by inference

Some of the features listed above have a possibility of being added to future iterations of the myCare web application, such as user to peer counselor matching services, where a user may participate in an interactive survey to be matched up with a peer counselor who is most knowledgeable in their area of mental health interest. However, providing journal functionality will probably not be a part of the myCare web application since maintaining such private information securely is a difficult task. Other features, such as, multi-user chatting must be given a lot of design consideration since controlling the threats of many regular users in one chat room is more difficult than one-to-one instantaneous messaging. The final list of supported features for the first release of the myCare web application can be found in the next section.

3.2.3 Supported Features

This is a listing of supported features in the myCare application. More detail is given about each feature in the following section.

- Service and Component Infrastructure (Informative Content)
- Different user roles
- Pseudonymous Logins
- (Moderated) Message Boards
- Instantaneous Messaging (peer to peer-counselor)
- Personal Profiles Infrastructure (site settings and customization; interests)

Terminology:

- Service: a mental health topic that an administrator is adding to the site (e.g. “Sexual Assault”, “Alcohol Abuse”)
- Component: a component that is available to a user within a topic of interest (e.g. FAQ, Resources at MIT, Message Board)

Service and Component Infrastructure (Informative Content)

It is up to the trained administrators and counselors to decide on the services they will provide and what kind of informative content that they wish to add to each service. However, the myCare web application provides an infrastructure for the addition of new mental health topics and associated components related to those topics. At the onset, the administrator can create a new mental health topic for the site, which will be available for users to view. Upon creation of a new mental health topic, the administrator will be able to choose from a set of components that users can access within a certain mental health topic.

Workflow for Informative Content:

(flow chart or other type of diagram; screenshots)

- Administrator logs in (authenticated and secure)
- Choose “Service Creator”
- Enter applicable service information (unique identifier, name of service, description)
- Choose components to add to service
- Create service

Different User Roles

The myCare online community must support different user roles for all types of users, with the right level of access control and credentials attributed to each user described in Section 3.1.

Pseudonymous Logins

For regular users who request a login, that login must be pseudonymous. To restrict identifiable information for usernames, they will be generated from a <Color><Animal><Number> combination. The color and animal will be chosen from a drop-down list, and the number is limited to three digits of user input. After the user enters all appropriate data, they click the “Create New Login” button to generate their login.

Moderated Message Board

The purpose of a moderated message board is to provide users with an asynchronous form of communication on a wide variety of topics.

- Users may submit messages to be posted on various subjects.
- Messages must be approved by trained peer-counselors to be made viewable to the general public (all web users). Pre-approved messages are only visible to administrators and counselors.
- Any messages not approved must be destroyed.
- Any potentially personal information must be anonymous and protected.
- Must have ability to post an anonymous message.
- Protocols for what information is allowed to be posted must be defined and followed.

Workflow for Moderated Message Board.

Each myCare “service” maybe contain a Moderated Message Board “component”, which is a list of threaded messages, all pertaining to a particular topic.

Users can:

- View messages
 - o Select appropriate service
 - o Select message board component
 - o Click on any message to view details
 - o Message details may include threads which can also be viewed
- Add new message
 - o Select appropriate service
 - o Select message board component
 - o Click on “Add new message”
 - o Fill in appropriate data
 - o Click on “Submit Message”
- Respond to a message
 - o From viewing message details page, click on “Respond to message”
 - o Take same actions as Add new message
- Counselor Approve/Delete Messages
 - o From viewing message details page, determine if the message can be viewed to regular users
 - o If yes, click on “Approve”
 - o Else, click on “Delete”

Instantaneous Messaging

The myCare mental health community will provide anonymous and private chatting between regular users and counselors. A user can choose to chat with a counselor, and they will be entered in to a queue for the next available counselor. When a counselor becomes available, the instantaneous messaging will commence until the user’s problems are resolved or until other time constraints prevent more

communication. A counselor must adhere to strict operating protocols, and the system must not log any of this communication.

Personal Profile Infrastructure

There are two uses for personal profiles in the myCare mental health site. The first is through site settings and configuration, so the user can save certain preferences. The other is through storing the user's interests so that certain content may become more available to the user or counselors more trained in their interests can be assigned to them for instantaneous messaging. The system must not require any personal profile information, and any information collected must be as unidentifiable as possible. While it is up to administrators and counselors to decide what type of information to ask for and to provide strict privacy policies to enumerate what kind of information is stored, the myCare web application provides an infrastructure for storing personal configuration information.

3.3 Degree of Protection Summary

Information Description ◇ What kind of information is stored in the application (databases, configuration files, etc.) ◇ Information communicated within the system.	Protection ◇ (Pseudo)Anonymous submission. ◇ Private communication. ◇ Secure storage.
General Information and Resources ◇ General Topics ◇ FAQs ◇ Contacts at MIT ◇ Emergency Actions ◇ Other websites	None: general website information
Moderated message boards ◇ User submits a message (message is unapproved). ◇ Counselor or trained user approves the message for general submission. ◇ Message is viewable for all users.	Secure until the information is “approved” on to the site for the general public to see → No protection needed after that ◇ Messages that are not “approved” are destroyed ◇ Messages are marked as “approved by” a certain moderator so that wrongly approved messages can be associated with a moderator.
Instantaneous Messaging ◇ Potentially sensitive information ◇ Should be mediated by “counselor” so no personal information is given	Communication must be private and anonymous.
Login information ◇ Username ◇ Password ◇ Needed for submitting message boards, chatting, etc.	Anonymous ◇ System generates a new login (Color_Animal_Number) to prevent users from having identifiable logins
Personal Configuration ◇ Personal interests in mental health	Make sure the information we ask for is not identifying. Ensure that information and privacy policies are strictly enforced.
System Logs	No system logs will be generated. Abuse of the system will be handled on a per-component basis.

Chapter 4

Research Topics

4.1 Overview

This section provides a background in to anonymity and privacy concerns by providing appropriate terminology and examples of existing research. Examples of different systems, such as Anonymizer.com [2]—which acts as a trusted proxy between a user, to maintain anonymity, and a website—are provided as a basis for designing the myCare web application.

4.2 Terminology

The following is a list of terminology that is used in discussing the technological design of the myCare mental health web application:

Anonymity: Lack of identification. In the myCare mental health application, we are concerned with the anonymity of a regular user, who is seeking mental health resources or support. Students living on the MIT Campus can maintain full anonymity, but can opt for creating a pseudo-identity in the form of pseudonymity.

Pseudonymity: Identity with regards to a pseudonym only, but real identity is still hidden. In other words, pseudonyms provide a linkability between a user and their communication within the system. [6]

Privacy: Control over personal and identifiable information to maintain anonymity or pseudonymity. The myCare application strives to maintain the privacy of users by not retaining sensitive or identifying information about its users, or using other techniques to protect user information.

Security: Ensuring that information is not intercepted by unauthorized parties. For the myCare project, security of the application server and database server are assumed, since that is a large area of interest by itself. However, security is used in the form of protecting communication traveling between the user and system—which, for instance, may be done by SSL or encryption with PGP.

Authentication: Ensuring that the identity of a user and/or their credentials is genuine. This is an enhancement to the security of the system by ensuring that only authorized users may access protected information.

PGP (<http://web.mit.edu/network/pgp.html>) [14]: Pretty Good Privacy (PGP) is a software tool that provides privacy through encryption.

Digital Certificates: issued by a Certificate Authority (trusted third party that verifies identities of entities) which proves a party's identity and credentials.

SSL: Secure Sockets Layer, protocol designed by Netscape Corporation to provide encrypted communications over the internet.

4.3 Related Work and Technologies

4.3.1 Overview

These are some examples of current technology available to deal with general communication over the internet [3]:

- Anonymous Browsers: surfing the web anonymously
 - Anonymizer: anonymizer.com [1]
- Enhanced privacy and security web browsing tools
- Encryption: enables privacy of many forms of communication
 - PGP
 - RSA
- Remailers: sending email with varying degrees of anonymity or pseudonymity

4.3.2 Anonymity and Pseudonymity

Anonimizer.com [1]. A user can use anonymizer.com as a trusted intermediary between himself and their desired target website. Anonymizer will handle http requests from the user and send them to the target website, providing “unlinkability between sender and receiver, given that the proxy itself remains uncompromised [6].” However, “unlinkability” is not always ensured since a user often connects from one location, so further protection must be made by handling other attacks. For instance, malicious third parties can still monitor the communication between the user and the proxy to disrupt anonymity and privacy.

Traffic analysis, Chaum's Mix-net [4]. To combat traffic analysis attacks, Chaum describes a public key cryptography system where users sending email will also communicate with a “computer called a *mix* that will process *each* item of the mail before

it is delivered [4].” And, the sender and recipient of an email are separated by “cascading” a series of “mix” computers. Forwarding and reply address information are still “sealed” or encrypted in the messages so that email recipients may still reply to the messages. Since tracing the sender through the “mix-net”, is difficult, anonymity may be preserved.

nym.alias.net: As a pseudonymous remailer, the service provided by *nym.alias.net* was to protect against anonymity attacks against the anonymity of users or abuse of the system to silence users [11]. *Nym.alias.net* allows for users to create a pseudonym, or *nym*, identity that appears on all emails, but preserves the real identification of the user. The system works by stripping away all identifiable information from the email, with each message sent out by the pseudonym server as only maintaining a public key, reply block, and configuration data [11]. The pseudonym remailer also had many attacks and abuse which were anticipated during the course of running the server, including harassment, email attacks, spam, and child pornography.

While the *myCare* system is different from a pseudonym remailer, there is still a need to maintain user anonymity as the first priority. And, learning from the design and implementation of *nym.alias.net*, it is important to address the identifiable information traveling through the system. Furthermore, abuse of *nym.alias.net* stemmed from lack of information monitoring between two private parties, which is different from *myCare* such that the only private communication between two users is instantaneous, un-logged communication. Otherwise, the information monitoring is inherently built in to the message board moderation protocols.

Onion Routing (<http://www.onion-router.net/>) [7]: Active from July 1997 [7] to January 2000, onion routing is a general framework for protecting against anonymity attacks which are susceptible through traffic analysis. Communication is hidden by making connections between two parties indistinguishable from communication from a

large number of different users. Onion-routing is based on the Chaum's mix-nets (described above), so determining specifically what two parties are communicating is difficult. The sender of a data begins by creating an "onion, which defines the path of the connection through the network [7]." At each connection point, a layer of the onion is peeled away, and the underlying packet is forwarded to its next destination. Onion routing can also be used with Anonymizer, for instance, to improve security and privacy by running Anonymizer as a "filtering proxy" on a computer trusted by the user, and then communication leaving the machine will be immune to traffic analysis attacks [7].

Crowds (<http://www.research.att.com/projects/crowds/>): Crowds is an approach to ensuring anonymity by incorporating users in to diverse "crowds" where the sender of a message is not detectable, since the source could be any user in the crowd [16].

So, through a wide variety of methods, sender anonymity can be achieved through using a trusted proxy or removing identifiable information from messages. However, to deal with traffic analysis attacks, messages can be routed through a complicated network of computers so the origin is untraceable, or users can be hidden in a large network of other users.

4.3.3 Privacy

Privacy Risks in A Recommender System [15]: A recommender system is one that will suggest new products and services for users based on previous preferences, ratings, or usage patterns. A simple example of a recommender system is using a nearest neighbor algorithm [15] where recommendations may be made for users who have similar ratings for products or services. However, if one user were to learn the rating algorithm used and had the ability to access statistics on what products were purchased by particular customers—the user could find all personal information

concerning those customers. Ramakrishnan, Keller,... describes this as “a realistic possibility given that e-commerce sites periodically provide databases to third-party consultants” [15] for a wide variety of reasons. The attacks in a recommender system such as this are related to “inference control”, where an attacker may have deduced some relationship, and can query additional sources to uniquely identify an individual.

4.3.4 Security

The security needs in the myCare application relate to access control, maintaining privacy of users, and user authentication. In web applications in particular, there are a number of security models that will facilitate these concerns [9]:

- Discretionary Access Control (DAC) Model: flexible policy where all access authorization for users, groups, and components are defined but does not provide a high degree of security.
- Mandatory Access Control (MAC) Model: provides more robust means in controlling “information flow to ensure confidentiality and integrity of the information.” One example is an application with several levels, where protected data cannot flow from a high security level to a lower one.
- Role-Based Access Control (RBAC) Model: models access based on security roles, and “security administration is greatly simplified by the use of roles to organize access privileges.”
- Access Control Models for Tasks and Workflows: task oriented control.
- Agent-based Control Model: access control based on processes that are modular and mobile

- Certificate-based Control Model: public-key infrastructure certificates, sufficient for simple applications

The different access control models described vary in degrees of flexibility, complexity, and security robustness. There are also differences in how access is controlled and administered: tied to information, users, groups of users, roles, decision processes, or tasks and workflows. All of these aspects will be taken in to account in developing the myCare application.

Chapter 5

Design

The overall design of the myCare mental health application incorporates anonymity and privacy techniques in protecting users from being identified. In general, the application will store as little information as possible about users and will not keep any logs as to usage.

The myCare application has typical three-tiered web application, client/server, architecture including user interface, application logic, and database server. Authentication modules ensure that counselors and administrators have proper credentials for entering the system. However, web application server and database server security is assumed for the purpose of this design. See Figure 5.1 for the different types of clients and roles of the application and database server.

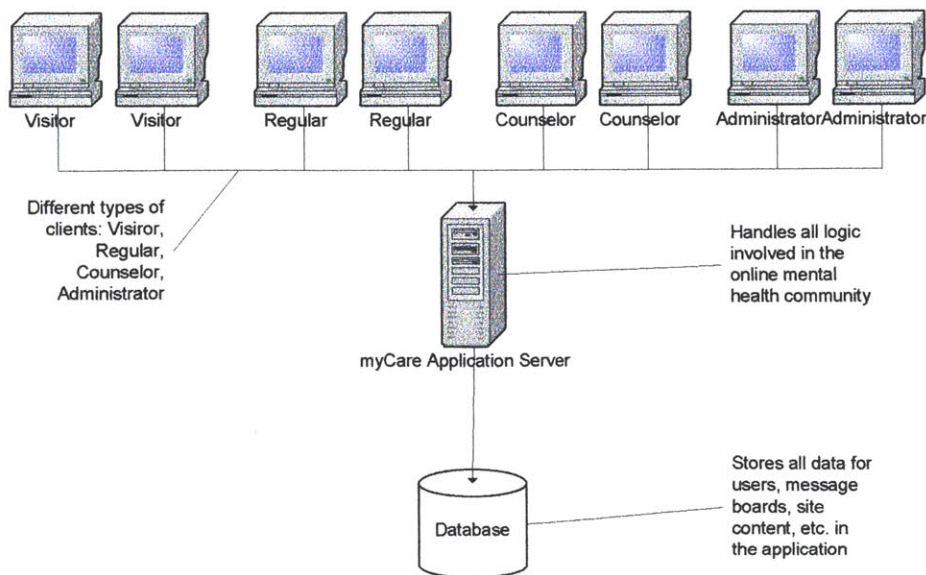


Figure 5.1: Overview of myCare mental health application.

5.1 Logins

5.1.1 Logging In

The logins in the myCare system provide for different user roles and are completely optional. Counselors and administrators need the correct credentials for entering in to the system, since these users are crucial to the proper working of the system and have additional access and responsibilities, in particular, MIT personal digital certificates. Regular users need no credentials, however, they need to be creating a login from an MIT IP address. This is the case because the basis of the myCare application is to build a support community and resource for members of the MIT community only—specifically students. Also, by limiting the users allowed to create pseudonyms to the MIT community, threats of having random web users abuse the system are reduced. A comparison of user logins is provided in Figure 5.2.

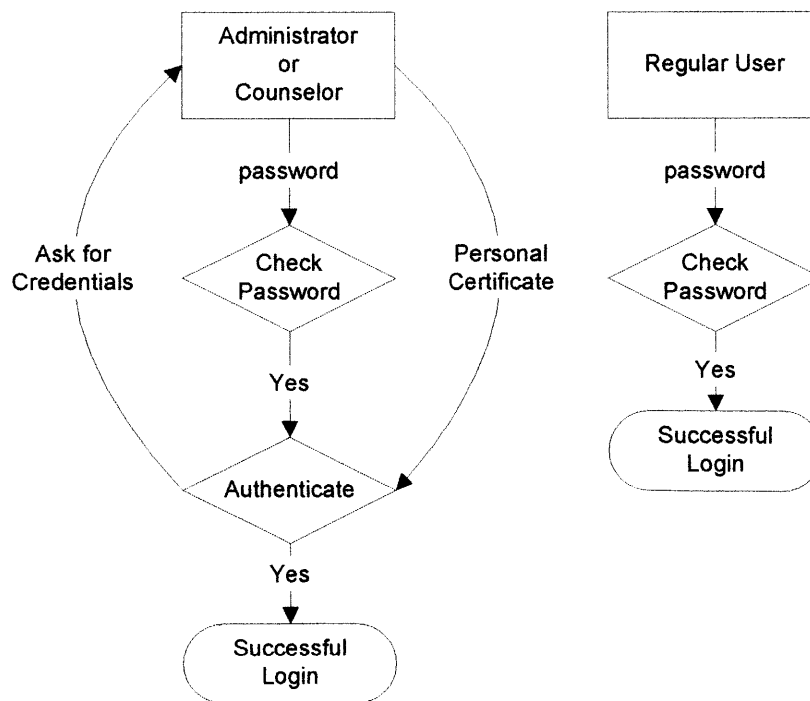


Figure 5.2: Comparison between logins of different types of users.

5.1.2 Creating User Accounts

Regular user logins in the myCare application are pseudonymous. However, there is a potential threat in users:

- (1) creating a username that is identifiable
- (2) creating a username to masquerade as someone else for misuse in the system

For the protection of regular users, strings are loaded from text files to generate <color-string><animal-string><number> where <number> is a three digit number. The user submits their desired pseudonym and password, and the application checks for potential duplicates. Once the user has chosen a unique pseudonymous username, the application persists the username and password, in encrypted form, to the database in a *Users* table, with a role of a regular user.

5.1.3 Administrators and counselors

Upon setup of the web application, there is one administrator account, from which other administrator accounts or counselor accounts can be created. An administrator submits necessary information for the account, including a new username and temporary password. The username is checked against the database for duplicates and is persisted if no errors occur.

5.1.4 Design considerations

One alternative design is to simply not provide pseudonymous usernames for regular users, and only require that administrators and counselors have pseudonymous usernames and passwords. However, pseudonyms provide users with a means of developing a relationship with a counselor in instantaneous messaging, for example. In message board discussions pseudonymous users may build up a reputation of providing interesting messages, helpful feedback, or other information.

Anonymous access is restricted to those users at an MIT IP Address for the creation of pseudonymous logins. An alternative would be to ask for the MIT personal digital certificate of the user, however, the myCare application should not ask for this information, since it contains the user's true identity. In the future, it may be possible to turn the myCare application in to a credentialized, pseudonym system. Building a "pseudonym system" [10] may be useful in the myCare application since regular users will want to know that they are talking to trained peer counselors and counselors, on the other hand, will want to know that they are talking to an MIT student, however, both parties wish to remain anonymous to each other. One pseudonym system possibility is that of the model discussed by Anna Lysynskaya, where there are "well-defined" users "where not only can credentials be shown anonymously, they can be granted to parties based on unlinkable pseudonyms [10]." So, it would be possible for administrators to give credentials to regular users who have demonstrated a great deal of knowledge in the myCare application in terms of mental health services.

Most likely, anonymous users will not reach full counselor status because they are not strictly trained in the myCare protocols or privacy policies, and it would be difficult to place blame or liability on those users. However, it is possible that users,

such as BlueCat444 from Section 2.3, who make useful contributions to message boards, may have other responsibilities and privileges, like being able to add to the FAQs section that normal users would not have access to.

5.2 Moderated Message Boards

5.2.1 General Message Structure

Each service in the myCare application has a message board. Moderators of the message boards are administrator or counselor users. And, each message belonging to the message board has:

- Author: some valid user identifier or “anonymous”
- Subject: description of the message
- Body: text of the message
- Creation date & time
- Approval status: indicates whether the message has been reviewed by a moderator
- Approved by: a valid user identifier with role of administrator or counselor who approved the message to be published to the public
- Parent message: reference to the parent message, if it exists’

5.2.2 Message Creation

First, a message is created by a user. All users have the ability to create messages—including visitors. However, visitors may only publish messages if they are logged in from an MIT IP Address, so that the general public cannot participate in the posting of messages, since they do not belong to the MIT community. All other users may add a new message or reply to existing messages, however, moderators’ messages are available to the public as soon as they are posted, while a visitors’ or pseudonym users’ messages are persisted within the system with their status as

“unapproved.” After the moderators have approved these messages, anyone visiting the myCare message boards can read these messages. Even if users are logged in to the myCare application with their pseudonymous username, they can still choose to post the message as anonymous. The creation date/time and the parent message are automatically populated by the system upon persistence.

5.2.3 Message Moderation

Next, moderators of the myCare system must read and approve messages. Once a moderator marks the message as approved, its status is updated in the database. If the message is not approved, the entire record is deleted from the database. The message also has the “approved by” information automatically attributed to the moderator, for potential training reasons or liability.

5.2.4 Viewing Messages

All users, including visitors, can view the approved messages. Visitors or regular users request to view all messages for a particular service. The database is queried, and only messages that have been approved are returned to the user. For moderators, all messages are returned, and those that have not been approved are marked “Need Approval”.

5.2.5 Design considerations

There are few design alternatives with respect to the moderated message board feature. Inherently, only information that has been approved for public viewing is only stored within the system, so that information does not need protection. Also, messages with potentially identifiable or are deleted from the system as soon as they are viewed by

a moderator, who adheres to the operation protocols in the myCare online mental health community (discussed in Chapter 8). So, only unapproved messages need to be protected. At this time, since the security of the database server is assumed, these messages are not encrypted. It is left up to the database access control and security to handle this protection of these messages.

5.3 Instantaneous Messaging

The chat module of the myCare application includes a chat server where counselors or administrators may enter the chatting module and begin to chat with users. Here, “chat” is used in the general sense. There may be support later on for many-to-many chat, but currently, only one-to-one chat, or instantaneous messaging, is supported between counselor and user. When a counselor or administrator enters the instantaneous messaging module, they are registered with the chat server. They can view the number of users requesting a messaging session, or exit the program. Once marking that they are available for chatting, their status is updated in the chat server.

Unlike the moderated message boards, any user can enter in an instantaneous messaging session with an administrator or counselor. A user requests to participate in a chat, is registered with the server, and when the next free correspondent is available, the user and correspondent will automatically be connected. The messaging server acts as a proxy between the user and correspondent so that pseudonymity is preserved. A regular (pseudonym) user may choose not to login to the system to remain anonymous, but if they are logged in, that pseudonym is displayed to the counselor or administrator engaged in the chat.

Ideally, onion routing should be used for this instantaneous messaging component. However, since onion mix servers are not currently running on a wide

basis, including this trusted proxy layer for anonymity is sufficient for the time being. The proxy is trusted since there is no logging of instantaneous messaging or connection information (such as IP addresses), peer counselors cannot view connection information of users, and peer counselors must follow the operating protocols stating that instantaneous messaging sessions must not be retained.

5.4 Service and Component Infrastructure

myCare administrators can add new services and components by using the infrastructure that is a part of the myCare web application. Services and components are decided by administrators and counselors, who work with a developer of the system to add a component. After the initial development of a component, a myCare administrator can use the myCare web application to add that component to new or existing services.

5.5 Personal Configurations and Profiles Infrastructure

Personal configurations are a simple mechanism for providing a better user experience. The information asked for is decided by administrators, who work with a developer of the system to add support for a configuration. If a user desires to, he loads the configuration page, enters appropriate data, and the information is persisted to the database. Other parts of the system will read the configurations from the database if affected. (See protocols section.)

Chapter 6

Software Architecture and Implementation

6.1 Overview

The myCare application is implemented predominately using IIS as the web server and Microsoft SQL Server 2000 as the database server. Encryption of communication is achieved through SSL and the generation of a myCare site certificate. The application layer itself is written in ASP.NET and C#. Authentication of administrators and counselors is achieved via MIT personal digital certificates. The instantaneous messaging component is implemented as a Java Applet so that users do not have to install a chat client. Figure 6.1 shows an overview of the entire system.

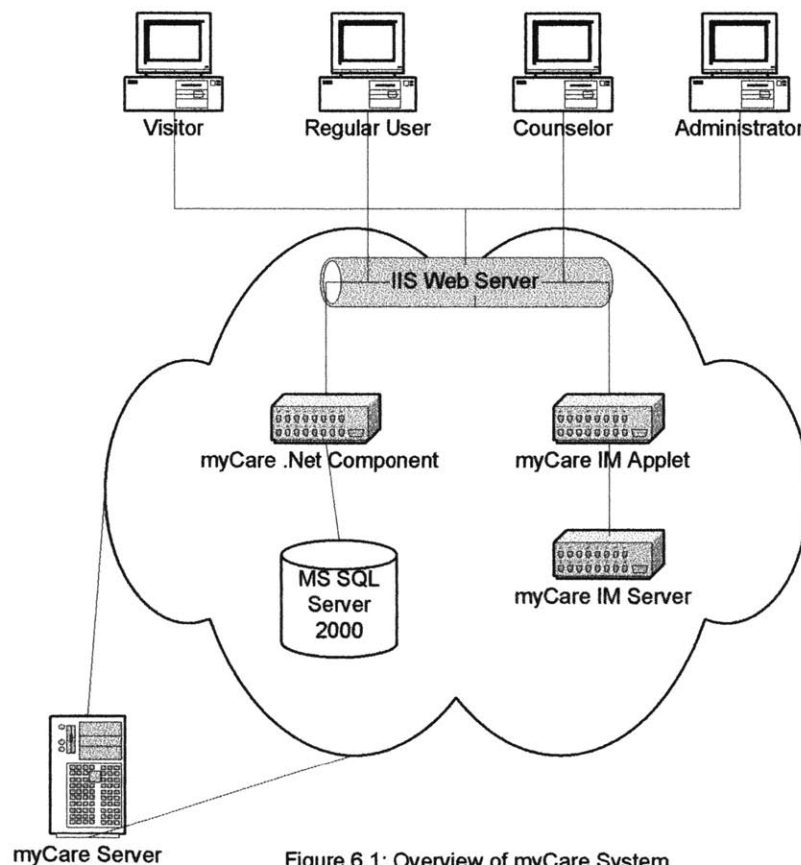


Figure 6.1: Overview of myCare System

Figure 6.2 shows an overview of the myCare system at runtime, in particular, how major services and components interact with users. This diagram shows that the myCare system contains users, an instant messaging server, and services with components. This is the myCare software application in the abstract.

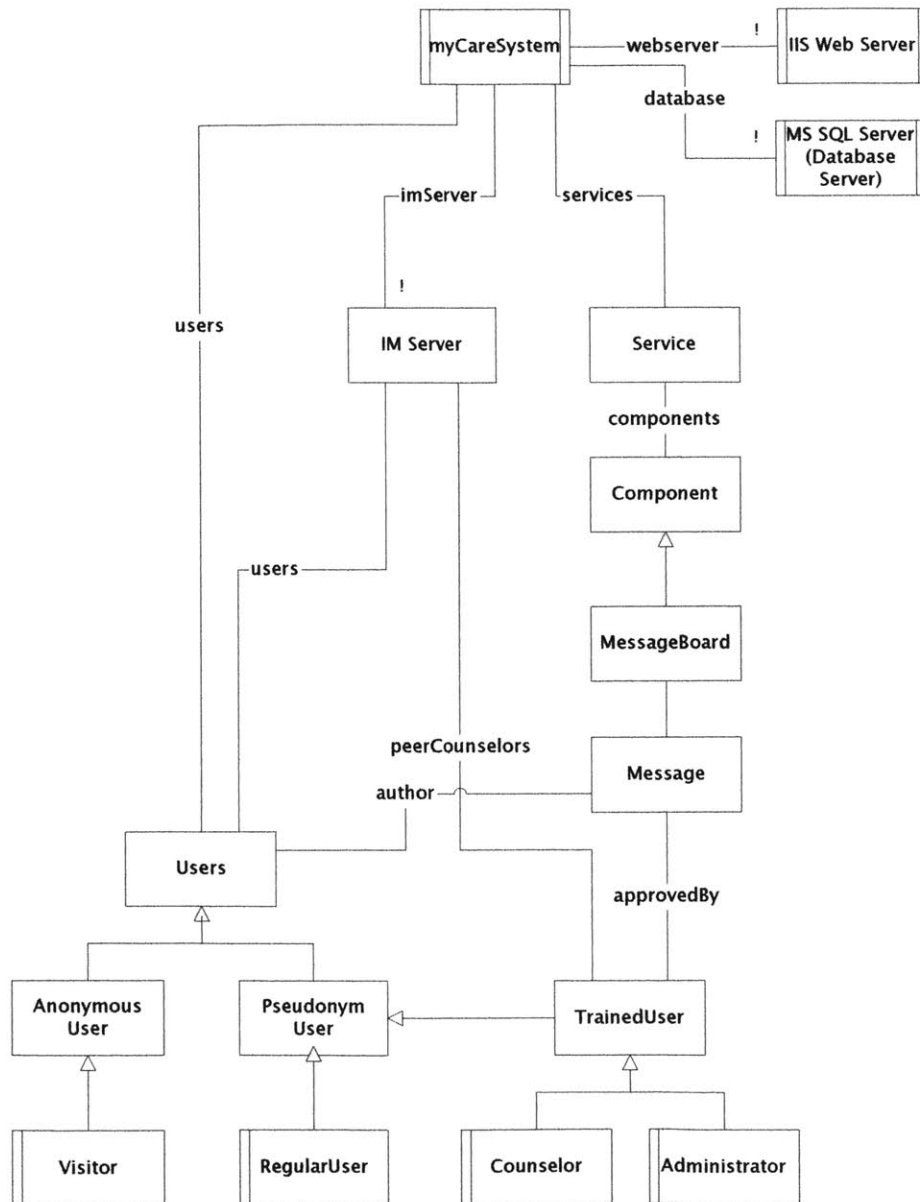


Figure 6.2: Brief overview of conceptual myCare system.

6.2 Software Architecture

6.2.1 myCare Web Application (.NET)

Figure 6.3 shows the modular architecture of the myCare web application. First, clients connect to the Microsoft IIS web server, through SSL and utilizing myCare server certificates (and personal certificates for counselors and administrators). The user interface is composed of an ASP.NET web layer that renders web pages. Modules in the web layer include:

- login and logout: contains pages for user account creation and management
- admin, counsel, reguser: starting pages for different user roles
- message: summary of messages, adding new messages, responding to messages
- images: images for the application
- chat: calls the myCare IM applet to start

The web layer uses tools and software modules in a C# backend layer. These modules include:

- data: classes that query and persist information to the database
- ui: common user interface tools
- util: enumeration of user roles or session state keys
- beans: data types for holding information

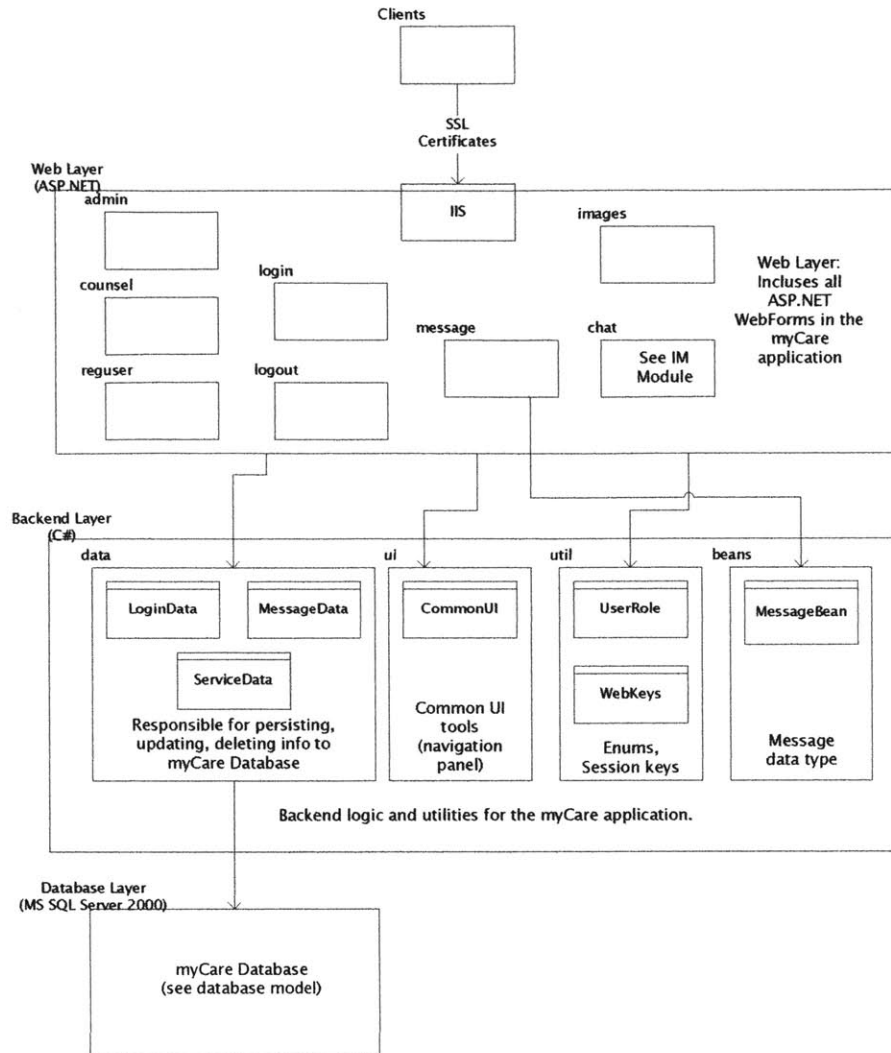


Figure 6.3: myCare System Modules

6.2.2 myCare Instantaneous Messaging

The myCare instantaneous messaging software is composed of a chat server module running on the same web application server as the rest of the system. Clients connect to the instantaneous messaging server through client Java applets. The architecture is split into three main packages:

- chat.client: client code for the myCare instantaneous messaging applet

- chat.common: common data structures used in both client and server code
- chat.server: all server code

The myCare IM application uses java.net Socket programming and java.lang.Thread. The user interfaces are implemented with Swing.

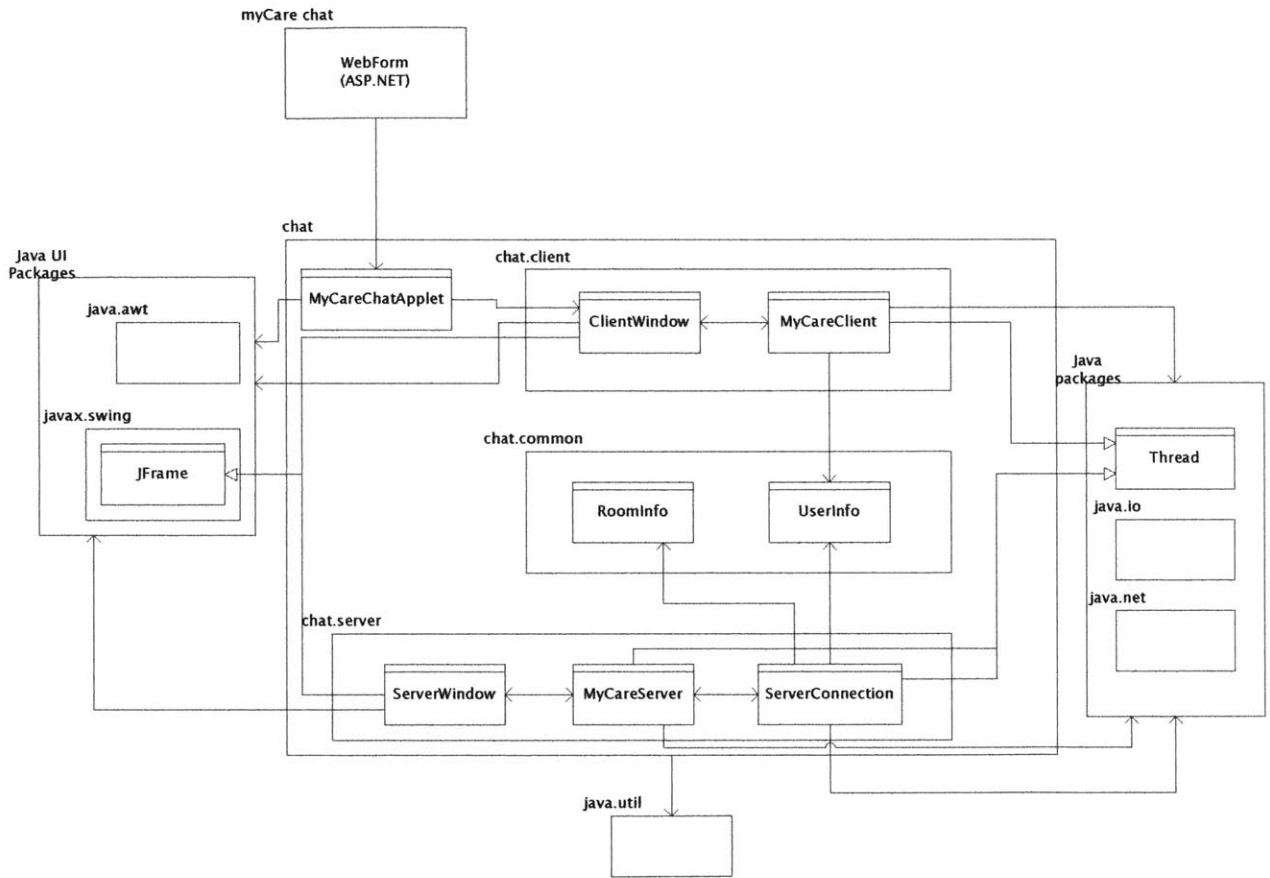


Figure 6.4: myCare Instantaneous Messaging Modules

6.3 Database

The myCare database server used is Microsoft SQL Server 2000. A simple relational database schema was developed to hold user information and service and component information. Figure 6.5 shows how the tables and entities in the database interact. When an administrator creates a service called “Depression” with serviceID, “DEPR”, a new record is added to the Service table. When a component, such as a message board, is added to a service, the Component table is updated with a new record with componentTableID (where the information for that particular component is stored) and the type of the component. It is the responsibility of developers adding components to create appropriate database schemas to support the new features.

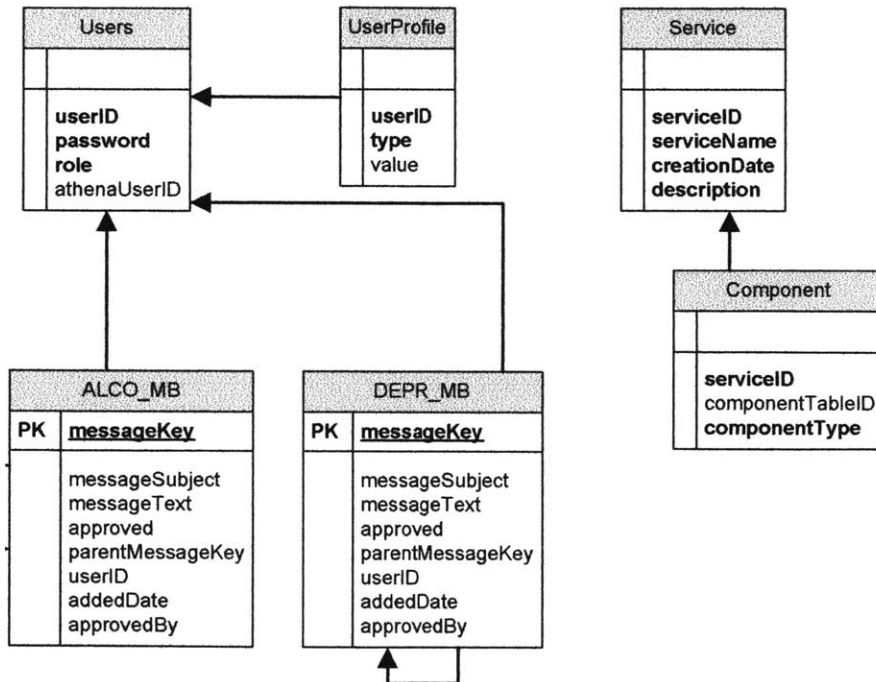


Figure 6.5: myCare database tables and relationships.

So, in Figure 6.5, since there are “ALCO_MB” and “DEPR_MB”, we can assume that there are two services with serviceID “ALCO” and “DEPR”, referring to “Alcohol Abuse” and “Depression” services. Furthermore, each service has one component, a

message board component, which points to the appropriate tables where information is stored for that component. The componentIDTableIDs for the message board components for the services “Alcohol Abuse” and “Depression” would be “ALCO_MB” and “DEPR_MB” respectively. So, to add a new component, a developer had to create a new componentType, write code to generate tables for storing component data in the database, and put a reference to that table in the Component table. Development of the message board component, for example, also includes new classes to query, add, and update messages in the message board tables. This database is intended to be a flexible way for new types of services, user profiles, and components to be added.

Chapter 7

Evaluation of the Design

7.1 Case Study 1: America Online, Inc.

In “Privacy and Self-Regulation in the Information Age”, a US Department of Commerce Report (http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm), America Online provided a “Perspective On Protecting Personal Privacy In the Interactive World” (<http://www.ntia.doc.gov/reports/privacy/selfreg6.htm>). In this article, AOL states that it generally does not monitor private communication or give personal information to third parties without user consent. However, they delineate what type of information may be stored in their system or used internally.

In addition to member billing information, AOL also logs communication with customer service, “general usage history”, or correspondences in complaining about other users. AOL also stores “navigation and transactional” information concerning usages patterns and merchandise purchasing, and the emailing system retains personal correspondences for a certain amount of time. This is a large difference between AOL privacy policies and practices than those of the myCare application. While AOL will retain very private information on users, any potentially private information in the myCare system will be deleted.

In the discussion of internal usage of the information retained in AOL’s systems, the reasons are multifold and range from providing better user experiences and customizations to research for generating advertising revenue. While advertising is not an issue for myCare—there is no need to retain and use navigation attacks, since usage patterns can be identifiable by inference. However, the myCare application does

attempt to build upon better user experiences by having personal customization tools, but the information is specifically requested and users do not have to generate user profiles. Also, the information requested is structured in such a way such that the information is not identifiable. Furthermore, the myCare privacy policy is slightly different from the AOL policy in that it describes what information is logged and ensures that there is no identifiable information kept on the site without user's consent or knowledge.

(The full AOL privacy policy can be found at::

<http://legal.web.aol.com/policy/aolpol/privpol.html>.)

7.2 Case Study 2: Medical Record Privacy

Complications of the myCare application are closely related to issues dealing with medical record privacy. Specifically in “A WWW Implementation of National Recommendations for Protecting Electronic Health Information [8]” certain practices are described for successful implementation of a medical record information service. The following is a summary of some of these concerns as well as support in the myCare application to handle those particular issues.

Practices [8]	myCare resolution
Individual authentication of users.	Supported for administrators and counselors.
Access controls.	Access from administrator to counselor to regular user status to certain information is controlled.
Audit trails.	Only information that is audited is message approval, where approved by is set with the userID of the person who approved the message. However, deleted messages are not audited, which means that responsibility for blame cannot be placed. The assumption made is that counselors are well trained and are liable in following protocol.
Physical security and disaster recovery Protection of remote access points Software discipline (virus checkers) System assessment (system vulnerability)	Not within the scope of this thesis—these are general security concerns with regards to application and database servers, but do have to be addressed at deployment.
Protection of External Electronic communications (encryption between data networks)	Supported through SSL

In general, all features for deployment of a reasonable medical records system are supported by the myCare application in terms of maintaining privacy and authentication of users.

Chapter 8

Deployment Notes and Issues

8.1 Deployment and Training

The myCare application is designed to be as anonymous as possible—meaning that we make no effort to find out the identity of users or log any information that can associate users with true identities. It is at the user’s own risk that he or she uses the myCare mental health community, and any mistreatment of mental health illnesses is not liable by operators of the myCare community. The administrators and counselors are trained students, who are not guaranteed to have any formal mental health education. On the other hand, it is up to administrators and peer counselors to devise and follow strict operating protocols and privacy policies and make these policies known to all users of the mental health application. It is up to the administrators deploying the operation to devise a stringent training method for peer counselors, working with any MIT faculty and medical groups as necessary.

The myCare software application is susceptible to the privacy and legal policies of the group deploying the application. For instance, if under law, the group deploying the myCare web application is subpoenaed by a government agency to provide all database information and application files contained in the myCare web application, then this information is handed over. However, the myCare application is designed in such a way that potentially identifying and/or private information is not persisted in the database or stored in system logs.

8.2 Operating Protocols

8.2.1 Administrator Accounts

It is recommended that administrator accounts only be used for the creation of other administrator and counselor accounts and application management. Also, administrator accounts should be created on a limited basis. While it is possible to post and approve messages and participate in instantaneous messaging with other users, it is not recommended. Instead the administrator can create a new counselor account and use that to participate in message boards and instantaneous messaging.

8.2.2 Message Board Approval

Message board approval is a complicated procedure due to the possibility of inference attacks. It is simple enough to disapprove any message submitted with the text containing a person's real name and address. However, there are ways of finding a user's true identity by way of cross referencing information with other sources. So, if there is information that is too specific about a user, the moderator must disallow that message as well. General guidelines are to disapprove messages with:

- Any personally identifiable information: name, phone number, address
- Any information that defames others
- Inappropriate and offensive topics
- Too much specific information or descriptions. For instance, a student specifying that he lives in a fraternity off campus and is a freshman taking a specific computer science course could potentially be easy to identify.

8.2.3 Instantaneous Messaging

Because students living off of the MIT campus may need immediate support from a counselor, there is no restriction on a user requesting an instantaneous messaging session with a counselor. However, it is at the counselor's discretion to not support the user if it is apparent that he is not an MIT student. Also, the counselor can, at any time, stop instantaneous message communication if the other party is being offensive or inappropriate. Following privacy practices, counselors should not retain records of the messaging sessions for private or public use.

8.2.4 Personal Configurations

Personal configuration information need to be limited, necessary, and generic non-personal information. By "necessary", the particular information asked for must dramatically improve usability of the web application for the user. It should be made clear that this information is completely optional.

8.2.5 Administrator and Counselor General Usage

While this is a web application, it is recommended that counselors and administrators participate in instantaneous messaging so that there are no distractions or disturbances to peer counseling processes. However, for message board approval and posting, administrators and counselors can choose to do so from remote locations.

8.3 Technical Privacy Policy

It is up to the deployment team (administrators and counselors) of the myCare software application to determine the exact privacy policy of the entire mental health service and organization. However, from a technical standpoint, the myCare application does **not**:

- Track navigation and usage patterns
- Log any information without user consent (such as IP addresses)
- Log any communication exchanged in instantaneous messaging
- Retain any personal information that users do not know about
- Retain any “unapproved” moderated message board messages

Chapter 9

Future Work

9.1 Services and Components

While administrators of the myCare application can create several services at this point, there is only one component implemented. As the deployment team of administrators and counselors have a clearer understanding of what components need to be added to the application, development must be done to implement that component in to the existing architecture so it may be added to new and existing services.

9.2 Personal Profiles

With the development of new components or for configuring existing components, administrators of the myCare online mental health community must contact developers to add a new type of configuration and incorporated it in to the component. In the usage scenario of pseudonym user, BlueCat444, a new personal configuration type must be added, asking the user for their topic of interests through the user interface, persisting that interface in the database, and incorporating those settings in to the components so that new messages in chosen topics will appear at login.

9.3 User Interface Improvements

Many improvements can be made to the user interface of the myCare web application. From a psychological standpoint, it may be feasible to design the user interface in such a way that a visually soothing experience is provided for users seeking mental health support. Everything from site layout, navigation, color scheme, and images can be changed to improve user experience and ease of use.

In addition, moderated message board user interface can be improved to display the treading of messages on the first message board summary page instead of requiring the user to drill down in to messages to view replies. Filtering, searching, sorting, and paging through messages should be added.

Chapter 10

Conclusions

The myCare mental health application is a software tool that can be used by a team of trained administrators and student counselors to provide an anonymous and private online community for MIT students. Assessing all possible privacy risks to different types of users is a difficult task. However, the myCare web application is a first step in creating a non-threatening mental health community, by providing a piece of software that maintains user privacy by securing communication, controlling information (moderation of message boards), and being careful about what information is retained in the system.

Where other web applications and services on the internet are focused in protecting information within the software system, myCare is slightly different in having its first objective be not retaining unnecessary or private information on in the myCare application. The users in the myCare system are the most important aspect. We attempt to facilitate user communication while protecting users. Administrators and trained student counselors must have an established set of operating protocols and privacy policies and follow them stringently, or the trust of the system is compromised. Students of the myCare online community must also be aware of what kind of identifying information they provide about themselves.

While most systems are concerned with external attacks, myCare is more concerned about possible threats to users through normal usage of the system. Accordingly, the functional requirements and design of the myCare web application is focused on minimizing the amount of personal information stored in the system, and an evaluation of the design is provided, rather than an evaluation of performance. The

myCare application is intended to be a reliable, extensible, and configurable mental health service to the MIT community or other organizations in the future.

Bibliography

- [1] AOL Privacy Policy.
<http://legal.web.aol.com/policy/aolpol/privpol.html>.
- [2] Anonymizer.
<http://www.anonymizer.com>.
- [3] Anonymous Communications on the Internet.
<http://www.aaas.org/spp/anon/links.htm>.
- [4] David Chaums. Untraceable electronic mail, return addresses, and digital pseudonyms. In *Communications of the ACM*, 4(2), pp. 84-88, February 1982.
- [5] Crowds.
<http://www.research.att.com/projects/crowds/>.
- [6] Roger R. Dingledine. The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven. MIT Master's Thesis. May 2002.
- [7] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, "Onion Routing for Anonymous and Private Internet Connections," In *Communications of the ACM*, 42(2), February 1999.
- [8] J. D. Halamka, P. Szolovits, D. Rind, C. Safran. A WWW Implementation of National Recommendations for Protecting Electronic Health Information. In *Journal of the American Medical Informatics Association*. 4(6):458–464, 1997.
- [9] James Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford: Security models for web-based applications. In *Communications of the ACM*, 44(2): 38-44, 2001.
- [10] Anna Lysyanska. Pseudonym systems. MIT Master of Science in Computer Science Thesis, May 1999.
- [11] David Mazières and M. Frans Kaashoek. The design, implementation and operation of an email pseudonym server. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, 1998.
- [12] MIT Mental Health Task Force Report, November 6, 2001.
<http://web.mit.edu/chancellor/mhtf>.
- [13] Perspective On Protecting Personal Privacy In the Interactive World.
<http://www.ntia.doc.gov/reports/privacy/selfreg6.htm>.
- [14] PGP.
<http://web.mit.edu/network/pgp.html>.

- [15] Naren Ramakrishnan, Benjamin J. Keller, Batul J. Mirza, Ananth Y. Grama, George Karypis. Personalization and Privacy; Privacy Risks in Recommender Systems. In *IEEE Internet Computing*, 5(6), November-December 2001.
- [16] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. In *ACM Transactions on Information and System Security* 1(1):66-92, November 1998.