IA 606: Security and Cryptographic Protocols

Group Project:

Anonymous Message Broadcast

Department of Information Assurance

St. Cloud State University

BY

Swathi Mannem

Shivendran Divakar Tiruchanpalli

Naga Suraj Maddi

Shiva Sai Ram Marupudi

Abstract

The dining cryptographer network, also called as DC-net devised by David Chaum for anonymous message broadcast. It is a privacy preserving communication protocol. A strong feature of DC-net is the strength of its security and also is not dependent on other schemes such as encryption. We have designed and created a DC-net implementation using a client-server model. We initially describe the theory of DC-net followed by the security support in the application and then about client server connection model and finally our implementation along with use case diagrams and screenshots of our application.

Introduction

Anonymity: In this world which is increasingly relying on digital technologies, addressing issue of protecting user privacy is of crucial importance. Anonymous communication allows users to communicate with each other without any fear of surveillance. An anonymity system[1] attempts to conceal relation between message and their recipients between messages and their actual senders or both. Today commercial and political entities have been increasingly engaging in complicated cyber warfare to damage, disrupt or censor important information content.

The dining cryptographer network popularly known as DC-Net is a privacy preventing communication protocol devised by David Chaum for anonymous message publication. The most attractive feature of DC net is its strength of security, which is inherent in protocol and not dependent on other schemes like encryption. Unfortunately, DC-net has a level of complexity that causes it to suffer from exceptional communication overhead and implementation difficulty that precludes its uses in many real world use cases.

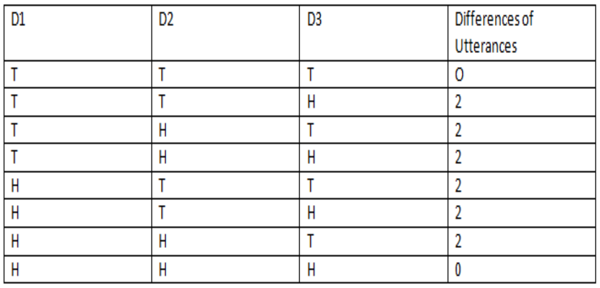
Preserving the anonymity of communicating parties is very crucial where knowledge of identity of the source of communicated messages could create conflict of interest, jeopardize the integrity or endanger the participants. Concept of maintaining anonymity is simple however difficult to implement.

Software Requirements:

Technology	Java
Database	My SQL
Operating System	Windows
IDE	Java Net beans

Dining Cryptographers Network:

The Dining cryptographer’s problem was first proposed by David Chaum [2][3] in 1988. He describes a taught experiment and proposes a solution for the same, he develops this as a thought experiment and proposes a solution, which he develops into a theoretical Dining Cryptographers protocol AKA. DC-net that can be used for broadcasting of unconditional anonymous messages. The theory behind DC-net is based on story of dining cryptographers where problem begins when three cryptographers are having dinner in a restaurant. Waiter informs that arrangements have been made for bill to be paid anonymously. One of the cryptographers will be paying the bill or it could be NSA. Three cryptographers want to respect each other’s privacy but they want to know if NSA would cover the bill. The truth table below indicates the results of sums of differences uttered as a result of comparison of coin-toss.



D1	D2	D3	Differences of Utterances
T	T	T	0
T	T	H	2
T	H	T	2
T	H	H	2
H	T	T	2
H	T	H	2
H	H	T	2
H	H	H	0

Figure 1. Results of Sums of differences uttered as a result of comparison of the coin toss

Peer-to-peer Model

With peer to peer the clients all make connections to each other in a ring design. For each bit to be transmitted the result from first stage of dc-net protocol are combined by sending them around ring network. The XOR results are passed to the next user. This process repeats until results have made entire circuit of ring.

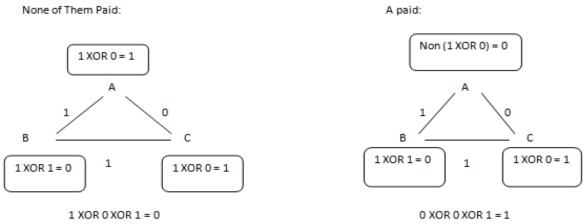


Figure 2. Dining Cryptographers Concept

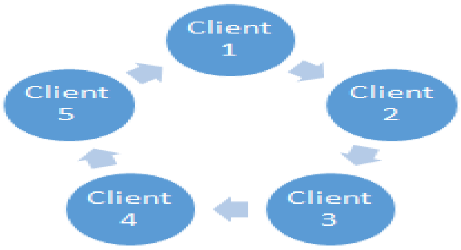


Figure 3. Peer – to – Peer Model

Hybrid Client Server

In this implementation the users send their results to a server, which XOR's and sends back the results. This model has the advantage of communication efficiency compared to peer-to-peer implementation.

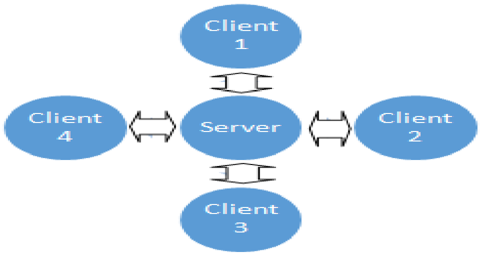


Figure 4. Hybrid Client Server Model

Client – Server Connection

The server is implemented as a dedicated application that acts as broadcast hub for clients as well as calculator for stage 2 of DC-net. Server cannot participate the same manner as that of client, however it sends information broadcasts when required. Client has the ability to send and receive messages. Clients handle stage 1 and send results to server. Clients have 2 operating rooms, one room for regular chat and other is used for anonymous chat. Once all the clients enter the anonymous room and are ready for the chat anonymous mode and countdown timer starts for session.

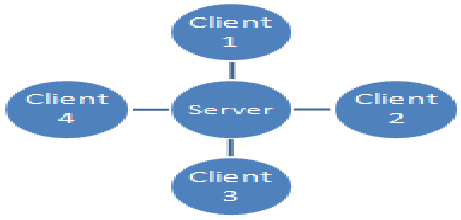


Figure 5. The Client – Server connection model

Once client connects and enters anonymous room and everyone are ready then server generates a random seed for every client in ring at connection point. This random seed is sent to every client as well as the client to their left. As each client has a seed and a corresponding seed for the ones on right they have 2 seeds with them. Once anonymous mode is being activated then client uses the 2 seeds to generate the results of coin toss.

The server logs stage 1 result as received but performs no further action until all stage 1 result bytes have been received from every client. Once all results have been logged from the client, the server XOR's all the results in the log. When clients receive stage two result a new round of Dc-net is triggered.

Security Support:

One-time pad (OTP) is an encryption technique which cannot be cracked if it is used correctly. In this technique plaintext is paired with a random secret key. Then each bit of the plain text is encrypted by mixing it with the corresponding bit from the pad by using the modular addition. If the key used is truly random, is at least as long as the plain text, is never used in whole or in part and is kept completely secret then the resulting cipher text will be impossible to break [4][5][6].

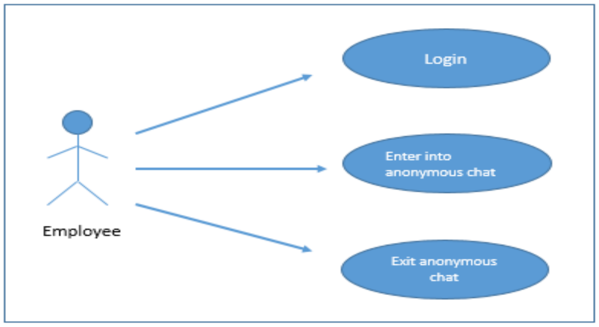
In our project we used one-time pad for sharing the secret key of the meeting to all the members of the meeting so that they can use their meeting ID and password to enter into the meeting. Thus adding a layer of security while sharing the password of the meeting

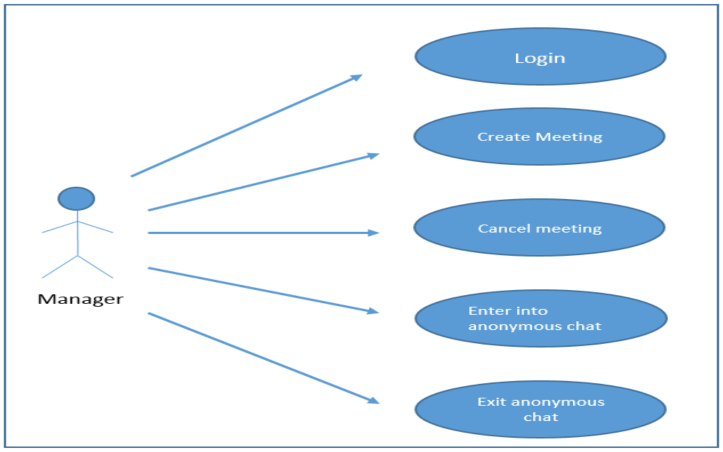
SHA-1 is a cryptographic hash function which stands for Secure Hash Algorithm 1 designed by the United States National security agency and is also a U.S federal Information processing standard published by United States NIST[7]. SHA-1 produces 160 bit (20-byte) hash value called as message digest. A SHA-1 value is typically a hexadecimal number which is 40 digits long.

We used the SHA-1 hash function to save the passwords of the users in the database. Thus securing the passwords from being exposed and hacked even though the database is compromised.

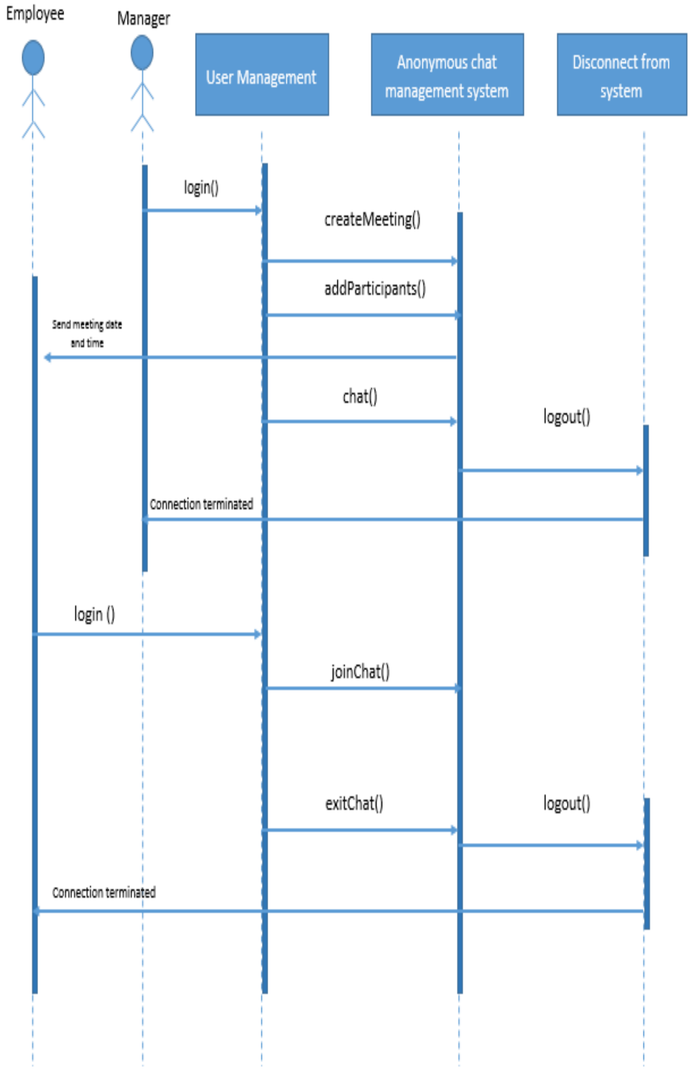
UML Diagrams

Use Case Diagram

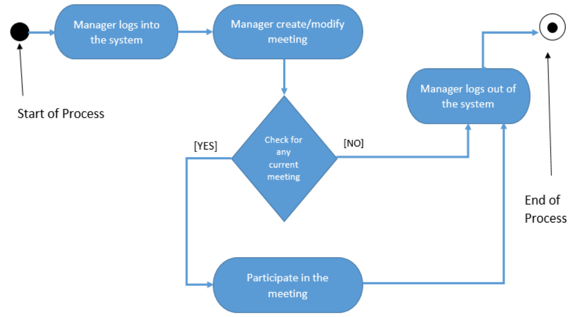




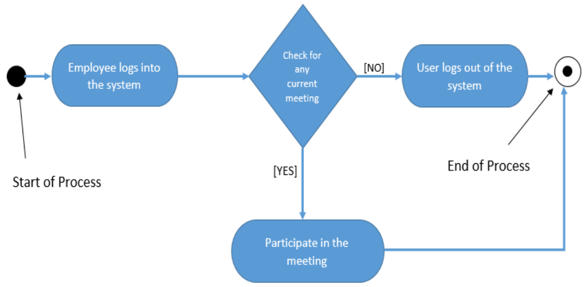
Sequence Diagram



Activity Diagram for Manager


Manager logs into the system
Manager create/modify meeting
Manager logs out of the system
Start of Process
[YES]
Check for any current meeting
[NO]
End of Process
Participate in the meeting

Activity Diagram for Employee


Employee logs into the system
Check for any current meeting
[NO]
User logs out of the system
Start of Process
[YES]
End of Process
Participate in the meeting

Implementation

Socket: A socket is one endpoint of a two way communication link between two programs running on network. It is bound to a port number so that TCP layer can identify the application that data is destined to be sent to.

TCP/IP Socket Programming

Server socket and socket are the two key classes from java.net package which are used in creation of client and server programs. Server program creates a specific type of socket which is used for listening to client requests. Whereas in case of a connection request it creates a new socket which helps in creating a new socket through which it exchanges data with client using i/p and o/p streams.

A simple server program in java involves the following steps:

Step 1: Opening the server socket

Step 2: wait for client request

Step 3: Create input output streams for communicating to the client

Step 4: Perform Communication with client

Step 5: Close socket

A simple client program in java involves the following steps:

Step1: Create a socket Object

Step2: Create input output streams for communicating with the server

Step3: Perform Input output or communication with server

Step 4: Close socket when done

Swing

A swing is a graphical user interface for java. It was developed to provide a sophisticated set of graphical user interface components than earlier Abstract window toolkit. The swing programming consists of the following steps:

Step1: JFrame

Step2: Window Listener

Step3: Adding a Panel

Step4: Fonts in Panels

Step 5: Basic Graphics

Step 6: Basic Event Handling

Step 7: Window Events

Step 8: Event Classes and Listener Interfaces

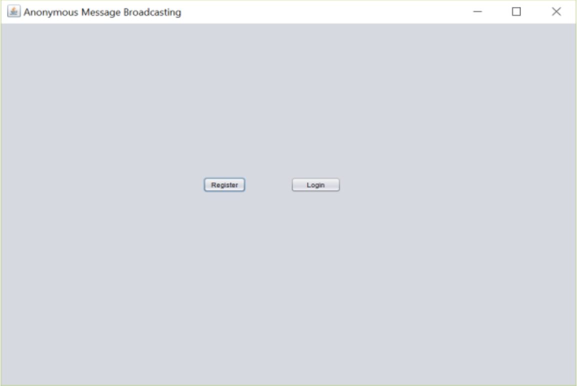
Step 9: Focus Event

Step 10: Keyboard Events and Sketch Demo

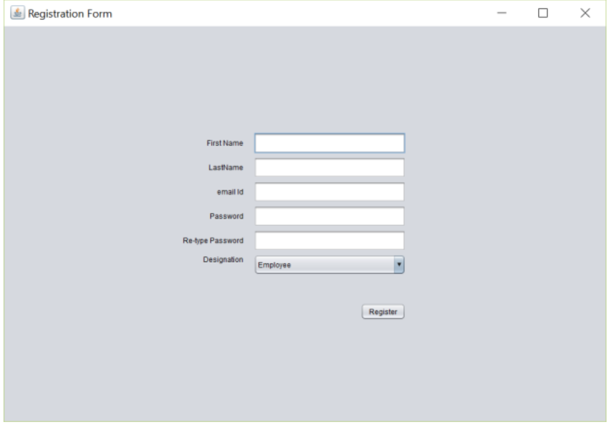
Step 11: Mouse Events and Mouse Demo

Step 12: Action Interface

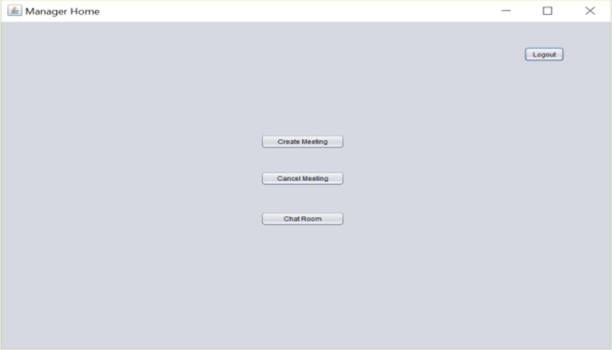
Screenshots



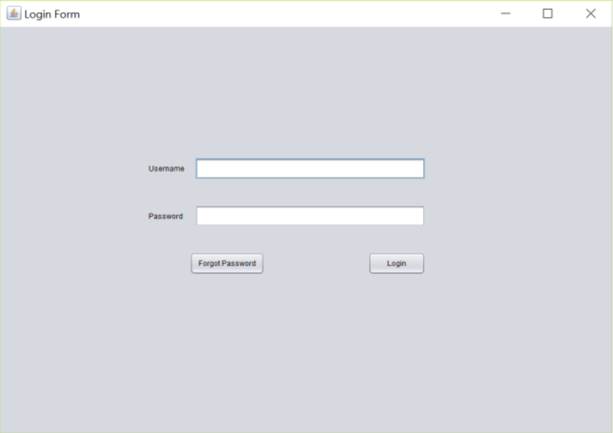
Home Page



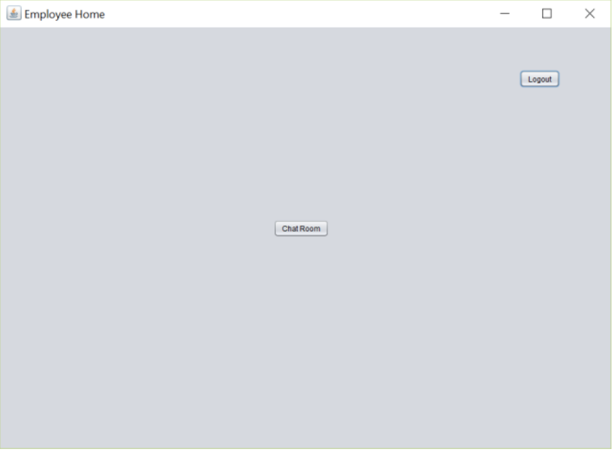
Registration Page



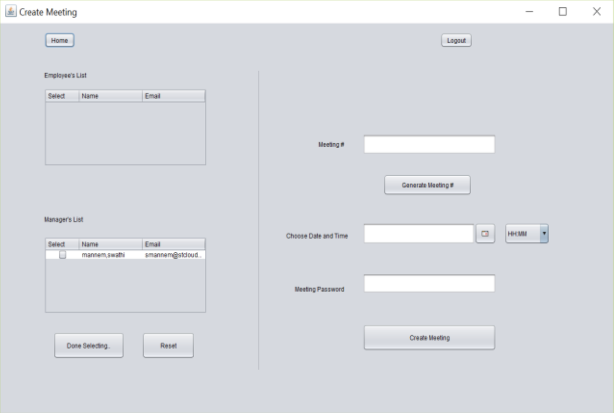
Manager Home



Login Page



Employee Home



Select	Name	Email

Select	Name	Email
□	mannem,swathi	smannem@stcloud...

Create Meeting

Discussion

We initially started to implement anonymous chat application as a web application and we have implemented half way and we were stuck up at a situation where we were in need to implement the Ajax technology in which we had limited knowledge and in the given time constraint we estimated that we cannot complete the project when moving at such a pace and then we decided to implement the project using the JAVA Swing technology which was more user friendly and we had enough knowledge to complete the project on time. We even decided to use RSA algorithm for the distribution of keys to the members of the meeting but had a difficulty in retrieving the public key from the database and using it to encrypt the password and hence implemented one-time pad which is even more stronger algorithm and successfully finished our project on time.

Conclusion

There are cases where privacy preservation is important even in the situations where communication is to take place like for example online surveys. The DC-Net (Dining Cryptographer network) was devised by David Chaum for anonymous message broadcast. In this project we were able to design an anonymous chat application which is an implementation of the DC-Net protocol. Here we can schedule and organize meeting to the members of the meeting and have an anonymous meeting hiding the person's details and gives freedom to discuss issues and talk openly without revealing your identity. There are a wide range of applications implementing this system such as confessions pages in Facebook, online surveys etc.

References

[1] Nissenbaum, H. 1999. The Meaning of Anonymity in an Information Age. The Information Society , 15:141-144

[2] Chaum, David. "The Dining Cryptographers Problem: Unconditional Sender and RecipientUntraceability." Journal of Cryptology, 1988: 65- 75.

[3] Chaum, David. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. "Communications of the ACM, 1981: 84-88.

[4] "Intro to Numbers Stations". Retrieved 13 September 2014.

[5] "The only unbreakable cryptosystem known—the Vernam cipher". Pro-technix.com. Retrieved 2014-03-17.

[6] "One-Time Pad (OTP)".Cryptomuseum.com. Retrieved 2014-03-17.

[7] http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf