CSEN1001:Computer & Network Security

Project Report

Steganography Chat

Team members:

Amr ahmed ali hassan	34-5236
Mahmoud Khalaf	37-17770
karim islam	34-8589
Nour Gamal	34-2471
Mahmoud abdelfattah	34-15954
Ahmed Sharaf eldin	34-4877

Motivation :

A lot of techniques are used to protect and hide information from any unauthorized users such as Steganography . Steganography is the science of hiding a message inside another message without drawing any suspicion to others so that the message can only be detected by its intended recipient . This project is a P2P chat application which applies steganographic technique to allow a secure communication in a complete undetectable manner.

Summary of the Project :

In Our project we made a Peer to Peer Chatting application that users can chat with each other in a secured way we handle access control for private chatting and secure so no one can attack them also we handled a broadcast message that send a message to all active users . The encryption method we used is steganography technique and we used least significant bit approach .we also do an authentication to be sure the users that register for the application we also hash with salt the passwords to not let any attacker to attack the database we also calculate the capacity and fidelity of the image as stats for the reconstructed image and there are some extra functions as logout that make the user inactive and logout from the application and deactivate function that used if the user want to deactivate from the application and the username and the password will be deleted from the database . We ensure a secured chatting application that the probability of attack is very low .

cryptographic algorithms (steganography technique) :

In this project we have proposed a image steganography P2P chatting application .Images are made up of pixels which usually refer to the color of that particular pixel . In greyscale images the pixel value range from 0 to 255 , 0 is for black and 255 for white , and increasing the value of the pixel make it more brighter . In our project we used LSB technique LSB standss for (Least Significant Bit) . We used LSB because if we change the last bit value of a pixel there won't be

much change or visible change in the image or in the color .For example if we change 0 to 1 there will be no much difference it will still black , but just a lighter shade .

-Advantages of LSB technique :

1) The Output image has a very slight difference from the input image .

2) It's easy to implement and very fast compared to other steganography techniques .

3)We can embedding large messages as we can embed the message in the last two LSBs not just only LSB.

-Disadvantages of LSB technique :

1) This technique can be attacked as it can be easily decoded by statistical attack as it much more effective than visual attack by taking the LSBs of the image and getting the message in binary format .

2) The image quality may be reduced if we embedding the message in more than one LSB .

functionalities :

1)Authentication (Login and Signup) :

In our project the client must sign up at the first use by user name and password to make sure that the clients enter the network is trusted . Username and password are saved in a database and the password is hashed before stored in the database . Login step is done if the client logout from the application and the username and password must be in the database .

2)Hashing Passwords :

In the project the passwords are hashed before stored in the database but even though the hashed passwords are not unique to themselves due to the deterministic nature of hash function (if we give the two identical passwords , the hash will be produced will be identical) .So the attacker can better predict the password that legitimate maps to that hash and once the password is known the same password can be used to access all the accounts that use that hash .So we used a salt additionally to the hash to prevent this attack .The Salt we used "NOUR" . Once the salt is added if two users enter same passwords , it will be hashed into different hashes .

3)Private Chat (Access Control) :

In the access control we grantee the integrity and confndiality , so the client can't claim that another client send him a message also the client can't denay that he didn't send a message ,also it grantee that the message will be sent as we provide integrity .Also to send to only one user you type @ and then followed by the username that you want to chat with .

4)End-End Encryption :

End-End Encryption is a method of secure communication that prevents 3rd parties from accessing data while transferred from one end to another .We used this encryption to prevent man-in-the-middle attack .This is done by encrypt the text in the client side .

-advantages of End-End Encryption :

- Privacy secured : There have been higher demands for making messages more secure due to more and more threats of hacker
- No government spies
- Connecting people better : People talk more freely with others when they are sure that their conversation will remain to themselves

5)Capacity (ratio of secret message to hosting image) :

Capacity is calculated by this equation : Capacity = (amount of hidden bytes/size of the image in bytes)*100.

We get the hidden bytes by get the length of the message that will be embedded in the image as every character is 1 Byte and we get the size of the image by get the length and the width of the image by pixels and get the all number of pixels then multiplie it by 3 as the image is RGB image .

6) Fidelity (distortion of image hiding the message, measured as Peak Signal to Noise Ratio):

The image fidelity is a measure of the accuracy of the reconstructed image and this is done by calculating peek signal to Noise Ratio (PSNR) from the original image and the reconstructed image .

7)Broadcast messages :

In Our Project we can send a broadcast message to all online users also encrypted by steganography technique , this done by a tab that send a message and send it to all other clients .

8)Logout:

This feature is extra feature and it make the client logout from the application and if he want to log again he must to go to the login page .

9)Deactivate Account :

The client can deactivate his account from the application therefore the username and the password will be deleted from the database .

10) Show Online Clients :

This Feature is an extra feature that allow to show the online users in the application and this allow the client to see the other clients to start chat with or to send broadcast .

Attack Scenarios :

1) Statistical Attacks :

This can be done if an attacker get the image that will be send to the other user and do some statistics on the image and get the binary image of the image and then can get the missing bits and therefore get the hidden message , we can overcome this attack by ensure the end-end encryption so no one can access the image and attack the clients .

2)Brute force Attack :

This Attack can be done if the attacker try to access and try alot of passwords but we can overcome this by hashing the passwords with salt and this make the brute force attack very costly and nearly impossible to access information .

libraries and frameworks :

We have used the following libraries and frameworks to ensure some of our security features:

1st: Steganography.

Steganography: Using the steganography framework. We have implemented the steganography algorithm to encrypt and decrypt text messages to Images.

2nd: Hashing.

Hashing: We have re-implemented the hashing and salts concepts in our project. So that all users' passwords are hashed before being pushed in our data-base.

3rd: Authentication and Access Control.

Authentication and Access Control: We have re-implemented the concept of user authentication and authorization from scratch. Once the user Signup, an entry in an excel file named "users.csv" created. The entry contains a hashed password.

References :

1) http://paper.ijcsns.org/07_book/200906/20090638.pdf

2) https://arxiv.org/ftp/arxiv/papers/1302/1302.2718.pdf

3) https://pdfs.semanticscholar.org/8fc4/f7bfbeb53c00d6f5e1ee7d0b09afd597b943.pdf

4) https://www.dreamincode.net/forums/topic/27950-steganography/

5) https://www.developer.com/java/ent/article.php/3530866/Steganography-101-using-Java.htm

6) https://www.dreamincode.net/forums/topic/200927-p2p-chat/

7) https://javabeginnerstutorial.com/node-js/chatbox-a-peer-to-peer-chat-application/

8) https://prestobear.com/2017/02/sample-java-peer-peer-chat-application/

9) https://stackoverflow.com/questions/31798244/java-chat-program-p2p

10) https://github.com/asamy/P2P-Chat/blob/master/src/p2pchat/Peer.java

11) http://www.informit.com/articles/article.aspx?p=30212

12) https://www.geeksforgeeks.org/introducing-threads-socket-programming-java/

13) https://www.geeksforgeeks.org/multi-threaded-chat-application-set-2/

14) https://codinginfinite.com/java-tcp-client-server-chat-application-sockets/

15) http://makemobiapps.blogspot.com/p/multiple-client-server-chat-programming.html

16) https://www.quora.com/How-do-I-implement-the-code-for-multi-server-multi-client-chatting-application-in-Java-I-already-have-the-code-for-multi-client-single-server-chatting