VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Securing Online Chat Based Application

Guided By: Dr Bhulakshmi Bonthu

J Component Project: BCI3001
Web Security
Slot: B2
Fall Semester 2021-22

Members Name:
Tanmay Kumar, **19BCE2146**
Mudit Jain, **20BCE0362**
Anusha Ajay Bamzai, **20BCE2833**

School of Computer Science and Engineering (SCOPE)

October, 2021

CONTENTS

ABSTRACT

Chat applications have become perhaps the most significant and famous application on smartphones. It has the ability of exchanging instant messages, images and documents which is cost free for the users to communicate with one another. All messages must be protected. The point of the project is to propose a chat application that gives End-to-End security that lets securely exchange private data with one another without agonizing or worrying over information. In addition to the protection of storage, a list of prerequisites to make secure chat application is introduced in this project and in view of these necessities, the application was planned. In short, we know that stealing the data is a big concern in these chat based applications. This application is going to be specifically for developers, who don't want their data to be leaked, and to achieve this, we need to consider some good security measures.

PROBLEM STATEMENT

In this project, we will be introducing methods to preserve the security and privacy of the chat based application. We will also describe a set of requirements for making a chat secure and implement it by using modern methods. To summarize, our main aim is to create and secure a fully functional website for online chat based communication from all the basic threats and vulnerabilities.

LITERATURE SURVEY

- **EMPIRICAL ANALYSIS OF WEB ATTACKS**
  By Daljit Kaur and Parminder Kaur

  WORK DONE:
  This paper has web attacks analysis from Website Hacking Incident Database (WHID).
  It analyzes various attacks on major categories of web sites. Vulnerable categories of web applications are also analyzed in this paper.

  KEY TAKEAWAYS:

  The pros of this idea are that initiatives are taken to prevent these types of break-ins. It would also encounter major occurring threats over the web applications. Coming to the cons, implementing security in SDLC takes more time, requires skilled staff and costs higher. Spending more on secure development of web applications may not be a wise decision as they do not contain any sensitive information.

- **CSRF PROTECTION IN JAVASCRIPT FRAMEWORKS AND THE SECURITY OF JAVASCRIPT APPLICATIONS**
  By Ksenia Peguero, Xiuzhen Cheng

  WORK DONE:
  This paper has studies related to how cross-site request forgery vulnerability is mitigated in several server side JavaScript frameworks. It also gives us an idea as to how creating frameworks that produce secure applications.

KEY TAKEAWAYS:
The pros of the idea proposed in this paper are that fewer vulnerabilities are there in closely located mitigation. Also, CSRF middleware provides APIs for creating and verifying CSRF tokens .Coming to the cons, this idea is limited by only one type of vulnerability (XSS) found in client-side code. The CSRF middleware does not provide any additional functionality for using the tokens in the session, cookies, or HTTP headers.

- **FIDO2 PUTS BIOMETRICS AT HEART OF WEB SECURITY**
  By Dunkelberger Phil

WORK DONE:
The ultimate end goal of this research paper is that banks/financial institutions issue biometric cards for free to end users. This is the model largely used worldwide today and a service most banking customers have come to expect.

KEY TAKEAWAYS:
The pros of the idea proposed in this paper is that FIDO standard paves seamless integration of multiple authentication methods, combining with other-biometric authentication. Biometric payment cards are better than low-cost payment card vendors. The disadvantages include, a crowded and uncoordinated ecosystem of custom coding and various APIs to handle each unique authentication method. Public/private key cryptography shrinks the attack surface by keeping biometric data stored on a particular device.

- **ELECTROLINT AND SECURITY OF ELECTRON APPLICATIONS**
  By Peguero Ksenia Cheng Xiuzhen

WORK DONE:
This paper includes analyzing vulnerabilities in Electron application, study common mitigation controls, using automatic and manual static analysis. It shows the effectiveness of the IDE plugin by applying the plugin’s suggestions to the analyzed open-source applications and demonstrating that they stop being exploitable after the applied fix.

KEY TAKEAWAYS:
This paper analyzes the Abstract Syntax Tree (AST). It shows which vulnerabilities are most common. Plugin idea is similar to a spell-checker, which provides contextual and actionable advice. This vulnerability is addressed with the HTTP protocol instead of the HTTPS protocol. The major cons of this approach include that it does not execute dataflow analysis. Moreover, the URL may be malicious or could be a URL to a legitimate site.

- **SECURE HASH ALGORITHMS AND THE CORRESPONDING FPGA OPTIMIZATION TECHNIQUES.**
  ACM COMPUTING SURVEYS
  By ZEYAD A Al -ODAT et al.

WORK DONE:
This research paper explains why FPGA is a reconfigurable hardware that supports a variety of design options. It also shoes devotion to the FPGA optimization techniques for the three hashing standards.

KEY TAKEAWAYS:
The idea proposed in this project works upon the improvement in the latest Secure Hashing algorithm for Cryptography. However, the performance is decreased unless loop unrolling is combined with other optimization methods. SHA3 consumes more power than the other standards thus, high frequency is needed and power consumption is high.

TECHNICAL SPECIFICATION

SOFTWARE REQUIREMENTS:

S.NO.	SOFTWARE DESCRIPTION	SOFTWARE USED
1.	Malware Database	VirusTotal
2.	Report Logging Database	Google Sheets

HARDWARE REQUIREMENTS:

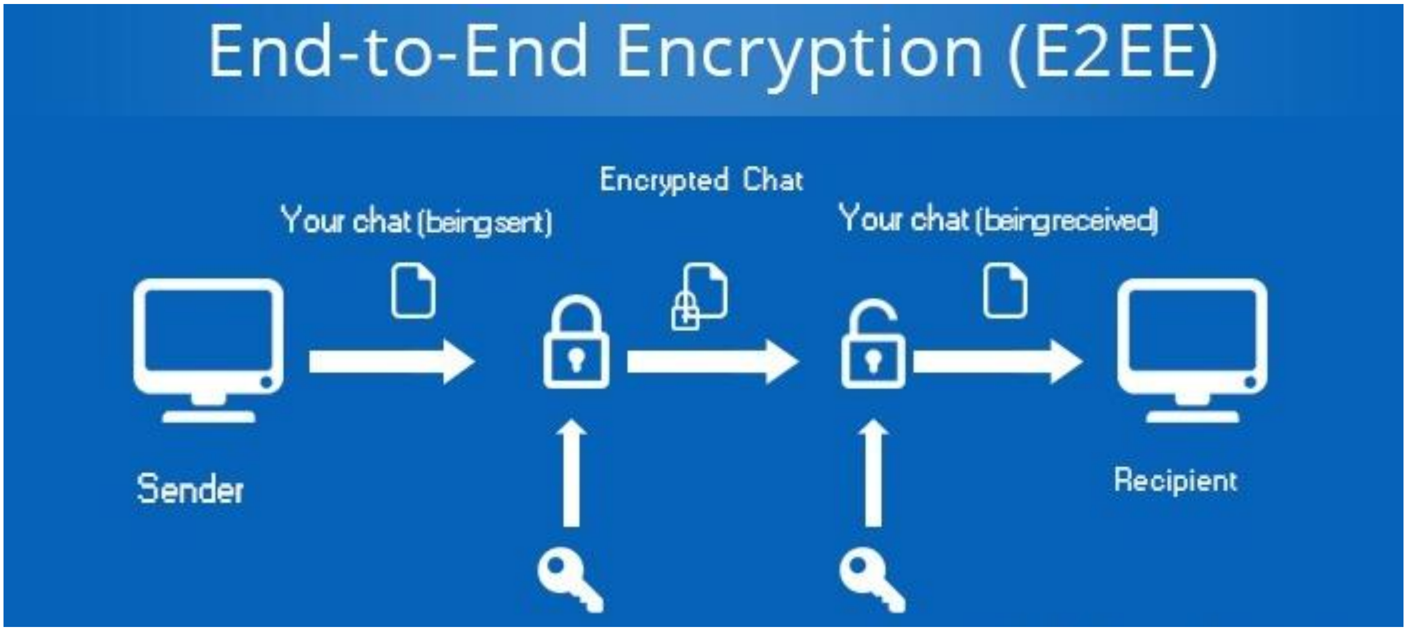
The following are the hardware specifications:

Processor: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
RAM: 16.0 GB (15.8 GB usable)
Storage: 512 GB SSD
Operating System: Windows 10

DESIGN APPROACH AND DETAILS

The proposed architecture is designed to be client server chat application. In client side when a user sets up the application, the user either selects sign up or login. In the server side, the chat server consists of users server and a message server. Users server manages users credentials. Message server handles messages between users by using fire base cloud messaging (FCM). In case of group chats, every time a user enters into the group, the other members in the group get notified about it.

This project aims at end-to-end encryption of messages as shown in the flow chart below:



CONCLUSION

In this project, we introduced a specification for preserving the security and privacy of the chat application. We described a set of requirements for making secure chat and implement it by using modern methods and lightweight for providing speed and good protection to its clients. We have tried to add session management, prevention from SQL injection, password protection, and standard level of data encryption. Clients can be confident that nobody can read their messages, even if the mobile phone reaches wrong hands cannot enter to the application and cannot access the data stored locally.

REFERENCES

- Empirical Analysis of Web Attacks - https://www.sciencedirect.com/science/article/pii/S1877050916000594
- CSRF protection in JavaScript frameworks and the security of JavaScript applications- https://www.sciencedirect.com/science/article/pii/S2667295221000258
- FIDO2 puts biometrics at heart of web security- https://www.sciencedirect.com/science/article/abs/pii/S0969476518301267#:~:text=%20FIDO2%20puts%20biometrics%20at%20heart%20of%20web,available%20to%201.5bn%20people%20and%20counting.%20More%20
- Electrolint and security of electron applications - https://www.sciencedirect.com/science/article/pii/S2667295221000222#:~:text=%20Electrolint%20and%20security%20of%20electron%20applications%20,on%20our%20previous%20work%20%5B6%5D%2C%20each...%20More%20
- Secure Hash Algorithms and the Corresponding FPGA Optimization Techniques.- https://dl.acm.org/doi/10.1145/3311724