International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 4, July-Aug-2022, ISSN (Online): 2395-566X

Design and Development of Security Algorithm Using Modified PGP Algorithm

Prof. Sushila Ratre, Suprit Pandurangi, Ashwin Nair, Vinay Kondabathula, AyushGajbhiye
Department of Computer Science and Engineering,
Amity University,
Mumbai, Pune Expressway, Bhatan
Post - Somathne, Panvel, Maharashtra, India
sushila.ratre@gmail.com, pandurangisuprit@gmail.com,ashwinnair99an99@gmail.com,
vinaykondabattula@gmail.comayushgajhbiye36@gmail.com

Abstract-With the rise of data protection regulations and the increasing fines, companies worldwide focus more on cybersecurity, especially on the safety and privacy of sensitive customer data. Source code can be related to a company's 'secret sauce'. At a fundamental level, one's intellectual property is represented by the code. This has a vast range starting from code to the protocols for implementation to deployment to marketing and sales. Hence security of the source code plays a very vital role. In the proposed system a modified PGP encryption algorithm that is better than the STEK algorithm currently being used by Meta is planned to be implemented. This algorithm uses both symmetric and asymmetric encryption and decryption of data which makes it better than STEK. Using this algorithm, a more secure private key for securing the data can be implemented. A larger key shall be generated by twiddling the source code if needed so as to generate the key of size 8192 bits. A dynamic PGP virtual disc can be used to create the predefined size, so as to handle the requirement of a big sized encryption key. This will be beneficial in handling both the size of the data and the key values so as to achieve efficient and feasible secured data. But sometimes, the PGP algorithm can be slower when sharing data over public platforms, So AES can be used, which is quick and good for large databases. There are many algorithms available in the market for encrypting the data.

Keywords-Security, Meta, PGP, STEK, Encryption.

I. INTRODUCTION

There is now a staggering amount of information available about people, companies, and organisations. Almost anyone who is prepared to pay for it can get this data for free on the Internet, regardless of whether they are legitimate consumers, credit card scammers, or identity thieves.

Generally, when people mention writing good software, they're talking about designing secure applications. This implies writing code that prevents vulnerabilities from developing while your software is in use.

However, what about protecting the source code alone, irrespective of the software? People frequently believe mistakenly that their source code is already securedbecause it is private. However, hackers are aware that having access to the source code can disclose other active threats and guide them toward application vulnerabilities.

1. How Different Big Companies Secure Their Source Code?

Facebook, Apple, Google, and Microsoft all use identical methods. They all keep a tight eye on the employees. To discourage the theft of trade secrets, most of them provide stock options, and they are eager to pursue legal action against offenders. These corporate companies have all shown that they are vulnerable to inside leaks, despite their resources. No matter how big or little your company is, it's crucial to be aware of this danger.

2. Zero Day Vulnerability:

A vulnerability in a system or device that has been publicly published but has not yet been fixed is known as zero-day vulnerability. A zero-day exploit is an exploit that targets zero-day vulnerability. Zero-day vulnerabilities are more dangerous for users since they were found before security researchers and software

developers were aware of them and before they could provide a fix. Cybercriminals rush to take advantage of these weaknesses in order to profit from their schemes.

System vulnerabilities exist until the vendor releases a patch. Targeted assaults frequently leverage zero-day vulnerabilities, while many campaigns still make use of older flaws.

3. Zero-day bugs found on Meta Services:
Two Facebook WordPress plugins contain a few zero-day vulnerabilities, according to researchers from the security company Plugin Vulnerabilities. The "Facebook for WooCommerce" plugin and the "Messenger Customer Chat" plugin both seem to have bugs, according to the security company. There are currently over 200,000 active installations of the previous plugin. The former has fewer than 20,000, however.

4. Source Code Security Methods:
During the phase of implementation, one needs to consider the following methods for improving source code security:

4.1 Implement Secure Development Practices: At the start of each process, you must develop a clear set of coding practices, rules, and procedures. This includes educating your development team on best security practices and providing them with documentation of the security protocols they must meet throughout the project. The Open Web Application Security Project (OWASP) provides a clear framework that is a good place to begin. Although it is designed for web applications, its concepts apply to all types of software development work.

4.2 Code Review: Education, code reviews, tools, and knowing where to focus your work are the keys to protecting source code. A 2015 App sec USA survey showed which vulnerabilities were most missed by automated tools and which were most frequently picked up.

4.3 In this case, "Insecure Direct Object Reference," "Sensitive Data Exposure," and "Missing Access Control" were most missed by automated tools.

4.4 Encrypt and Monitor Data in Transit: Encrypting your data is essential for protecting your source code. Furthermore, data in transit is very sensitive. Finding techniques to protect your code when it is transferred between members of the development team is, therefore, a good idea.

4.5 DevSecOps: There are many security-related tasks that developers can and should share responsibility for, but they are frequently left to a small team of security professionals. The idea behind DevSecOps is to involve developers as early as possible in the security process. Developers are arguably the people with the closest ties to the source code, thus it stands to reason that they would bear some of the burdens of ensuring its security.

4.6 Control Access and storage: Store source code in well-secured code repositories. Only developers and security professionals should have access to source code repositories. Anyone who isn't familiar with coding shouldn't be given access. We can dramatically reduce the danger of insider threats by restricting who has access. Utilize authentication, authorization, and access control to safeguard your code.

II. LITERATURE REVIEW

Pawan Kalyani Feb 2020 [9] have described the parent and other subsidiary companies - Facebook and Instagram,controversial WhatsApp privacy policy and WhatsApp user viewpoint discussed the point why people are shifting more WhatsApp to other apps ? Due to the factor of new privacy policy that the company from there side is not clearing whether there user data will share with parent company.

Anu Singh, 2021 [10] have discussed an analysis of WhatsApp's new privacy policy with emphasis on the right to erasure what was the role of intermediary in the protection of right to erasure.

Dr.Govind Singh et al, May 2021 [11] have discussed the Socio-legal analysis of WhatsApp privacy policy 2021 in India. Issues Related to New WhatsApp Policy like a Personal Data Breach, Confusion over Type of Data Shared, Breaking of Assurance by WhatsApp over Ad Feature are also discussed.

D. Sanchari Das et al.Aug 2020 [12] have compared country wise users between Saudi Arabia and India and issues related to joining an unknown group whom we don't know, even how WhatsApp privacy can be more secure.

Sanjay Rawat et al., Jan 2009 [13] have described Security Code Analysis (SCA) that aims to discover/uncover security-related bugs in the code that may pose vulnerability. Objective of security code analysis, Types of code analysis mainly Static source code analysis, Static binary code analysis, Dynamic source code analysis and Dynamic binary code analysis.

Zeineb Zhioua et al., Jul 2014 [14] have described the security properties, static code analysis and techniques for static code analysis. Control-flow and Dataflow are two of the commonly adopted formal methods for program representations. Control-flow analysis is Symbolic analysis and Information-flow analysis. The point why Graph Match is mainly focused on the order and sequence of instructions.

Sidharth Chamarty, Jul 2020 [15] have discussed Legal Status of Data Privacy in India. India does not have a law that is specifically aimed at data protection, what data is covered/protected under the various legislations? The IT (Reasonable Practices) Rules, 2011 state that "sensitive personal data or information of a person" includes passwords, medical information, etc and the International Scenario between US and UK, and comparing it with India.

III. PROPOSED ALGORITHM

We would like to propose a secure algorithm that will be better than the STEK encryption. We propose PGP Encryption for securing Meta.

PGP key encryption algorithm uses both symmetric and asymmetric keys to encrypt data being transferred across the network while STEK is a symmetric key algorithm that uses the same key for encryption and decryption of data.

1. We can implement PGP in following ways:

PGP can be implemented using different softwares:-

1.1 GnuPG: GnuPG has access modules for a variety of public key directories, a flexible key management system, and the ability to encrypt and sign your data and communications. The command line tool GnuPG, usually referred to as GPG, has features that make it simple to integrate with other programmes. Both Linux and MAC use it.

1.2 Gpg4win: Using encryption and digital signatures, Gpg4win enables users to send emails and files securely. The contents are shielded from reading by unauthorised parties thanks to encryption. Digital signatures guarantee that the message was not altered and was sent by the specified sender. It is used in Windows.

1.3 Encrypto: Files can be encrypted with Encrypto before being sent to friends or coworkers. Simply place a file into Encrypto, create a password, and send the data asusual with the added protection. For both Mac and Windows, it is free**.**

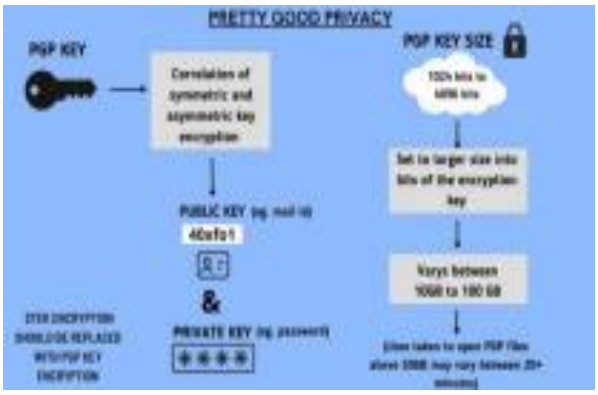

Fig 1. PGP.

2. Increasing the size of encryption PGP for security advantage:

By referring to Fig 1.0, we can learn that PGP key sizes can range between 1024 and 4096 bits. The standard key size is 2048 bits. The larger the key, the more secure it is, but it takes longer to generate. Some smart cards and tokens have a key size limitation of 1024 bits. Larger keys require more computation time to use, which can make this fast unworkable. Care should be used when selecting sizes to preserve interoperability because different OpenPGP implementations could also utilise different upper boundaries for public key sizes. The common top limit for implementations as of 2007 is 4096 bits. We can generate larger size keys, though some source code twiddling may beneeded, you can generate 8,192 bit keys.

Adynamic (resizable) PGP virtual disc is one that can expand in size when new files are added to it, but it maintains its initial size until more space is required. We simply need to specify the maximum sizethat we would like the disc to be because PGP Desktop handles this operation. If you'd like, you can compress this disc at a later time. Only FAT or FAT32-formatteddiscs can use this kind of PGP Virtual Disk. In fact, we've seen some instances of 16,384 bit keys generated courtesy of the "Cyber Knights Templar (CKT)" builds of PGP "back in the day."

3. Data that can be transferred with PGP Keys:

If we set the PGP key size to a larger size of bits for the key. The data sent may vary between 10 GB - 100GB .And may take 20+ mins to encrypt the data sent.Though, the file is divided into chunks that are transmitted to a pipe object while being encrypted. A chunk's bytes are read in the same order that they were written from the pipe object.

IV. RESULT ANALYSIS

The results demonstrate some performance variations between platforms and PGP distributions, as well as some disparities with earlier published evaluations of the various encryption algorithms. A hybrid cryptosystem called PGP is mainly used for secure email. The total number of keys does not equal the total number of users because users might self-generate multiple keys. When we combined keys with different email addresses to identify users who had multiple keys, we found that there were a lot of keys.

A well-known tool called Pretty Good Privacy, or PGP, was used to encrypt and decrypt emails sent over the internet and authenticate communications with digital signatures and store encrypted files. Any encryption tool or application that adheres to the OpenPGP public key

cryptography standard is now referred to as PGP. Public key cryptography, conventional encryption techniques, digital signatures, and certificates are all part of PGP's distinctive combination that helps protect sensitive information you communicate over the internet. But despite all of its measures, hackers still have a chance.

PGP may not have achieved encryption for the public in nearly three decades due to its low user base of less than one million, but the mobile messaging software WhatsApp has reached a billion users in just a few short years (Metz 2016). Unlike commercial products and thus market solutions like emails, instant messaging products like WhatsApp are built with encryption and enabled by default. Unprotected communication gradually disappears in the context of the growing use of mobile devices and instant messaging, giving users access to private messages by default.

V. CONCLUSION

In this research we have seen the encryption algorithm that is better than current STEK encryption that meta uses. We have found that PGP Encryption Algorithms will be much better than STEK as they will provide much more security than STEK. We have researched two algorithms and we have come to a point that AES is quick and performs well in large databases and closed systems. When sharing data over an open network, PGP should be used, however it can be slower and performs better for single files. We have also found out about what all things should be kept in mind while doing secure programming.

ACKNOWLEDGEMENT

We would express our sincere gratitude to Dr Deepa Parasar and Prof. Rajesh Bhise for their guidance and support.

REFERENCES

[1] Goyal, N., Nekritz, K., & Iyengar, S. (2019, May 29). Building Facebook's service encryption infrastructure.Engineering at Meta; engineering.fb.com.https://engineering.fb.com/2019/05/29/security/ervice-encryption/

[2] How does end-to-end encryption work? | Facebook Help Center. (n.d.). How Does End-to-End Encryption Work? | Facebook Help Center; www.facebook.com. Retrieved July 24, 2022, from https://www.facebook.com/help/786613221989782

[3] Pretty Good Privacy - Wikipedia.(1991, January 1). Pretty Good Privacy - Wikipedia; en.wikipedia.org. https://en.wikipedia.org/wiki/Pretty_Good_Privacy

[4] What is PGP Encryption? Pretty Good Privacy Explained | Fortinet. (n.d.).Fortinet; www.fortinet.com. Retrieved July 24, 2022, from https://www .fortinet.com/resources/cyberglossary/pgp encryption #:~:text=Pretty%20Good%20Privacy%20Definition, Paul%20Zimmerman%2C%20a%20political%20activist UNTERFINGHER, V. (2022, May 30). What is PGP Encryption and How does it Work? Heimdal Security Blog; heimdalsecurity.com.

[5] https://heimdalsecurity.com/blog/what is-pgp-encryption-and-how-does-it work/

[6] How to Write Secure Source Code for Proprietary Software. (2022, July 5). freeCodeCamp.Org; www freecodecamp org.cdn.ampproject.org. https://www freecodecamp org.cdn.ampproject.org/c/s/www.freecodecamp.org/news/how-to-write secure-source-code-for-proprietary software/amp/

[7] Hashim, A. (2019, June 19). Zero-Day Vulnerabilities Found In Two Facebook WordPress Plugins. Latest Hacking News; latest ackingnews.com.

[8] https://latesthackingnews.com/2019/06/19/zero-day-vulnerabilities-found-in two-facebook-wordpress-plugins/

[9] Clement, Mark. "How Do Large Companies Protect Their Source Code? - Stop Source Code Theft." Stop Source Code Theft, www.stop source-code-theft.com, 28 Sept. 2018, https://www.stop-source-code theft.com/how-do-large-companies protect-their-source-code/.

[10] Kalyani, Pawan. (2020). An Empirical Study on "Whatsapp Privacy Policy" Analyzing the Real Cost of "Free" Apps in an Online Social Network:: In Contrast to Other Player like Telegram, Signal etc JMEITFEB0801001. 10.5281/zenodo.4584744. 2022. [online] Available at:

[11] <https://www.researchgate.net/publication/349811360_An_Empirical_Study_on_Whatsapp_Privacy_Policy_Analyzing_the_Real_Cost_of_Free_Apps_in_an_Online_Social_Network_In_Contrast_to_Other_Player_like_Telegram_Signal_etc_-_JMEITFEB0801001>[Accessed 26 August 2022].

[12] Anu Singh , Right to Erasure and Whatsapp's Privacy Policy: An Analysis, 4 (2) IJLMH Page 524 - 533(2021), DOI:http://doi.one/10.1732/IJLMH.26100

[13] Rajpurohit, Dr. Govind Singh and Kumar Yadav, Dr. Raj, A Socio-Legal Analysis of WhatsApp Privacy Policy 2021 in India: A Contemporary Study (May 21, 2021).Available at SSRN: https://ssrn.com/abstract=3850579 or http://dx.doi.org/10.2139/ssrn.38 50579.

[14] Das, Sanchari & Dev, Jayati & Camp, L. (2018). Privacy Practices, Preferences, and Compunctions WhatsApp Users in India. https://www.researchgate.net/publication/327867176_Privacy_Practices_Preferences_and_Compunctions_WhatsApp_Users_in_India

[15] Rawat, Sanjay & Saxena, Ashutosh. (2009). Application Security Code Analysis: A Step towards Software Assurance. International Journal of

Information and Computer Security (IJICS). 3. 86-110. 10.1504/IJICS.2009.026622. https://www.researchgate.net/publication/215697205_Application_Security_Code_Analysis_A_Step_towards_Software_Assurance

[16] Zhioua, Zeineb &Roudier, Yves. (2014). Static Code Analysis for Software Security Verification: Problems and Approaches. Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014. 10.1109/COMPSACW.2014.22.

[17] https://www.researchgate.net/publication/282859666_Static_Code_Analysis_for_Software_Security_Verification_Problems_and_Approaches

[18] Chamarty, Sidharth. "Data Privacy in India: A Legal Analysis with Special References to Whatsapp Snooping | ProBono India." Data Privacy in India: A Legal Analysis with Special References to Whatsapp Snooping |