JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY (JKUAT)

DEPARTMENT OF COMPUTING

BCT 2406: PROJECT RESEARCH AND DEFINITION

PROJECT PROPOSAL REPORT

ENHANCING DATA CONFIDENTIALITY IN INSTANT MESSAGING (IM) APPLICATIONS USING THE ADVANCED ENCRYPTION SCHEME (AES)

AUTHOR:

NAME: MBADI BRIAN **REG NO:** SCT212-0130/2016

SUBMISSION DATE: ______________________ SIGN: _____________________

COURSE: BSC. COMPUTER TECHNOLOGY

SUPERVISOR 1:

NAME: DR MICHAEL KIMWELE

SIGN: ___________________________ DATE: __________________________

SUPERVISOR 2:

NAME: __________________________

SIGN: ___________________________ DATE: __________________________

Abstract

Data security and end-to-end encryption (E2EE) ensures the confidentiality of data sent from one endpoint to another in an Instant Message (IM) application. With end-to-end encryption, only the sender and receiver can decrypt and read the messages sent over the channel. In an Instant Messaging system, there are several vulnerable areas in which encryption needs to be applied to guarantee the overall security of the system. These areas include data storage, both in the user's mobile phone and backed-up data in the cloud. This research aims to come up with practical and efficient methods of enhancing data confidentiality in Instant Messaging applications using the Advanced Encryption Scheme (AES) block cipher. Based on the results of this research, an Instant Messaging system will be developed to showcase how these results can be used in a real-life application.

Keywords: Data security, Instant Messaging (IM), End-to-end-encryption, Advanced Encryption Scheme (AES)

Contents

1. Background/Introduction

Background Information

Instant Messaging (IM) technology is a type of online chat that offers near real-time message transmission over the Internet through a stand-alone application or embedded software. Instant Messaging first appeared on multi-user operating systems in command-line interface systems like Compatible Time-Sharing System (CTSS) and Multiplexed Information and Computing Service (Multics) in the mid-1960s and was used as notification systems for services like printing, but quickly changed to being used to facilitate communication with other users logged into the same machine. Some of these systems such as ntalk and ytalk used peer-to-peer protocol while others such as talker and IRC used client-server network architecture.

Modern-day, GUI based messaging clients gained popularity in the mid-1990s with PowWow, ICQ, and AOL Instant Messenger. In the 2010s, social networking and social media services such as WhatsApp, WeChat, Facebook gained traction and also incorporated Instant Messaging as one of their key features. This enabled them to gain popularity and slowly replace instant messaging applications such as AIM.

In a bid to ensure user privacy, data integrity, and law compliance, instant Messaging applications employ several security features, one of them being end-to-end-encryption (E2EE), but they still have some drawbacks.

In November 2014, the Electronic Frontier Foundation listed seven security measures that Instant Messaging platforms should employ, they include:

- Having communication encrypted as it is being transferred from the sender to the recipient

- Having communication encrypted with keys that the Instant Messaging service provider does not have access to. This can be achieved by end-to-end-encryption
- Enabling users to independently identify their correspondent's identity
- Ensuring that previous communications are secure even if the encryption keys are stolen
- Providing the system's source code open to independent review
- Having the software's security designs well-documented
- Having a recent independent security audit.

Despite all these security measures, there are still some loopholes in the security of data in Instant Messaging, most importantly, end-to-end encryption (E2EE).

Common problems facing end-to-end encryption (E2EE)

End-to-end encryption (E2EE) is meant to ensure the confidentiality of data sent from one endpoint to another in an Instant Messaging environment. For instance, when two people send messages to each other via Instants Messaging, only them (the sender's and receiver's devices) should be able to decrypt these messages. However, some drawbacks undermine the integrity of end-to-end encryption, they include:

a. Unencrypted cloud backups

Some Instant Messaging services offer backups on the internet, so in case the user loses their device, they can restore all of their data. However, these backups are usually stored in cleartext, which means that they are not always encrypted. This effectively undermines end-to-end encryption. An attacker who succeeds in attacking the service provider can have access to all the unencrypted backups.

b. Vulnerable endpoints

Smartphones are less secure than desktop computers. These smartphones usually contain all of your messages in cleartext, so an attacker can simply read all of your messages by attacking your smartphone. This is a weakness that is easy to exploit. Intelligence services and police departments take this approach due to the ease of breaking into a smartphone.

c. Insecure encryption algorithms or implementations

Some Instant Messaging services implement custom self-developed encryption algorithms because sometimes the National Security Agency undermined AES and RSA, so they have to use “no-name algorithms” in order to stay secure. The golden rule is to only use publicly-known and audited algorithms.

However, focusing on algorithms isn’t enough. A product cannot be deemed to be secure if it uses “AES-256”, “RSA-4096” or some “military-grade encryption”. The actual implementation of algorithms is what matters.

d. Personal data and metadata on servers

Some services store most of your personal data on servers out of your control in cleartext. For example, XMPP servers store all of your contacts, group memberships and other information in cleartext even if you are using end-to-end encryption. Furthermore, admins can monitor whether your device only received a certain message or if you actually read this particular message. On the other hand, Signal keeps most data on the devices to avoid disclosure to servers.

Proposed Encryption Method

The proposed solution aims to solve the problem by offering both local and server-side encryption using the Advanced Encryption Scheme (AES) block cipher.

2. Problem Statement

Despite Instant Messaging being so popular and several measures such as end-to-end-encryption being taken to guarantee its data security, it still has some weaknesses. This is because most of the effort has been placed in maintaining security and accuracy of data that is being sent by the sender to the recipient and vice versa, compromising on other areas such as the end points; user information being stored in their mobile phones and backup in the cloud. From a research by Megan Squire (2017), she found out that if someone can gain control of a device, they can read the messages without needing to decrypt them. This project proposal addresses these security concerns and seeks to build an application with stronger security features that address all of these problems.

Case Study

Direct communication between students and lectures outside class has always been a challenge. The current system is in such a way that, outside class, the lecturer communicates with the students' class representative, who in turn sends the message to the other class members. Being human, the class representative might forget to convey the message to the class members or due to incomplete understanding he/she may give out partial or inaccurate information to the other class members. Also, some students take time to grasp some of the concepts that they have been taught in class, mostly because they are slow learners or the concept was too complex to be understood in a single lesson. This normally leaves them in a state whereby they cannot ask the lecturer any question because they do not know exactly what to ask, or in other terms, they do not know exactly what it is that they have not understood. This forces the students to go and read those concepts again during their free time so that they can understand them. When they get stuck and need to ask the lecturer a question, they have to wait till the next lesson, which in most cases will be the next week. This is made even tougher in cases whereby the lecturer is yet to send their notes to the students. Shy students may also have difficulty in asking the lecturer questions while in class. This makes them seek help from their fellow classmates who do not have a good understanding of the topic like the lecturer.

To solve the above problem, a system that would simplify and enhance direct communication between the students and lecturers needs to be developed. The system will have a messaging platform that will enable students to ask lecturers questions, outside class hours, pertinent to what the lecturer is teaching them. It will also provide the lecturers with a platform that will enable them to send class materials such as notes and assignments to their students, and enabling the students to download and view those documents. The system will have two main modules, the student module and lecturer module.

2.1Research Questions

The research aims to answer the following questions:

- What would be the most efficient Advanced Encryption Scheme (AES) key size to use?
- What are the drawbacks of the Advanced Encryption Scheme (AES) and how can they be solved?
- What is the most efficient way of implementing the proposed solution in an application?

2.2Research Objectives

The general objective of the proposed system is to improve data confidentiality in Instant Messaging applications.

The research is expected to achieve the following specific objectives:

- To find the most secure Advanced Encryption Scheme (AES) key size to use
- To come up with effective solutions to any limitations of the Advanced Encryption Scheme (AES)
- To come up with the most efficient way of implementing the Advanced Encryption Scheme (AES)

2.3Scope

The research will be focused on the use of Advanced Encryption Scheme (AES) block cipher to encrypt and secure data in an Instant Messaging system. The end result will be the development of an Instant Messaging application that applies the proposed methods to secure its data.

3. Justification

User data needs to be secure both while in transit and while at storage. This project research seeks to improve security of data in Instant Messaging applications by using the Advanced Encryption Scheme (AES) block cipher to secure data while at storage. Mostly in the user's mobile phone, where the data is usually stored in cleartext, making it vulnerable for attacks from malicious people such as hackers. This project research is to benefit users of Instant Messaging (IM) services by providing more security features that will ensure that their data is safe at all times and not vulnerable to attacks from malicious people.

4. Literature Relevant to The Proposal

According to a research (Squire, 2017) concerning the Central Intelligence Agency's (CIA) hacking tools, it was highlighted that if someone can gain control of a mobile device, they can read the messages without needing to decrypt them. This is due to the fact that most messages in mobile devices are stored in cleartext, without any encryption whatsoever, leaving them vulnerable to attacks from hackers. However, with the proposed solution, this will not be possible because the messages will be encrypted before they are stored and the private key hidden safely within the application. Also, by applying code obfuscation (M. Ceccato, 2009), my code will be encrypted, making it difficult to understand, hence preventing man-at-the-end attack and deterring reverse engineering. This will ensure maximum security for the user's private key.

In a research carried out on the limitations of end-to-end encryption (Jakub, 2018), it was discovered that some Instant Messaging service providers who offer backups over the internet, usually store the backed up data in an unencrypted form, due to their algorithms of generating the users' private keys being mobile phone dependent. Meaning if the user changes their mobile phone, they will be given a new private key hence making it impossible to decrypt the backed-up data. The storage of unencrypted backup messages effectively undermines end-to-end encryption. If an attacker manages to attack the service provider, they will gain access to all the unencrypted backups. With the proposed system, however, this problem will not be there since the method of generating the private keys will not be machine-dependent, but user account-dependent. This will ensure that the users' messages are always encrypted regardless of the place where they are being stored.

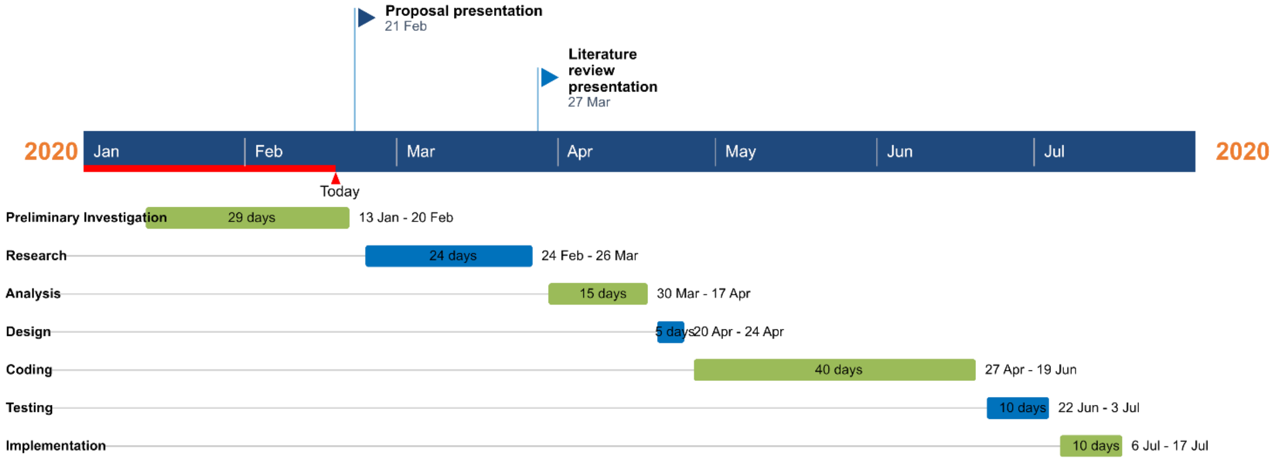
Another weakness of the existing encryption methods as was discovered in a research (Gaber, 2018) was that most systems that have been hacked usually use insecure encryption algorithms which are normally caused by the systems implementing their own custom, self-developed encryption algorithms, which are not implemented correctly. Focusing on algorithms is not enough. A product may use ‘military-grade encryption’ but if the implementation of those algorithms is not correct, the overall security of that product can never be guaranteed. The proposed solution will not have these flaws since it will have implemented the Advanced Encryption Scheme (AES) correctly and accurately.

5. Research Methods and Design

The following research methods will be used to come up with some of the system requirements:

- Secondary Data Analysis – the aim is to go through several books, more so those that have information on data security, to know which security measures to apply, so as to ensure that the system is as secure as possible.
- Experimental research – this will be used to determine ways of implementing the desired feature, how successful implementation is and any weaknesses to be worked on.

6. Schedule



7. Budget

Item	**Description**	**Amount (KSh)**
Data Bundles	To be used for research and development of the proposed system	1500 per month * 6 months + 9000
Total		9000

8. Conclusion

Instant messaging (IM) is a very useful tool for communication. Data confidentiality in IM systems should therefore be a priority. Several approaches have been taken to enhance that levels of data confidentiality in these systems, but there still exits some weak points. These include storage of cleartext messages both locally in the mobile device and in the cloud as back up. The proposed solution aims to improve data confidentiality by using the Advanced Encryption Scheme (AES) to encrypt and decrypt these messages, hence making them inaccessible to unauthorized parties such as hackers.

References

1. Tom Van Vleck. "Instant Messaging on CTSS and Multics". Multicians.org. 2012-05-11 http://www.multicians.org/thvv/mail-history.html
2. "Secure Messaging Scorecard. Which apps and tools actually keep your messages safe?". Electronic Frontier Foundation. 4 November 2014. https://www.eff.org/node/82654
3. Morris C, Scott RE, Mars M, Department of TeleHealth, University of KwaZulu-Natal, Durban, South Africa, Stud Health Technol Inform. 2018.
4. Squire M, (2017), End-to-End Encryption Isn’t Enough Security, The Scientific American
5. Jakub, (2018), Limits of end-to-end encryption, InfoSec Handbook
6. Padlmpky, Snow and Kager, 2008, Limitations of End-To-End-Encryption in Secure Computer Networks, Deputy for Technical Operations Electronic Systems Division Air Force Systems Command United States Air Force
7. M. Ceccato et al., "The effectiveness of source code obfuscation: An experimental assessment," 2009 IEEE 17th International Conference on Program Comprehension, Vancouver, BC, 2009