A Secure Framework For Messaging on Android Devices For Honey Encryption

V.Hima Bindu[1], D.Amrutha Valli[2]
[1, 2] COMPUTER SCIENCE AND ENGINEERING
[1, 2] G. PULLAIAH COLLEGE OF ENGINEERING AND TECHNOLOGY

Abstract- *The different encryption techniques can be used for the security to transfer messages over unsecured network. Yet the hackers can hack these messages using different hacking methods. Hence to avoid these kinds of attacks and to provide a secure network, we use the encryption techniques. For android based devices, the target proposed approach is to flourish a secured network using honey encryption. Honey encryption uses symmetric key cryptography techniques which prevents the messages from brute force attacks. This paper shows how to integrate honey encoding with Blowfish and AES algorithms and compare their performance. Blowfish with honey encryption technique produce efficient result when compared with the other.*

Keywords- Blowfish, Honey Encryption, AES, Messaging communication.

I. INTRODUCTION

Messaging and their services are playing a pivotal in the world today. As they are used in innumerable applications like mobile banking, gmail, healthcare, etc. Confidential information is sent through messaging services by the users. The information that is sent through messaging is stored in messaging centre and it can be seen and modified by network provider staff. Thus it is not an appropriate communication media. The information can be hacked without effort from messaging centre and can be modified. There are at least four security constraints in message security as shown below:

II. INTEGRITY

It prevents from unauthorized parties can alter the information like deleting, writing and creating files. The encryption of the information can be done in two ways. They are:

- Secret Key Encryption Systems
- Public Key Encryption Systems

1. Secret Key Encryption

Encryption and decryption process is done through single key. This secret key should be available to all the members those are involved in the communication. If the key is hacked then hacker can decrypt and read the messages. for example AES,DES etc., AES encryption of the message is done using single key and requires more processing when compared to others. It is highly secure and its configuration is complex.

DES is a block cipher type. It provides confidentiality to the messages that are sent to a great extent.
It is unsecure to use DES as it is Short Length Key and can be easily broken.

2. Public key encryption

Encryption and decryption process is done through a pair of keys. The message that is encrypted by others can be decrypted by any one of the key.One of the key must be kept secret so that the communication is secure and one of the key is used as public key and the other is used as private key.

III. MESSAGING COMMUNICATION ATTACKS

The network has several messages that are to be travelled. Each message may undergo several types of attacks. Some of the attacks are:

- **Man in the middle attack**

The attacker relays and alters the messages that is being communicating between two parties. The two parties assume that communicating directly with each other but in the middle eavesdropper is intercepting their messages and they are been altered. Attacker acts as a proxy who is been able to add, delete and modify the messages.

- **Brute force attack**

A brute force attack is a major threat that is faced by the web users today, where the attacker tries to capture the password with all possible combinations of letters, digits and symbols. Almost all the people keep the dictionary words as their password which helps the attacker to guess the password. It is a time and resource consuming process, the attackers uses some tools and software's to hack the secret information. The alternate name for this attack is "dictionary attack".

- **Side channel attack:**

A side channel attack is any attack based on information gained from the physical implementation of a computer system rather than weakness in the implemented algorithm itself examples: cryptanalysis, software bugs. Timing data, power utilization, electromagnetic releases or even sound can give an additional wellspring of data, which can be misuse the frame work. Some side channel attacks require technical knowledge of the internal operation of the system. Many side channel attacks are view of factual techniques spare headed by Paul Kocher.

- **Impersonation attack**

Impersonation attack is an active attack in which attacker acts as the character of authenticated user. Practice of pre-texting as another person with the goal of obtaining information or access to a person, company, computer system is defined to an impersonation. Attacker gets the privileged information by various methods. Attackers get the password by just reading it once on the camera, dictionary words also help to get the password. Sometimes attacker attack on the computer and monitors the history and saves passwords to gain access to the user account.

IV. PROBLEM IDENTIFICATION

As studied various research papers based on the messaging security and found various security threats and problems in messaging communication. We need to solve them and improve the system performance. The major problems identified in the traditional approaches are as follows:

- **Desktop implementation:**

Honey encoding approach needs to be implemented in the android based devices for messaging security against brute force attack as it exists on the desktop bases messaging system.

- **Time consuming:**

AES encryption technique which has more complex rounds requires more processing time to display the result when it is used with honey encoding. Android based mobiles are not advised to use AES for messaging as they need immediate response.

- **Single level security:**

Single level encryption algorithm is provided to the messaging application to the existing system in a single level security. Attacker can easily guess the key and hack the message, so more security is needed.

V. BACK GROUND

1. Honey Encryption:

Honey encryption is a useful encryption technique which is developed by Ari Jules and Thomas Ristenpart .Honey encryption is a type of data encryption that produces cipher text. When it is decrypted with wrong key by the attacker, presents a plausible-looking yet incorrect plaintext password or encryption key. It pivot on encoding and decoding scheme which is introduced in cryptography conference. It is used with the conventional encryption technology, which make it difficult to distinguish the output message whether it is true or fake.

Operation On Honey Encryption:

The drawback of systematic password based encryption can be recovered with low entropy passwords, Juels and Ristenpart introduced honey encryption. The idea to encrypt the plaintext X with the password Kpand the decryption of cipher text results in plausible looking plain text X' with wrong password kp'. A distribution transforming encoder (DTE) is used for encoding and decoding of message as bit string, denoted DTE=(ENCODE,DECODE).in brief, overall process is

HE[DTE,Sym.E]=(henc,hdec),

where Sym.E is conventional symmetric encryption . The ciphertext C=henc(kp;X)and decryption works X=hdec(kp;C)

2. Distribution Transforming Encoder (DTE)

Suppose p be a probability distribution over the original message space XS, meaning that a user selects X belongs to XS for encryption with the probability p(X).A DTE encoder X as an n-bit seed S as belongs to {0,1} power n or we can say that S ϵ {0, 1}n. That is the original message encoded into seed space S. One message may be appointed by many seeds belongs to S from which the encoder selects one such seed uniformly at random. At the receiver side, inverse process of encoding is happened for generating the plaintext from the corresponding seed value, which is known as decoding. In other words, given S, we can decode through the inverse DTE decode (S)=X, which returns seed space S's individual corresponding message. With a DTE that gives strong security, decode accurately generates p. In this case selecting S evenly at random from {0,1}n and decoding to obtain X=decode(S) return approximately the original X. In other words, DTE is a fine model of message distribution.

3. AES

The Advanced Encryption Standard (AES), is a symmetric cipher which is widely used for data encryption and decryption .it is six times faster than triple DES.AES is a block cipher and take 128bit block of input data for encryption and decryption. In this algorithm mainly 3 different size keys used for encryption so it comprises of three block ciphers:AES-128,AES-192 and AES-256.Each cipher encrypts and decrypts data in blocks of 128 bits using keys of 128-,192- and 256- bits, respectively. AES is a secret key algorithm so it uses same key for encryption and decryption.
Working

First the plaintext block is put into an array then the processed data in number of rounds repeatedly to transform it, the figure of rounds is manifested by the key size. For key length 128 bit, 192 bit and 256 bit it takes 10 rounds, 12 rounds and 14 rounds respectively.

VI. PROPOSED METHODOLOGY

The below given are the phases present in this methodology

Phase 1: Registration

1) Firstly user registers by providing credentials who is participating in message based communication.
2) Alongside other credentials the device's IMEI number which is registered should be stored on the server.
3) Before communication an appropriate key is provided to the user which should be invaded in the authentication procedure.

Phase 2: Secure message communication using honey encryption

1) The message which is in the form of plain text uses distribution transforming encoder (DTE) to encode and decode the text as bit string.
2) The entropy of the message is high in the present case. In the information theory the uncertainty of information is measured as entropy .The entropy is high because the message is of variable length.
3) By using Statistical coding scheme (SCS) the messages are encoded. The code table in this scheme is Cumulative Massive Function (CMF) and CMF of nth character of the message is given as:

$$F_{cmf}(c_k)= \quad (1)$$

In the equation above n is the Markov process order and S is the possible character set number in the code table. In the above equation xi= cj ǀXi-1:i-n shows that the near n-1 character influences the ith character of message. Based on the incidence of appearance probability of each character is adjusted by calculating according to the frequency of appearance.

4) According to SCS a code table is constructed and to encode and decode the messages it is shared between sender and receiver.
5) By using the Blowfish encryption the decoded or encoded message is again encrypted. Both the sender and the receiver share a public key. The public key is the one which is used in encryption/decryption process.

Phase 3: Prevention of Brute force attack

1. In case of a brute force attack to generate plausible looking text the N-Gram model is used.
2. An N-Gram string is generated for every unauthorized authentication attempt in order to confuse the hacker. This can be done when a device with unauthorized IMEI number is detected by the server during the communication process.
3. Using open NLP tools and by combining the synonyms and antonyms for the words in the messages the N-gram is constructed. An alternative from the word replaces the punctuation word in a predefined dataset. And the antonyms and synonyms replace a noun if present.

VII. PROPOSED MESSAGING APPLICATION IN ANDROID

We use the android studio tool and the java language to code the concept in order to implement the proposed methodology. By using honey encoding technique the plain text which is considered as input is encoded to produce the encoded text .Then a produced text is cipher at the sender side by using a secret key algorithm to encrypt the encoded text. At the receiver side by using the same symmetric cipher and the shared secret key the cipher text which is received is first decrypted to produce the encoded text. Then the honey decoding process decodes the encoded text to consruct the native message. Distribution Transforming Encoders (DTE) are used at the encoding phase to produce the text which is intermediate and which looks plausible. Here we use N-gram concept for Distribution Transforming Encoder. We use open NLP-tools to generate N-grams. With an optional separator the N-Gram is generated with the class used in N-Gram generator class and a list of n-gram strings are returned.

VIII. EXPERIMENTAL ANALYSIS

In our experiment a single android device is treated as both the sender and the receiver which is known as a simulated approach of the messaging system. The figure to show the output of messaging is given as

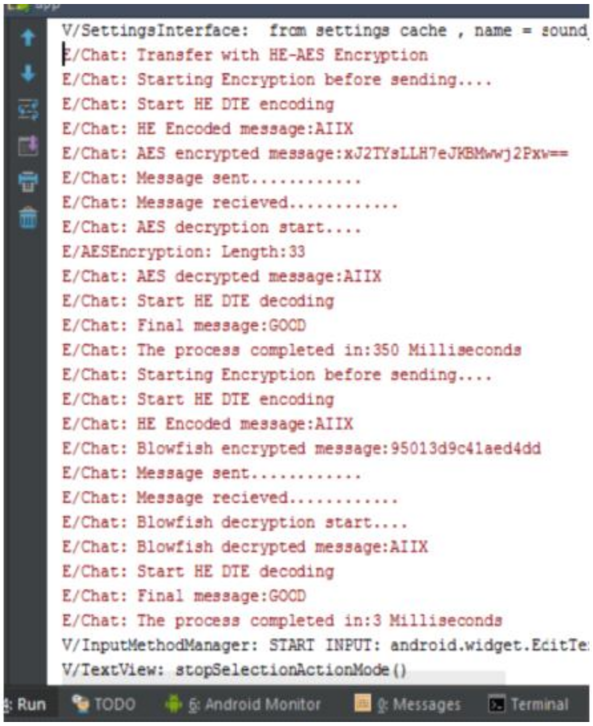
Figure 1. Messaging Screen

Honey Encoding and the Encryption process occurs at sender side when we send a message. We calculate the processing time by applying AES algorithm with honey encoding. Then we calculate processing time for the same input message by applying Blowfish algorithm with honey encoding. When we compare Blowfish with HE and AES with HE, Blowfish with HE takes less time. So in the android devices Blowfish with HE will be the secure messaging communication.

Hence by using honey encoding and Blowfish respectively problems like brute force attack and more processing time can be reduced.

Table 1. Execution Time Example

	HE_AES (Execution Time in millisecond)	HE_Blowfish (Execution Time in millisecond)
34	350	4
58	450	4
50	350	3
114	950	12



```
V/SettingsInterface:  from settings cache , name = sound
E/Chat: Transfer with HE-AES Encryption
E/Chat: Starting Encryption before sending....
E/Chat: Start HE DTE encoding
E/Chat: HE Encoded message:AIIX
E/Chat: AES encrypted message:xJ2TYsLLH7eJKBMwwj2Pxw==
E/Chat: Message sent............
E/Chat: Message recieved............
E/Chat: AES decryption start....
E/AESEncryption: Length:33
E/Chat: AES decrypted message:AIIX
E/Chat: Start HE DTE decoding
E/Chat: Final message:GOOD
E/Chat: The process completed in:350 Milliseconds
E/Chat: Starting Encryption before sending....
E/Chat: Start HE DTE encoding
E/Chat: HE Encoded message:AIIX
E/Chat: Blowfish encrypted message:95013d9c41aed4dd
E/Chat: Message sent............
E/Chat: Message recieved............
E/Chat: Blowfish decryption start....
E/Chat: Blowfish decrypted message:AIIX
E/Chat: Start HE DTE decoding
E/Chat: Final message:GOOD
E/Chat: The process completed in:3 Milliseconds
V/InputMethodManager: START INPUT: android.widget.EditTe
V/TextView: stopSelectionActionMode()
```

Figure 2: Execution Time Chart with Honey Encryption

Using our proposed methodology we develop a messaging application then the steps for encoding and encryption are followed. A message screen appears to the user when the application is executed in an android device like smart phone. When the user types a message and sends then

Step 1: With the honey encoding the message is first encoded and then the encoded text.

Step 2: The produced text is cipher when the encoded text is encrypted with the AES algorithm. And the produced cipher text is sent to the receiver. Then the encoded text is produced when the cipher text is decrypted with the AES decryption algorithm at the receiver side. Then using the honey decoding scheme the decoded text obtained from encoded text to give the plain text. Then overall processing time is calculated and AES Blowfish time is displayed in millisecond on the android monitor screen.

Step 3: Here the encoded text is produced when the same message in step1 is encoded with honey encoding.

Step 4: The produced text is cipher when the encryption is done with the Blow fish algorithm to the encoded text and the cipher text is sent to the receiver. At the receiver side with the Blowfish decryption algorithm the cipher text is decrypted to encoded text.The decoded text is obtained from the encoded text to produce the original plain text using honey decoding scheme. Then the overall processing time is calculated and the HE Blowfish time is displayed in millisecond on the android monitor screen.

The Blowfish produces the best results with HE since it takes smaller processing time compared to AES with HE. The above process is be visible in the output screen of android monitor as follows:

REFERENCES

[1] Joo-Im Kim and Ji Won Yoon “Honey chatting: a novel instant messaging system Robust to eavesdropping over communication”, Center for Information Security Technologies (CIST) Korea University, Seoul, Republic of Korea IEEE 2016 ,fjooimkim, jiwon_yoong@korea.ac.kr

[2] Joseph jaeger,Thomas Ristenpart & Qiang tang, “Honey encryption beyond message recovery security” , Eurocrypt, 2016.

[3] Ari Juels, Thomas Ristenpart “Honey Encryption: Security Beyond the BruteForce Bound” EUROCRYPT 2014

[4] Navin Tyagi, Jessica Wang, Kevin Wen, Daniel Zuo “Honey Encryption Application”, Computer and Network Security, Spring 2015

[5] G. Sowmya, D.Jamuna, M.Venkatakrishna Reddy, “Blocking of Brute Force Attack”, International Journal of Engineering Research & Technology(IJERT), ISSN:2278-0181 Vol. 1 Issue 6, August2012

[6] Nahri Syeda Noorunnisa1, Dr. Khan Rahat Afreen ”Review on Honey Encryption Technique” International Journal of Science and Research (IJSR) ISSN : 2319-7064, 2015-16

[7] Ankita Verma1, Paramita Guha , Sunita Mishra, “Comparative Study of Different Cryptographic Algorith ms”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 5, Issue 2, March - April 2016, ISSN 22786856

[8] Neetesh Saxena ,Narendra S. Chaudhary “EasySMS: A Protocol For End-to-End Secure Trans-mission Of SMS” IEEE Transactions OnInformation Forensics And Security, Vol. 9, No. 7,July 2014

[9] P. Princy “A Comparison Of Symmetric Key Algorithms DES, AES, BLOWFISH, RC4, RC6: A Survey” International Journal of Computer Science & Engineering Technology ISSN : 2229-3345 Vol. 6 No. 05 May 2015

[10] Priyanka Chouhan, Rajendra Singh,” Security Attacks on Cloud Computing With Possible Solution”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, January 2016

[11] Varsha S. Bari1,Nileema R. Ghuge,Chaitali C. Wagh,Sayali R. Sonawane ,Mr.M.B. Gawali“, SMS Encryption on Android Message Application”, IJARIIE-ISSN (O)2395-4396 Vol-2 Issue-2 2016