Enhanced Email Authentication

Imtiyazul Haq[1] and Dr. Jitendra Nath Srivastava[2]

M.Tech, Computer Science, Invertis University, Bareilly, India

Professor, Department of Computer Science, Invertis University, Bareilly, India

Abstract: A numerous efforts have been done in the field of email to make it more secure. More than twenty years' public key cryptography has been used to communicate through secure channel. As we know day by day the hackers/intruders increasing rapidly to breach one's authenticity. Hence it become necessary to keep information more confidential. In the age of digitization, it is hard to make secure communication because intruders monitor each action of user to collect some of our confidential information i.e. business, account information etc. Nowadays, we are using only one layer (username and password) that is not enough to keep one's secret information. Thus, we are going to introduce two layer that uses voice recognition to overcome the current problem.

Keywords: PEM, S/MIME, PGP, Key logger attack, Brute force attack

I. INTRODUCTION

Email system is very commonly used application because ease of its simplicity one can utilize. This technology has revolutionized the communication we make today. Its usage increased extremely in the last few years and number of users globally joined this technology. The prevalent use of email caused the number of ominous being made about the dark side our technological revolution to increase and we are becoming uniquely vulnerable to many mysterious and malicious threats. Worms, viruses and other type of malicious software targeting our email inboxes too propagate. Phishing and other forms of fraud attacks have been using email as their primary communication channel to trick users into giving out their credentials. Email could have been a killer application for the Internet if none of the problems mentioned above exist.

The authentication play an important role in email because it is the first step to enter one's account. So it become necessary to keep our email authentication more and more secure. Nowadays we are using only one layer authentication i.e. username and password for email technology which is not enough to keep our information secure. Several brute force attacks have been done to breach one's authentication. There are many types of attacks tried by intruders to forge personal information of a user such as shoulder surfing [1], man in middle attack etc.

A. Key loggers attack

This is preinstalled Action of tracking the key struck on the keyboard (user is unaware that there-action is being monitored). Basically, there are two types of key logging software based and hardware based.

a) Software based key loggers

These are software programs designed to work on the target computer's operating system. There are five categories of this key loggers-

I. Hypervisor based

II. Kernel based

III. API based

IV. Form grabbing based

V. Memory injection based.

b) Hardware based key loggers

Hardware based key loggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

Keyboard hardware

Hardware key loggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer and the computer.

B. Biometric based authentication

It is a type of technology enhanced by using cryptography. Biometric technique is becoming very popular because of its simplicity and hassle free use. Actually, its basically used for authentication purpose of individual. Biometric technology uses biometric recognition algorithm [2]. Biometric technology can be classify in two categories i.e. Physiological based technique in which the physiological characteristics of a person are collected such as facial analysis, fingerprint, hand geometry, retinal analysis and DNA etc. for verification purpose and another technique is Behavior based techniques includes signature, key-stroke, voice analysis and measure behavioral characteristics.

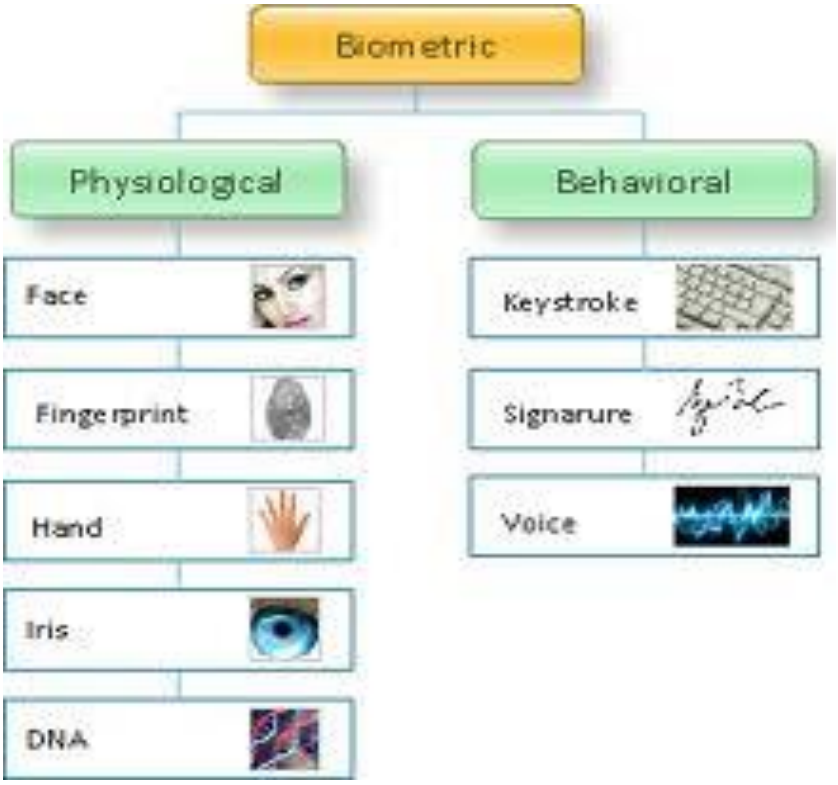

Figure 1. Biometric based recognition [3]

II. RELATED WORK

In the last 30 years, numerous efforts have been made to make secure email possible, if not all over. This section describes brief discussion of the standards, algorithm that were developed.

A. Existing System and Approach

PEM (Privacy Enhanced Mail): In mid-1980, the Internet Activities Board's Privacy Task forced started to develop standards designed to provide end-to-end encryption for email [4]. These standards became known as PEM and they defined a way to provide encryption and signature for ASCII email messages based public-key cryptography using the RSA (Rivest Shamir and Adelman) algorithm.

Using PEM, if Alice wants to send an encrypted message M to Bob then Alice will have to do the following:

1. Encrypt M using Bob's public key K_b public which must be published in digital certificates as defined by the X.509 CCITT standard. After encrypting M, C = K_b public (M) is obtained.
2. Send C to Bob.

When Bob receives C, Bob should do the following:

1. Decrypt C using his private key K_b private which must be stored on his computer. After decrypting C, M = K_b private (K_b public (M)) is obtained.

S/MIME (Secure Multipurpose Internet Mail Extensions):

When MIME (Multipurpose Internet Mail Extensions) was introduced, RSA Data Security re-implemented the PEM concept on top of the MIME standard and called it S/MIME. MIME defines mechanisms for sending other kinds of information in email, including text in languages other than English using character encodings other than ASCII as well as 8-bit binary content such as files containing images, sounds, movies, and computer programs [5].

Because of single root with a single certification policy proved to be problematical in PEM, S/MIME implementations do not implement a strict hierarchy of certificates, but instead accommodates any number of trusted CA (Certificate Authority) [6]. S/MIME these days is integrated into many email clients like Microsoft Outlook, Netscape Communicator, Lotus Notes, and others. However, S/MIME is not integrated into any web-based mail systems like Gmail, Hotmail, Yahoo, etc. On web-based mail systems, S/MIME digitally signed S/MIME messages appear as ordinary messages with an additional attachment name smime.p7s, while S/MIME messages that are sealed with encryption are indecipherable [6].

PGP (Pretty Good Privacy):

In 1991, Phil Zimmermann released a program called PGP that provides cryptographic privacy and authentication for email. PGP uses public-key cryptography (as in PEM and S/MIME) and includes a system which binds the public key to user identities [7]. If Alice wants to send an encrypted message M to Bob using PGP then PGP does the following at Alice's side (denotes concatenation):

1. Generates a shared key K_s.
2. Encrypts M using Ks to obtain C1 = K_s (M).
3. Encrypts M and Ks using Bob's public key K_b public which must be stored in Alice's public key database. After encrypting C1 and K_s, PGP obtains C2 = K_b public (C1|Ks).
4. Sends C2 to Bob.

When Bob receives C2, PGP does the following:

1. Decrypts C2 using Bob's private key K_b private stored on Bob's computer. After decrypting C2, PGP obtains C1|Ks = K_b private (K_b public (C2)).
2. Decrypts C1 using K_s to get M = K_s (C1).

Previous Approach

A few years ago, Ahmed Obied [8] proposed an approach using biometric based authentication. He presented a new email security technique that uses fingerprint recognition to authenticate users and provide them with a transparent process of signing and verifying email messages. The idea is to enroll a user fingerprint, associate the fingerprint with a record that is unique to that user, and

finally use the user's fingerprint and unique record to authenticate the user, sign the user's email

message, and verify other users' email messages. Our approach was implemented as an email client called SEFR.

III. PROPOSED WORK

We have discussed many of existing technologies to email security. The cryptographic techniques in internet is useful only when the process of encrypting and decrypting is transparent. Keeping the amount of user interaction minimum and providing security functionality for users without having them learn a complex new user interface or algorithm is essential.

We present a new approach for email security that uses voice sample recognition [10] to authenticate the users and provide them with a transparent process of signing and verifying email messages. The main idea is to enroll a user voice sample, associate the voice sample with a record that is unique to that user, and finally use the user's voice sample and unique record to authenticate the user, sign the user's email message, and verify other users' email messages.

A. Components

Environment: This approach is designed and implemented on a Pentium processor running Windows 7. The Python language is used to write to code. This approach is implemented using MatLab.

Database and voice samples:

To store the user's account information (username and password), the user's voice sample. We used a MySQL server. The database table contains account information. The account table has the following fields: username (varchar), password (varchar), voice sample (varchar). We have recorded two voice samples through sound recorder using laptop mic.

B. Enroller

In this phase, database, voice template and enroller are required. A database is required to store the user's email account information (username and password), the user's voice template and the hash values of email- sent, so here MYSQL server is used. The user can use mic of laptop or other similar device to record his voice. Enroller play an important role in the registration phase, user have to provide the enroller with their recorded voice template. If both the recorded voice template and dynamic voice sample matches successfully, the user is allowed to send or receive email. In our approach Secure-Hash Algorithm-1 (SHA-1) [9] is used to hash the value of password and voice template. The user want to check if-their email account information and voice template have been already registered or not. In the enrollment phase the enroller takes the username and password and check if a voice template has been already registered if so, then the enroller downloads the voice template and display it to user. If a user want to register using an account that already exists then this email display an error message.

C. Login

Since users tend to forget their passwords or simply use weak passwords that allow an adversary to break into their email accounts, we used a second authentication layer that uses voice sample. By having 2 layers of authentication (knowledge-based and biometric-based), breaking into an email account becomes very difficult. No one will be able to break into an email account on this technique unless he has your account username and password, and your voice sample. Following figure show the Main page for voice recording.

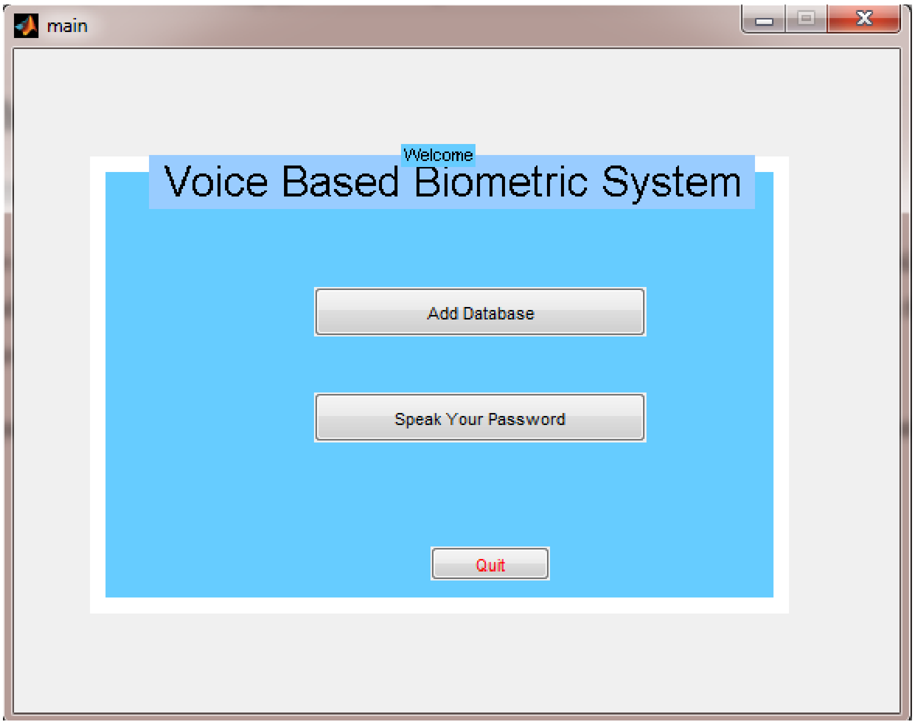

Figure 2. Main page for authetication

IV. CONCLUSION

Public key cryptography has been used for many years to protect email system via encryption and digital signature. But due to technical, social and usability issues it becomes less secure. So, we presented an approach for enhancement of email security. In our approach, we used two layer of authentication i.e. voice sample and knowledge based authentication. This will help from attacks like shoulder surfing, man in middle attack and email spoofing.

Biometric-based authentication has the potential to be the next big thing of the World Wide Web.

Conflict of Interest: The authors declare that they have no conflict of interest

Ethical Statement: The authors declare that they have followed ethical responsibilities

RFERENCES

[1] Viresh Chapte, Yogesh Mali, Grid based authentication system, International Journal of Advance Re-search in Computer Science and Management Studies, 2(10), 2014.

[2] Biometric recognition algorithm, *https://en.wikipedia.org/wiki/Biometrics*.

[3] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller. How to make secure email easier to use. In Proc. of the SIGCHI conference on Human factors in computing systems, pages 701 – 710, 2005.

[4] PEM William Stallings―Cryptography and Network Security‖, 3rd Edition.

[5] RFC 1521, MIMIE, http://www.faqs.org/rfcs/rfc1521.html.

[6] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller. How to make secure email easier to use. In Proc. of the SIGCHI conference on Human factors in computing systems, pages 701 – 710, 2005.

[7] RFC 1939, Post Office Protocol, Version 3, *http://www.faqs.org/rfcs/rfc1939.html*.

[8] Secure Email with Fingerprint Recognitionobieda@cpsc.ucalgary.ca and *http://www.cpsc.ucalgary.ca/obieda*

[9] Secure Hash Algorithm (SHA-1), William Stallings—Cryptography and Network Security, 3rd Edition.

[10] Sukhwinder Singh, Parveen Saini, Hidden Markov Model Based Approach for the Development of Voice Based User Machine Interface, International Journal of Advanced Engineering Research and Applications, vol-1, issue-1, (2015).