ISSN: 2321-7782 (Online)
Volume 2, Issue 4, April 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Improving Security of Password and Classification of Threaten Emails

S. Lavanya[1]
Department of Information Technology
E. G. S. Pillay Engineering College
Nagapattinam, Tamil Nadu – India

P. Suganya[2]
Department of Information Technology
E. G. S. Pillay Engineering College
Nagapattinam, Tamil Nadu – India

E. Elakiya[3]
Department of Computer Science and Engineering
E. G. S. Pillay Engineering College
Nagapattinam, Tamil Nadu – India

E. Vijayavani[4]
Department of Information Technology
E. G. S. Pillay Engineering College
Nagapattinam, Tamil Nadu – India

Abstract: ***The utilization of passwords in E-mail applications is especially fragile because of the possibility of off speculating assaults. In this paper we propose our model S-MAIL for strong computationally secure password using simple conventional encryption technique along with threaten E-mail classification using content inspection mechanism in E-mail application. S-MAIL focused us on a large number of key factors in determining the unnecessary and illegal emails by providing the automatic threaten email detection. In this model we define an idea of equivalence between messages and also additionally portray when passwords are used securely in a message or in a set of messages. More importantly, we demonstrate that typically secure employments of passwords are likewise computationally secure.***

Keywords: password security; conventional encryption; classification; threaten email; content inspection mechanism.

I. INTRODUCTION

Mail, or post, is a method for transmitting information and tangible objects, wherein written documents, typically enclosed in envelopes and also small packages are delivered to destinations around the world. Electronic mail, most commonly abbreviated email and e-mail, is a method of exchanging digital messages. E-mail systems are based on a store-and-forward model in which e-mail computer server systems accept, forward, deliver and store messages on behalf of users, who only need to connect to the e-mail infrastructure, typically an e-mail server, with a network-enabled device for the duration of message submission or retrieval. Even though email systems are well classified and they are possessed with well defined structure, in security aspect they are too weak. Passwords stored in back end don't have more authentications. Hence it might have been hacked.

Passwords and other weak secrets sometimes used as cryptographic keys in security conventions and somewhere else. The utilization of fragile secrets is especially sensitive due to the possibility of offline guessing. In such an attack, information that relies on upon a weak secret is utilized as a part of checking supposition of the values of the frail secret. Passive attacks such as password guessing do not need the interaction with users, so they are not much easy to detect. Brutus attack may be done out after an active attack, based on the exchange of messages in the course of active attack.

The sustained supremacy of passwords over all other methods of authentication is a major discomfiture to security researchers. As technology moves ahead in other areas, passwords tenaciously endure and reproduce with every new web site. Widespread discussions of unconventional authentication schemes have come with no state-of-the-art answers.

E-mail has zero cost when sending large volume of email resulting in illegitimate email overwhelming the vast majority of the email traffic. There is no pre-processing and restrictions on incoming mails. Things that are those associated with spam makes use of email to send group of unwanted advertisements to make influence over individuals to buy products that will generate revenue. Other actors, such as phishing utilizes email as a means to gain personal information. Even though other factors use email as a medium to get right to make use of computer networks with susceptible information or to interrupt network operations.

Previous researches on E-mail security has been focused on techniques to detect and prevent malicious E-mail receiving at user's inbox [1]. There are approaches ranging from simple filtering techniques to complicated machine learning algorithms. Most deployments of email filtering have been focused to address spam and phishing. But there is very little research on filtering methods applicable to threatening E-mail received in large enterprises, government sectors wherever authentication is considered.

In this paper we have addressed the shortcomings of previously identified problems by using efficient cryptographic techniques on password and classification of threaten E-mails by using data repository that has a collection of obvious threaten words used. Since all S-MAIL actions are rule based decisions as configured in the threaten email module, uniform processing for finding threaten contents is obtained and guess works are completely eliminated.

II. Related Work

A. Password Systems

Many approaches have been proposed in the security aspect for the management of password. One of the methods is to use centralized, trusted authentication services, such as Microsoft's Passport initiative [4]. In this the users have to log on to the services using a password and are then authenticated to web sites. But the approaches have met little sensation. First, they need technical changes on the part of every site that uses them for authentication. Second, users have been aware about placing much confidence and susceptible information under the control of a centralized system. Security of passport has been investigated. Password Safe application takes the approach of letting users to select their own password and then store it in the place where safety is assured. It stores the passwords and other sensitive data in an encrypted database on the user's machine, secured with a master password. Lucent Personal Web Assistant (LPWA) [5] assigns permanent passwords for every service that can be computed whenever they are needed. It works as an proxy server that users access with a master username and password. PwdHash by Ross et al., applies hash-based technique on the client side. It acts as a web browser plug-in, flawlessly swap values submitted via site password fields with hashes of those values and the site's domain name. Its purpose is to afford a protection against "phishing" or "spoofing" attacks by linking site passwords to the domain name of the server.

B. Filtering of E-mail

Approaches based on authentication for filtering email has been devised to validate that an email was sent using a legitimate path for the advertised domain name and to ensure that the domain name has not been spoofed by a malicious actor. This happened very earlier in the email transmission when a sending email server connects to a receiving email server. This type of filtering directs to a response like the email can either be accepted or rejected based on the authentication result. Sender Policy Framework (SPF) [6] and Sender-ID by Wong and Schlitt and Lyon and Wong describe the methods for domain authentication. Both rely on the sending system publishing valid email server records in the Domain Name System (DNS). The receiving system is then able to verify that an email advertised as coming from a particular domain actually came from email servers authorized to send email on behalf of that domain. SPF and Sender-ID are very similar in approach and remote Internet Service Provider). The difference between CSV and SPF /Sender-ID results in a different approach for handling spoofing. With CSV, it is necessary to make sure that the server is sending email and spoofing controls have to be handles on the server side. With SPF/Sender-ID, it requires to ensure that the sending IP address is valid on the receiver side. DomainKey mechanism [9] described by Delaney, Allman et al.., Leiba and Fenton influence a public/private key cryptographic where the sending email server signs the email with

a private key and the receiving email server validates the signature by retrieving the public key. It is same like SPF/Sender-ID in that Domain Keys legalize that the server is authorized to send email for a domain advertised in the From email headers. Other authentication approach Single-Purpose Address (SPA) described by Ioannidis and Trustworthy Email Addresses (TEA) [7] described by Seigneur et al. uses a cryptographic based email address. Policy in SPA uses an expiration date and authorized senders who are allowed to use the SPA. And it is done at the receiver. TEA is a challenge-response authentication scheme which uses hashing mechanism to authenticate that a new received email is being sent from the correct email server. A threat member could register a new domain, and outfit it with the suitable authentication capacity and then send threaten mails from that domain.

III. PROPOSED WORK

The main objective of this paper is to provide security of passwords and to classify threaten emails from bulk emails. After reviewing the strength and the weakness of each and every method we propose a new methodology in encryption and decryption of password and classification of emails based on simply matching the words stored at the backend. The major strength of SMAIL is high security of password and greater efficiency in classification of emails.

A. Proposed Methodology

S-MAIL deals with security issues. Encryption plays a major role in security. User's password should be confidential. To save it from being hacked, enhanced encryption is provided. The password is encrypted using Classical Encryption Techniques and it is stored. Enhancement is provided in number of rounds of encryption. The techniques used for encryption are:

- Substitution
- String Twister

The above techniques are applied on password in random manner to provide extra encryption. This strategy adds more security on confidential information. This minimizes and eliminates the possibility of tracing passwords. Because hacker can't guess which particular algorithm is followed and the rounds of encryption.

B. Encryption Procedure

The encryption procedure involved in password management is as follows:

1) Use Substitution method on the password.
2) Split each character from the resultant word.
3) Find the ASCII word of 7 bits for each and every character separately.
4) Convert the 7 bit integer into 8 bit integer.
    a. Store an ASCII of 7 bits of an word in a integer array.
    b. Pick the first bit of forthcoming ASCII of the array.
    c. Suffix the first bit with the present ASCII of 7 bits.
    d. Iterate it till the last array item.
    e. Suffix the rest of the bits of last array item with zeroes.
5) Convert the 8 bit integer into hex code.
6) Find the middle character of the resultant string.
7) Swap the two halves based on the centre character.

In Step-1, substitution is used. In Step-7 & Step-8, String twister is used.

Substitution makes use of the file stored for reference. Data have been entered in the file such that for all possible characters that includes alphabets for both lower case and upper case, numerals, special characters are present in two columns but in random manner. First column indicates the character received as user entry and the second column indicates the character to be placed instead of the received one.

After performing account origination, the work of this encryption method starts. The user's password is encrypted in above described format and it is stored as backup. Each time the user needs the password for logging in, the password is retrieved in encrypted form itself then the reverse process of above stated encryption procedure is applied.

C. Decryption Procedure:

The decryption procedure is as follows:

1) Swap the two halves based on the middle character.
2) Convert the hexa decimal code to 8 bit integer.
3) Convert the 8 bit integer into 7 bit integer.
    a. Trim out the zeroes added in suffix part of integer string.
    b. Pick out the number of integer bit strings from previous string stored and prefix them with the forth coming string.
    c. Iterate the statement 'b' of 3rd step for whole array of strings.
    d. Form all the 7 bit strings.
4) Find the character format specification for all ASCII bit strings.
5) Change it to string format.

Outcome of 5th step of the decryption procedure is the password which was entered by the end user initially.

String Twister method that offers well suited encryption that can't be guessed by hacker because the procedure involved in this module hasn't been implemented yet anywhere. This is our own logic that has been present in our S-MAIL system that adds more features in security aspect.

D. Threaten Mail Supervision

This is the core part of our project which provides more security to our S-MAIL system. Threaten messages that are received in the form of mails are identified easily just by a server request. This deal with highly authenticated security check which involves in detecting emails contained threaten messages. This has two main things to be done.

- Threaten email identification
- Threaten email classification

E. Threaten Email Identification:

This is one of the interesting parts in our S-MAIL system. This identifies and supervises the incoming emails and their contents. This is the decision maker part which is embedded with collection of threaten words stored over the database at the back end. This purely deals with the message contents of the mail. This may include:

- Sender's id
- Subject of mail
- Content of mail
- Stored content of S-MAIL's threaten part

As above stated, each and every word of the received mail content is checked for finding threaten messages. The mail's subject part is also checked.

Procedure Involved in identifying threaten messages:

1) The received email is noted and monitored by S-MAIL system.
2) The 'subject' and 'content' are highlighted for security check.
3) Each and every word are picked out of the mail and they are compared against the list of threaten words stored in the file which acts as backend.
4) If any words are matched with the list of words stored, a count variable initialized previously gets incremented.
5) Above stated 4th step is iterated till the last word found in mail.
6) When the count variable exceeds a certain value, the mail is identified as threaten.

The above stated procedure is followed for every incoming email. There is no work allotted for user here, because all the works are implicitly done by our S-MAIL system. After performing the 'Identification of Threaten Email', the S-MAIL system routes to 'Threaten Email Classification' part.

F. Threaten Mail Classification

This classification procedure of threaten email deals with directing the threaten mail to a separate mailbox. After checking the mail contents, S-MAIL gives assurance in deciding the storage area for the particular security checked mail.

This module will start working as per the output of 'Threaten Email Classification' module. If the mail is found as threaten, it is sent to 'Threaten' partition. Otherwise it directs the mail to be stored in 'inbox'.

IV. RESULTS

Our methodology uses the Substitution and String twister techniques for encryption and decryption to provide more security over passwords. Moreover it classifies the threaten emails based on the matching of words in content and subject with the collection of threaten words stored in our database. Iteratively it will check for the threaten words in the email until it reaches the last word. In our paper we have experimented with 200 words at the backend to check whether the incoming email is a threaten email or not. Mails contained threaten contents are splitted by S-MAIL automatically and the legitimate mails are identified. Thus our methodology just focuses on the high level encryption and decryption of passwords and classification of threaten emails based on matching of scary words. So in these experiments, we only concentrate on how far it securely stores the passwords and how well correctly classifies the emails.

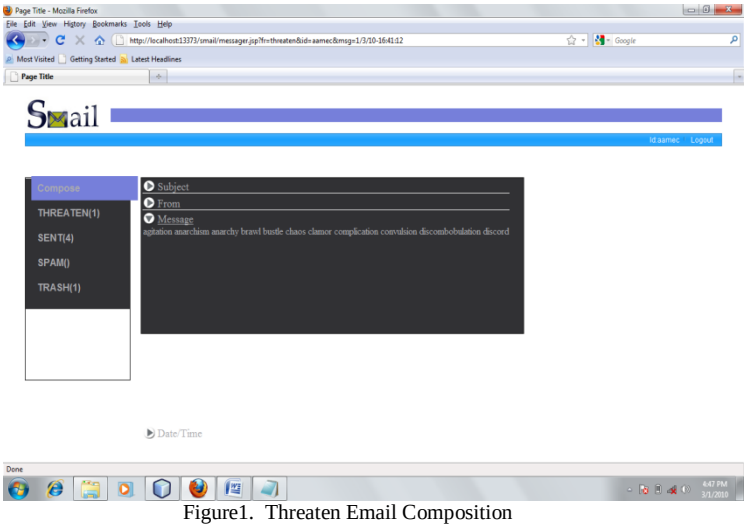


Figure1. Threaten Email Composition

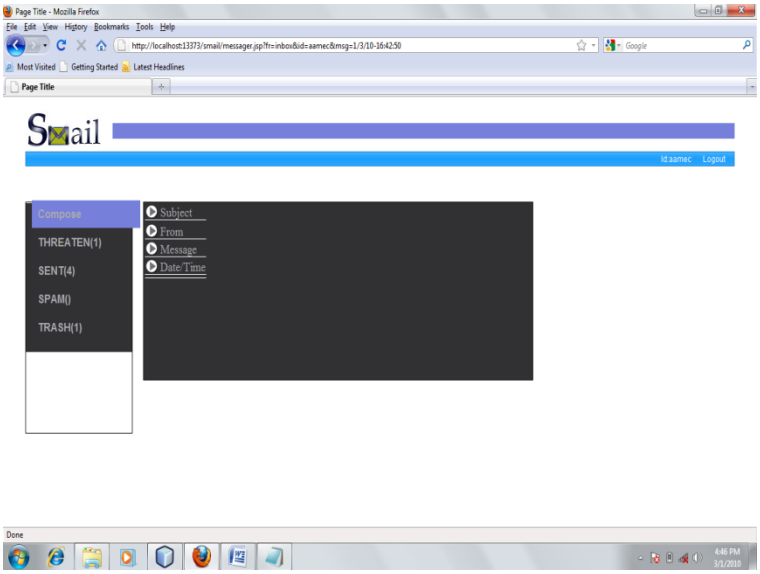


Figure2. Threaten Email Partition

V. FUTURE ENHANCEMENT

Further, in future as the technology improves, S-MAIL can be customized to include threaten contents in the form of images as well as encrypted words. The level of encryption can be enhanced more but it will lead to slower process. As the technology improves, it can be recovered.

VI. CONCLUSION

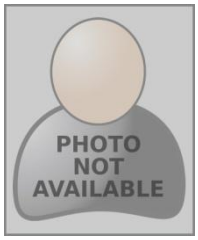
S-MAIL focused us on a large number of key factors in determining the unnecessary and illegal emails by providing the automatic threaten email detection. Since all S-MAIL actions are rule based decisions as configured in the threaten email module, uniform processing for finding threaten contents is obtained and guess works are completely eliminated. Through the appliance of various encryption technologies, the level of security on confidential information has been increased. The whole system is automated and manual interventions are avoided in most cases. Decisions are taken usually in a matter of seconds. It provided near-instantaneous approval or supervised decisions. Clients are notified every time if they come across any threaten contents.

References

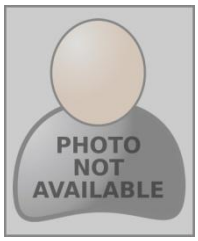
1. S.Appavu alias Balamurugan and R.Rajaram, "Learning to Classify Threaten E-Mails", Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference.
2. Ducheneaut N and Watts L., "In search of coherence: areview of e-mail research, Human-Computer Interaction 20", 2004.
3. Rohan Mahesh Amin, "Detecting targeted malicious email through supervised classification of persistent threat and recipient oriented features", 2011.

4. www.microsoft.com/security/resources/default.aspx
5. David M. Kristol, Eran Gabber, Phillip B. Gibbons, Yossi Mattias, Alain Mayer, "Design and Impementation of Lucent Personal Web Assistant", Information Sciences Reasearch Centre, Bell Laboratories, Lucent Technologies.
6. M. Wong, W. Schlitt , "Sender policy framework (spf) for authorizing use of domains in e-mail", 2006.
7. Michel Deriaz and Jean-Marc Seigneur,"Trust and Security in Spatial Messaging: FoxyTag, the Speed Camera Case Study", in Proceedings of the 3rd International Conference on Privacy, Security and Trust, ACM [to appear], 2006.
8. J.-M. Seigneur and C. D. Jensen, "User-Centric Identity, Trust and Privacy", blind peer-reviewed accepted book chapter of "Trust in E-services: Technologies, Practices and Challenges", Idea Group Publishing, 2007.
9. E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC5672, 2007
10. William Stallings," Cryptography and network security", fifth edition ISBN 0-13-6097049

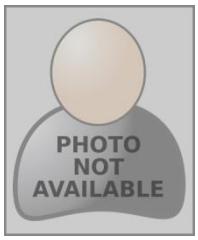
AUTHOR(S) PROFILE



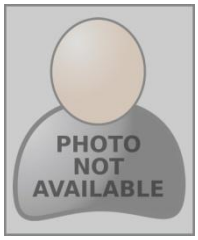
S. Lavanya received her B. Tech., IT from Anna University, Chennai in 2010 and M.E Computer Science and Engineering from Anna University, Chennai in 2012. At present working as Assistant Professor at E. G. S. Pillay Engineering College, Nagapattinam. Her research interest includes text classification and information security in general.



P. Suganya received her B. E., CSE from Anna University, Chennai in 2010 and M.E Computer Science and Engineering from Anna University, Chennai in 2012. At present working as Assistant Professor at E. G. S. Pillay Engineering College, Nagapattinam. Her research interest includes web services, SOA and Mashup in general.



E. Elakiya received her B. Tech., IT from Anna University, Chennai in 2010 and M.E Software Engineering from Anna University, Chennai in 2012. At present doing Ph.D at Anna University and working as Assistant Professor at E. G. S. Pillay Engineering College, Nagapattinam. Her research interest includes information retrieval, text classification and text mining in general.



E. Vijayavani received her B. Tech., IT from Anna University, Chennai in 2010 and M.E Computer Science and Engineering from Annamalai University, Chidambaram in 2012. At present working as Assistant Professor at E. G. S. Pillay Engineering College, Nagapattinam. Her research interest includes image processing and speech recognition in general.

