International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Manage the Attacks in Online and OTIP using HMAC

K. Anbuthiruvarangan[1], B. Prakash[2]
[1]*Assistant Professor, Dept. of Computer Science Engineering, Thangavelu Engineering College, Chennai, India*
[2]*Assistant Professor, Dept. of Computer Science Engg., Adhiparasakthi Engineering College, Chennai, India*

***Abstract*: With the developing digital era, the users are more vulnerable to various types of security threats such as Phishing (RAT) ,a serious security threat to the internet users in which the intruder sends an email which looks legitimate, where the RATs are usually downloaded invisibly with a user - requested program such as game or in this case an email attachment. RATs provide a backdoor for administrative control over the targeted computer, from which the intruder will be allowed to access all sensitive and confidential data such as banking application, which needs more security. It is important to prevent such phishing attacks. One of the ways to prevent the password theft is to authenticate a user without the use of the text password. In this paper we propose an idea which eliminates the use of the permanent text passwords, by authenticating the user through image based password. After image based authentication, the user will obtain the One Time Password (OTP) using the messaging service available in the internet. The image based authentication method relies on the user's ability to recognize the pre-chosen images from a grid of pictures which appears in a random manner. This project integrates one time Image password based authentication and HMAC based onetime password and to achieve high level of security in authenticating the user and these algorithms are very economical to implement.**

***Keywords*: RAT, OTP, HMAC, OTIP, Authentication**

1. Introduction

This Remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet. Remote Access Trojans (RATs) that make it onto a computer, undetected, give someone far away all the control they need of the victim's computer. RATs are generally sent through emails by 'riding' what looks like as a trusted file attachment such as a PDF, Excel spreadsheet or Word doc. Once the victim opens the email and clicks on the attachment, they may actually see a useful or trustworthy looking PDF, XLS or DOC open up but at the same time the RAT is being installed. Some less sophisticated RATs will display a fake error message 'file corrupted' so you think the attachment didn't come through completely and didn't open. Many RATS can disable antivirus and firewall software or create covert channels to bypass them, when sending and receiving information, commands, data and files. The one-time password (OTP) schemes may solve various problems caused by traditional static passwords, especially for the concern of eavesdropping and replay attacks. In OTP schemes, a user uses different passwords generated by token or software every time they login onto the server, and it is hard to calculate the next valid password from the previous passwords. Once a password is used, it will not be used for a second time. Image based authentication is included to provide additional security integrated with OTP. With IBA, when the user performs first time registration on a website, he makes a choice of several secret categories of images that are easy to remember, such as pictures of natural scenery, automobiles. Every time the user logs in, a grid of randomly generated images is presented to the user. The user identifies images that were previously selected. One-time access code is generated by the selected images, making the authentication process more secure than using only a static text password. It's significantly easier and advantageous for the user because he has to remember only a few categories to recognize the selected images. This paper is organized as follows. In section 2, we review the functionalities and effects of RAT. One Time Password generation and delivery will be discussed in section 3, followed by the authentication techniques in section 4. Applications will be seen in session 5.Finally, the conclusion is given in section 6.

2. Functionalities and effects of rats

RATs typically provide attackers with comprehensive command repertoires for file management, process scheduling, and system configuration manipulation. File management features include potentially destructive operations such as delete/move a file or directory on victim systems. The process scheduling component in a RAT permits intruders to create, view, and/or terminate running processes at will. The configuration manipulation element allows RATs to alter the behavior of the victim system by for instance disabling its security features after modifying the Windows Registry. RATs can often operate as device controllers being able to open/close CD-ROMs, disable the mouse and network cards, intercept keystrokes and/or screen snapshots, flip the victim's screen or change its resolution, monitor password dialog boxes and clipboards, capture audio/video of the victim's environment, and finally, crash the victim. The re-direct feature of RATs

allows an attacker to chain various services together and ultimately forward the results to a specified destination, making it trivial for intruders to hijack network connections, intercept private data, and inject fake messages. By functioning as packet sniffers, RATs can also monitor a victim's network activities and determine its topology. Furthermore, by scanning the entire system of the victim machine, including its garbage bin, a number of RATs can collect personal information such as user accounts, passwords, credit cards, and Email addresses.

3. One time password generation and delivery

One time password can be generated in any of the two ways:

- Time-synchronized OTP: In time-synchronized OTPs the user should enter the password within a certain period of time else it gets expired and another OTP must be generated.
- A counter-synchronized OTP: With counter-synchronized OTPs, a counter is synchronized between the client device and the server. The device counter is advanced each time an OTP is requested.

For example, consider hash-based OTPs wherein we use hash algorithms such as SHA-1 and MD5 that can be used to compute the OTP. A cryptographic hash function also called one-way function maps message of arbitrary length to a fixed-length digest. Thus, a hash-based OTP starts with the input parameters (synchronization value, username, and password), runs them through the cryptographic hash function, and produces the fixed-length password, i.e., OTP.

- *Delivery of OTP is done by:*
- *Text messaging:* It is the common method used for the delivery of OTP.
- *Instant Message Services and Email:* These services are almost common and the cost of using them is negligible

4. Authentication techniques

A. Image based authentication

The Image-based authentication is based on Recognition Techniques. When the user registers for first time in a web site they select set of images that are easy to remember, such as natural scenery, automobiles etc. Every time the user logs into the site, they are provided with a grid of images that is randomly generated. The user can identify the images that were previously selected by him. It is significantly easier for the user because they need to remember a few simple images only. IBA is based on a user's successful identification of his set of images. When the user logins for the first time, the website displays a grid of images, which consists of images from the user's password set mixed with other images. The user is authenticated by correctly identifying the password images. Performing brute force attacks or other attacks on such systems is very difficult. A set of different images are selected to authenticate the user. The Image Identification Set (IIS), for each user is then stored at the Authentication System. When a user logins, the IIS for that user is retrieved and used to authenticate that particular user. The system does not store the images but the category of the images are stored in IIS as images are large files. This technique is also more secure and requires less memory. If this step is successful, next OTP is generated and send to the user email-id.

B. HMAC-based one-time password algorithm

This paper describes an algorithm which is used to generate Time-synchronized OTP values, based on SHA-1 based Hash Message Authentication Code (HMAC). This is called as the HMAC-Based One-Time Password because here OTP is generated based on HMAC. One Time Password is obviously one of the easiest and most popular forms of two-factor authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as a secure and stronger forms of authentication, and allowing them to installed across multiple machines including home computers, mobile phones etc. When the user selects the pre-selected images to login an OTP is generated and sent to the user's e-mail id. The user is then directed to next page where the user is asked to enter the OTP. The user gets the OTP using the e-mail account and enters it. If the OTP is verified the user succeeds in logging in the system.

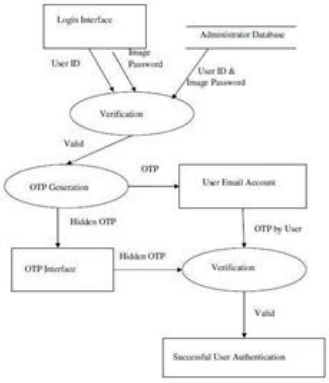

Fig. 1. Password algorithm

OTP value should be of reasonable length such as an 8-digit value. It is desirable for the OTP value to be a numeric digit so that it can be easily entered. E - User-friendly mechanisms should be available to resynchronize the time.

5. OTIP

One time image password is a next step of image based authentication, where it employs the same technique of IBA but instead of generating a separate OTP after IBA ,In OTIP we do it combined, as the user selects the preselected picture that he selected before in the grid of similar pictures, in every picture there will be a hexadecimal code will be encrypted with those pictures, once the selects the picture the hexadecimal code will be shortened or shortened to a decimal code, so the user could

easily type the code in the predefined space, once the code is entered by the user it now converts the code to the same hexadecimal code, making the RAT or another malware to crack the code, but if the user enters the wrong code the whole grid of pictures gets refreshed again and sent to his/her mail, and once again the same process repeats ,so this emphasis a person not to lessen the options available. A user could have a maximum of 3 tries. Suppose if the user selects a certain brand of bike during creating his account, different brands of bike pics will be sent to him during request of OTIP, so the user has to remember the picture he/she selected .We use the same algorithmic generation for OTP and is explained below.

A. Increased level of security

If OTP gives 50% security, OTIP will give the user 70% security, as this to get its own drawbacks, but it surely provides a higher rate of security than one time password (OTP) or image based authentication (IBA)

B. Algorithm for code conversion

For converting hexadecimal to decimal:

- Divide the decimal number by the desired target radix (2, 8, or 16).
- Append the remainder as the next most significant digit.
- Repeat until the decimal number has reached zero.
- For converting Decimal to Hexadecimal:
- Divide the decimal number by 16. Treat the division as an integer division.
- Write down the remainder (in hexadecimal).
- Divide the result again by 16. Treat the division as an integer division.
- Repeat step 2 and 3 until result is 0.
- The hex value is the digit sequence of the remainders from the last to first.

C. Algorithm requirements

- The algorithm MUST be time synchronized. B - The algorithm SHOULD be economical to implement by reducing the amount of hardware required.
- The algorithm MUST work with any sort of code generating tokens.
- The value displayed on the token or any mail message should be easy to read and entered by the user.

6. OTP algorithm description

The OTP algorithms are based on an increasing time value function and a static symmetric key known only to client and server. In order to create the OTP value, a HMAC- SHA-1 algorithm is used. Since the output of the HMAC-SHA-1 calculation is 160 bits, we have to truncate this value to a smaller digit so that it can be easily entered.

OTP (Key,T) = Truncate(ToHex(HMAC-SHA-1(Key,T)))

Where –Truncate converts the value generated through HMAC-SHA-1to an OTP value.

A. Generation of OTP value

The algorithm can be described in 3 steps:

Step-1: Generate the HMAC-SHA-1 value Let HMK = HMAC-SHA-1(Key, T) // HMK is a 20-byte string

Step-2: Generate a hex code of the HMK. HexHMK=ToHex (HMK)

Step-3: Extract the 8-digit OTP value from the string OTP = Truncate (HexHMK)

The Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

B. Operation

- MessageDigest md = MessageDigest("SHA1") md.update(Key,T)
- output = md.digest()
- buf = hexDigit((output >> 12) & 0x0f)
- otp=buf.toString()
- otp=otp.substring(0,7)

7. Applications of OTP

Google is currently using one time password. Hotmail is also using one time password to provide high security to users. RBI made OTP compulsory for transaction made with credit card. All banking systems are using OTP. E.g.:- ICICI Bank, HDFC, Citi Bank, Axis, SBI etc.

8. Conclusion

The proposed system integrates the security techniques one time image password and Hash-MAC based onetime password. Initially, the Image Based Password Authentication is done where user is authenticated using image password that was previously selected by the user himself, in which there is a hidden password that is encrypted with every picture and the user has to select the right picture to move on with the next step followed by the Hash - MAC based One Time Password which uses SHA-1 algorithm for the generation of a secure one time password. This authentication technique is simple and highly secure. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function and in this paper SHA-1 is used for the calculation of HMAC. SHA-1 being a most widely accepted cryptographic hash function due to its high security Computer as compared to other cryptographic hash functions such as MD5 adds to the security of HMAC. Recovery of lost password based on secret question and answers can be a future enhancement.

References

[1] Jeong, Jongpil, Min Young Chung, and Hyunseung Choo. "Integrated OTP-based user authentication scheme using smart cards in home networks." In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, pp. 294-294. IEEE, 2008.

[2] Shivraj, V. L., M. A. Rajan, Meena Singh, and P. Bala Muralidhar. "One time password authentication scheme based on elliptic curves for internet

of things (IoT)." In Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, pp. 1-6. IEEE, 2015.

[3] Parmar, Himika, Nancy Nainan, and Sumaiya Thaseen. "Generation of secure one-time password based on image Authentication." Journal of Computer Science and Information Technology 7 (2012): 195-206.

[4] Liao, Shuren, Qiuyan Zhang, Chao Chen, and Yiqi Dai. “A unidirectional one-time password authentication scheme without counter desynchronization,” In Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on, vol. 4, pp. 361-364. IEEE, 2009.

[5] FIPS, PUB. "198 (Federal Information Processing Standards Publication) The Keyed Hash Message Authentication Code (HMAC)." Information Technology Labratory, National Institute of Standards and Technology, Gaithersburg, MD: 20899-8900.

[6] Kamran Sameni, Nasser Yazdani, Ali Payandeh, “Analysis of Attacks in Authentication Protocol of IEEE 802.16e”. International Journal of Computing and Network Technology. Nov. 2012.