Volume 2 No.8, AUGUST 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Authentication and Virus Detection Enhancement for Client and Server Applications

Ghossoon. M. W. Al-Saadoon
Ass. Professor, Head Dep.of MIS
College of Administrative Science, Applied Science University
Manama, Kingdom of Bahrain
dr.ghoson@asu.edu.bh

ABSTRACT

Security issues are a core part of distributed computing systems, and are part of everyday life since they are used in web servers, email, mobile phones, bank transactions etc. Applications which send an unencrypted password over a communication channel are extremely vulnerable. In addition, the only techniques that have been applied to most systems are security properties such as secrecy and authenticity. A system usually needs to identify its legal users for providing its services therefore, there is a need to construct an authentication system in the client server model to make sure the sent message is confidential, integral, and non-repudiate and secure.

The objective of this paper is to provide strong authentication for client and server applications by using secret-key cryptography and to detect any infected packets through analysis using a TCP damp sniffer. The solution consists of two main parts: authentication and virus detection. Authentication is the first part in which login process is required. The AES symmetric key encryption is used to encrypt the password to guarantee confidentiality while message digest is another way to prove the integrity checking. The results obtained in this paper consists of a non-repudiation method which can create the digital signature and virus detection, which can be done through analysis of the payload that has been captured by using Tcpdump sniffer. Finally, the cryptographic authentication system with secure file payload analyzer can be constructed successfully and will be able to detect an infected packet as well as delete it.

Keywords— *Secret-key cryptography, Netbean Software, AES symmetric encryption, Tcpdump sniffer, and MD5 Hash Cryptography.*

1. INTRODUCTION

Nowadays there is no sufficient security because most packets sent are easily spoofed by a third party [1]. In all cases, however, authentication systems depend on some unique piece of information known only to the individual being authenticated and to the authentication system. Such information may be a classical password, some physical property of the individual, or some derived property [2]. The user is considered authenticated if the *authenticating* system can verify that the shared secret was presented correctly. To make sure the packet sent is *confidential*, the use of an encryption method is required. Thus, an encrypted password can prevent hackers or intruders from trying to sniff it. The content of the packet is only known between the sender and receiver. Next, the usage of the message digests information to make sure the integrity of the packet sent is kept safe. *Integrity* checking confirms that no other people can alter the content of the message. When both confidentially and integrity are combined non-repudiation will be assured. Digital signature occurs when the sender "signs" a message with the private key to prove that the message has been sent from the sender. Finally, all the packets sent are secure [3]. In addition, worms or viruses are very well known and easily propagated nowadays. Worms or viruses may damage or ruin the system. Thus it is necessary to create a system that can detect and filter out the malware [9, 10].

2. UNSECURE DATA TRANSMISSIONS PROBLEM

This problem appears when there are unsecure data transmissions. We have to ensure the security of the authentication process and makes sure the data is encrypted and decrypted in the correct way because there are many malware attacks – worms which can infect the system we must also make sure that messages are sent with confidentiality, authenticity, integrity and non-repudiation.

3. RELATED WORKS

ShaiHalevi and Hugo Krawczyk -2001- studied protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses a pair of private and public keys while the client has only a weak human- memorable password as his/her authentication key. Remarkably, this analysis shows optimal resistance to off-line password guessing attacks under the choice of suitable public key encryption functions [7].

- Matt Bishop-2004- devised privacy enhanced mail protocols, which specify a set of protocols for sending electronic mail that provides privacy, integrity, and sender authenticity; under certain circumstances, and also provides non-repudiation. Its presents some background information on electronic mailing systems, some relevant aspects of cryptography, constraints leading to design decisions, and how to send a privacy-enhanced message [4].
- Min-HuaShao Jianying Zhou and Guilin Wan -2008- introduced, certified e-mail as a value-added service for standard e-mail systems, in which the intended recipient gets the mail content if and only if the mail originator receives non-repudiation evidence that the message has been received by the recipient [5].

4. TERMINOLOGY

The proposed development includes a cryptographic authentication system (MD5) to secure file payload analysis by using Netbean software. The software tools used for implementation are Java Servlet which used to construct a client-server model.

4.1 Software tools

Some of the software tools used in implementation for this research is the following:

Vmware Workstation, Ubuntu Operating System, Netbean IDE ver. 6.51 and JRE, and Tcpdump [11].

4.2 Worm Threat

Email worm which is used in this paper is an essential communication medium for today's connected society. As such, it gradually became the main propagation vector of malicious software (malware) [2] and used to cover every malware that propagates using - email over a computer, it is also a self-replicating computer program [4, 5].

4.3 MD5 Hash Cryptography

MD5 is a popular one-way hash function which is used to create a message digest for digital signatures. It takes a message and converts it into a fixed string of digits, also called a message digest [6,7].

5. ATTACK METHODS

There are two methods of attacks: an attachment with malicious content and HTML mail with embedded scripts.

5.1 Attachments with malicious content

Email messages can include file attachments, where hackers can send infected files and hope that the recipient will open them. The method makes use of social engineering to urge the end user to run the file. Yet, other methods exist which allow a skilled and possibly malevolent cracker to inject code through email and run custom-made applications automatically while the end user reads the email text [9].

5.2 HTML mail with embedded scripts

Nowadays, all email clients can send and received HTML mail. HTML mail can include scripts and Active Content, for example JavaScript and ActiveX controls, which can allow programs or codes to be executed on the client machine. Outlook and other products use Internet Explorer components to display HTML email, meaning they inherit the security vulnerabilities found in Internet Explorer. Viruses based on HTML scripts have the added danger of being able to run automatically when the malicious mail is opened [10].

6. THE PROPOSED SOLUTION

The system diagram consists of three important phases System, User, and Upload file, as shown in **Figure 1.**

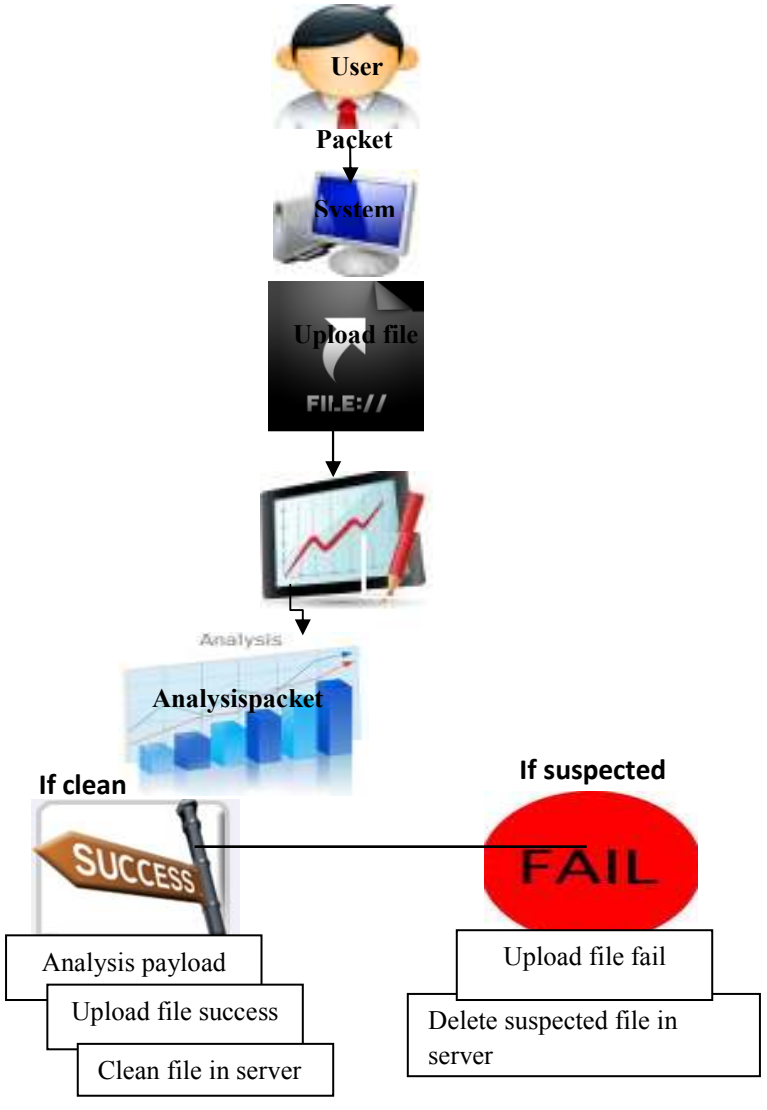

Figure 1: Overall Diagram of System

6.1 System Phase

There are two parties after establishing a connection, *the authentication* (authentication, confidentially, integrity and non-repudiation), and *detect worm* (capture Trojan horse by Tcpdump).

a) First, satisfy the connection between client and server.
b) Clients are prompted to enter the password and username to get authentication. Three important elements must be encrypted; these are hash code password, hash password in plaintext as well as system current time. The encrypted elements will form a digital signature. The purpose of scrambling the message is to cipher the message (random character) so that snoopers and hackers cannot understand the message. Besides that, it also has to use MD5 message digest. This is to guarantee the message integrity and authentication, as no other people other than recipient can read the massage or alter the content of the message.
c) The server will process this to verify the identity of the user and will be considered as an authenticated user, and then the string will be decrypted to become the original string.
d) Next- the hash code will be compared with the hash of the password plaintext- If the password matches, it is an authenticated user and this will guarantee the file's integrity.
e) The user should check the Trojan virus when he/she uploads the file. This can be done by capturing the data by using Tcpdump software. The payload of packet header should be analyzed if there are 20 lines of 00 00 00 00, then may be it is suspicious as a worm, and the system will delete the file. On the other hand, if there is a clean file, the file can be uploaded successfully.

6.2 User Phase

When login has been successfully completed as shown in Figure 2, the user can browse the file that he/she wishes to upload. The right hand side will show the session unique ID, encrypted long string, decrypted long string, password in hashed md5, password in plaintext, user login time and counter. If trials are made more than three times, users will loss the chance to login again, as shown in Figure 3.

Figure 2: Main Page for successfully login

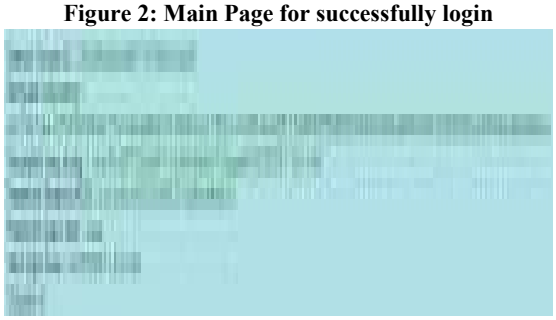

Figure 3: Encrypted and decrypted string

6.3 Upload Phase

It is the same function as error handling during login page. The dialog box is used to alert customers to select a file for uploading, see Figure 4.

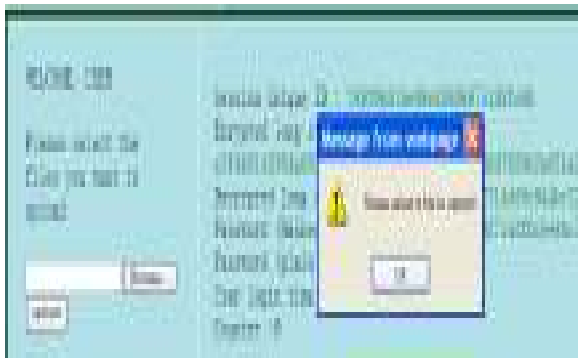

Figure 4: Error handling for upload file

Figure 5 shows the information of the uploaded file. It will show the file name of the uploaded file, the content type and file size. The maximum file size that can be uploaded is 1 Mb. Besides that, it will show the status of the file and the payload that has been saved in the text file. If the file is a clean file, it will show the status as clean, and the file can be uploaded to the server.

Figure 5: File uploaded successfully

```
fileItemFactory.setSizeThreshold(1 * 1024 * 1024);
```

Statement 1 explains size threshold, which content to be stored on disk. The maximum size that can be uploaded is 1 MB.

```
fileItemFactory.setRepository(tmpDir);
```

Statement 2 is the set of temporary directories used forstoring the uploaded files of size above threshold.

```
StringpayloadPath=request.getContextPath()+"/UploadedFiles/payload.txt"

if (!is_file_suspected) {

String path = request.getContextPath() + "/UploadedFiles/" + filename;

payloadPath = request.getContextPath() + "/UploadedFiles/payload.txt";
```

First it gets the status of the files. If TRUE, the file was suspected otherwise if FALSE, the clean file was uploaded. If the file is clean and uploaded successfully, the user can view the payload of the uploaded file. The clean payload must have the encapsulated IP header and TCP header where the header includes the information of IP total length, Time-To-Live (TTL), checksum, identification etc. Besides that, it contains the encrypted information of each line of payload the scramble message kept the content secret.If file status is suspected, the upload will have failed. The infected file will be deleted from the server automatically, see Figure 7.

Figure 7: File upload failed

The payload will show that the file has come from the client to the server. The IP address of the client is 192.168.10.1 and for server is 192.168.10.130. The file transmission uses TCP protocol as it is an intranet transfer.

The destination port is the port opened by the server. However, when Trojan Bagle appears, the payload pattern will show all 00 00 00 00 in the first 20 lines. However in line 21, it must show that the payload contains 20 e0 53 00 and this kind of pattern will be repeated, a few days later. This is the behavior of Trojan Bagle. Besides that, it does not show any encrypted data for each line. It is obviously different from the clean payload, as in the example above. Thus we suspect that this is the infected file, see Figure 8.

Figure 8: View the payload.txt of clean file

7. RESULT

The result includes the system test and its strength, as follows:

7.1 System Testing

There are several units to be tested in the system:-

1. *Connection establishment* which includes the following: Vmware Workstation acts as a server and window acts as a client. It is, able to start a client server connection; the server is able to listen for a connection from the client and to track the connection status of the client.

2. *Encryption AES* which enable the encryption and the decryption of the password for security purpose; it also proves the confidentially of the password.
3. *File transfer* – the client is able to upload the file to the server and then receive the uploaded file by the client to gets the correct files.
4. *Analysis of payload*- The server is able to run the Tcpdump to capture the packet in the transmission of data and save the packet in text form to identify or filter the clean file or infected file.

7.2 System Strength

The strength of system is the security mechanism which occurs between client and server, like authentication and authorization.

- The file integrity checking was done to make sure that both client and server are getting the desired file that is to be used by MD5 hash.
- The AES encryptions for the password are used to prevent intruders from trying to sniff the password.
- The digital signature is done to prove the non-repudiation.
- Error handling is carried out to make sure that jobs submitted by users are in the correct format.
- The Trojan Bagle worm detection system should be in place.

8. CONCLUSIONS

The cryptographic authentication system with secure file payload analyzer has been successfully designed and constructed, with the conclusion as follows:

- Users can authenticate with confidentiality, integrity, non-repudiation and security.
- Worm detection is necessary to select a specific type of virus and gain the knowledge to distinguish the behavior and characteristic of the virus selected (Bagle Trojan horse).
- With sniffer packets, analysis of the payload is essential to distinguish and detect the presence of a virus, and to verify whether the file is clean or suspicious.
- However, the packet sniffer runs behind the engine and it is hard to observe its result.

REFERENCES

[1] Brijendra Singh,"Network Security and Management", University of Lucknow, Prentice-Hall of India,2007.

[2] Don Libes "Authentication by Email Reception National Institute of Standards and Technology", 1998 .

[3] Sim2k ,"News Virus Attack a Concerns", retrieved January 2010 http://www.sim2k.com/SIMformation/4_04nsltr.pdf

[4] Stig Anderson, "Detecting and Characterising Malicious Executable Payloads ", Information Security Institute, Faculty of Information Technology, Queensland University of Technology, 2008.

[5] Stamatios and V. Kartalopoulos "A primer in Cryptography Communication", University of Oklahoma, 2006.

[6] Matt Bishop"Privacy-Enhanced Electronic Mail Department of Mathematics and Computer Science", Dartmouth College, Hanover, 2000.

[7] Min-HuaShao ,Jianying Zhou and Guilin Wan " On the Security of a Certified E-Mail Scheme with Temporal Authentication Institute of Information Management", National Chiao Tung University , 2004.

[8] Tcpdump official website, retrieved December, 2010.http://www.tcpdump.org/

[9] "F-Secure Antivirus company- Virus descriptions", 3 February, 2010 http://www.f-secure.com/v-descs/bagle.shtml.

[10] P.C.vanOorschot," Message Authentication by integrity with Public Corroboration", Canada, School of Computer Science Carleton University, 2009.

[11] ShaiHalevi and Hugo Krawczyk , "Public-Key Cryptography and Password Protocols", IBM T.J. Watson Research Center, 1999.

[12] William Stallings,"Network Security Essentials Application and Standard",3rd Edition, Prentice Hall, 2008.

Authors Profile

Ghossoon M.W. AlSaadoon is Ass. Professor in Network security &DataBase, Dr.Al-Saadoon is a Head Department of Management Information Systems & Director of Academic Staff Performance Development Center at the Applied Science University College of Administrative Science, Manama, and Kingdom of Bahrain. She holds PhD degree in computer science from the Iraqi commission for computers & informatics /institute for postgraduate studies in informatics, 2006 in addition; she is a membership of CSC- journals & ISACA member. Dr. Al-Saadoon has more than 19 years of experience including project management experience in planning and leading a range of IT-related projects. Dr. Al-Saadoon supervised many computer and communication

engineering students leading to Ph.D. and M.Sc. degree in computer and communication engineering in UniMap.

Dr. Al-Saadoon has three awards (two from Ministry of Science Technology and Innovation (MOSTI) and One from UniMap University).