Fakulti Teknologi Maklumat dan Sains Kuantitatif

UNIVERSITI TEKNOLOGI MARA

JURNAL TEKNOLOGI MAKLUMAT DAN SAINS KUANTITATIF

Jilid 9, Bil. 1, 2007 ISSN 1823-0822

Universiti Teknologi MARA

Fakulti Teknologi Maklumat dan Sains Kuantitatif *ISSN: 1823-0822* *Jilid 9, Bil 1, 2007*

UNIVERSITI
TEKNOLOGI
MARA

JURNAL TEKNOLOGI MAKLUMAT DAN SAINS KUANTITATIF

Kandungan **Muka Surat**

Universiti Teknologi MARA

DARI MEJA PERUNDING

Assalamualaikum w.b.k dan salam sejahtera kepada semua pencinta ilmu. Alhamdulillah, dapat kita terbitkan Jurnal Teknologi Maklumat dan Sains Kuantitatif Jilid 9, Bil. 1, 2007 ini. Saya merakamkan berbanyak-banyak terima kasih kepada mantan dekan, Prof.Madya Dr Adnan Ahmad yang memberikan galakan untuk penerbitan walaupun kadangkala susah untuk mendaptkan penulis-penulis yang berminat. Bermula dari 1 hb.Disember, 2007 fakulti telah diterajui oleh dekan yang baru, iaitu Prof. Dr Zainab Abu Bakar. Moga-moga dengan dekan yang baru, mudah-mudahan kita akan dapat suntikan semangat yang baru dan masing-masing baik dari fakulti di UiTM mahu pun dari IPTA yang lain berlumba-lumba untuk terus menulis .

Melalui penulisan dan bacaan dapat kita menambahkan ilmu pengetahuan kita. Kemajuan dan peningkatan tamadun maanusia adalah juga melalui penyebaran ilmu. Di era Teknologi Maklumat dan Komunikasi (ICT) dan globalisasi ini, penyebaran ilmu boleh dibuat secara pantas dengan melayari internet atau pun pmelalui blog-blog ilmiah. Namun begitu, hasil ilmuwan melalui karya penulisan dalam bentuk, jurnal, proceeding mahu pun laporan projek adalah masih releven dan penting . Malahan dewasa ini, penyebaran ilmu di pusat-pusat pendidikan tinggi mahu pun organisasi penyelidikan, kaedah ini masih jadi pilihan utama.

Saya berharap semua penulis-penulis semasa dan yang akan datang tetap gigih untuk menulis supaya karya kita dapat dimanfaatkan oleh semua pihak yang cintakan ilmu.Untuk para pendidik, hasil karya anda akan menjadi satu rangsangan untuk siswa-siswi muda kita mendaptkan ilham untuk giat dalam penulisan.

Terima kasih.

Ketua Penyunting.

Prof. Dr. Mohd Sahar Sawiran.

Securing Password Transmission For FTMSK Webmail System Using Cryptographic Hashing

Prasanna Ramakrisnan, Md Rosli Md Daud,
Mohd Nor Hajar Hasrol Jono, Azlan Abdul Aziz
Faculty of Information Technology & Quantitative Sciences
UiTM, Shah Alam.
prasanna@tmsk.uitm.edu.my, rosli@tmsk.uitm.edu.my, hasrol@tmsk.

Abstract:

Password is a popular way for authenticating a user to asystem. This method is widely used in many online systems and email systems. This method ensures that only the legitimate users have access to the system. Analysis on the security of the method is important as it is exposed to many kind of attack these days. In this paper, the password vulnerability on the method used by an existing webmail system at FTMSK (Fakulti Teknologi Maklumat dan Sains Kuantitatif) is presented. A simple prototype defence mechanism to modify the existing login page by finding the hashing procedure was developed. We have shown that by implementing cryptographic hashing algorithm, the weakness found in the existing webmail system can be overcome.

Keyword – *authentication, hashing, password, security.*

1. Introduction

Attack can be classified into active and passive attack. Passive attacks using sniffers are becoming more frequent on the Internet. The attacker obtains a user id and password that allows him to logon as that user. Password Sniffer can monitor and capture passwords through LAN. It works passively and doesn't generate any network traffic, therefore, it is very hard to be detected by others [Packet Sniffer.net, 2003].

There were pros and cons of using 'sniffer'. Dsniff is a well-known data and password 'sniffer'. It can snag passwords off the wire from many different protocols, including FTP, Telnet, Web, POP3, IMAP, LDAP, Citrix ICA, pcAnywhere, SMB, Oracle SQL*Net, and numerous others (Edward, 2000). In order to prevent such attacks people have been using identification schemes [USENIX Association, 1995].

2. Current Network

The current network implementation at FTMSK can be viewed as shown in figure 1 below.

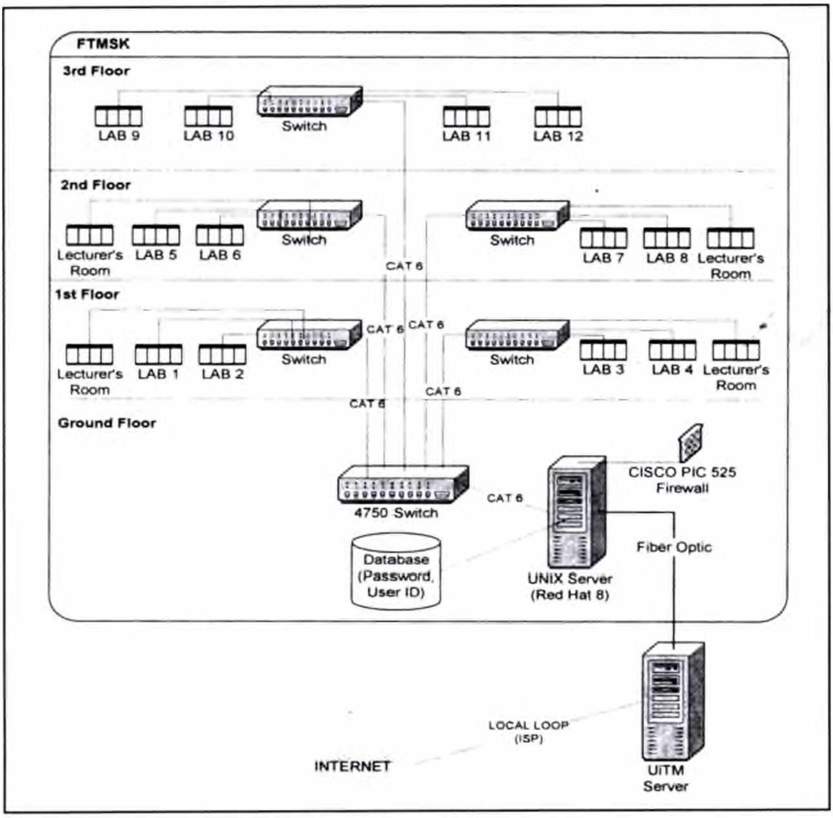
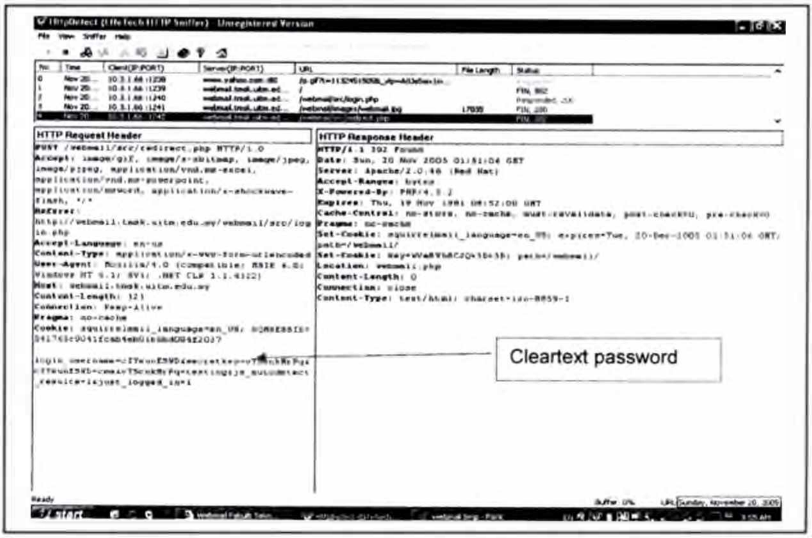


Figure 1: FTMSK Network Architecture

Every computer lab has its own small LAN, which is actually connected to the switch. However, the third floor of FTMSK's building has only been equipped with one switch, which connects to the computer lab's host. The connection of all switches in FTMSK's building emulates the star network topology. FTMSK has also using new cable (CAT 6) on it's internal network together with fiber optic cable as a trunk that route FTMSK's network to the UiTM server. There is also a server with Cisco PIC 525 firewall that stores email databases in the server room.

3. Sniffing Test on the Current Webmail System

Passwords are protected at database server using encryption scheme in UNIX using MD5 hashing algorithm. However, this service does not secure the in-transmission password. Someone who has access to the network connecting the client and server has the capability of eavesdropping the plaintext password. We had placed a HTTP Sniffing program in the network to see the communication between webmail client and webmail server. From the client computer, we accessed the webmail login page, entered the username and the password (our password was "testing") and pressed the button "Login". The communication then was recorded by the HTTP sniffer which was located between the webmail client and the webmail server. The screen shot below shows the result.



No.	Time	Client(IP:PORT)	Server(IP:PORT)	URL	File Length	Status
0	Nov 20...	10.3.1.66:1238	www.yahoo.com:80	/s-gf7k=1132451508_yip=AI3e5ex1n...		[illegible]
1	Nov 20...	10.3.1.66:1239	webmail.tmsk.uitm.ed...	/		FIN, 302
2	Nov 20...	10.3.1.66:1240	webmail.tmsk.uitm.ed...	/webmail/src/login.php		Responded, 2X
3	Nov 20...	10.3.1.66:1241	webmail.tmsk.uitm.ed...	/webmail/images/webmail.jpg	17035	FIN, 200
4	Nov 20...	10.3.1.66:1242	webmail.tmsk.uitm.ed...	/webmail/src/redirect.php		FIN, 302

HTTP Request Header

```
POST /webmail/src/redirect.php HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/vnd.ms-excel,
application/vnd.ms-powerpoint,
application/msword, application/x-shockwave-
flash, */*
Referer:
http://webmail.tmsk.uitm.edu.my/webmail/src/log
in.php
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Host: webmail.tmsk.uitm.edu.my
Content-Length: 121
Connection: Keep-Alive
Pragma: no-cache
Cookie: squirrelmail_language=en_US; SQMSESSID=
[illegible]

login_username=[illegible]&secretkey=[illegible]
[illegible]=testing&js_autodetect
_results=1&just_logged_in=1
```

HTTP Response Header

```
HTTP/1.1 302 Found
Date: Sun, 20 Nov 2005 01:51:04 GMT
Server: Apache/2.0.46 (Red Hat)
Accept-Ranges: bytes
X-Powered-By: PHP/4.3.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: squirrelmail_language=en_US; expires=Tue, 20-Dec-2005 01:51:04 GMT;
path=/webmail/
Set-Cookie: key=[illegible]; path=/webmail/
Location: webmail.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Cleartext password

Figure 2: Sniffing test on the current webmail

The result of sniffing test is obtained after the webmail page is open. The 'Get' function indicated that client side has received the data from the server. The client then loaded with the content of 'login.php' from the server, such as image, input field and their corresponding label. This is the file that constructs the web form for the current FTMSK Webmail.

The data posts to the server, indicated by 'POST' function. It posts the content in 'redirect.php' file. There were certain kinds of protection to protect the password such as the usage of Secret Key that append to the original password entered. However this technique is not secure at all as the cleartext of password still can be sniffed easily.

Therefore we found that FTMSK current webmail login system is not secured from this kind of attack. It is important to hash the password before transmitting it to the server.

4. Secure Login Prototype using Cryptographic hashing

To overcome this weakness, we have applied the cryptographic hashing function on the client side so that the entire password entered by users will be transformed into hashed before sending it to the server. The webmail database will keep the record of the username as well as the corresponding hashed password. When the user keys in the username and password to login to the system, the password is first transformed to its hash using MD5 algorithm before it is sent to the server. The corresponding password hash stored in the server database for that particular username will be compared with the hash password sent by user. If they are matched, the access to the webmail system is granted to the user, otherwise the access is denied.

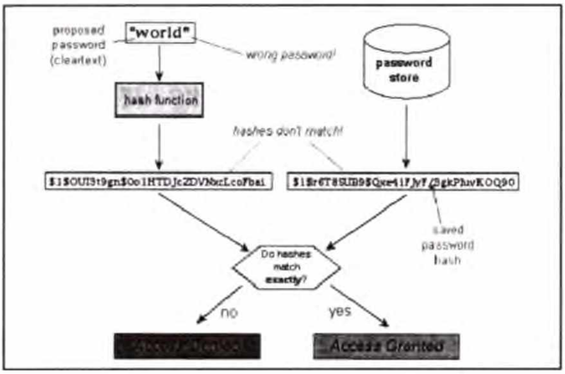


Figure 3: Secure login using cryptographic hashing

4.1 Construction of the prototype

We developed a simple prototype for the login page where transmission of the password is carried after the password is hashed on the client side.

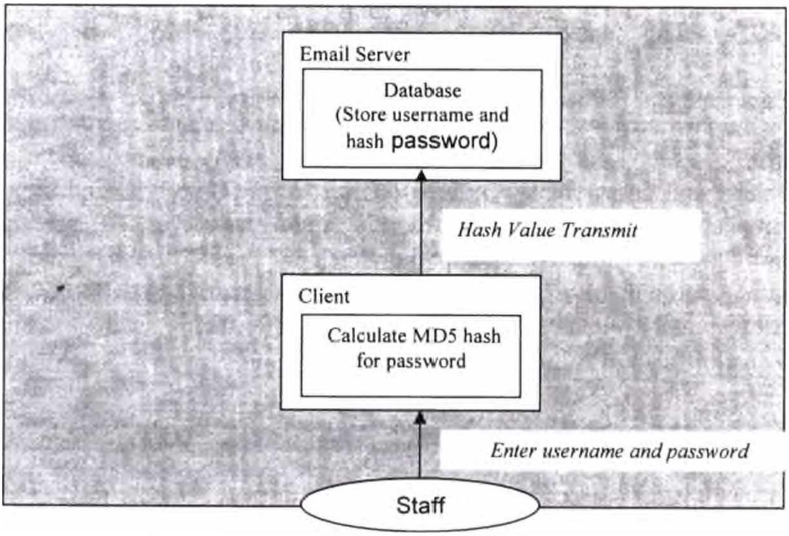

Email Server
Database
(Store username and hash password)
Hash Value Transmit
Client
Calculate MD5 hash for password
Enter username and password
Staff

Figure 4: Secure login prototype

The prototype was constructed for the purpose of demonstration on how to apply one-way hashing function at the client side of client / server architecture. It was constructed using Hypertext Markup Language (HTML) for creation of web-base user interface, JavaScript to run hashing process using MD5 algorithm, PHP 4 for connection to the MySQL database and the server was powered by Apache 1.3.33.

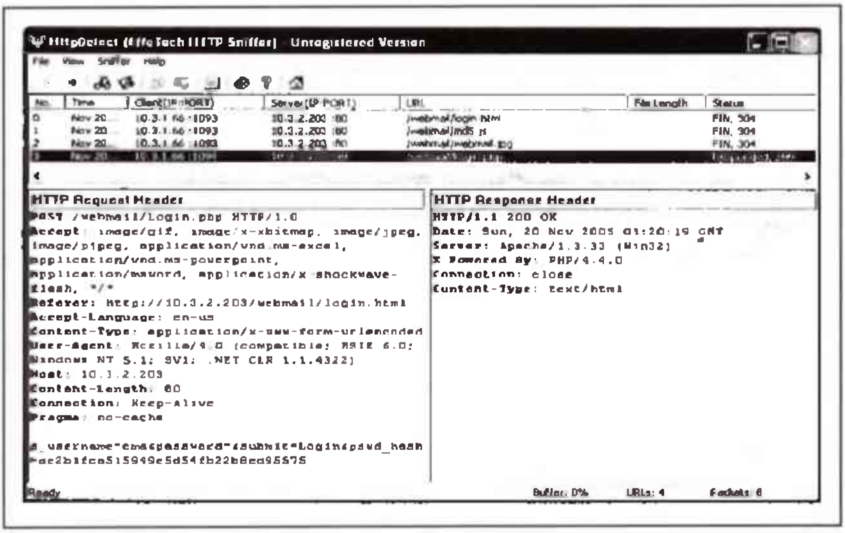
The secure Login System is used for authentication purpose. This means that by providing a correct username and password, a user will be authenticated and can access their mailbox. This web based form was created and named as, 'Login.html'

The web form of Webmail Login System will load after running on local host using an Internet browser. It can be done by typing 'http://localhost/webmail/Login.html' at address field of web browser. The password field is also transform into the MD5 hash value before transmitted to the server.

A correct username with corresponding password is entered to the 'username' field and 'password' field, in order for the staff to be authenticate or able to access email. After entering the information, staff can be authenticate by clicking on 'Login' button. Staff entering the correct username with corresponding password is authenticated. The incorrect username and password entered will cause the system to return to the 'Login.html' page. This means that it will direct the user staff back to the state.

4.2 Sniffing Test on the Prototype.

The same http sniffing test was carried out on the prototype. This test was done on the localhost where the webmail client, webmail server and the sniffing program was placed on the same machine. We typed in the same username and password as the previous test in the prototype and recorded the http communication between the client and the server. The screenshot below shows the http communication track by the sniffing program. The communication involve 'GET' and 'POST' method exactly like the test on the actual webmail system carried out before except for the password was shown in hashed instead of original plaintext password.



No.	Time	Client(IP:PORT)	Server(IP:PORT)	URL	File Length	Status
0	Nov 20 ...	10.3.1.66:1093	10.3.2.203:80	/webmail/login.html		FIN, 304
1	Nov 20 ...	10.3.1.66:1093	10.3.2.203:80	/webmail/md5.js		FIN, 304
2	Nov 20 ...	10.3.1.66:1093	10.3.2.203:80	/webmail/webmail.jpg		FIN, 304
3	Nov 20 ...	[illegible]	[illegible]	[illegible]		[illegible]

HTTP Request Header

```
POST /webmail/Login.php HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/vnd.ms-excel,
application/vnd.ms-powerpoint,
application/msword, application/x-shockwave-
flash, */*
Referer: http://10.3.2.203/webmail/login.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Host: 10.3.2.203
Content-Length: 80
Connection: Keep-Alive
Pragma: no-cache

s_username=cms&password=&submit=Login&psd_hash
=ac2b1fca515949e5d54fb22b8ea95575
```

HTTP Response Header

```
HTTP/1.1 200 OK
Date: Sun, 20 Nov 2005 01:20:19 GMT
Server: Apache/1.3.33 (Win32)
X-Powered-By: PHP/4.4.0
Connection: close
Content-Type: text/html
```

Figure 5 Sniffing test on the prototype

5. Findings and Discussion

Password is known as one of a security method. It is used as an authentication when using email. From the sniffing test done, we can conclude that the plaintext password is not secure and can be obtained by the parties in between the transmission. Therefore, password needs to be encrypted in order to ensure its security when it is traveling through transmission media.

The sniffing test using http sniffer on the existing webmail system at FTMSK has shown that there is vulnerability in the system. Even the webmail system was not meant for sending confidential information but protecting the password is very crucial for authentication purpose.

The test on the prototype had successfully proves that protection of password at client side is worthwhile. Original password was not detected by the sniffing program. This is due to the password was first transformed to hash value before transmitted through the transmission media for authentication purpose.

6. Conclusion

One-way hashing function is a technique which can be used to enable the encryption. Password hashing should be done on the client side to protect passwords. MD5 and SHA-1 are examples of algorithm that were involved in one-way hash functions. Both were produced in the year of 1994 and came from the same extension. The development of a prototype using MD5 function has been tested successfully.

References

Edward, M.J (2000). *Think You're safe from Sniffing?* [On-line]
http://www.windowsitpro.com/articles/articlesID/8578/8788.html
Packet Sniffer.net (2003). *Password Sniffer*, [On-line]
http://www.packet-sniffer.net/password-sniffer.htm
USENIX Association(1995). *Simple Active Attack Against TCP*. [On-line]
http://www.usenix.org/publications/library/proceedings/security95/fullpapers/joncheray.txt