Security against Password Sniffing using Database Triggers

Vishal Mishra[1], Nidhi Verma[2]
M.E. final year Student[1,2]
Computer Science And Engineering Department[1,2]
Thapar University, Patiala, Punjab, India[1, 2]
vishal_mishra@live.com, nidhi02.is@gmail.com[1]

Abstract- Sniffing is one of the most common attacks on the confidentiality of the data. The attacks usually aim at finding out the passwords and other login information. The data packets carrying the password in clear text can reveal themselves to the attacker thus compromising the confidentiality. There are methods to avoid such a scenario but all of them can be bypassed. Those which cannot be bypassed involve a lot of overhead. All these points play a big role in sniffing attacks. This paper presents a cost effective, simple yet effective technique against sniffing attacks on the passwords. This paper focusses on using triggers on databases to manipulate the values of the passwords every time a client logs in.

Index Terms- Attacks, Confidentiality, Sniffing, Triggers, Security.

1. INTRODUCTION

The world has turned digital these days and so is the way that information is being stored. Digital media and internet store a huge amount of information these days which can range from a news article or a magazine to important military and government data. The thing which has proved it to be the biggest threat to the digitalization is that all the information being stored in digital format on the internet is accessible to anyone. The only wall which stands between compromising of this information is the various security principles which come into play. Authentication plays a big role among one of them and so does the confidentiality. Confidentiality refers to limiting information access rights to authorized users only. This prevents access by or disclosure to the people who are not meant to see the information. Authentication methods like user-IDs and passwords, that uniquely identify data systems' users and control access to data systems' resources, underpin the goal of confidentiality.

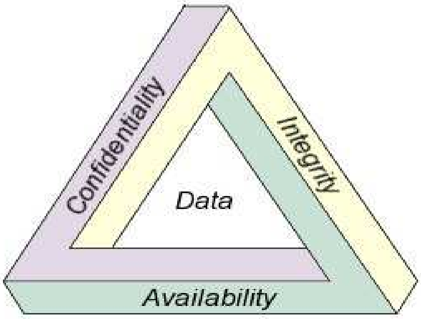

Fig 1. Security Principles

Confidentiality is the big challenge as the attacks on the internet are generally targeting the revelation of the secret data. This can be termed as good as telling the password to someone by oneself. So the issue of securing passwords came into being.

Internet is based on the use of shared media which caters to a lot of people at a single time. Thus it is obvious that compromising the shared channel simply disclose all the data. Even worse is the case of wireless networks in which everything travels through the air. Hence the aim of most of the attackers is to simply sniff of look at the data travelling through the shared media. This attack basically aims at capturing all the data travelling through the air and looking inside them to find the crucial data. If the password is travelling in the clear text which means without any encryption or obfuscation then this leads to immediate security compromise.

The problem does not end here as now days many methods have come into being which not only can break the encryptions and obfuscation but can also stop the creation of the secure connections. It can simply be proved from the existence of tools like SSLStrip which can stop the creation of a secure https connection. This further adds to the leakage of the passwords. This paper deals with creating mechanism specifically designed to stop the sniffing attacks from taking place. The paper first discusses the importance of the password hiding and then discusses the way to resolve the problem

2. CURRENT WORK

The present work focusses mostly on using of either the encryption standards or the one time passwords for hiding of the passwords. Encryption can solve almost all the problem but since the attacker can succeed in not letting the creation of a secure session by the victim the encryption scenario has not been considered. This is done due to the reason that most of the websites allow browsing at both http as well as https. It is very easy for an attacker to stop the https connection from taking place thus the connection automatically gets downgraded to http. http sends traffic in clear text hence the problem. Currently the use of one time passwords is in use for many transactional purposes. The work related to this paper mainly derives its roots form this domain.

According to Li Yinxiang *et al.*[1] the world's major banks, financial system because of security vulnerabilities caused by tampering with the accounts and economic circumstances of the loss have occurred; identity authentication technology will be a high degree of attention and applications in major banks and financial systems. Authentication refers to communications between the parties can determine the identity of each other, knowing each other is indeed who says he is , it is an important mechanism to achieve one of network security. Without a third party and just a one-time password authentication technology One Time Pad (OTP) authentication is a good solution. OTP main idea is: during the logon process by adding uncertainty to the process each time you log extract derived from the password is not the same as last, to improve the login process safety.

In the S / KEY password sequence of authentication scheme, the number of iterations diminished with the number of certification. Once the number of iterations was reduced to 0, the user cannot log in again

Daniel L. McDonald *et al.* [2]have highlighted the importance of the One Time Pad which being used even by defense forces. They created a special software package for marine forces of United States of America. The paper stated that the U. S. Naval Research Laboratory's OPIE (One-time Passwords in Everything) Software Distribution was an enhancement of Bellcore's S/KeyTM 1.0 package. OPIE improved S/Key in several areas, including FTP service with one-time passwords, and a stronger algorithm for generating one-time passwords. OPIE diverged from S/Key in select design decisions and in the behavior of certain programs. While not a total security solution, OPIE can be an important part of one. OPIE and its evolutionary predecessors have been used for over a year in parts of NRL. Its use has taught the authors lessons on implementation, usability, deployment, and future directions for improvement.

One-time Passwords in Everything should be a rule for machines that wish to defeat password sniffing attacks. The NRL OPIE distribution has improved upon earlier work in one-time passwords, as well as bringing it to more platforms. Experience with our software has pointed out better ways of doing things, as well as what still needs to be done. OPIE, while not a complete security solution, precludes a widely used class of attacks on networked computer systems.

These papers form the basis of the proposed solution to the problems stated as follows in context to sniffing attacks on the passwords. The next section will focus on why OTP even after being a perfect solution is not so perfect along with the other issues. Another purpose which can be served by the proposed method in this paper is safety from social engineering attacks like shoulder surfing. The current work going on in this field is summarized as follows.

As per Manu [3] and others who developed EyePassword, a user enters sensitive input (password, PIN, etc.) by selecting from an on-screen keyboard using only the orientation of their pupils (i.e. the position of their gaze on screen). This will be instrumental in making eavesdropping by a malicious observer largely impractical. Results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard, error rates were similar to those of using a keyboard and subjects preferred the gaze-based password entry approach over traditional methods.

According to Susan *et al.* [4] when users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual’s authentication session. This is referred to as shoulder-surfing and is a known risk, of special concern when authenticating in public places. Until recently, the only defense against shoulder-surfing has been vigilance on the part of the user. Their paper reported the design and evaluation of a game-like graphical method of authentication that is resistant to shoulder-surfing. The Convex Hull Click (CHC) scheme allows a user to prove knowledge of the graphical password safely in an insecure location because users never have to click directly on their password images. However, the protection against shoulder-surfing came at the price of longer time to carry out the authentication.

3. PROBLEM FORMULATION

As discussed earlier the main problem in password sniffing is the transfer of the password in the exact form in the communication medium. The next problem that is to be considered is however different.

The issue with the websites having OTP for logging in is not possible due to the fact that the cost of having such a system is quite high and cannot be afforded by some of the institutions. Let us discuss the problems associated in detail:

3.1. *Shared media problem*

Shared media is one of the biggest issues in the password sniffing. A dedicated link is a costly affair and can neither be used everywhere nor it can be afforded. Majority of the currently laid network works on the shared links whether they are wired or wireless.

Both the media have their own problems regarding sniffing attack. Sniffing attack in wireless though is much easier that the wired networks because of the air being the media in former. Wired networks are a bit more secure but still suffer from the problem of network taps and mirrored ports when it comes to sniffing. This problem as such cannot be resolved and will always continue to be there due to vast variety of nodes, cost and irregular architecture of the network. The only thing which can be done is improving the hiding techniques on the password itself.

3.2. *OTP Infeasibility*

In 1949, Shannon proved the perfect secrecy of the Vernam cryptographic system, also popularly known as the One-Time Pad (OTP). Since then, it has been believed that the perfectly random and uncompressible OTP which is transmitted needs to have a length equal to the message length for this result to be true. This is called as the perfect secrecy in the world of cryptography. The mathematical formulation of this proof was something like:
Shannon's Theory of Secrecy Systems [5]:

Let fM1;M2; : : : ;Mng be the message space.
The messages M1;M2; : : : ;Mn are distributed with known probabilities p(M1); p(M2); : : : ; p(Mn) (not necessarily uniform).
Let fK1;K2; : : : ;Klg be the key space.
The keys K1;K2; : : : ;Kl are distributed with known probabilities p(K1); p(K2); : : : ; p(Kl).
Usually (but not necessarily) the keys are uniformly distributed: p(Ki) = 1=l.
Each key projects all the messages onto all the cipher texts, giving a bipartite graph:

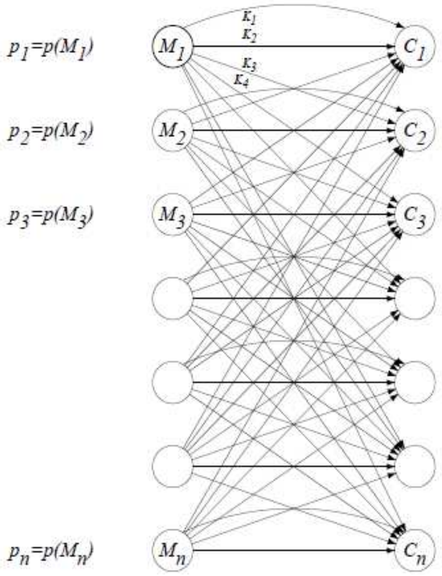

Fig 2. Shannon Perfect Secrecy

Thus no one cipher produced by a key can be mapped to or be same as another cipher using the same key. Using this it was proved that the perfect secrecy comes only from using OTP

Even after OTP being perfectly secret it is not used because of the fact that otp requires key to be random and as long as the message. Also a key used once cannot be used again which makes it even more infeasible. All the researches that are being made on this field aim at making the security conditions similar to OTP which has not succeeded till this day. Though modified versions of OTP are being used but they are used only by bigger organizations which can bear the cost of having OTP.

3.3. *Https and the cost associated*

With Otp being out of scenario encryption by other mechanisms was the second best choice. For this use Https came into being which uses secure shell to create encrypted sessions while browsing. This scheme requires a certificate by the third party certificating authority which again is a costly affair and cannot be used by the simple organizations. There are various standards which are needed to be ensure before the certificate could be applied and hence the problem. Also the attacker can bypass the https at the initial stages and completely prevent its victim from using the https connection.

4. PROPOSED SOLUTION

With all the problems discussed above it is observed that the overhead associated with these techniques is quite huge and some low overhead technique is required for the same. This paper proposes use of the database triggers for modifying the value of the password every time the user tries to access his account.

4.1 *Components Required*

The main components required by this system shall be:

- Database engine
- Pool of Random Operations
- Notification System
- Scripting engines behind the website

4.2 *Working*

The System works by simply updating the database every time a login attempt is made so that during the time of verification of the authentication a new password is generated every time. In this scenario whenever a user will try to login an operation from the pool of operations shall be picked at the random. These may include operations like Addition, subtraction, Xor etc. Then a new trigger on the database shall be fired up which will simply update this value of the password in the database itself using the previously generated random operation. This model works perfectly for the numeric alphabets. The operations used in the updating must be simple and shall be communicated to the user via a text message. The operation like adding one to each digit in the password is a perfect example. Once the user gets the message the password can be computed by the user easily and can be typed in to login. This will be an effective technique because of the fact that the password which can be sniffed in clear text will actually not be in its original form. Even if the attacker sees the password it won't get the actual hold of it. This can be used as a fool proof technique because the real password shall never be disclosed. When a user will login or a session will expire a new trigger shall be fired up changing the value of the changed password back to its original form. There are a lot of advantages to this approach for making the verification process secure.

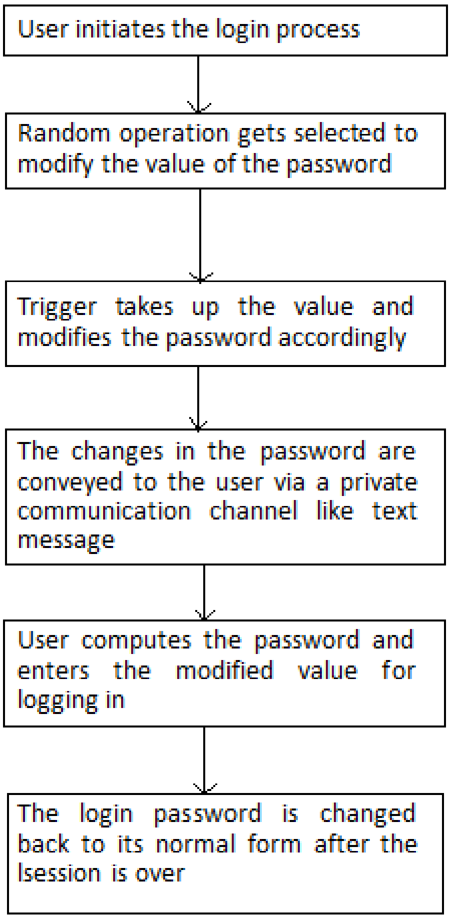
User initiates the login process
Random operation gets selected to modify the value of the password
Trigger takes up the value and modifies the password accordingly
The changes in the password are conveyed to the user via a private communication channel like text message
User computes the password and enters the modified value for logging in
The login password is changed back to its normal form after the lsession is over

Fig 3. Flow Graph Of The Model

4.3 *Component Interaction*

The component interaction model will basically have a user, a website, a scripting engine, a database engine and a pool of simple random operations with a proper notification system. User needs to be able to perform simple operations chosen for hiding of the password. A special training manual can also be provided to the users to understand the operations better. A simple php engine was used for creation of the scripts performing database queries on the background of the website. Sql was used for creation of databases. Sql server 2008 along with Sql server 2008 Management Studio was used for handling the databases. For notification system the textual messaging services on cell phones was implemented.

The scenario built as a part of this project was extremely low cost and effective. The main need of the project is to choose the random function carefully and non-repetition of the randomly generated function used.

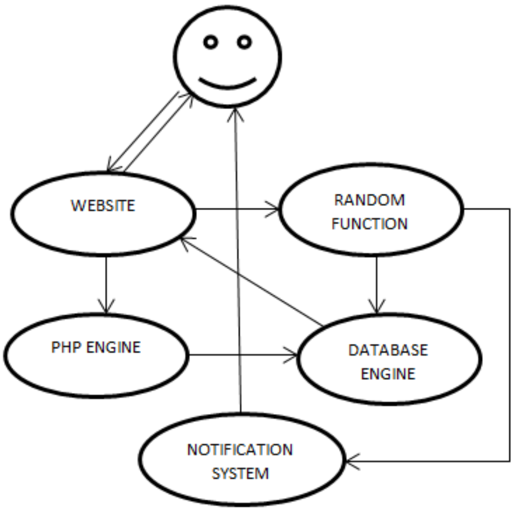

Fig 4. Component interaction

5. ADVANTAGES

The method used for preventing sniffing against the passwords has following advantages:

- The System is extremely low cost because of non-requirement of costly certifications and encryptions.
- The system is less time consuming than because of its simple and easy computations
- The system works well for both http and https
- Considerably reduced chances of disclosure due to modifications in database rather than scripts.
- Even if the attacker sniffs the password it won't be able to get actual password
- Even if actual password is known to attacker by some other means the random operation value won't give away the login.
- Helpful in other security attacks like shoulder surfing of the passwords when user is unaware of physical presence of the attacker.

6. CONCLUSION AND FUTURE SCOPE

Big companies and organizations can pay for costly security measures but it is difficult for small scale organization to do the same. Though there need for security is no less than big companies but the options available to them are few. The model proposed under this paper can be extremely effective in solving the problem of sniffing which gives an edge in the security. The main advantage of the model is using of the triggers to change the database before retrieval of the values. This will ensure good security even in those scenarios where secure connections are not being made. This can even be used as an additional authentication step in complex authentication schemes. This model ensures total protection from disclosure attacks like sniffing, shoulder surfing, dumpster diving and overhearing. In future, prevention of sniffing using alphanumeric passwords shall be considered along with better randomized password scrambling and manipulating operations.

REFERENCES

[1] Li Yinxiang; Lizhi Zhong; (2010) Research on the S / KEY One-Time Password Authentication System and its Application in Banking And Financial Systems; International Conference on Digital Content, Multimedia Technology and its Applications, Seoul, Korea; IEEE ;pp. 172-175.

[2] Daniel L. McDonald; Randall J. Atkinson; Craig Metz (1995);One Time Passwords In Everything (OPIE): Experiences with Building and Using Stronger Authentication; Proceedings of the Fifth USENIX UNIX Security Symposium.

[3] Manu Kumar; Tal Garfinkel; Dan Boneh; Terry Winograd;(2007) Reducing Shoulder-surfing by Using Gaze-based Password Entry; 3rd symposium on Usable privacy and security; ACM Society; pp. 13-19

[4] Susan Wiedenbeck; Leonardo Sobrado; Jean-Camille Birget; Jim Waters;(2006) Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme; Conference on Advanced visual interfaces; ACM Society; pp. 177-184

[5] Ueli M. Maurer ;(1992) Conditionally-perfect secrecy and a provably-secure randomized cipher; Journal of Cryptology, Volume 5, Issue 1, pp. 53-66.