QR code based authentication system for websites

[1]Shraddha Naik, [2]Monam Pandey, [3]Ashish Patil

[1,2,3]Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Dombivali, Maharashtra, India.

Abstract — In today's technology world, many web sites have features that are only accessible after registering a user account on them. These sites include forums, on-line games, corporate Intranets and many on-line shops. The sites are typically secured through a system whereby a user chooses both a unique user name and a password that will be used to authenticate them. An alternative system proposed here is more convenient for users, and in many cases more secure by removing the requirement for the user to choose or remember a password. QR code based authentication system provides the user with much easier login and access to the resources they need.

Keywords —Security, Password-less login, QR code, Android, User Authentication, One time Password.

I. INTRODUCTION

According to the existing system, user follows certain steps to get access to the system, every time the user wants to login they are needed to enter username and corresponding password, if the user has forgotten the password. The user click on option as 'forgot password?', then the user is provided with the link for password reset through email. Further the user reset his password and gets the access for the system or website. Thus the basic idea is that instead of using a password to authenticate each user, a temporary secret code is sent to them over a secure channel. Email or SMS is that (mostly) secure channel. It's almost as if the backend server makes up a temporary, one-use password each time a user wants to log in and whispers it in their ear.

The interesting thing is that we already use exactly this flow for password reset of emails. This is why we recommend taking advantage of this so you could stop remembering your passwords. It would be very useful if we can find an innovative way of accessing cloud services, which neither involves memorizing dozens of alphanumeric combinations, nor adds layers of complexity for users. For password-based authentication methods, their security is mainly determined by the difficulty of guessing a user's password.

Unfortunately, passwords usually have low entropy and are easier to guess than users think. To further enhance the security of password-based web applications, a promising solution is to deploy a technology called two-factor or multifactor authentication, in which a user is required to provide additional authentication information besides passwords.

The second piece of information is typically generated by a physical token such as RSA SecurID or a software application as Google Authenticator. If different service providers set up their own two-factor authentication services, users may have to experience painful registration and login processes repeatedly. A naive way to reduce users' burden for holding multiple passwords for different cloud services is to store users' credentials in a single device or service, and use certain key derivation functions to generate temporal passwords for sequential logins. However, this approach exposes the authentication server as a primary target of attackers.

The other approach [4] is to employ an Internet-scale identity system that defines standardized mechanisms enabling the identity attributes of its users to be shared between web applications and cloud services. A number of technologies and standards such as OpenID and OAuth have emerged to deliver an Internet-scale identity system during the past few years. The basic idea of those identity systems is to authenticate users with the aid of trusted Identity Providers (IDPs).

Recently, Bonneau et al. presented a comprehensive evaluation for two decades of proposals to replace text passwords for general-purpose user authentication on the Internet. Their evaluation results have demonstrated the difficulty of replacing passwords and highlighted the research challenges towards designing a password-less login scheme.
In this contribution, we propose this system, an innovative security framework for password less universal login. This salient feature comes from the adoption of push message services for mobile devices and public-key cryptography. Different from most existing login solutions, the servers in system are not able to generate users' credentials. As a potential application of the system security framework, we have applied it to build a password less mobile payment solution for tackling the recent MintChip [1] challenge.

II. LITERATURE SURVEY

Passwords are a commonly-used method of authentication. A unique sequence of characters is presented to the system when identification is needed [1] [2]. This sequence is then compared with a stored sequence, perhaps after some transformation (e.g., encryption). A match provides the proof of identity. One weakness with password systems is the choice of the password. If the choice of possible characters to use in the password is too small, or if the overall length of the password is too short, the password may be comprisable. Even a rich character set may not be sufficient to create secure passwords lithe combination of characters is restricted to an arbitrary set of possibilities. Thus, good password choice should avoid common words and names.

The typical sequence for registering and logging on to a web site forum normally follows the sorts of steps described below as used by web sites like CiteSeerx, http://citeseerx.ist.psu.edu/:

The user chooses to register on the web site.

1) A registration form captures a minimum of the following:
    a. A user name.
    b. The desired password.
2) The contact email address.
3) An email is then sent to the user containing an activation link.
4) The user clicks on the activation link.
5) The user can now log in to the site using their user name and password.
6) The user has access to the site as an authenticated visitor.

The purpose of the activation link (when used) is not to increase the security of the user's account, but rather to make it more difficult for an attacker to automate the process of signing up to the forum. Password based authentication systems appear easy to implement, but are vulnerable to attacks from two directions: losses caused by the theft of the database containing user account credentials and weak passwords chosen by the users. Many users choose very weak passwords and often reuse the same password for multiple web sites. Breaches have been caused where even experienced system administrators have chosen weak passwords. In fact, users are unwilling to remember long and complex passwords, the sort they must use to be secure. Although there is a large amount of advice available to developers on how to more securely manage passwords (i.e. the use of salts and good quality hashing algorithms) many high profile sites have failed to look after user passwords until after there has been a breach. For example. The popular new aggregating website Reddit, www.reddit.com, lost an undisclosed number of passwords when part of a backup was stolen. The disclosure was caused due to an ill-advised "feature" whereby users would be able to recover their original password rather than having a new one sent to them. Another problem not often discussed with password based sites is that if a password is discovered by a third party then the end-user is often unaware of the breach. This is most evident in phishing attacks.

When a user forgets their password a new one must be generated for them as the password is not stored by a properly written password based system. There are various mechanisms proposed for handling forgotten passwords.

- Regenerate a new password and email that to the user.
- Generate a password reset token and email that to the user.

III. EXISTING SYSTEM

The existing system [2] is structurally very similar except the user is never asked to either choose nor enters a password. Because the user doesn't need to remember or choose a password a much longer password can be chosen by the system. The existing system as an end user sees it consists of the following steps:

- ✓ The user chooses to register on the web site.
- ✓ A registration form captures a minimum of the following:
    - A user name.
    - The contact email address.
- ✓ An email is then sent to the user containing an activation link.
- ✓ The user clicks on the activation link.
- ✓ The user has access to the site as an authenticated visitor.

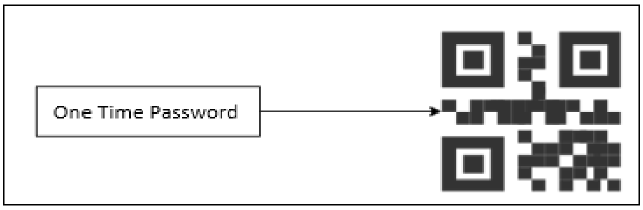
From a user's perspective the system appears simpler and there is no password to remember. The account however becomes tied to the browser that they used when they followed the activation link. Although this tying of the account to the browser may seem inconvenient, for some use cases it is an advantage.

Simple implementations would limit a user to a single browser at a time, but it is possible to allow multiple browsers. The existing system is not intended to try to solve all problems of current forms/cookie-based authentication, only those associated with users choosing weak passwords.

IV. PROPOSED SYSTEM

1) In this system every user will have a secret username which will be known to that user only; This username will be binded with the mac address of the user's device.

2) For this username during login process on a web service a One Time Password will be generated which will be embedded into QR code [3].



3) The user will use its device to scan the QR code and will send the decoded OTP to the web service.

4) The username and user's device mac address are binded due to which user can simply login using its own device.

5) This is a secure way in which user don't have to remember password. The user has access to the site as an authenticated visitor

V. WORKING AND IMPLEMENTATION

Here three device will come into picture one will be PC client from where the user will be accessing the website, second will be the Mobile client which will be used by him to gain access to the system and third will be the server who will be handling all the procedures.

A. *Registration process*

1) We will be requesting form from the server from PC client and the server will respond to our request by providing the form.

2) While registering for the website user will be filling his contact details and email address which will be used to contact him in future just in case if user forgets his username or his device is lost. Since we are trying to reduce the steps required for login, here no password will be used. One thing to note down is username he will type must be unique and it must be kept secret by the user. After filling this details we will submit those to the server.

3) After checking that the username is not taken by any other user server will generate One Time Password (OTP) for the corresponding username which will be embedded into the QR code and this QR code will be displayed on the registration Form. OTP before encoding into QR code will be encrypted by server using AES algorithm and hence can only be decrypted by the server [5] [6] [7].

4) Now here the requirement is that user must install android application for this system. This application will be used to scan the QR code provided by registration form, app will Decode this QR code and get the encrypted OTP. At the same time app will also fetch MAC address of the device and will combine both OTP and the MAC address as a package and will send to the server.

Once this OTP is decrypted and verified by the server generated for the username it will make an entry of the received MAC along with the Username provided by the user. This process binds User's mobile with his Account details. Hence while login user don't need to use password, instead he will use his mobile in the same way he used it for registering.

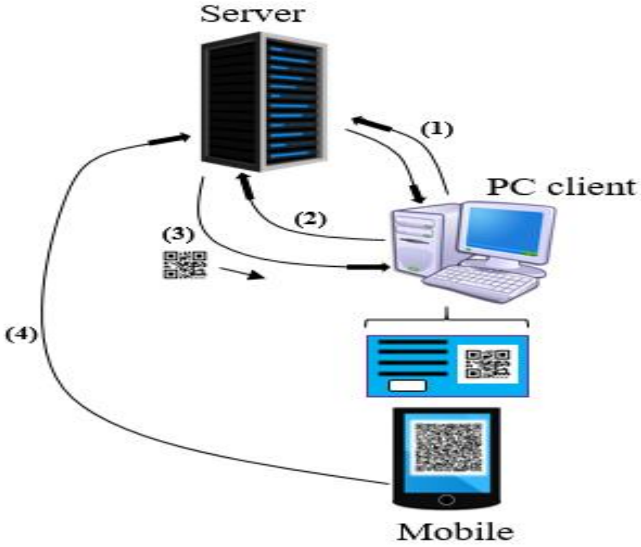


Fig.1 Registration and login steps

B. *Login process*

To login into the system web form will ask user for his username. After providing the one, server will again generate OTP and embed it into the QR code in the same way done for registration phase. Similarly user will use his phone to scan the QR code with the app, with the same phone that was used while registering, because application will be sending again device MAC along with the decoded OTP. If the MAC along with the corresponding Username matches with Mac and the username provided during registering process the user will gain access to the system. Similar to registration process same steps will be repeated except here we will be needing user to provide his username.

VI. APPLICATIONS

This system can be applied to the current forums and websites to ease the registration process.

Integration of different online accounts with the single application can be made to perform authentication of these accounts via single system.

It can replace Smart Card and Swipe Card: It requires the separate scanner to scan the smart card. Smart card has less storage as compare to QR code and swipe card can be cloned.

VII. EXTENSIONS

This system would consume less time when the frequency of login is more and session period is of few seconds. It would be great if it is used in booking sections or ticket generation systems. Consider instead of ticket providers on a railway station there are booths having display and printing facilities which are connected to internet and will print ticket for the users. A user would fill his travelling locations in the android application which is connected to user's bank account. After selecting this locations user need to go to this booth and scan the QR code displayed on this booth, phone will simply interact with server, perform payment and will trigger corresponding booth to print ticket. This would reduce man power required as well as increase efficiency of the system. Here user don't need to provide any username or password.

VIII.CONCLUSION

Using one time password eliminates the factor of remembering the passwords, but it is an overhead of using a new password at every single time the user logins. The above system takes the advantage of this facility as well as makes it efficient for a user to use this one time password.

The pair of System embedding OTP into QR code in a cryptic approach and the pertinent application decoding the corresponding code makes the process effortless for the user to access the system. This system covers 2 key points of any authentication system i.e. "what you know ?" and "what you have?", while the user just need to remember his username and carry his phone known to be today's basic need.

It makes registration simpler and reduces it to 1 step which is beneficial for user. Although verifying the user's email address is mandatory requirement, but linking restricted username with user's phone delays this requirement.

Moreover different sites and forums restrict privileges to their resources for guest users. Implementation of QR code based authentication over this resources would be convenient for both entities as it would eliminate procedures involving two step verification.

QR code Based login, as a mode of Password-less Login implementations is uncommon because it doesn't have to be relied on the Third-party Authentication or Authorization. It should however be easier for many users and has the potential for improved security for most users as well. It is also no harder to implement than a properly implemented password-based authentication system.

ACKNOWLEDGMENT

We sincerely wish to thank our project guide Prof. Nagamani for her ever encouraging and inspiring guidance. We thank our project coordinator Prof. Uttara Gogate for giving us proper guidance and timely motivation. We also express our deepest thanks to our Head of Computer Department Prof. P.R.Rodge whose benevolent helps us making available the computer facilities to us for our project in our laboratory and making it true success. We would like to thank our college principal Dr. J. W. Bakal for providing lab faculties and permitting us to go on with our project. We would also like to thank our colleagues who helped us directly or indirectly during our project.

REFERENCES

[1] Bo Zhu,Xinxin Fan and Guang Gong – " *Loxin , a solution to passwordless universal login*, IEEE paper, 2014".

[2] Kirit Saelensminde and Prof. Veera Boonjing - "*A simple password less authentication system for web sites*, Seventh International Conference on Information Technology IEEE paper, 2010"

[3] Kuan-Chieh Liao, Min-Hsuan Sung, Wei-Hsun Lee, Ting-Ching Lin - "*A One-Time Password Scheme with QR-Code Based on Mobile Phone*" 2009 Fifth International Joint Conference on INC, IMS and IDC.

[4] Renjie Weng – "*Password-less login Everywhere, Journal of Stevens Institute of technology*, Hoboken, NJ07030".

[5] *Cryptography and Network Security: Principles and Practice*, 5th edition Book by William Stallings.

[6] *Cryptography and Network Security* by Book by behrouz a forouzan.

[7] *Security in Computing*. 4th edition Book by charles p. pfleeger.