ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Providing Security for Web Application using Android Application

V.Divya
M.Tech Student,
Dept of CSE,
Jawaharlal Nehru Institute of Technology,
Hyderabad.

G.Deepthi, M.Tech
Associate. Professor,
Dept of CSE,
Jawaharlal Nehru Institute of Technology,
Hyderabad.

ABSTRACT:

Text watchword is that the most well liked style of user authentication on websites as a result of its convenience and ease. however, user's passwords unit of measurement in danger of stolen and compromised beneath all completely different threats and vulnerabilities. firstly, users typically select weak passwords and utilize constant passwords across completely different websites. routinely reusing passwords causes a upshot once academic degree person compromises one watchword, she's going to exploit it to attain access to plenty of internet sites. second, writing passwords into un-trusted computers suffers watchword criminal threat. associate in nursing person can launch several watchword stealing attacks to grab passwords, like phishing, key loggers and malware. during this paper, we've an inclination to vogue a user authentication protocol named opass that leverages cell phones of users and sms(short message services) to thwart watchword stealing and watchword utilize attacks. opass solely desires each collaborating information processing system possesses a unique signaling, and include a tsp in registration and recovery stages. the opass, users alone would really like to recollect a semi permanent watchword for login on all websites. When evaluating the opass epitome, we've an inclination to believe opass is economical and cheap differentiate with standard network propensity mechanisms.

KEYWORDS: opass, recovery, registration.

1. INTRODUCTION:

OVER the past few decades, text word has been adopted because they essential for user authentication to websites. Folks while registering accounts choose user name and text words as password on an internet site. So as to log into the website with success, users should recall the chosen passwords. Generally, password-based user authentication will resist brute force and wordbook attacks if users choose sturdy passwords to provide enough entropy. However, password-based user authentication features a major drawback that humans aren't specialists to hold grip on text strings. Therefore, most users would opt for easy-to-remember password although they recognize the password was unsafe. The other crucial problem is that users tend to recycle passwords across numerous websites. In 2007, Florencio and Harley showed that a user reuses a word across three.9 totally different websites on average. Word recycle causes users to lose sensitive info stored in numerous web links. If a hacker compromises one among their passwords. This attack is named because the counter sign employ attack. The top of issues area unit causes negative influence of human factors. Therefore, requires human factors into thought once planning a user authentication protocol. Up to now, researchers have scrutinized a spread of technology to reduce the negative influence of human factors within the user authentication procedure. Since humans area unit superior in memory graphical passwords than text passwords many graphical countersign schemes were designed to handle human's countersign recall down side exploitation password management tools is another. These tools mechanically generate sturdy passwords for every website, that addresses password employ and countersign recall issues. The advantage is that users solely have to be compelled to bear in mind a master countersign to access the management tool. Despite the help of those two technologies graphical password and countersign management tool the user authentication system still suffers from some considerable drawbacks. Although graphical countersign could be a nice plan, it's not nonetheless mature enough to be wide enforced in observe and is still prone to many attacks. Countersign management tools work well; but, general users doubt its security and therefore feel uncomfortable concerning exploitation it. What is more, they have hassle exploitation these tools owing to the dearth of security information. Besides the countersign employ attack, it's conjointly vital to consider the results of countersign stealing attacks. The adversaries steal or compromise passwords and impersonate users' identities to launch attacks, collects sensitive data, perform unauthorized payment actions, or leak money secrets. The phishing is that the most typical and economical countersign stealing attack. In keeping with APWG's report, the number of distinctive phishing websites detected at the second season. Several previous studies had proposed schemes to defend against countersign stealing attacks. Some researches specialized in three-factor authentication rather than password-based authentication to supply a lot of reliable user verification. Three-factor verification depends on what you recognize (e.g., password), what you have got (e.g., token), and World Health Organization you're (e.g., biometric). To pass the verification, the user should input a countersign and supply a pass code generated by the token and scan her biometric options (e.g., fingerprint or pupil). Three-factor verification could be a comprehensive defence against password stealing attacks; however it needs comparative high value. Thus, two-factor verification is a lot of enticing and sensible than three-factor authentication.

2. PREVIOUS SYSTEM:

- In present days, most systems rely on static passwords to verify and validate user's identity in online transactions.
- By using static passwords there is no full verification and any one can hack that even.
- The string password been accepted as the primary mean of user verification for websites. People select their username and text password when registering in their accounts on a website in order to log into a website successfully, user must recall selected passwords.

LIMITATIONS:

- In the existing system, user's use the same password for each and every website have to login in this process the hackers may get the password using some malfunction.
- In the existing system, using the same password for each and every website causes users to lose sensitive data. In order to avoid this proposed system introduce the graphical password but it is also not effectively performed.

3. PROPOSED SYSTEM:

- The state-of-art is generating a secret key for each individual user.
- And we will be using Long term password Generation algorithm and MD5 to generate a secret key.
- This secret key is sent to the account holder's mobile directly using the GSM Modem.

ADVANTAGE:

- The main approach of opass is free users from having to remember or type any password into conventional computer for verification. Opass involves a basic cell phone, which is used to generate one-time password and new communication channel, SMS, which is used to transmit verification messages.

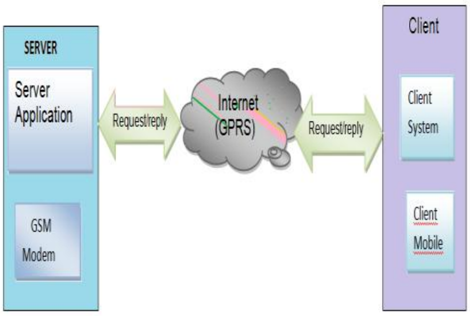

Fig:1 Architecture Diagram

4. RELATED WORK:

REGISTRATION PHASE:

The aim of this phase is to allow a user and a server interacts with a shared secret key to authenticate login for particular user through mobile application. The user opening the oPass application installed on cell phone then enters id and website url or domain name to the application. The mobile application program on user mobile sends account id and url to the tele - communication service provider (TSP) through a 3G network connection to make a request of registration. Once the TSP received the account id and url, it trace the user's phone number based on SIM card. The TSP plays the role of third-party to distribute a shared key among user and server. The shared key used to encrypt registration SMS. The TSP and the server will connect and established an SSL tunnel to secure communication. The TSP forwards account id, and to the assigned server. The Server will generate information of user account and reply response, including server's id, and server's phone number. The TSP then sends id, and a shared key to user's mobile phone. Once process of receiving response is finished, the user continues to setup a long-term password with his phone.

LOGIN PHASE:

The login stage begins when the user sends a request to server through an un trusted browser (on a kiosk). The user use cell phone produces a one-time password. From the pre shared secret details, server can verify and particular user.

The application protocol starts when user desire to log into favourite web site. However, it begins login procedure by accessing desired website via a browser on an un trusted kiosk. The browser sent a request to account ids. In second step, server supplies id to our developed browser. Meanwhile, this message is forwarded to cell phone through GSM Modem. After getting message from cell phone inquiries related information from its database which includes a server's phone number and other parameters. Secret shared credential can reproduce by inputting the correct key on cell phone. The one-time password for current login website is recomputed if it received equal the previously generated, the user is legitimate or server will reject that particular login request. After successful verification, the server sends back a successful message through the Internet, if the user is successfully log into the server then concern website opens in our developed web browser.

RECOVERY PHASE:

Recovery phase is designated for some specific conditions; for example, a user may lost cell phone. The application protocol able to recover oPass setting on new cell phone assuming that user still uses the same old phone number. Again, the user has to install oPass application program on new cell phone then able to launch the application program to send a recovery request with old account id and requested server id to TSP through a 3G connection. As mentioned before, id would be domain name or link of server. Same like in registration, TSP can traced phone number based on SIM card and sent account id details to server through an SSL tunnel. The server receives request, probes concern account information in its backend database to checks if account is registered or not. If account id exists, the information used to compute secret details will be fetched and sent back to user. This directive method of recovery phase includes all elements for generating the next one-time passwords to user. When the cell phone application program receives message like in registration stage, it forces user to enter long-term password to generate correct one-time password.

During the last step, the user's cell phone encrypts the secret details and server nonce to a cipher text. The recovery SMS message is delivered back to the server for verification. Similarly, the server computes decrypts this message to ensure that user is already recovered. At this point, new cell phone is recovered and ready to perform further logins. For the next login, otp will be used for user verification.

GSM MODEM IMPLEMENTATION:

Global system for mobile modem is special type modem which accepts SIM card and operating with a subscription to mobile operator, same as phone. According to mobile operator point of view, a GSM modem visualized like a mobile phone. By importing the comm Driver and connecting the Modem to the PC with a serial port.

5. CONCLUSION:

In this paper, we tend to planned a user authentication protocol named oPass that integrated a cell phone and uses SMS to eliminates password stealing and countersign utilize attacks. The browser users assume that each web site possesses a novel number. We also assume that a tele-communication service provider participates in registration and recovery phases. Through oPass, every user solely has to remember a long-run countersign that has been accustomed shield her radiotelephone. Users area unit free from typewriting any passwords into un trusted computers for login to all websites. From the past used schemes, oPass is the first user authentication protocol to prevent countersign stealing (i.e., phishing, key logger, and malware) and countersign utilize attacks at the same time. The reason is that oPass adopt one-time countersign approach to ensure independence between every login. To create oPass totally functional, countersign recovery is additionally thought of and supported when users lose their cell phones. Users can recover their oPass system with reissued SIM cards and long-run passwords.

REFERENCES:

[1]. S. Gawand E. W. Felten, “Password management strategies for online accounts,” in SOUPS’06: Proc. 2nd Symp. Usable Privacy Security, New York, 2006, pp. 44–55, ACM.

[2]. C. Herley, “A large-scale study of web password habits,” in WWW ’07: Proc.16th Int. Conf. World Wide Web, NewYork, 2007, pp. 657–666, ACM.

[3]. S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, “Multiple password interference in text passwords and click-based graphical passwords,” in CCS’09: Proc. 16th ACM Conf. Computer Communications Security, New York,2009, pp.500 – 511, ACM.

[4]. M. Vijayalakshmi and A.Kannan,” proactive location-based context aware service using agents”, International Journal of Mobile Communications, vol.7,no.2,pp.232 - 252,2000.

[5]. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and Analysis of graphical passwords,” in SSYM’99: Proc. 8th Conf. USENIX Security Symp, Berkeley, CA, 1999, pp. 1–1, USENIX Association.

[6]. A. Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in Proc. Int. Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7]. J. Thorpe and P. van Oorschot, “Towards secure design choices for implementing graphical passwords,” presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.

[8]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,” Int. J. Human-Computer Studies, vol. 63, no. 1–2, pp. 102–127, 2005.

[9]. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, “Design and evaluation of a shoulder surfing resistant graphical password scheme,” in AVI ’06: Proc. Working Conf. Advanced Visual Interfaces, NewYork, 2006, pp. 177–184, ACM.

[10]. B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in CCS ’02:Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.