IJDCST @Feb-Mar, 2014, Issue- V-2, I-2, SW-17
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Providing Security against Password Stealing and Password Reuse Attacks

[1]Rahul Aditya Kidambi[2]Dr. N.Chandra Sekhar Reddy[3]Mukunda Reddy
[1]M.Tech(CSE), Institute of Aeronautical Engineering College , Hyderabad-500043, A.P, India
[2]Professor, CSE dept , Institute of Aeronautical Engineering College , Hyderabad-500043, A.P, India
[3]Professor, CSE dept, Institute of Aeronautical Engineering College , Hyderabad-500043, A.P, India

ABSTRACT: Text watchword is that the hottest variety of user authentication on websites as a result of its convenience and ease. However, users' passwords square measure at risk of be purloined and compromised under totally different threats and vulnerabilities. Firstly, users often choose weak passwords and reprocess constant passwords across different websites. Habitually reusing passwords causes a domino effect once associate degree person compromises one watchword, she will exploit it to achieve access to a lot of websites. Second, writing passwords into untrusted computers suffers watchword stealer threat. An person will launch many watchword stealing attacks to snatch passwords, like phishing, key loggers and malware. In this paper, we have a tendency to style a user authentication protocol named oPass which leverages a user's cellular phone and short message service to thwart watchword stealing and watchword reprocess attacks. OPass only needs every taking part web site possesses a novel phone number, and involves a telecommunication service supplier in registration and recovery phases. Through oPass, users solely would like to remember a semi permanent watchword for login on all websites. After evaluating the oPass epitome, we have a tendency to believe oPass is economical and affordable compared with the standard internet authentication mechanisms.

KEYWORDS: opass, recovery, registration

INTRODUCTION:

OVER the past few decades, text word has been adopted because the primary mean of user authentication for websites. Folks choose their username and text passwords when registering accounts 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 in memorizing text strings. Thus, most users would opt for easy-to-remember passwords (i.e., weak passwords) although they recognize the passwords may well be unsafe. Another crucial problem is that users tend to recycle passwords across numerous websites. In 2007, Florencio and Herley indicated 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 websites if a hacker compromises one among their passwords. This attack is named because the countersign employ attack.The on top of issues area unit caused by the negative influence of human factors. Therefore, it's vital to require human factors into thought once planning a user authentication protocol. Up to now, researchers have investigated 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 downside exploitation password management tools is another . These tools mechanically generate sturdy passwords for every web site, 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 2 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. Adversaries steal or compromise passwords and impersonate users' identities to launch malicious attacks, collect sensitive data, perform unauthorized payment actions, or leak money secrets. 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 have proposed schemes to defend against countersign stealing attacks. Some researches specialize in three-factor authentication rather than password-based authentication to supply a lot of reliable user authentication. Three-factor authentication 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 authentication, 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 authentication could be a comprehensive defense against password stealing attacks, however it needs comparative high value.Thus, two-factor authentication is a lot of enticing and sensible than three-factor authentication.

LITERATURE SURVEY:

Towards Secure Design Choices For Implementing Graphical Passwords

We study the impact of selected parameters on the size of the password space for "Draw-A Secret" (DAS) graphical passwords. We examine the role of and relationships between the number of composite strokes, grid dimensions, and password length in the DAS password space. We show that a very significant proportion of the DAS password space depends on the assumption that users will choose long passwords with many composite strokes. If users choose passwords having 4 or fewer strokes, with passwords of length 12 or less on a 5 × 5 grid, instead of up to the maximum 12 possible strokes, the size of the DAS password space is reduced from 58 to 40 bits. Additionally, we found a similar reduction when users choose no strokes of length 1. To strengthen security, we propose a technique and describe a representative system that may gain up to 16 more bits of security with an expected negligible increase in input time. Our results can be directly applied to determine secure design choices, graphical password parameter guidelines, and in deciding which parameters deserve focus in graphical password user studies.

Purely Automated Attacks OnPasspoints-Style Graphical Passwords

We introduce and evaluate various methods for purely automated attacks against PassPoints style graphical passwords. For generating these attacks, we introduce a graph-based algorithm to efficiently create dictionaries based on heuristics such as click-order patterns (e.g., 5 points all along a line). Some of our methods combine click-order

heuristics with focusof- attention scan-paths generated from a computational model of visual attention, yielding significantly better automated attacks than previous work. One resulting automated attack finds 7-16% of passwords for two representative images using dictionaries of approximately 226 entries (where the full password space is 243). Relaxing click-order patterns substantially increased the attack efficacy albeit with larger dictionaries of approximately 235 entries, allowing attacks that guessed 48-54% of passwords (compared to previous results of 1% and 9% on the same dataset for two images with 235 guesses). Our results show that automated attacks, which are easier to arrange than human-seeded attacks and are more scalable to systems that use multiple images, pose a significant threat to basic PassPoints-style graphical passwords.

3. Password Management Strategies For Online Accounts

Given the widespread use of password authentication in on- line correspondence, subscription services, and shopping, there is growing concern about identity theft. When peo- ple reuse their passwords across multiple accounts, they in- crease their vulnerability; compromising one password can help an attacker take over several accounts. They sometimes failed to realize that personalized passwords such as phone numbers can be cracked given a large enough dictionary and enough tries. We discuss how current systems support poor password practices. We also present potential changes in website authentication systems and password managers.

A Large scale Study Of Web Password Habits

We report the results of a large scale study of password use and password re-use habits. The study involved half a mil- lion users over a three month period. A client component on users' machines recorded a variety of password strength,\ usage and frequency metrics. This allows us to measure or estimate such quantities as the average number of pass- words and average number of accounts each user has, how many passwords she types per day, how often passwords are shared among sites, and how often they are forgotten. We get extremely detailed data on password strength, the types and lengths of passwords chosen, and how they vary by site. The data is the large scale study of its kind, and yields numerous other insights into the role the passwords play in users' online experience.

RELATED WORK:

Registration Phase:

The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins by opening the oPass program installed on her cell phone she enters IDu (account id she prefers) and IDs (usually the website url or domain name) to the program. The mobile program sends account id and url to the telecommunication service provider (TSP) through a 3G connection to make a request of registration. Once the TSP received the account id and the url, it can trace the user's phone number based on user's SIMcard.

The TSP also plays the role of third-party to distribute a shared key between the user and the server. The shared key is used to encrypt the registration SMS with AES-CBC. The TSP and the server will establish an SSL tunnel to protect the communication. Then the TSP forwards account id, and to the assigned server. Server will generate the corresponding information for this account and reply a response, including server's identity ID, a random seed, and server's phone number. The TSP then forwards id, and a shared key to the user's cell phone. Once reception of the response is finished, the user continues to setup a long-term password with her cell phone.

Login phase:

The *login* phase begins when the user sends a request to the server through an untrusted browser (on a kiosk). The user uses her cell phone to produce a one-time password, e.g., , and deliver necessary information encrypted with to server via an SMS message. Based on pre shared secret credential, server can verify and authenticate user . The detail flows of the login phase. The protocol starts when user wishes to log into her favourite web server (already registered). However, begins the login procedure by accessing the desired website via a browser on an untrusted kiosk. The browser sends a request to with account IDs. Next, server supplies the ID and a fresh nonce to the browser.

Meanwhile, this message is forwarded to the cell phone through GSM Modem. After reception of the message, the cell phone inquiries related information from its database via IDs, which includes server's phone number and other parameters The next step is promoting a dialog for her long-term password. Secret shared credential can regenerate by inputting the correct on the cell phone. The one-time password for current login is recomputed If the received equals the previously generated, the user is legitimate; otherwise, the server will reject this login request. Upon successful verification, the server sends back a success message through the Internet, if the user is successfully log into the server,

Recovery Phase:

Recovery phase is designated for some specific conditions; for example, a user may lose her cell phone. The protocol is able to recover oPass setting on her new cell phone assuming she still uses the same phone number (apply a new SIM card with old phone number). Once user installs the oPass program on her new cell phone, she can launch the program to send a recovery request with her account ID and requested server ID to predefined TSP through a 3G connection. As we mentioned before, ID can be the domain name or URL link of server. Similar to registration, TSP can trace her phone number based on her SIM card and forward her account ID and the to server through an SSL tunnel. Once server receives the request, probes the account information in its database to confirm if account is registered or not. If account ID exists, the information used to compute the secret credential will be fetched and be sent back to the user.

This message Procedure of recovery phase. Includes all necessary elements for generating the next one-time passwords to the user . When the mobile program receives the message, like registration, it forces the user to enter her long-term password to reproduce the correct one-time password. During the last step, the user's cell phone encrypts the secret credential and server nonce to a cipher text. The recovery SMS message is delivered back to the server for checking. Similarly, the server computers and decrypts this message to ensure that user is already recovered. At this point, her new cell phone is recovered and ready to perform further logins. For the next login, one-time password will be used for user authentication

GSM Modem Implementation:

GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. Importing the comm Driver and connecting the Modem to the PC with serial port.

CONCLUSION:

In this paper, we tend to planned a user authentication protocol named oPass that leverages cellphones and SMS to thwart password stealing and countersign utilise attacks. We assume that each web site possesses a novel number. We also assume that a telecommunication service supplier participates in the registration and recovery phases.The look principle of oPass is to eliminate the negative influence of human factors as much as doable. 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 untrusted computers for login on all websites. Compared with previous schemes, oPass is that the 1st user authentication protocol

to prevent countersign stealing (i.e., phishing, keylogger, and malware) and countersign utilise attacks at the same time. The reason is that oPass adopts the 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 cellphones. They'll recover our oPass system with reissued SIM cards and long-run passwords.

REFERENCES:

[1] B Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[2] 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.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in *WWW '07: Proc. 16th Int. Conf. World Wide Web.*, New York, 2007, pp. 657–666, ACM.

[4] 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.

[5] I. 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 TechniquesE-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.