A Review on Two Level Graphical Authentication Against Key-Logger Spyware

Kanchan V. Warkar
Department of Information Technology,
Bapurao Deshmukh College of engg, Sevagram

Prof. Nitin J. Janwe
Department of Computer Technology,
R.G.C.E.R.T, Chandrapur,

ABSTRACT
Spywares has become major problem now days. This type of software may track user activities online and offline. Password collection by spywares is increasing at a shocking pace. The problem of entering sensitive data, such as passwords, from an untrusted machine, is obviously insecure; however roaming users generally have no other option. They are in no point to review the security status of, Internet cafe or business center machines, and has no alternative to typing the password. The difficulty of mounting a collusion attack on a single user's password makes the problem more tractable than it might appear. This problem of password security can be improved by biometric based authentication and graphical authentication, however availability and cost of biometric authentication is considerable problem. In this paper, we present an alternative user authentication based on two levels of security walls, first based on pin code and second use Images that is resistant to keylogger spywares. this method that uses a strengthened cryptographic hash function to compute fast and secure passwords for arbitrarily many accounts while requiring the user to memorize only few memorable points in the image. In addition to keylogger spywares our design is also highly resistant to brute force attacks, modification attack and prone to Dictionary attack, allowing users to retrieve their passwords from any location so long as they can execute our program and remember a short secret.

1. INTRODUCTION
Spywares has become serious threat to computer security. According to the pew Internet & American life project (PIP) survey 50% of Internet users see software programs like spyware as a serious threat to their online security [3]. The term spyware first came into use in 1995; today spyware is a serious and persistent problem that none of the known internet security technologies like firewalls or anti-viruses can address fully. Anti-spyware technology was first introduced in 2000, but the surge of newer anti-spyware solutions continues even today, it gives a clear indication of the commonness of Spyware as an ever growing problem.

There are different ways through which spyware can enter into a computer system for example as a software virus or as the result of installing a new application. It can impair the operation of computers, causing them to crash and interfering with the ability of consumers to use them. Spyware programs often cause significant degradation in system performance. Spyware can even cause computers to crash. Microsoft reported that 50% of its customers computer crashes are traceable to spyware [4]. Spyware may use so many system resources that users are no longer able to use their keyboard, mouse, and their cursors freeze. Spyware can impair the operation of computers, causing them to crash and interfering with the ability of consumers to use them. Spyware programs often cause significant degradation in system performance.

There was general agreement that spyware can assert control over the operation of computers in ways that substantially limit the ability of consumers to use their computers. For example, some spyware programs change users' browser setting, which is often referred to as "browser hijacking." Spyware may change the web page displayed when the browser first opens, i.e., the home page, and frustrate efforts to replace that home page with the user's original home page. Spyware may also insert links to its own websites into the user's "Bookmarks" or "Favorites" list. One spyware program, for instance, intercepts search queries sent to Google, a popular search engine, and then displays its own search results. The search results appear to be from Google but contain links to pornographic websites that would not have appeared with an actual Google search. Moreover spyware risks are not limited till the degradation and harming computer performance and operations. Spywares can also, steal the user's personal information and do tracking of a user's online activity. The most serious privacy risks arise when spyware installed on a computer includes password hijackers or keylogger.

A keylogger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e.g., a mailing address or telephone number), financial information submitted as part of an online transaction, and the contents of emails or instant messages. One can have firewall installed in a computer, however normally firewalls are designed to block specific kinds of threats and look only at certain attributes of incoming transmissions, much like the post office looks only at the addresses or attributes on a letter, but does not look at, or attempt to evaluate, the letter's content. Some of the major spyware categories are adware, malware, keylogger, browser helper objects, worms, Trojans, password hijackers, E-mail flooders, firewall killers, spoofers, hacking tools, dialers, tracking cookies, remote administration tools, backdoors and annoyance tools. We have focused mainly on the password hijackers and Keylogger spywares as these are the most insidious threats to a user's personal information. Passwords, credit card numbers, and other sensitive or personally identifying information are potentially exposed.

2. ALTERNATIVE USER AUTHENTICATION
Most of the applications are based on text based password entry for user authentication, however there are some other promising solutions for user authentication like image-based authentication and biometric authentication.

All user authentication schemes are based on three fundamental pieces of information: what you know, what you have, and who you are [5] which, also corresponds to token based authentication, knowledge-based authentication and biometric authentication. For proving who they are, users can provide their name, email address, or a user ID. Since this information provides no assurance of identity, some system operators are beginning to employ biometrics (such as fingerprints, voice recognition, iris scans, or retinal scans) as methods of user

identification. For proving what they have, users can produce service cards (i.e., ATM cards), physical keys, digital certificates, smart cards etc) [6]. For proving what they know, users can provide a password or pass phrase, or a personal identification number (PIN). This information is essentially a secret that is shared between the user and the system. Knowledge based techniques are the most widely used authentication techniques and include both alphanumeric and graphical authentication.

In graphical authentication, system use one or several images to authenticate a user rather than typing a password. Biometric authentication techniques are further categorized into Physiological and Behavioral based schemes, such as fingerprints, voice recognition, iris scan, or facial recognition are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Recently, efforts have been made towards graphical authentications schemes, which are resistant to password hijackers and keylogger spywares and prevent stealing of users password.

3. LITERATURE REVIEW

M. N. Doja and Naveen Kumar was presented an alternative user authentication based on Images that is resistant to keylogger spywares. They were designed and implemented a method that uses a

strengthened cryptographic hash function to compute fast and secure passwords for arbitrarily many accounts while requiring the user to memorize only few memorable points in the image. In addition to keylogger spywares their design is also highly resistant to brute force attacks and prone to Dictionary attack, allowing users to retrieve their passwords from any location. In their paper "Image Authentication Schemes Against Key-logger Spyware" [1]. They were used MD5 algorithm for authentication.

Alphanumeric passwords also have drawbacks, most notably in terms of memorability and security like hacking of password. This has led to innovations to improve these password schemes. The underlying idea is that, using images will lead to greater memorability and decrease the tendency to choose insecure passwords because human's ability of visual memory is much more powerful than the textual memory. This was suggested by D. Bensinger, at their paper "Human memory and the graphical password"[7].

The first idea for Image/graphical passwords was explained by Blonder [8]. His approach was to let the user click, with a mouse or stylus, on a few selected regions in an image. If the correct regions were clicked-on the user is authenticated, else the user was discarded. According to Blonder graphical password scheme, only pre-processed images can be used; the click regions can only be chosen from certain pre-designed regions in the image. This implies that the users cannot provide images of their own for making passwords, and users cannot choose click places that are not among the pre-selected ones.

Some similar schemes are being proposed like Passlogix [8] has developed a graphical password system where, users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse.

One alternative scheme is proposed in [9] which accepts user input of alphanumeric password can be entered through virtual keyboard which accepts the input from mouse however this approach lead to the memorability problem and in effect harms the security.

Another technique "PassPoint" system on the same line of graphical password has been developed by Wiedenbeck, et al. [10] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password.

4. PROPOSED AUTHENTICATION TECHNIQUE

In client server based mechanism as user name cannot be kept secret, so any unauthorized user can theft user name/UID's easily, in the earlier system hacker apply this login name as an authorized user to access server system after validation check for user name password image for that user which is stored at server was appeared because server has no idea that he/she is a unauthorized user posing like a authorized one. The proposed technique overcomes this problem by using one more stage of authentication, in this case user has to type correct pin code which is available only with the authorized user and server system , after this validation check next level of authentication appears is image perfect greed selection. This proposed technique will definitely more secure than the other alternate authentication techniques.

This design also allows the user to choose their own images, digital photos of landscapes, paintings, etc. Moreover, user can choose any places that attract them as click regions; such places are easier to remember. However, allowing arbitrary click locations lead to a stability problem, which will be overcome by this design. The problem is that one cannot expect users to click always on exactly the same location Calculating a tolerance around each chosen pixel area can improve the range of user to select the same chosen point but to improve the security of the system, the selected password or pixels must be stored in the hash form instead of plain form, and hashing does not allow approximation: two passwords that are almost (but not entirely) identical will be hashed very differently [2]. Hence this approach will partition the image into squares grid, The square grids are displayed to the user, this eliminate the possibility that a user may choose a click point that happens to be close to an edge of a partitioned square grid.

In this system user would create his or her portfolio from the set of images that are generated by dividing the user's own image or any other image into number of grid squares and each of the squares would represent an independent image [1]. User may choose any image stored in the database or can select any image from his or her private database, further user will be asked to select few grid squares out of it by clicking at various portions of the image. Those grid squares are passed through secure one way hash function SHA-1 which will generate 160 bit fixed length unique output; this output will be stored in the password file and will act as a password for the user in future. The hash should also depend on the secret key, which will be the click points. Furthermore, the hash should not be easily forged or estimated without the knowledge of the key. Although they are very secure, these hash functions are not robust as they are very sensitive to every bit of the image data. This is undesirable and inconsistent with human visual perception [12]. As a result, this paper proposed the grid-based evaluation to compute the hash of the password clicks. This SHA-1 algorithm will take the pixel values of the image grid squares selected by the user as a input and will produce a 160 bit unique value which will be stored in the password file. Once the user has chosen the image grid squares, those grid squares sequence would become his or her password for entering the system. When the user tries to log on next time, after entering the user name he or she will be presented with the same image that was used for password creation. User will be

prompted to select the same grid square sequence, which was selected for password creation; if the user selects the same sequence then he or she is allowed to log on else not.

4.1 First Level of Authentication

1) User enters login name from remote machine.

2) After validation of user name, virtual keybord appers for user.

3) user click correct pin no through virtual keypad.

4)check this no with the pin no. stored at server database. If it is correct then it goes for the Second Level Of Authentication otherwise try again msg will be displayed for user.

4.2 Second Level of Authentication

User will Select an image. (Image with large number of memorable points should be preferred)
Divide the whole image into equal sized square grids.
As soon as the first click takes place on the image, start recording the grid pixels and the sequence in which user has selected the grid square images.
8 bits each for Red, Green, Blue and one more component, which is luminance, is recorded for each pixel.
Link list is formed in which each node will have data for one grid square image.
Recording continues till the user clicks to finish entering password. The selected grid square images are represented with black-bordered squares.
The whole link list is passed to the temporary buffer where padding and appending of length will be done before sending it as an input for SHA-1.
Final password of the selected image grid squares is selected. Password file consists of the sequence of the values generated by SHA-1 without mentioning the user name.
This password will be compared to the list of password stored in the password file and if any matching is there login will be successful else not.

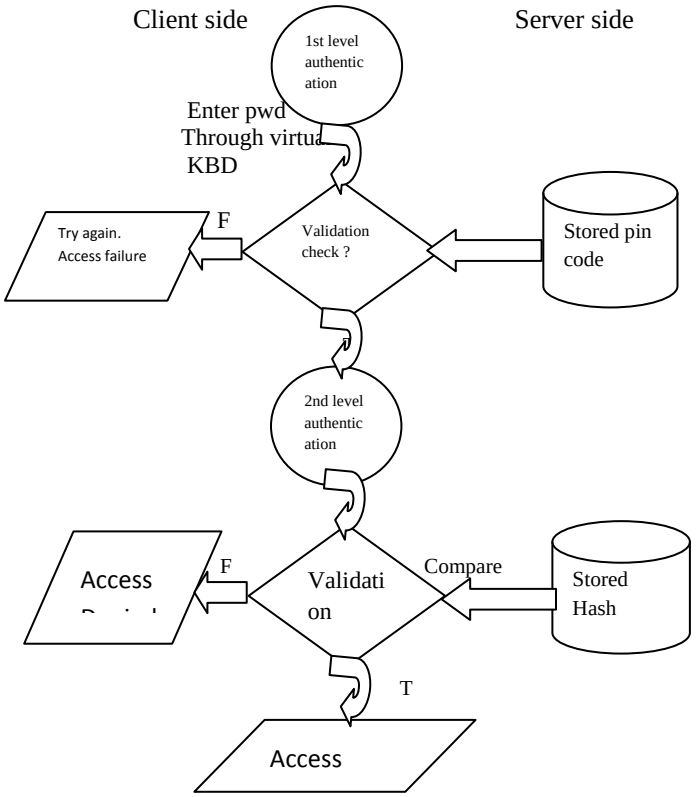

Fig 1. Flow diagram of two level authentication.

5. CONCLUSION

Generally computer systems access is based on the use of alphanumeric passwords. The image based user authentication is highly resistant to keylogger spywares and difficult to hack. Also, our scheme has better password space over alphanumeric passwords and reduces the brute force attack of passwords as well as modification attack. Similarly, image authentication has an advantage in password space over Blonder-style graphical passwords in term of retention of password. Image authentication that makes passwords more memorable and easier for people to use and, hence, it is more secure. Specifically, we proposed an image authentication, which uses hash function to store the password point on the images in the form of pixels. It is recommended to use well featured images, as it will give more variation in the pixel values, moreover well featured images are quite easier to recognize. Besides user authentication, image passwords may also be used in other security applications where conventional passwords have been used traditionally. This technique will definitely more secure than other alternate authentication techniques.

6. REFERENCES

[1] M. N. Doja and Naveen Kumar, "*Image Authentication Schemes Against Key-logger Spyware*", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008 IEEE DOI 10.1109/SNPD.2008.166.

[2] White Paper, "Combating the Spyware menace: Solutions for the Enterprise", *London, United Kingdom*, http://www.omniquad.com/, Accessed January 2008.

[3] Susannah Fox, "Public Policy Spyware: The threat of unwanted software programs is changing the way people use the Internet", *Pew Internet and American Life Project*, July 2005, http://www.pewinternet.org/PPF/r/160/report_display.asp, Accessed January 2008.

[4] Tim Johnson, "Spyware is a Blended Threat: Your security demands a layered approach", *White paper*, September 2005, www.surfcontrol.com, Accessed January 2008.

[5] J. Thorpe, and P.C. Oorschot, "Towards secure design choices for implementing graphical passwords", *ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*, Washington, DC, USA, Vol. 3, pp. 664 – 666, 2004.

[6] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin, "The design and analysis of graphical passwords", *Proceedings of the Eighth USENIX Security Symposium*, pp. 1–14, 1999.

[7] D. Bensinger, "Human memory and the graphical password",http://www.activetechs.com/solutions/security/sso/bensinger.pdf. Accessed January 2008.

[8] Blonder, G.E., 1996. Graphical passwords. United States Patent 5559961.

[9] Passlogix,V-Go, www.passlogix.com, Accessed January 2008.

[10] M.D. Fleetwood, M.D. Byrne, P. Centgraf, K. Dudziak,B. Lin, and D. Mogilev, "An analysis of textentry in Palm OS: Graffiti and the Virtual Keyboard".*Proc. HFES 46th Annual Meeting , Santa Monica:HFES*, 2002, pp. 617-621.

[11] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice", *in Symposium on Usable Privacy and Security(SOUPS)*, at Carnegie-Mellon Univ., Pittsburgh, 6-8 July 2005.

[12] Rachna Dhamija and Adrian Perrig, "Déjà Vu: A User Study Using Images for Authentication", *9th Usenix Security Symposium*, August 2000.

[13] Robert Morris and Ken Thompson, "Password Security: A Case History", *Communications of the ACM*, 22(11), pp. 594-597.