One Touch Logon: Replacing Multiple Passwords with Single Fingerprint Recognition

Beomsoo Park[†] , Sungjin Hong[†] , Jaewook Oh[†] , Heejo Lee[† *], *Member*, IEEE, and Yoojae Won[‡]
[†] Korea University [‡] Korea Information Security Agency
heejo@korea.ac.kr

Abstract — *User authentication is still heavily reliant on the use of passwords, and the security problems associated with passwords are becoming more and more serious. The main causes of these problems are the prevalence of password sniffing and the difficulty of password management due to the increased number of accessible systems. In this paper, we propose a personal password management system called "One Touch Logon", which replaces the annoying password-based authentication systems with a simple touch-and-login method. The effectiveness of the proposed system is demonstrated by implementing it on widely-used legacy systems such as Microsoft Windows and Web site logons. This mechanism is easy to implement and integrate with current password-based systems through the use of an inexpensive consumer electronic device allowing for fingerprint recognition. Moreover, eliminating the burden of memorizing multiple passwords enables the user to choose hard-to-guess passwords and further increases the utilization of Internet services while improving their accessibility. Our empirical study shows that One Touch Logon gives more benefits as the number of employing sites increases, especially when exceeding the number three*[1].

Index Terms — Password sniffing, fingerprint authentication, password management, biometric recognition.

I. INTRODUCTION

Probably the most common technique employed for user authentication involves the use of passwords. However, the deficiency of traditional password-based access systems is well known and has even led some researchers to predict the disappearance of this kind of system [4]. When people want to set their passwords to words they can easily remember, it is easy to crack by guessing or by simple brute-force dictionary attacks. Longer passwords are more secure, but harder to remember. In the event, stronger passwords cause more cost of maintaining help desk calls for forgotten passwords.

There are two main reasons that make the situation worse as time goes on. The reasons are the ease of password sniffing and the difficulty of managing multiple passwords.

Ease of password sniffing: Passwords can be disclosed by monitoring packets traveling to remote systems, because conventional login mechanisms, including those associated with telnet, ftp, login, rsh and http, transmit the user identification (ID) and password as plain text. Also, malicious attackers can gather passwords by logging keystrokes on the target machine. Recent Internet worms promote such activities, because they propagate rapidly without user intervention and silently install keyloggers on client machines, thereby increasing the possibility of private data being rendered public.

Difficulty of password management: The growth of the Internet has substantially increased the number of passwords that the user has to remember. To overcome this difficulty, users tend to use a single password for multiple systems, but the use of such a shared password may increase the potential weakness of all of the systems. Using a separate password for each system is more secure, but increases the burden on the user, who then has to remember a lot of different passwords. Furthermore, many services have security policies which require the user to change his or her password regularly, thereby further increasing the number of passwords kept in mind. Thus, the proliferation of passwords and the resultant complexity of password management has become an important issue.

Many attempts have been made to construct better authentication systems. One approach to this problem is to make a management system that handles multiple passwords for the purpose of user convenience and security [15] [16]. Password management systems store all ID and password pairs in one place, and use them to access individual systems. However, these mechanisms are still susceptible to keystroke logging attacks, since master authentication still requires the password to be typed on the keyboard at least once, for the purpose of authorizing the user.

Another approach is to check an additional condition, such as the possession of a valid smart card, which is called *two-factor authentication*. Two-factor authentication enhances the security by examining two separate factors, viz. something you know -- a password -- and something you have -- a token, a mobile phone or your own computer. However, two-factor authentication has the same problem as password management and additionally requires extra hardware -- installing a card reader for remote access -- which poses a portability problem for legacy systems in particular cases.

[1] This work was supported in part by the ITRC program of the Korea Ministry of Information & Communications under the grant IITA-2005-(C1090-0502-0020) and the BK21 program of the Korea Ministry of Education..

B. Park and S. Hong are now with LG Card, Seoul, Korea.

J. Oh is now with the R&D IT Infra Group, Samsung Electronics, Suwon, Gyeonggi 443-742, Korea.

H. Lee is with the Department of Computer Science and Engineering, Korea University, Seoul 136-713, Korea.

Y. Won is with the Information Security Technology Division, Korea Information Security Agency, Seoul 138-160, Korea.

[*] To whom all correspondence should be addressed.

Biometric approaches have been developed for controlling access to individual systems with greater security and more convenience [1]. Biometric authentications are based on physical or motion measurement, such as the fingerprint, iris pattern, face, hand geometry, and so forth. In terms of security, biometrics has many good points such that it is not easy to be forged and cannot be forgotten, and is not easily guessed [2]. One remarkable biometric approach is the use of keystroke biometrics, which seeks to identify individuals by measuring the keystroke dynamics of their typing rhythm [14].

As another alternative to password authentication, the use of graphical images was proposed in [11] and [12]. However, little work has been done to verify the effectiveness of using graphical password schemes to access dozens of different systems. Furthermore, an authentication mechanism using alternative information instead of a password usually requires significant modifications to be made to the authentication components of legacy systems.

Notebook computers which provide the functionality of logon to Microsoft Windows and Web sites through fingerprint recognition are already being marketed, but their mechanism is embedded and cannot be used in other legacy computer systems.

The objective of this study is to devise a personal authentication system which is compatible with legacy systems such as Microsoft Windows and Web site logons, and manages the login information required to access multiple systems, while being immune to keylog-based password sniffing attacks. In order to prevent the sniffing of passwords, we propose the use of biometric information for master authentication. Among various biometrics, fingerprint recognition is a well-developed and mature technology, which is readily available in the form of relatively inexpensive consumer devices. Thus, we shows a reference implementation using fingerprint recognition.

We propose an authentication system called ``One Touch Logon," which replaces the use of multiple passwords with a single fingerprint recognition and enables a user to access a new system without incurring the extra burden of remembering an additional password. Following master authentication with fingerprint recognition, a proper ID and password is chosen systematically from a secure repository of passwords for the purpose of accessing the registered systems. The design principles of One Touch Logon are as follows:

1. Portability
2. One-touch recognition
3. Deployability to legacy systems

In the next section, we describe the design of the proposed system. Section III shows the operation of Windows logon with One Touch Logon. Automatic login processes to web sites are explained in Section IV. The effectiveness of One Touch Logon is shown in Section V. Finally, Section VI concludes this paper.

II. System Design of One Touch Logon

One Touch Logon (OTL) is designed to replace the use of multiple passwords with single fingerprint recognition. OTL consists of four main components, viz. fingerprint recognizer, KeyBank, FINA and FnP smart logon, as shown in Fig. 1. We have an initial target on the prevalent end-user system, i.e., Microsoft Windows, which is the most widely deployed operating system with a reported market share of more than 97% in September 2003 according to OneStat.com [5].

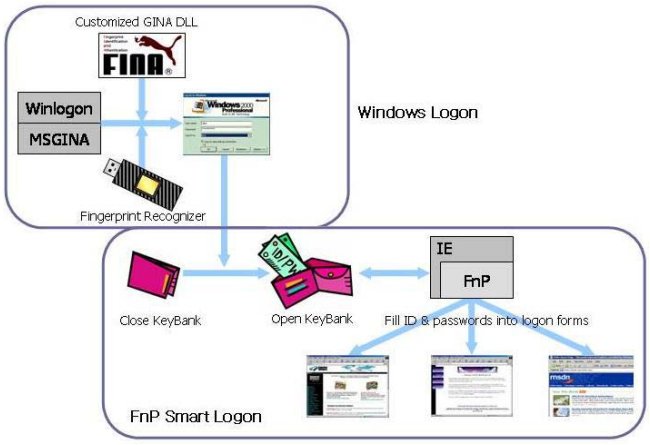

Fig. 1. Architecture of One Touch Logon.

Fingerprint recognizer: Many inexpensive fingerprint recognition devices are available on the market. Also, various forms of consumer equipments are possible such as portable biometric authenticators [3], and fingerprint recognition USB devices with a memory space [10]. Using such a device offers the advantage of biometric authentication, while retaining the portability of the system, by storing the authentication information in the portable memory space.

KeyBank: All passwords are stored in a protected area, which is called the KeyBank. Only a successful Windows logon through fingerprint recognition provides access to the KeyBank. In the case when the KeyBank is portable, the user can use OTL wherever she goes. To accomplish this, a memory space in the form of a USB stick can be used. Also, above mentioned fingerprint recognizers with a memory space can even give more benefits such as the safety of stolen KeyBank.

FINA: GINA (Graphical Interface for Network Authentication) is a replaceable security module for Windows operating systems such as Windows 2000, XP or 2003. GINA is a convenient place to attach new methods of authentication to the Windows logon. FINA is our replacement for GINA, which stands for fingerprint authentication for Windows logons. While GINA requires the user to type a valid ID and its password using the keyboard, FINA uses one touch of a registered finger. Following the acquisition of a correct fingerprint, FINA loads a corresponding ID and password pair, and then passes them to the Windows logon process.

FnP Smart Logon[2]: This component is used to handle smart logon to registered web sites. Fig. 1 shows how FnP Smart Logon works for accessing web sites with an automated login process. FnP Smart Logon detects a logon form during web browsing, and loads a corresponding ID and password to the web site. We can take advantage of the browser helper object (BHO) when implementing FnP Smart Logon in Microsoft Internet Explorer. BHOs enable us to catch a relevant event with ease, and Section IV will give more information on this subject.

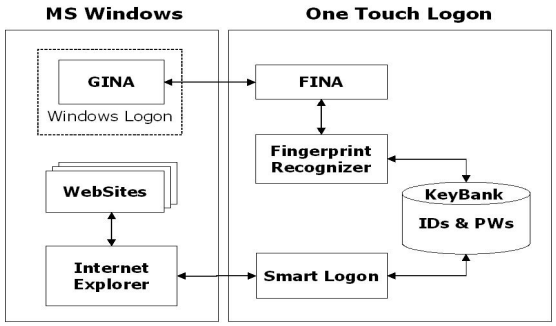

Fig. 2. Four components of One Touch Logon.

The interactions among the components are shown in Fig. 2. FINA, as an authentication master authority, allows the user to access the KeyBank following the recognition of his or her fingerprint. When the user accesses a web site which has a logon form, FnP Smart Logon attempts to logon with the corresponding ID and password obtained from the KeyBank.

III. Windows Logon: Authenticating Master Authority

This section describes the implementation of OTL in order to replace Windows Logons. Windows systems provide the ability to replace the default logon with another authentication method through the GINA interface.

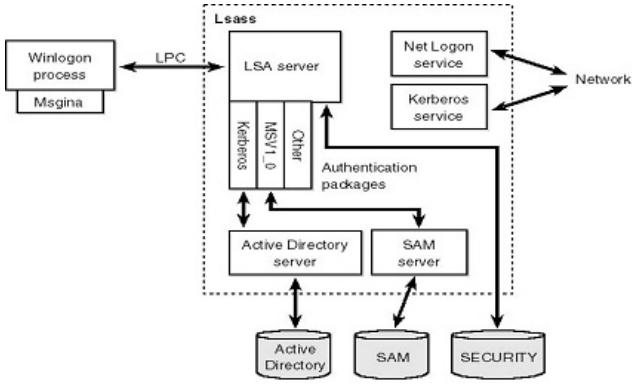

Fig. 3. Windows logon system.

Fig. 3 shows the Windows logon processes which are associated with several elements. Among these different elements, Winlogon and MSGina.DLL are the key to understanding Windows Logon (shortly, Winlogon). Winlogon is responsible for managing security-related user interactions. Winlogon guarantees that an untrusted process cannot gain control of the desktop during logon. Also, Winlogon calls MSGina's exported functions when certain events occur.

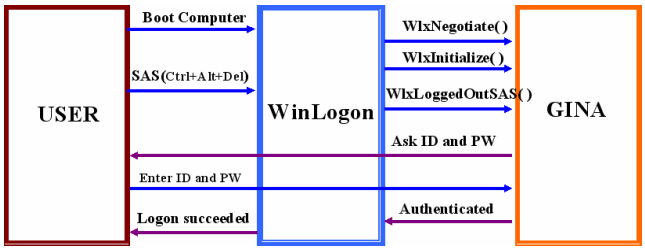

Fig. 4. Interaction of Winlogon and GINA.

GINA is implemented as a single DLL file and this file can be replaced with another one. By replacing the GINA DLL (MSGina.DLL) with the module customized for OTL (FINA.DLL), we can provide another method of user authentication. For it to work well with Winlogon, the customized GINA DLL must be able to export a set of functions, thus Winlogon attempts to identify a user with the new authentication method. Fig. 4 shows the functions called in the case of a user logon, which are in a subset of functions exported by GINA. Thus, the logon-related functions can be implemented in FINA as shown in Fig. 5, while the other functions are imported from GINA.

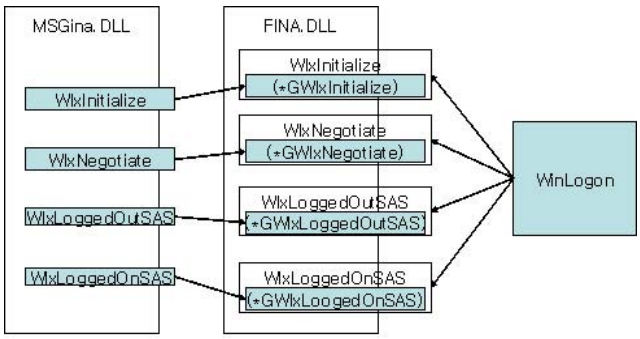

Fig. 5. FINA as a replacement for GINA.

Before calling the imported function, GWlxLoggedOutSAS (which is the same as the WlxLoggedOutSAS function in MSGina.DLL), we create and show a dialog window for performing fingerprint recognition. Thus, we can modify the WlxLoggedOutSAS interface, in order to allow authentication through fingerprint recognition. Also, the function needs to have a procedure which allows the ID and password to be obtained from the KeyBank, and passed to the Winlogon process.

The WlxLoggedOutSAS function may operate differently according to the version of Microsoft Windows. Nonetheless, the new interface FINA can be implemented by modifying GINA, in order to intercept the callback function of the Windows' default user authentication dialog. FINA also successfully passes the ID and password to the dialog and then posts the button-click message required to complete the logon procedure.

[2] FnP stands for ``fingerprint and play."

IV. Web Site Smart Login: Managing Multiple Passwords

This section describes the utilization of OTL for accessing web sites with the proper logon information. When a user accesses a web page, OTL recognizes the logon form by a heuristic algorithm. If a logon form is detected, then OTL requests fingerprint authentication. If the authentication succeeds, OTL automatically fills in the ID and password for the site. Thus, OTL completes the logon to the web site without requiring any keystrokes.

A. BHO (Browser Helper Object)

A BHO is a small program that runs automatically whenever Internet Explorer is started. Internet Explorer is the dominant web browser with a reported global market share of 93.9% in May 2004 according to *OneStat.com*. A normal Win32 process runs with its own address space, and crossing the boundary of the process is prohibited by Windows. On the contrary, once a BHO is implemented and registered, Internet Explorer will load it each time it starts up, and such an object runs in the same memory context as the browser so that it can perform any action on the browser. For example, a BHO could detect the browser's typical events, such as GoBack, GoForward, and DocumentComplete, access the browser's menu and toolbar and make changes to them, create windows to display additional information on the currently viewed page and install hooks to monitor messages and actions.

B. FnP Smart Logons

The processes of the FnP Smart Logon can be described as follows.

1. When receiving the "DOCUMENT COMPLETE" message, get the document just downloaded.
2. Try to find the input tag in the document, which may be used for requesting a password authentication.
3. If the tag is found, request fingerprint authentication.
4. If authenticated, retrieve the proper ID and password from the KeyBank. If not found, register the site.
5. If the ID and password is obtained, insert it into the input tag for filling in the logon form.
6. Perform a task of submitting the filled form which contains the ID and password. .

It is assumed that the password field is used for entering the password and that the field immediately preceding it is used for entering the ID.

C. Detecting and Filling in the Logon Form

While there is no standard form for web-site logons, they usually have three inputs, i.e., the ID, password and submit. Fig. 6 shows the conventional HTML code for web-site logons. Even though there are various types of web logons, we can detect a fairly large amount of logon forms heuristically. One way is to search the input form for the ``password'' type attribute, and then find the nearest field immediately preceding it with the ``text'' type, and consider it to be the ID field. This implies that checking the attributes of input forms enables us to identify logon forms. Thus, our detection algorithm tries to find an input tag whose type is ``text'', and then find an input tag whose type is ``password''. If no tag corresponding to a logon form is found, it tries again by searching the sub-frames recursively, including both multi-frames and inner-frames. In this way, we can detect the existence of a logon form in most web sites.

```
<FORM>
<INPUT type="text" name="id"><BR>
<INPUT type="password" name="pw"><BR>
<INPUT type="submit">
</FORM>
```

Fig. 6. The common form of web-site logons.

D. Managing Logon Information

A user may use a different ID and password for each web site, instead of using the same ID and password for every site. Thus, we need to store the authentication information for each site. The information includes the three fields of the URL, ID and password. When FnP smart logon detects a logon form, it checks the KeyBank for the availability of logon information corresponding to the URL. If the logon information is not found, we can start the registration of the current site.

Confidentiality is another issue involved in storing such sensitive information. In order to keep the passwords secret, we can store them in a separate storage area accessible only to the authorized user. Also, we can encrypt the information by using the master password (e.g., the Windows logon password) as an encryption key. When needed, the password can be decrypted and used by the FnP smart logon procedure to fill in the logon form.

V. Evaluation of One Touch Logon

A. Effectiveness of the OTL mechanism

Fig. 7. A storage used for storing KeyBank, accessible to a person after valid fingerprint authentication.

In order to confirm the validity of OTL, we implemented it on Microsoft Windows systems. As a fingerprint recognizer, we make use of a fingerprint recognition device with a memory, which is shown in Fig. 7. OTL with FINA works on Windows operating systems supporting the GINA interface, which include Windows 2000, Windows XP and Windows 2003. Fig. 8 shows the Windows logon procedure replaced by FINA, in which a user can logon to the system by touching the fingerprint reader with the registered finger. This shows no need to enter an ID and password pair through a keyboard when OTL is employed for Windows Logons.

Fig. 8. Windows logon session integrated with FINA.

FnP Smart Logon works with versions of Internet Explorer superior than 4.0. Fig. 9 shows the screen image pertaining to the detection of a web site with a logon form and the resulting request for fingerprint recognition. In order to evaluate the effectiveness of FnP Smart Logons, we examined the top 100 sites according to the ranking on *http://www.alexa.com*. Among these 100 sites, 65 had the normal logon form as Fig. 6, while 27 had no logon form and 2 sites were unavailable due to server or network failure. Thus, we confirm that FnP is compatible with more than 90% of the most popular sites (65/71 = 91.5%). 6 sites have abnormal logon forms. They include the implementation with server side programs (e.g., ASP, JSP, PHP and CGI) and the use of a FLASH animation, which do not allow OTL to examine their source codes. Thus, OTL can compatible with every web site which allows us to check the part of logon procedure.

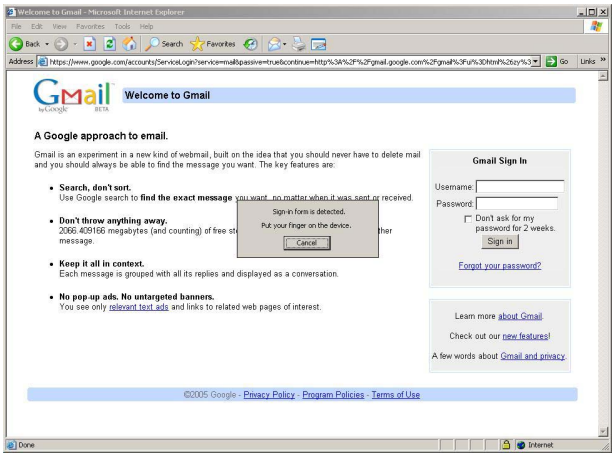

Fig. 9. FnP smart logon detects a login form and requests user authentication by touching the fingerprint recognition device.

B. *User experience*

We conducted an empirical study for comparing manual login with OTL. Participants are 30 persons and 10 web sites are used for the experiment. The web sites used are Daum, Naver, Empas, Cyworld, Yahoo, Korea.com, Paran, Nexon, Hangame, Gmail, which are considered as the ten most popular portal sites in Korea. The participants consist of 20 men and 10 women, and among them 9 persons are majoring in computer science area. Each participant is requested to setup an individual password for each web site one by one repeatedly. After setting up the password for i-th site ($1 \le i \le 10$), the user was asked to logon to one site chosen randomly among i sites.

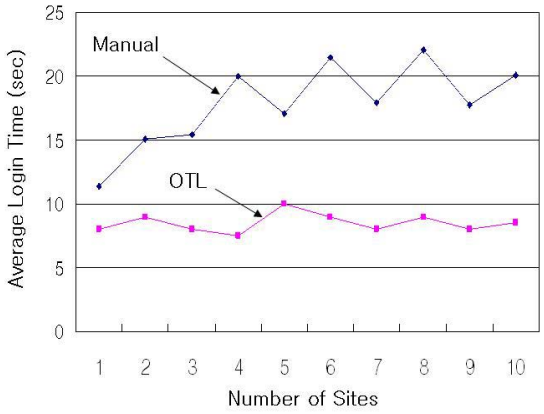

Fig. 10. The average login time for logging into a web site.

We first measured the average time for logging into one site as the number of accessible sites increases. As shown in Fig. 10, manual login takes longer than OTL as the number of sites increases. Especially when the number of sites is larger than three, the gaps become more prominent. The range of the login time moves from 12 ~ 15 seconds to 17 ~ 22 seconds when exceeding the number three, while the time for OTL is remaining around 8 ~ 10 seconds. Fig. 11 shows the login success ratio as a function of the number of sites. Increasing accessible sites causes to retry the login procedure due to an incorrect password entered. It shows that OTL is useful as the number of accessible sites increases.

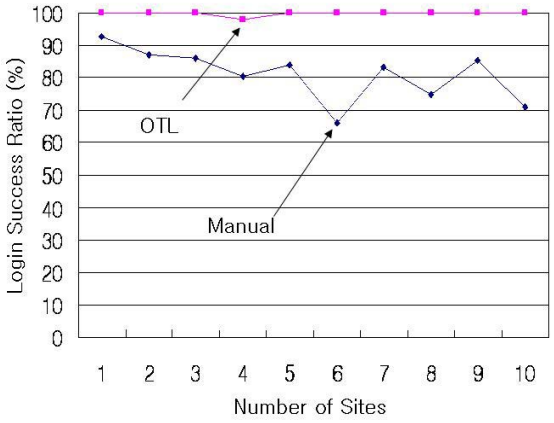

Fig. 11. Comparison of login success ratio.

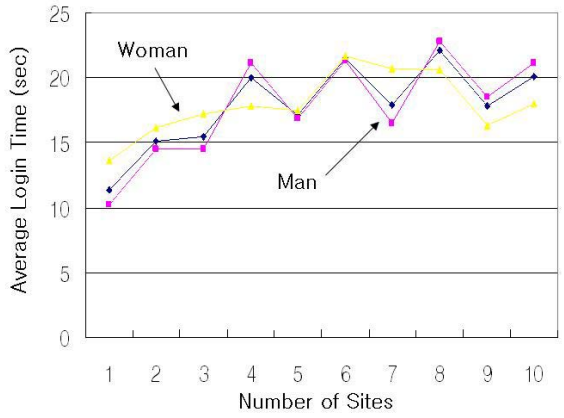

Fig. 12. Average login time for men and women.

Fig. 12 shows the average login time for men and women, respectively. And Fig. 13 shows the average login time for major and non-major persons. The gap between major and non-major are wider than that of men and women. This implies that the less-experienced peoples have bigger trouble as the number of accessible sites increases.

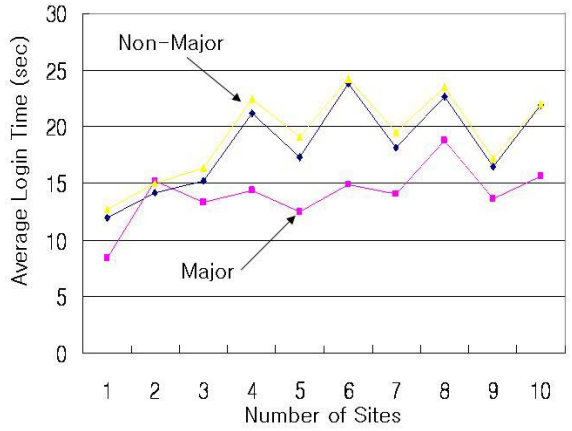

Fig. 13. Average login time for major and non-major persons.

C. *Security analysis of OTL and its extension*

The KeyBank is a potential target of attacks, since all of the IDs and passwords are stored in the central repository. In addition to the protection by encryption, we can enhance the security of the passwords. By changing the passwords periodically, we can reduce the time during which stolen passwords can be used for valid authentication.

Currently, OTL is designed for Windows and web site logons, however we can extend the concept of OTL to other password-based applications such as SSH, TELNET, RLOGIN and FTP. It is obviously impossible to support any of these protocols without modification of the client program. However, automatic logons can be enabled in the client program by integrating the interface of FnP smart logons as the form of API. The generalization of OTL will be undertaken in the future.

VI. Conclusions

Conventional ID-password authentication systems are still the most popular ones. However, as users visit more and more sites due to the growth of the Internet, the number of passwords that they have to remember increases substantially and it becomes increasingly difficult to manage them safely. Moreover, keyloggers silently installed by self-propagating malicious codes are forcing us to find an alternative authentication mechanism deployable to legacy systems. One Touch Logon (OTL) is proposed for the purpose of simplifying password management, while simultaneously rendering password sniffing impotent on local machines. Multiple IDs and passwords can be managed by OTL, which allows users to login to legacy systems by touching a fingerprint reader. The effectiveness of OTL is shown by the reference implementation on Windows systems and web site logons with a password inquiry form. The proposed mechanism works properly for current Windows systems and also handles more than 90% of popular web sites by detecting a logon form automatically.

Acknowledgment

We would like to thank Mr. Keun Park for many helpful suggestions and the experiment of user experience.

References

[1] A. K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: Personal Identification in a Networked Society*, Kluwer Academic Publishers, 1999.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Security & Privacy*, pp. 33-42, March/April 2003.

[3] D. D. Hwang, I. Verbauwhede, "Design of portable biometric authenticators -- energy, performance, and security tradeoffs," *IEEE Trans. Consumer Electron.*, Vol. 50, No. 4, pp. 1222-1231, Nov. 2004.

[4] M. Kotadia, "Gates predicts death of the password," *ZDNet News*, Feb. 25, 2004.

[5] OneStat.com, "Microsoft's Windows dominates the OS market on the web according to OneStat.com," September 24, 2003. http://www.onestat.com/html/aboutus_pressbox24.html

[6] Microsoft, *The Microsoft Developer Network: Winlogon and GINA*, 2005. http://msdn.microsoft.com

[7] D. A. Solomon, M. E. Russinovich, *Inside Windows 2000*, Microsoft Press, 2000.

[8] S. Roberts, *Programming Microsoft Internet Explorer*, Microsoft Press, 1999.

[9] C. Pokpirom, "Adding your logo to Winlogon's dialog," Dec. 2002. http://www.codeguru.com/Cpp/W-P/system/misc/article.php/c5683.

[10] NAVI Co. Ltd., "Touch key technical overview -- fingerprint recognition USB device with memory," Jun. 2003.

[11] R. Dhamija, A. Perrig, "DejaVu: a user study using images for authentication," *Usenix Security Symposium*, 2000.

[12] D. Davis and F. Monrose and M. K. Reiter, "On user choice in graphical password schemes," *Usenix Security Symposium*, 2004.

[13] J. Yan, A. Blackwell, R. Anderson and A. Grant, "Password memorability and security: empirical results," *IEEE Security & Privacy*, pp.25 -- 31, Sep./Oct. 2004.

[14] A. Peacock, X. Ke and M. Wilkerson, "Typing patterns: a key to user identification," *IEEE Security & Privacy*, pp.40 -- 47, Sep./Oct. 2004.

[15] Softex, Inc., "OmniPass: multiple password managing product by Softex," http://www.softexinc.com.

[16] Siber Systems, Inc., "RoboForm: password manager, form filler, password generator, fill & save forms," http://www.roboform.com.