Overview of issues with non-conventional user authentication methods

Sanjay Nair
Department of Computer Science
University of Southern California

1 Introduction

Authentication is a process of verifying the identity of an entity that it claimed to be. Typically, there are two parties involved in the process of authentication: *user* and *authenticator*. The process of authentication requires the user to prove her identity to the authenticator. In a computer environment, standalone or networked, the authenticator is typically a computer system and the user is typically a human. Most of the computer systems grant access to the user only after the user performs a successful authentication operation.

There are three main techniques used for user-to-computer authentication: *knowledge* based authentication, *biometric* based authentication and authentication based on *token/smart cards* [2]. Today's computer systems rely heavily on knowledge based schemes for user authentication. Because of their widespread usage, this scheme is also referred as conventional authentication scheme. A conventional authentication scheme relies on a text based secret known as password that is shared between the user and the authenticator. During the authentication process user presents her password to the authenticator which in turn compares this password with the user's password in its possession. If the passwords match, the authentication process is successful. This form of authentication is very easy to setup and very easy to use.

Many studies have shown that knowledge based authentication scheme using a text password to be deficient and major cause of system break-ins. [2]. This is because the design of these systems often ignores the human factor in the overall security domain. Humans are considered to be the weakest link in the security chain. Given a choice, humans typically chose a weak password that is easy to remember. This poses a great security risk as the weak password can be easily cracked using trivial password cracking methods [6].

Over the years alternatives schemes, also referred as non-conventional schemes, such as *graphical passwords*, *biometric authentication* and authentication based on *token/smart cards* have been proposed to address the shortcomings of conventional authentication schemes [2]. It is widely believed that these authentication schemes are more secure and less vulnerable to attacks compared to the conventional authentication scheme. Despite this belief, password based conventional scheme is continued to be used as the predominant form of user authentication.

The main focus of this paper is to outline the issues with the non-conventional authentication schemes listed above. This paper also discusses the main reasons that *may* have prevented them from being adopted widely as conventional authentication scheme. Section 2 outlines the issues with conventional authentication scheme in detail. Section 3, 4 and 5 describes the issues with graphical passwords, biometric schemes and token/smart card based schemes respectively. Finally, conclusions are presented in section 6.

2 Issues with conventional authentication scheme

Conventional authentication scheme requires the user to present a user id and a text based password to an authenticator. Users often choose easily guessable passwords on systems where they are allowed to choose their own passwords. Unfortunately most of these passwords are not secure and can be easily cracked by an attacker. A study conducted by Morris and Thompson found that 86% of the user chosen passwords were of bad quality and can be easily broken by mounting trivial attacks such as exhaustive search and dictionary attacks[6]. The system could force the user to enter a strong password from a large character set, or the system itself could choose a strong password for the user. This may force the user to write down the password somewhere since

strong passwords are typically difficult to remember [3]. This opens up another hole in the security system as the attacker can concentrate now on obtaining the written/stored password rather than breaking other difficult parts of the security chain.

Another issue with text based passwords is that they can be easily shared among people [2]. Passwords can be transmitted over email or phone very easily. For example, your bank sends you the online banking password through email. An attacker can now concentrate on breaking your less secure email account rather than breaking your more secure online banking account.

A more serious issue with the passwords is that users tend to use same password across different domains. This is especially true if the user have large number of accounts. For example, users might use same password for email account, internet chat group account and online banking account. If internet chat group account is compromised, user's online banking account is also compromised.

In the following sections, we'll look at some of the alternative authentication methods that can be used to solve the issues with the conventional text based password scheme.

3 Graphical passwords

Humans are known to have remarkable ability to recall images as compared to texts or words. Graphical passwords try to utilize this ability to improve the security of the knowledge based authentications systems. Graphical passwords can be of two types: *recall* based, and *recognition* based [1]. Recall based password use the same concept as text based passwords; user recalls the image from the memory during the authentication and presents this to the authentication system. In recognition based systems, user will be presented with number of images during the authentication process and the user selects images that she had selected during the registration process.

A recall based password scheme known as *Draw-a-Secret* scheme, requires the user to draw a picture on an n x n grid. The password is the image drawn on this n x n grid. The drawing is then mapped to a sequence of coordinate pairs of cells through which it passes. The order of the drawing is also maintained in the sequence. If the user breaks the drawing flow – for example user releases the mouse button – a distinguished co-ordinate pair is inserted to the sequence [4]. This scheme suffers from some of the same vulnerabilities of the text based password scheme. Since the images are stored as text, most of the issues listed in section 2 are applicable here too. Another issue with this approach is that an eavesdropper may see what the user is drawing as password during authentication.

Most recognition based schemes follow a three phase approach: *registration phase*, *training phase* and *authentication phase* [2]. During registration phase, user will be presented with n images out of which she chooses k images as her password. Training phase is used to help user to get familiarize with the chosen passwords so that user can recognize them easily during authentication phase. During authentication phase, user will be presented with various images (including decoy images) across multiple screens. The authentication is successful only if the user successfully picks the images she selected during the registration process.

A recognition based password scheme known as *passfaces*^{TM} lets the user to choose n faces out of k faces. A study conducted on security of *passfaces*^{TM} found that the system is vulnerable to many attacks [1]. One major issue with this scheme is that the password is easily guessable given the user's demographic information. Faces chosen by users were highly predictable since their choices were greatly influenced by their gender, race and attractiveness of the faces. Another issue with this scheme is that the passwords can be exhaustively searched given reasonably low values of k and n. Another scheme known as Déjà vu was developed to address guessable issue with the *passfaces*^{TM} approach [2]. In this scheme users were presented with random arts instead of faces. These arts can be derived from keys known as seeds. The idea is to force the user to select a password that is independent of his demographic information.

There are some major issues with graphical passwords that may have prevented it from becoming the predominant form of authentication. One major issue with the graphical passwords is *usability* [10]. The registration and authentication process is cumbersome and takes too long compared to text-based password schemes. A typical authentication process requires the user to select images from multiple screens and at times this can be time consuming and frustrating. Another issue with graphical password is its *security*. Graphical passwords are susceptible to guessing attacks as well as exhaustive search attacks. Also, very little research has been done to study the security aspects of graphical passwords. It is also not clear how human recognition will fare if the user has large number of accounts. Users can get easily confused with pictures across multiple authentication domains and chances are they'll make mistakes when choosing images. If the user makes number of mistakes then the system may lock the account for a period of time. This opens up a possibility of mounting denial of service attack on users account.

A graphical password requires users to access terminals that are capable of displaying graphical images. This means users cannot use this scheme for authenticating in a command line environment. This presents a problem as users need to have two schemes: one for graphic capable terminals and one for non-graphic capable terminals. This presents a serious problem where the user needs to use same authentication scheme for both graphical as well as command line interfaces.

4 Biometric based authentication scheme

Authentication schemes based on biometric systems use physiological or behavioral aspects of a living person for authentication purposes. Some of the characteristic that can be used for authentication are: fingerprints, structure of the hand, iris scan, keystroke patterns etc. [5]. Biometric based authentication is widely regarded as highly secure authentication scheme as biometrics are hard to forge. A typical biometric authentication scheme follows a two step approach: registration and authentication. During the registration phase user needs to provide the required biometric information to the authenticator. For example, if the fingerprint is the biometric information, user needs to provide this information to the authenticator in a secure way. The authenticator typically stores this information in digital format. During the authentication phase user provides the biometric information typically using a biometric scanner and the authenticator compares this with the information that is in its possession.

There are some major issues with biometric authentication scheme that may have prevented it from becoming the predominant form of authentication. One main issue with biometric authentication scheme is *privacy*. Users typically do not like to use their physical or behavioral characteristics for authentication purposes. For example, users mostly associate fingerprinting with criminal activity [5]. Also, if the biometrics information is stolen users have no way of replacing them. It is important to understand that biometric information is not a secret. It is not easy to forge biometric information, but it is easy to steal them [9].

Instruments that capture biometric information typically cost a lot of money. For example, a highly accurate fingerprint scanner equipped with thermal sensors could cost hundreds of dollars. Users will be reluctant to spend this kind of money for just authenticating with an email server or even online banking account. Another major issue with biometric systems is *accuracy*. Unlike passwords, biometric information tends to vary over multiple logins. If the tolerance level of the system is low then it will reject many legitimate user login attempts. This is known as False Alarm Rate (FAR). On the other hand if the tolerance level of system is high then it may authenticate imposters. This is known as Imposter Pass Rate (IPR). A good biometric device should handle these two factors carefully in order to reduce false positives and imposter pass-through [5]. Another issue with biometric authentication scheme is *speed*. As in case of recognition based graphical passwords, the authentication process can be time consuming. If the rejection rates are higher, user may not be willing to use this form of authentication.

5 Token/Smart card based authentication scheme

Token/smart card based authentication scheme enable the users to perform authentication using devices known as token cards or smart cards. This scheme relies on an authentication method known as *two-factor authentication* [11]. Two-factor authentication requires the user to present a unique token together with a secret such as password or PIN. Traditional token base authentication scheme uses a device known as token card that provides a one-time pass-code. This pass-code typically changes in every minute. The authentication process requires the user to present this one time pass-code along with user's secret to gain access to the computer system.

Smart cards are more capable than the traditional token cards. A typical smart card is a credit card shaped device that contains an embedded microcontroller and a small amount of memory [8]. Some smart cards also have a clock system, keypad and a display. The microcontroller inside the smart card is capable of generating cryptographic keys that can be used for various security purposes including user authentication. A user needs to activate the smart card by entering a PIN before it can be used for performing other operations. Most of the computer systems also require a smart card reader in order to communicate with the smart card.

Smart card offers more secure authentication mechanism to users by providing a cryptographically strong key for authentication [7]. Most of the smart card authentication schemes rely on the public key cryptographic methods to perform authentication. For example on windows, a smart card can be used to authenticate the user to the windows platform using the Kerberos protocol. After the user inserts her smart card into a smart card reader, windows local security manager prompts for the user to enter the secret for the smart card. Windows local security manager uses this PIN to access the smart card and retrieves the user's cryptographic certificate. This certificate is typically signed by a trusted Certificate Authority. The local security manager sends this certificate to the key distribution center (KDC) which in turn verifies the certificate for authenticity. If the certificate is valid, then the KDC encrypts the login session key and the Ticket Granting ticket with the public key obtained from the user's certificate [11]. Smart card can use this information to complete the authentication process.

This paper concentrates on the issues with smart cards instead of token cards as they have been the main focus of the contemporary research. There are some major issues with smart card based authentication scheme that may have prevented it from becoming the predominant form of authentication. The main issue with smart card based authentication is *cost*. Smart card and smart card reader needs to be present on every machine where the user might be authenticated [8]. Both smart card and smart card reader cost money. The cost will be higher if the smart card includes a clock system, display and keypad. The smart card also needs to be tamper proof or tamper resistant. If an attacker opens up the smart card, she should not be able to read the contents of the smart card memory. Also, many systems would require the user's digital certificate to be signed by a trusted third-party. All these will contribute to the higher cost of smart card based solution

User need to authenticate first with the smart card using a PIN before it can be used. Most likely his PIN is going to be weak as humans need to remember them. Some of the security problems listed in section 2 is also applicable here. Instead of a PIN, user can also use biometric information such as fingerprint to authenticate with the smart card. In case of a smart card without a built in keypad, the PIN could be supplied using an external keyboard. This keyboard could be used to record the PIN and card information for use in a later attack [8].

Another major issue with smart cards is *distribution* and *maintenance*. If every account you want to login uses a unique smart card, then you'll end up carrying a lot of smart cards in your valet. Regardless of the cost, this will present a major maintenance problem. On the other hand if you only have one *super* smart card that can be used across multiple domains then it presents a security threat. If this smart card is stolen and the attacker cracks the PIN, then it will affect the security across multiple domains. In case of a

super smart card the big question is who issues them? Currently, there is no centralized authority or authorities that are responsible for distributing and maintaining the smart cards. Without this it will be difficult to persuade the user to use smart cards for performing authentication operation.

Conclusions

This paper presented an overview of issues with non-conventional authentication systems. In today's systems, knowledge based authentication using a text password is the predominant form of user authentication. This is the case even though many studies have shown them to have number of serious shortcomings. This paper also presented the major issues with knowledge based authentication schemes.

Over the years many researchers have proposed non conventional authentication schemes such as *graphical passwords*, *biometric authentication* and *token/smart card based authentication* as an alternative to the conventional authentication scheme. This paper looked at major issues with these alternative schemes and speculated the reasons that prevented them from being used as widely as conventional knowledge based authentication scheme. Usability is one of the major issues with graphical passwords. Recognition based graphical authentication is very time consuming and cumbersome. Also, little research has been done in to understand the security implications when using graphical passwords. Major issue with biometric authentication is privacy. Biometric authentication scheme that relies only on biometric information is not viable as this information is not a secret. Biometric information can also be used in two-phase authentication schemes. This scheme is not used widely because of the high cost of biometric scanning equipment. Smart card based authentication scheme provides an attractive solution that address some of major issues with knowledge based authentication schemes. Unfortunately there are some major issues with this approach also. Distribution and maintenance of smart cards are two big issues with this authentication scheme. Another big issue with the smart card based authentication scheme is *cost* which need to be addressed before it can be used widely.

Future research on graphical passwords should address the usability issues with this scheme. Recognition based graphical password is a powerful concept and if the major issues with them are solved, it could become the next predominant form of authentication scheme. Smart card based authentication scheme is also gaining momentum as more and more systems supports this capability. Microsoft® is coming up with new operating system code named Vista™ that supports smart cards natively. Microsoft is also planning to support a software based smart card solution known as InfoCard™ to improve the authentication security. Many banks are considering smart card based solution to enhance the security of authentication and other online transactions. Future research on smart cards should come up with innovative ways to cut down the costs of smart cards as well as solving the smart card maintenance problems. Critical issues with smart card based solutions need to be addressed before it could become the predominant form of authentication scheme.

Until the major issues with non conventional authentication schemes are solved, knowledge based authentication scheme using text passwords will continue to remain as the predominant form of user authentication in computer systems.

References

[1] Darren Davis, Fabian Monrose, and Michael K. Reiter. "*On user choice in Graphical Password Schemes*". In proceedings of the 13th USENIX Security Symposium, pages 9-13, San Diego, California, August 2004.

[2] Rachna Dhamija and Adrian Perrig. "*D´ej`a Vu: A User Study Using Images for Authentication*". In proceedings of 9th USENIX Security Symposium, pages 45-58 Denver, Colorado, August 2000.

[3] [Feldmeier90] David.C. Feldmeier and Philip.R. Karn. "*UNIX Password Security - Ten Years Later*". In proceedings of Crypto conference, published as Lecture Notes in Computer Science, No.435, pages 44-63, August 1990.

[4] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael Reiter, Aviel D. Rubin, "*The Design and Analysis of Graphical Passwords*". In proceedings of the 8th USENIX Security Symposium, pages 1-14, Washington, D.C, August 1999.

[5] Hyun-Jung Kim. "*Biometrics – Is it a viable proposition for identity authentication and access-control?*" Computers & Security, Vol. 14, No. 3, pages 205-214, 1995.

[6] Robert T Morris and Ken Thompson, "*Password Security: A Case History*". Communications of the ACM, vol. 22, no. 11, pages 594-597, November 1979.

[7] Molva, Refik, and Tsudik, Gene, "*Authentication Method with Impersonal Token Cards*". In proceedings of the IEEE Symposium on Research in Security and Privacy, pages 56-65, May 1993.

[8] Bruce Schneier and Adam Shostack. "*Breaking up is hard to do: Modeling security threats for smart cards*". In proceedings of the USENIX workshop on smartcard technology, pages 175-185, Chicago, Illinois, May 1999.

[9] Bruce Schneier, "*The Uses and Abuses of Biometrics*". In proceedings of the Communications of the ACM, vol. 42, no. 8, page 136, August 1999.

[10] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen. "*Graphical passwords: A survey*". In proceedings of 21st Annual Computer Security Applications Conference, pages 463-472, Tucson, Arizona, December 2005.

[11] Microsoft TechNet article on smart cards. "*The Secure Access Using Smart Cards Planning Guide*". In Microsoft TechNet, http://www.microsoft.com/technet/security/topics/networksecurity/securesmartcards//default.mspx, June 2005.