ISSN 2395-1621

Review Paper on Keyring Managing for Information Security using Mobile Computing

[#1]Disha Vyavahare, [#2]Renuka Satpute, [#3]Kapil Sane, [#4]Priyanka Chavan

[1]disha.vyavahare@gmail.com
[2]11satpute.renuka@gmail.com
[3]kapilsane@gmail.com
[4]priyankachavan2907@gmail.com

[#1234]Department of Computer Engineering

Padmabhooshan Vasantdada Patil Institute of Technology
S.N. 33/22, Near. Chandni Chowk,Opp. Athashree Project,
Pirangut Road, Bavdhan, Pune, Maharashtra 411021, India

ABSTRACT

Use of Internet gives us an idea of saving all the passwords together. Based on this idea, this paper provides a method to store the information on encrypted form so that whenever the user forgets his password or wants to get glance of the password, he/she can view it by just decrypting the information (passwords) that are saved on the device. People reusing their password for multiple accounts are prone to malicious attacks. Compromising one password can help an attacker take over private and important data from several accounts. Therefore to Manage and secure the passwords of various accounts this Android application comes into picture which can be installed on the Android smart phones .It is mainly about how to protect the passwords, and also encrypt them. A one-time password (OTP) is used when user forgets the main password, or he can use the finger print scanner.

ARTICLE INFO

Article History

Received: 23rd November 2016

Received in revised form :

23rd November 2016

Accepted: 25th November 2016

Published online :

2nd December 2016

Keywords: **Encryption, OTP, Password Management, Information Security, Master Key/Password, AES.**

I. INTRODUCTION

Management of passwords has become a tedious task now-a-days. Therefore to manage and secure the passwords of various accounts this Android application comes into picture which can be installed on the Android smart phones. In this Application user creates one master key for the application that manages the passwords. In this application user can store multiple passwords of accounts like Gmail, yahoo, Net-banking, ATM pin, shopping websites or any other account password. This application will be developed for smart-phones taking into considerations the current increasing usage of smart-phones .Once the user uses the master key to open the application he will be able to view all the passwords stored in the categorized format. If in case user loses his smart phone then the third user will not be able to see the passwords. In this application one web portal option is available. By accessing the web portal service user can use the self-destruct option that will clear all the data stored in the application in their smart phone. Compared with the traditional it has no OTP. It can provide a more convenient and comfortable environment to the user. OTP can be sent to recovery mail or mobile number in case of password recovery. OTP is One-Time Password which is unique and can be used only for one login or transaction. OTPs usually a time limit i.e. after a particular time OTP expires and cannot be used. Hash tables are used to compare passwords of websites and Email ids to avoid repetitive passwords. Thus warning the user to change the passwords. AES encryption System for Mobile module is used, as it is convenient than other Encryption keys. It is a data storage-equipment combined with 128bit encryption key. Due strong encryption capacity, the user need not have to worry about his passwords. It can save expensive authentication time and costs, while improve the network coverage greatly. Its stable performance provides a strong support platform for remote data transmission and monitoring equipment. In this application user can add notes with title for storing memos.

Private Image vault is also available for users to store the images which are hidden from gallery. Dummy Website fetching password from DB when password forgotten (On Call).

II. RELATED WORK

Many projects are trying to overcome poor password practices. There are several researchers who have suggested using graphical passwords like doodles [1], a series of random art images [2], people's faces [3], or points within an image [4]. The theory with these systems is that images are easier for people to recognize or recall than text. In contrast, Yan et al. and Bunnell et al. have focused on text passwords, looking at recall rates. [5, 6]. Others have looked at various tools for users to manage their passwords, specially password hashing systems. Both LPWA and PwdHash automatically fills in the passwords based on specific user input [7, 8].Site Password [9] and a remote version of PwdHash display the generated password for the user. Browser functions such as Internet Explorer's AutoComplete and Firefox's Saved Passwords then relieved the user's burden to memorize several passwords. Researchers have also conducted pragmatic studies of password use and management.

Several papers rely on interview data to understand the management of passwords by the users. Adams and Sasse concluded that users do not understand password policies and lack motivation [10]. Weirich and Sasse further study approaches towards strengthening password management [11, 12]. Their studies indicated that users to some extent, deny their vulnerability. Dhamija and Perrig used interview data to estimate that entrants had one to seven unique passwords for ten to fifty websites [2]. Brown et al. surveyed college students and asked how many passwords they had. Students had on an average of 8.18 password uses with 4.45 unique passwords [13]. Riley also did a survey to focus on online accounts which indicated similar results [14]. Based on the Hash Visualization technique [15] Dhamija and Perrig [2] proposed a graphical authentication scheme. In this technique, the user is asked to select a certain number of images from a set of random pictures. These are generated by a program. Then the user will be authenticated by the means of identification of the preselected images. Akula and Devisetty's algorithm [16] is similar to the technique proposed by Dhamija and Perrig[2]. The difference is that by using hash algorithm SHA-1, the authentication is more secure and requires less memory as it produces a 20 byte output. Weinshall and Kirkpatrick [17] depicted several authentication schemes, such as picture recognition, object recognition, pseudo word recognition.

This study revealed that among the three schemes discussed, pictures are the most effective. Pseudo codes can also be used as an alternative but it requires proper setting and training. Jansen et al. [18-20] proposed a graphical password mechanism for mobile devices. During the enrolment, a user selects a theme (e.g. cat, sea, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. During the authentication the correct sequence of the registered images must be entered. Thus rendering that the image sequence length is generally shorter than the textual password length. So to address this problem, two pictures can be combined to compose a new alphabet element. Takada and Koike discussed a similar technique for mobile devices. In this technique users are allowed to use their favourite image for authentication [21]. During authentication, for verification a user has to go through several rounds. At each round, the user either selects a pass-image among several images or chooses nothing if pass-image is not present. The user is authorized only if all verifications are successful. Pass-image makes it easier for user to remember their password images. Allowing users to register their own images as password image technique is a secure authentication method in comparison with text-based passwords. But this technique would make the password even more predictable, if the attacker is familiar with the user.

III. OVERVIEW OF PASSWORD MANAGERS

Password managers differ in many aspects, including functionality, availability of source code, database format, supported platforms and access to cloud storage. Some popular password managers have their own database format. This is especially true for the password managers that are embedded in major browsers. Several independent password managers share the same database format. So even though each password manager provides a different user experience, the storage format is the same. We assume that the password managers themselves implement what the format specifies .We researched the best possible security achievable in a given specific storage format. For this reason our survey focuses essentially on password managers that provide local storage, at least as an option. We inspect nine popular password database formats. Three password managers used by in-browser are: Google Chrome, Mozilla Firefox and Microsoft Internet Explorer and six database formats used by a large number of independent password managers: 1Password, KDB, KDBX4, PasswordSafe v3, PINs and RoboForm.

TABLE I COMPARISON OF SYSTEMS

Existing System	Proposed System
Not User friendly due to complicated UI design.	Simple design and Easy to use.
Data gets erased randomly when system updates.	Data won't be deleted without the user's permission.
User can select only One password lock as master password.	Two Password lock combination will be available.
Users are charged particular amount after free trial.	Will be available free of cost.

IV. FRAMEWORK AND ARCHITECTURE

This section mainly introduces the detailed design of the software. The system software, which is developed with C programming language, has two main modules, one for Biometric scanner, for sending One Time Password and for voice recognition. The overall design consists of Encryption which is AES 128bit encryption in which users bank account nos. are stored, Voice Recognition for which DSP processor is required, Finger print recognition for pure recognition of

user and for authentication OTP is used to send a short message to users with a SIM card.

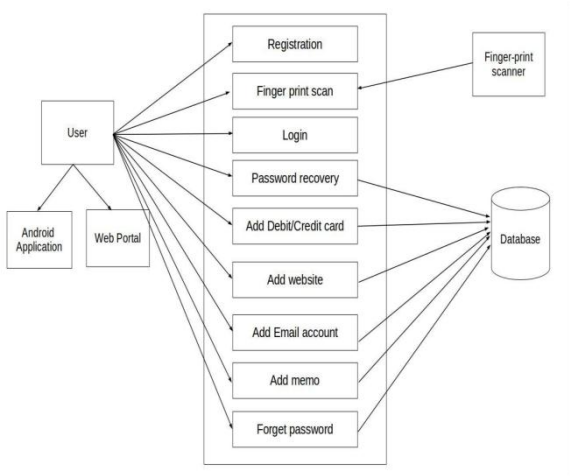

FIGURE I : ARCHITECTURE OF PASSWORD MANAGER

User can access web-portal as well as android application. User can register the fingerprint with the help of fingerprint scanner. Next time when he tries to login this authentication method can be used. Categorization (Debit/Credit Cards, Shopping, Email Account's, other Account's) is present. User can activate Master password over all categories. In case of theft or any other issue one can delete all information present on the cell-phone application by using the option on web portal.OTP can be sent to recovery mail or mobile number in case of password recovery. Sometimes people tend to select passwords that are short and easy to remember. In some cases where passwords are complicated, people might write them down somewhere which is in it self a security risk. That is why a biometric system would be a better alternative to PIN or password based security methods.

A. Finger-Print Lock

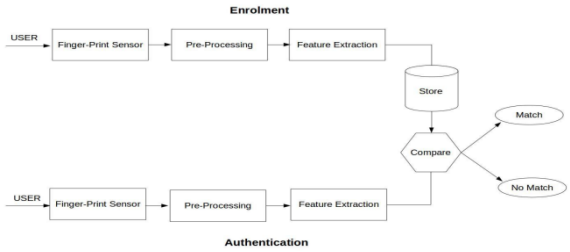

FIGURE II : BLOCK DIAGRAM OF FINGER PRINT LOCK

The User will have to register his Finger Print with the help of finger-print scanner. The sensor will detect the Finger-Print and processing will take place for feature extraction. The scanned finger print image will be stored in the storage database. Next time when the user will try to unlock using finger-print scanner finger-print feature will be extracted and will be compared with the one stored while registration. If the Match occurs then user will be able to login successfully. If Match fails then user will face login failure

B. Voice Recognition Lock

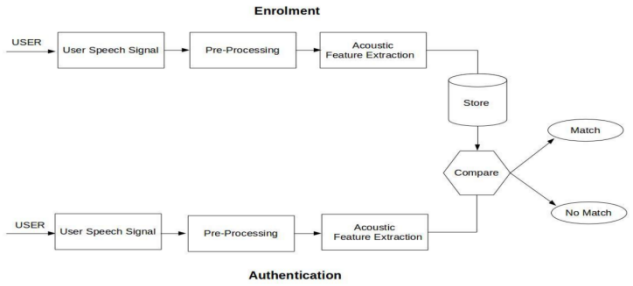

FIGURE III : BLOCK DIAGRAM OF VOICE RECOGNITION LOCK

User will have to register his voice/speech by speaking. The sensor will detect the speech signal and processing will take place for Acoustic feature extraction. The recorded voice will be stored in the storage database. Next time when the user will try to unlock using voice recognition lock acoustic feature will be extracted and will be compared with the one stored while registration. If the Match occurs then user will be able to login successfully. If Match fails then user will face login failure.

C. Passphrase Lock

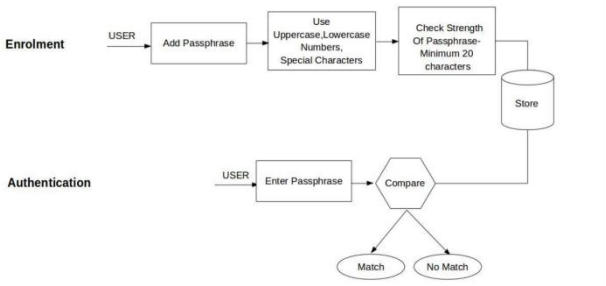

FIGURE IV : BLOCK DIAGRAM OF PASSPHRASE LOCK

The User will have to register the Passphrase. A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security. User will have to choose a phrase that includes Uppercase and lowercase letters, numbers and special characters like _ , @ ,) , (etc. The strength of passphrase should be minimum 20 characters long. The passphrase will be stored in the storage database. Next time when the user will try to unlock using passphrase the entered passphrase will be compared with the one stored while registration. If the Match occurs then user will be able to login successfully. If Match fails then user will face login failure.

D. Intruder Alert

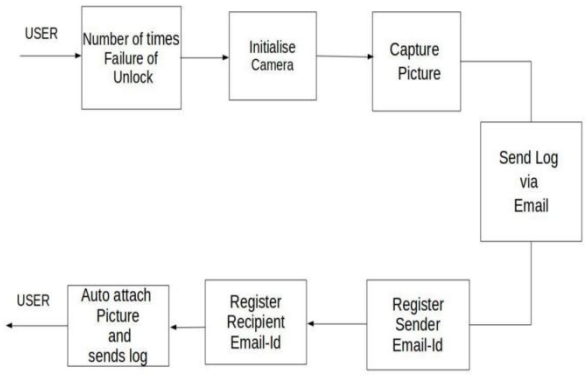

FIGURE V : BLOCK DIAGRAM OF INTRUDER ALERT LOCK

When the user sets the intruder alert timer to 3 i.e. unlock failure time = 3 then after the 3rd attempt the front camera will be initialised and picture of the intruder will be captured. This captured picture of the intruder will be sent from the registered sender's email id to the registered recipient's email id thus alerting the user.

V. BIOMETRIC AUTHENTICATION TECHNIQUES AND SYSTEMS

A. Biometric Face Recognition

There are many different types of biometric authentication systems. Some of the obvious ones are voice, fingerprint, and face recognition. Other biometric authentication systems consist of gait recognition i.e. person's way of walking and artificial intelligence that adapts to the owner's uniqueness while combining other methods. There are two types of face recognition conventions: face verification and face identification. Face identification is used for matching input identity with already registered identity while face verification is used to authorize proper access. The cell phone's camera is utilized to capture facial points. This adds extra protection against breaching this method. Authentication by a photo and authentication by an image captured by another were the two different attempts made against a facial recognition biometric system. The results of the experiment showed there was an illegal authentication of success rate of 87% with just a face photo and 97% with a captured image. Based on these results, face recognition does not seem to be very secure, especially when someone could use a photo from an online social network such as Facebook or MySpace.

B. Biometric Voice Recognition

In this research three seconds was coded into the cell phone's database using a VOCODER. Once the voice was digitized, new input given by the user was compared to the previous recordings for verification. A phoneme is the smallest unit of sound. A phoneme is also very unique. Therefore for reference only a small portion would have to be recorded. A proposed passphrase was also recorded in addition to just voice which would add extra protection against breaching this method. Another study used a biometric voice recognition system which exchanged a digital signature token encrypted and confirmed by voice.

C. Biometric Gait Recognition and AI

This research showed how cell phone authentication could be implemented by gathering gait data. Gait recognition verifies authentication automatically by the way a person walks. A PIN would be required in case the user is not walking. This method is always recording and gathering data without the user having to make any physical inputs. Three methods viz. Machine Vision Based, Floor Sensor Based, and Wearable Sensor Based Gait Recognition were used for gait recognition to be successful. The researchers believed that biometric authentication if used independently would be unsafe. As a result, the researchers proposed a cell phone which would adapt to its owner like a digital pet (ePet). A system which makes decisions to increases the rate of success where an intelligent agent extracts data in real time from the environment is an Artificial Intelligent system. In this research method, the "ePet" would authenticate a user based on the physical environment, physiological and biological factors, as well. The 'ePet' algorithm used both gait data and location tracks in combination with other biometrical authentication methods like face, voice, and fingerprint recognition.

D. Biometric Fingerprint Recognition

Fingerprint recognition may seem to be more secure because a fingerprint is extremely unique and difficult to mimic. This research was conducted using an external USB optical fingerprint sensor and the Biometric Image Software. A different fingerprint authentication method was discussed in another article involving an optical fingerprint reader as well. 2D code provides a more effective security protocol. While QR codes are more secure and reliable. The information gathered is detailed basic ridge patterns and specific characteristics. Both of these researches were different method to the same type of biometric authentication system. Penetration attempts were made against a fingerprint authentication system using an artificial fingerprint.

The Module for Biometric Fingerprint method

Fingerprint Matching Based on Identification and Authentication is one of the oldest and most popular methods. A fingerprint consists of a series of furrows (shallows trenches) and ridges on finger's surface. The uniqueness is determined based on the patterns of PAM allowed applications and Oss to be independent of authentication mechanisms in a UNIX ridge-ending, bifurcations, divergences, and enclosures-MINUTIAE. A typical fingerprint template can show from 30 to 40 minutiae points. Minutiae based approach is commonly adopted by most Fingerprint Scanners. Authentication success is decided by matching score (threshold). The provided sample must exceed a predefined threshold limit.

Biometric Authentication Provider:

The Biometrics enrolment and authentication system provides a facility to enrolment, authentication, management.

JAAS (Java Authentication and Authorization Service): Java API framework that allows implementing authentication authorization mechanisms in Java applications.

PAM (Pluggable Authentication Module):
PAM environment, particularly Solaris and Linux. Unix is less compatible, Linux is more compatible which is in php , java.

The three basic patterns of fingerprint ridges are the arch, loop, whorl.

Arch: The ridges enter from one side of the finger, rise in the centre forming an arc.

Loop: The ridges enter from one side of a finger, form a curve.

Whorl: Ridges form circular round point on the finger.

Fingerprint Processing:

Enrolment of fingerprint image from the sensor plays an important role. The reason is that the way people put their finger on the mirror to scan can affect the result of searching and verifying process. For verification function, many techniques are available to match fingerprints such as correlation-based matching, minutiae-based matching, ridge-based matching. However, the most popular algorithm was minutiae based on matching algorithm.

A fingerprint sensor is an electronic device used to capture image of the fingerprint pattern. The captured image is called a live scan, which is digitally processed to create a biometric template has extracted features which is stored and used for matching. Many technologies are used including RF, thermal, piezo electric.

Optical:

Optical fingerprint imaging captures digital image of the print using visible light. The surface of the sensor, where the finger is placed, is known as the touch surface. Then comes the light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger then passes via phosphor layer to an array of solid state pixels i.e. a charge-coupled device. An untidy touch surface can cause a bad image of the fingerprint. Its demerit is capturing quality of finger's skin. For instance, if skin is dirty or marked, it's difficult to capture image properly. Also, it is possible for an individual to erode the outer layer of skin. However, unlike capacitive sensors, it's not susceptible to electrostatic discharge damage.

Capacitance Sensor:
Capacitance sensors use principle of capacitance. In this method of imaging, the sensor array pixels each acts as a plate of a parallel-capacitor's plate, the dermal layer which is electrically conductive and non-conductive epidermal layer acts as a dielectric. The iPhone 6 uses a capacitance fingerprint sensor.

Algorithms:

Matching algorithms are used previously stored templates of fingerprints against candidate's, for which, either the original image must be directly compared.

These algorithms are:-

Pattern-based

Pixel-based

Pressure based etc.

Pattern-based (or image-based) algorithms:

Pattern based algorithms compare both basic fingerprint patterns and the previously stored template and a candidate fingerprint. This requires that the images should be aligned in the same orientation. For this, the algorithm finds a central point in the fingerprint image. In a pattern-based algorithm, type, size, and orientation of patterns are aligned within fingerprint. The candidate fingerprint image is graphically compared with the template.

Direct (optical) correlation is not used as it is not very efficient for large database. Comparison direct for correlation des images nearest particular plus utilize, can easily be used efficiently. The general shape of the fingerprint is usually used to pre-process the images and reduce the search in large databases. Several categories have been defined in the Henry system: whorl, right loop, left loop, arch, and tented architecture. Pattern matching algorithms are using the general shape of the ridges.

The Module for Sending One Time Password

A one-time password (OTP) is a password that is valid for only one login transaction, on a computer system or any other digital device. The most important advantage that is addressed by OTPs is that, in contrast to static password, they are not vulnerable to repel attacks. This means that a potential intruder who manages to record an OTP that was already used to conduct a transaction will not be able to use it, since it will no longer be valid. A second advantage is that when user uses the same password for multiple systems it is not made vulnerable for all of them, if the password for one of these is known by an attacker. A number of OTP systems also aim to ensure that a session cannot be easily interpreted without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

1) Methods for generating OTP

Time-synchronized:

A time-synchronized OTP is related to a piece of hardware called a security token. Each user is given a personal token that generates a one-time password. It might look like a small calculator or a keychain with an LCD that shows a number that changes occasionally. Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server.

To get the next password in the series from the previous passwords, one needs to find a way of calculating the inverse function. Since function was chosen in one-way, this is extremely difficult to do. An intruder who happens to see a one-time password may have access for OTP to re-login so it

becomes useless once that period expires. The S/KEY system and its derivative OTP are based on Lamport's scheme.

Methods for delivering OTP

Text Messaging:

The most common technology used for the delivery of OTP is via text messaging. Because text messaging is a communication channel available in all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone. Text messaging has a great authentication to reach all consumers with a low total cost to implement. But cost of text messaging for each OTP cannot be acceptable to some users. OTP over text messaging may be encrypted using an unknown standard, which several hacking groups report can be successfully decrypted within minutes or seconds, or else the OTP over SMS might not be encrypted by one's service-provider at all. .

In 2011, Google has started offering OTP to mobile and landline phones for all Google accounts. The user can receive the OTP either as a text message or via an automated call. In case none of the user's registered phones is accessible, then the user can even use one of a set of previously generated one-time backup codes as a secondary authorization in place of the dynamically generated OTP.

Mobile Phones:

A large number of customer already own a mobile phone for purposes other than generating OTPs. A user wishing to access a protected resource, such as an internet banking site, uses the Mobile Token App to generate a One-Time Password. The application can be PIN protected. The Mobile Token App is available for all leading mobile devices.

2) Web-based methods:

This method relies on the user's ability to recognize pre-chosen category pictures from a randomly generated grid of pictures. While registering on a website, the user chooses several categories of things such as cats, dogs, boats, cars and flowers. Each time the user logs into the website they are presented with a randomly generated grid. The grid consists of pic alphanumeric character. The user looks for the pictures that fit in their categories and enters the associated alphanumeric characters to form a one-time access code.

3) Hardcopy:

In some countries, the bank sends to the user a numbered list of OTPs that are printed on paper. While, some banks send plastic cards with actual OTPs concealed by a layer. The user has to the scratch off the layer to reveal a numbered OTP. For every online transaction or login session, the user is required to enter a specific OTP from that given list. In Germany and many other countries like Austria and Brazil, those OTPs are typically called transaction authentication numbers i.e. TANs.

VI. SELECTION OF PLATFORM

Android platform is designed to be more tolerant than many of its predecessors. The device runs on Linux operating system upon which Android applications are executed in a secure fashion. Each android application runs in its own sandbox Application. A core set of applications for everyday tasks, such as Web browsing and email, are included in android devices as in-built, which ensures highest reliability and excellent long term stability. As a product of the OHA's vision for a robust and open source development environment for mobile, Android is a source development platform. The platform was designed for the sole purpose of encouraging as a free and open market that user might want to have and software developers might want to develop it for.

VII. CONCLUSION

With the help of Fingerprint Recognition, Voice Recognition is not only used in traditional security systems, but also be applied in monitor and control access control more and more efficiently. Based on various passwords, this paper has given a design method of authenticity. Biometric authentication is a better alternative and gives stronger security when combined with other technology. Overall, the majority of faces, voices, and fingerprints are not duplicated unless replicated. The only negative aspect to biological and physiological identification is that biometric patterns cannot be revoked. To protect these important valuable data, a system other than PIN or password verification must be used because many cell-phones are lost or stolen on a daily basis.

ACKNOWLEDGEMENT

We would like to thank our guide Prof. S.P. Jadhav and HOD, Department of Computer Engineering Prof. Dr. B.K Sarkar and for their support and guidance throughout our review work. We express our gratitude towards them for giving us this opportunity. We would also acknowledge the authors of the base paper as well as references for their work and inspiration.

REFRENCES

[1] J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better authentication. In Proc. of Ext. Abstracts CHI 2002, pages 868–869, New York, NY, USA, 2002. ACM Press.

[2] R. Dhamija and A. Perrig. Dej`a vu: A user study using images for authentication. In Proc. of the 9th USENIX Security Symposium, 2000.

[3] S. Brostoff and M. A. Sasse. Are passfaces more usable than passwords: A field trial investigation. People and Computers XIV - Usability or Else: Proceedings of HCI 2000, pages 405–424, 2000.

[4] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: effects of tolerance and image choice. In SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security, pages 1–12, New York, NY, USA, 2005. ACM Press.

[5]J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. IEEE Security and Privacy, 2(5):25–31, 2004.
[6] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat. Cognitive, associative and conventional passwords: Recall and guessing rates. Computers and Security, 16(7):641–657, 1997.
[7] E. Gabber, P. B. Gibbons, Y. Matias, , and A. J. Mayer. How to make personalized web browsing simple, secure, and anonymous. Financial Cryptography, page 1732, 1997.
[8]B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell. Stronger password authentication using browser extensions. 14th Usenix Security Symposium, page 1732, 2005.
[9] A. H. Karp. Site-specific passwords. Technical report, Hewlett-Packard Laboratories. http://www.hpl.hp. com/personal/Alan Karp/site password/ site password files/site password.pdf.
[10] A. Adams and M. A. Sasse. Users are not the enemy. Commun. ACM, 42(12):40–46, 1999.
[11]D. Weirich and M. A. Sasse. Persuasive password security. In Proc. of Ext. Abstracts CHI 2001, pages 139–140, New York, NY, USA, 2001. ACM Press.
[12]D. Weirich and M. A. Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In Proc. of NSPW 2001, pages 137–143, New York, NY, USA, 2001. ACM Press.
[13] A. S. Brown, E. Bracken, S. Zoccoli, and K. Douglas. Generating and remembering passwords. Applied Cognitive Psychology, 18(6):641–651, 2004.
[14]S. Riley. Password security: What users know and what they actually do. http://psychology.wichita. edu/surl/usabilitynews/81/Passwords.htm, February 2006.
[15]A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.
[16]S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.
[17]D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
[18]W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.
[19]W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.
[20]W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.
[21] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795 /2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

