MANTECH Publications

Journal of Digital Image Processing and Computer Vision
Volume 2 Issue 3

A Remote User Authentication Operation Using Carp Schemes

A. Aafiya Thahaseen

Assistant Professor

Department of Computer Science & Engineering

Al-Ameen Engineering College, Karundevanpalayam, Nanjai Uthukuli Tamil Nadu, India

Corresponding Author's E-mail id: *aafiyab.e@gmail.com*

Abstract

Image based password schemes are constructed to authenticate users. Graphical passwords are composed with images and sketches with human memory for visual information. Improved password memorability and strength against guessing attacks are the key benefits of graphical password schemes. Graphical passwords are classified into three main categories. They are recall, recognition and cued-recall methods. Recall based graphical password systems are draw metric systems. Recognition based systems, also known as cogno metric systems or search metric systems. Cued recall systems typically require that users remember and target specific locations within an image.

Graphical passwords and Captcha schemes are integrated to perform the user authentication with improved security mechanism. Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. Online guessing attacks, relay attacks and shoulder surfing attacks are handled in CaRP. CaRP is click-based graphical passwords where a sequence of clicks on an image is used to derive a password. Dynamic captcha challenge image is used for each login attempt in CaRP. Text Captcha and image-recognition Captcha are used in CaRP scheme. Text CaRP scheme constructs the password by clicking the right character sequence on CaRP images. CaRP schemes can be classified into two categories recognition based

CaRP and recognition-recall based CaRP. Recognition-based CaRP seems to have access to an infinite number of different visual objects. Recognition-recall based CaRP requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. Password information is transferred and verified using hash codes. Secure channels between clients and the authentication server through Transport Layer Security (TLS).

The system is improved with distribution analysis and transmission security features. Pattern based attacks are handled with Color and Spatial patterns. Pixel colors in click points are considered in the color pattern analysis model. Pixel location patterns are considered in the spatial pattern analysis model.

Keywords: *Carp Schemes, Authentication Operation, Transport Layer Security (TLS)*

1. INTRODUCTION

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. In our system, the task of selecting weak passwords is more tedious, discouraging users from making such choices [12]. In effect, this approach makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password—a feature lacking in most schemes.

We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) [11] and conducted user studies evaluating usability and security. This paper

presents a consistent assimilation of earlier work [10] and two unpublished web studies, reinterprets and updates statistical analysis incorporating larger data sets, provides new evaluation of password distributions, extends security analysis including relevant recent attacks and presents important implementation details. This systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues, to advance understanding as is prudent before practical deployment of new security mechanisms. Through eight user studies, we compared PCCP to text passwords and two related graphical password systems. Results show that PCCP is effective at reducing hotspots and avoiding patterns formed by click-points within a password, while still maintaining usability.

2. CAPTCHA AND ITS TYPES

CAPTCHAs based on reading text — or other visual-perception tasks — prevents blind or visually impaired users from accessing the protected resource. CAPTCHAs do not have to be visual. Any hard artificial intelligence problem, such as speech recognition, can be used as the basis of a CAPTCHA. Some implementations of CAPTCHAs permit users to opt for an audio CAPTCHA. Other implementations do not require users to enter text, instead asking the user to pick images with common themes from a random selection.

For non-sighted users, visual CAPTCHAs present serious problems. Because CAPTCHAs are designed to be unreadable by machines, common assistive technology tools such as screen readers cannot interpret them. Since sites may use CAPTCHAs as part of the initial registration process, or even every login, this challenge can completely block access. In certain jurisdictions, site owners could become target of litigation if they are using CAPTCHAs that discriminate against certain people with disabilities. For example, a CAPTCHA may make a site incompatible with Section 508 in the United States. In other cases, those with sight difficulties can choose to identify a word being read to them.

While providing an audio CAPTCHA allows blind users to read the text, it still hinders those who are both visually and hearing impaired. According to sense.org.uk, about 4% of people over 60 in the UK have both vision and hearing impairments. There are about 23,000 people

in the UK who have serious vision and hearing impairments.

According to The National Technical Assistance Consortium for Children and Young Adults Who Are Deaf-Blind (NTAC), the number of deaf blind children in the USA increased from 9,516 to 10,471 during the period 2004 to 2012. Gallaudet University quotes 1980 to 2007 estimates which suggest upwards of 35,000 fully deaf blind adults in the USA. Deaf blind population estimates depend heavily on the degree of impairment used in the definition.

The use of CAPTCHA thus excludes a small number of individuals from using significant subsets of such common Web-based services as PayPal, GMail, Orkut, Yahoo!, many forum and weblog systems, etc. Even for perfectly sighted individuals, new generations of graphical CAPTCHAs, designed to overcome sophisticated recognition software, can be very hard or impossible to read. A method of improving the CAPTCHA to ease the work with it was proposed by Protect Web Form and was called "Smart CAPTCHA". Developers advise to combine the CAPTCHA with JavaScript support. Since it is too hard for most of spam robots to parse and execute JavaScript, using a simple script which fills the CAPTCHA fields and hides the image and the field from human eyes was proposed.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), also known as Human Interactive Proof (HIP), is an automated Turing test in which both generation of challenges and grading of responses are performed by computer programs. CAPTCHAs are based on Artificial Intelligence (AI) problems that cannot be solved by current computer programs or bots, but are easily solvable by humans [9]. A client who provides a correct response to a challenge is presumed to be a human; otherwise a bot. CAPTCHAs have been widely used as a security measure to restrict access from bots.

3. RELATED WORK

Many graphical passwords schemes have been proposed to date and several surveys are available [6]. Here we concentrate on click-based graphical password schemes, wherein a user clicks on a set of points on one or more presented background images and work related to guessing attacks on graphical passwords. In V-go users click on a sequence of predefined objects in the picture. In Blonder's proposal, users click on

a set of predefined tap regions. Jansen et al. propose a variation, which requires users to click an ordered sequence of visible squares imposed on a background image; the squares are intended to help users repeat click-points in subsequent logins.

PassPoints allows users to click a sequence of five points anywhere on an image while allowing a degree of error tolerance; studies suggest promising usability. A 16 related commercial system designed for the Pocket PC, called VisKey, allows the user to choose the number of click-points and to set the error tolerance.

The security of click-based graphical passwords has been examined [5]; for security analyses of other types of graphical schemes see also Davis et al. and van Oorschot et al. [13]. One way that an attacker could predict hot-spots is by using image processing tools to locate areas of interest. Dirik et al. [1] use an image processing tool for guessing PassPoints passwords to guess single-session user passwords for two images, one being a particularly simple image. For the other image, their method guessed 8% of passwords using an attack dictionary with 232 entries where the full space was 240 entries. In other work, Thorpe et al. examine an automated method, guessing 9.1% and 0.9% of passwords on two images, using an attack dictionary with 235 entries compared to a full pasword space of 243 passwords. The method of Thorpe et al. focused only on a variation of stage 1, ordering an attack dictionary based on the raw values of the resulting saliency map, whereas the present paper uses the entire model including stage 2. In a preliminary version of the present work, Salehi-Abari et al. [7] guess 8-15% of passwords for two representative images using dictionaries of less than 224.6 entries and about 16% of passwords on each of these images using dictionaries of less than 231.4 entries, where the full space is 243.

Basic click-order patterns were first introduced and evaluated in combination with human seeded attacks; the only pattern in common with the present work is regular DIAG. Chiasson et al. [3] analyze a set of patterns for three click-based graphical password schemes: PassPoints and two variants named Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP) [2]. In CCP and PCCP, a user clicks on a single point on each of five images, where each image is dependent on the previous click-point. They show that the design of the

interface impacts whether users select clickpoints in some predictable patterns and implied that such patterns in user choice might reduce the effective password space. The present paper mathematically models click-order patterns and uses them to mount purely automated attacks, demonstrating and experimentally quantifying then degree to which certain patterns can be used to efficiently search the password space.

Thorpe et al. [5] introduce human-seeded attacks and demonstrate their efficacy against Passpoints-style graphical passwords. Human-computed data sets were used in two human-seeded attacks against passwords from a field study on two different images: one based on a first-order Markov model another based on an independent probability model. Using their human-computed data sets, a dictionary based on independent probabilities contained $231.1 - 233.4$ entries and found 20-36% of field study passwords and a dictionary based on the first-order Markov model found 4-10% of field study passwords within 100 guesses. These attacks require the attacker to collect sufficient click-points for each image and are image dependent, thus requiring per-image costs for systems with multiple images.

4. CARP SCHEMES

A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on.

Captcha distinguishes human users from computers by presenting a challenge, beyond the capability of computers but easy for humans [8]. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. The new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call CaRP. CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike

other click-based graphical passwords, images used in CaRP are Captcha challenges and a new CaRP image is generated for every login attempt.

The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons: 1) It causes denial-of-service attacks and incurs expensive helpdesk costs for account reactivation. 2) It is vulnerable to global password attacks whereby adversaries intend to break into any account rather than a specific one and thus try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold to avoid triggering account lockout.

CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.

CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used.

5. RECOGNITION-RECALL CARP

In recognition-recall CaRP, a password is a sequence of some invariant points of objects. An invariant point of an object (e.g. letter "A") is a point that has a fixed relative position in different incarnations (e.g., fonts) of the object and thus can be uniquely identified by humans no matter how the object appears in CaRP images. To enter a password, a user must identify the objects in

a CaRP image and then use the identified objects as cues to locate and click the invariant points matching her password. Each password point has a tolerance range that a click within the tolerance range is acceptable as the password point. Most people have a click variation of 3 pixels or less. Text Point, a recognition recall CaRP scheme with an alphabet of characters, is presented next, followed by a variation for challenge response authentication.

5.1. *Text Points*

Characters contain invariant points. Some invariant points of letter "A", which offers a strong cue to memorize and locate its invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of characters is selected to form a set of clickable points for TextPoints. The internality ensures that a clickable point is unlikely occluded by a neighboring character and that its tolerance region unlikely overlaps with any tolerance region of a neighboring character's clickable points on the image generated by the underlying Captcha engine. In determining clickable points, the distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images. In addition, variation should also be taken into consideration. For example, if the center of a stroke segment in one character is selected, we should avoid selecting the center of a similar stroke segment in another character.

Instead, we should select a different point from the stroke segment, e.g., a point at one-third length of the stroke segment to an end. This variation in selecting clickable points ensures that a clickable point is context-dependent: a similarly structured point may or may not be a clickable point, depending on the character that the point lies in. Character recognition is required in locating clickable points on a TextPoints image although the clickable points are known for each character. This is a task beyond a bot's capability.

5.2. Text Points 4CR

For the CaRP schemes presented up to now, the coordinates of user-clicked points are sent directly to the authentication server during authentication. For more complex protocols, say a challenge-response authentication protocol, a response is sent to the authentication server instead. TextPoints

can be modified to fit challenge-response authentication. This variation is called TextPoints for Challenge-Response or TextPoints4CR.

Unlike TextPoints wherein the authentication server stores a salt and a password hash value for each account, the server in TextPoints4CR stores the password for each account. Another difference is that each character appears only once in a TextPoints4CR image but may appear multiple times in a TextPoints image.

This is because both server and client in TextPoints4CR should generate the same sequence of discretized grid-cells independently. That requires a unique way to generate the sequence from the shared secret, i.e., password. Repeated characters would lead to several possible sequences for the same password. This unique sequence is used as if the shared secret in a conventional challenge response authentication protocol.

In TextPoints4CR, an image is partitioned into a fixed grid with the discretization grid-cell of size μ along both directions. The minimal distance between any pair of clickable points should be larger than μ by a margin exceeding a threshold to prevent two clickable points from falling into a single grid-cell in an image. Suppose that a guaranteed tolerance of click errors along both x-axis and y-axis is τ , we require that $\mu \geq 4\tau$.

In entering a password, a user-clicked point is replaced by the grid-cell it lies in. If click errors are within τ , each user-clicked point falls into the same grid-cell as the original password point. Therefore the sequence of grid-cells generated from user-clicked points is identical to the one that the authentication server generates from the stored password of the account. This sequence is used as if the shared secret between the two parties in a challenge-response authentication protocol.

Unlike other CaRP schemes presented in this paper, Text- Points4CR requires the authentication server to store passwords instead of their hash values. Stored passwords must be protected from insider attacks; for example, they are encrypted with a master key that only the authentication server knows. A password is decrypted only when its associated account attempts to log in.

6. AN EFFICIENT USER AUTHENTICATION USING CARP

The CaRP scheme is enhanced with strength analysis and security features. Pattern based attacks are handled with Color and Spatial patterns. Pixel colors in click points are considered in the color pattern analysis model. Pixel location patterns are considered in the spatial pattern analysis model. Dictionary attacks and transmission attacks handling process is also improved with high security. Password security level assessment mechanism is used in the graphical password construction process. Cryptography (RSA) and data integrity (SHA) schemes are also integrated with the system to improve the security level in online applications. CAPTCHA and graphical password schemes are used for the user authentication process.

Pixel physical and spatial properties are used in the strength analysis process. Transmission security is improved with integrity verification mechanisms. The system is divided into six major modules. They are CaRP with Text CAPTCHA, authentication server, CaRP with image Recognition CAPTCHA, pattern analysis, attack handler and enhanced CaRP scheme.

Character sequence selection is used in CaRP with Text CAPTCHA scheme. The authentication server is designed to manage and verify the user accounts. CaRP with Image Recognition CAPTCHA scheme uses the recognition and recall mechanism with image objects. The color and spatial patterns are analyzed under the pattern analysis module. The directory and shoulder surfing attacks are handled under attack handler module. Enhanced CaRP Scheme integratesthe security and attack control mechanism for user authentication process.

6.1. CaRP with Text CAPTCHA

Textual characters based CAPTCHA is used in Text CaRP scheme. Password is constructed by selecting character sequences in the text CAPTCHA collection. The textual CAPCHA characters are dynamically rearranged at the time of recognition process. Password details are converted into hash codes and applied in verification process.

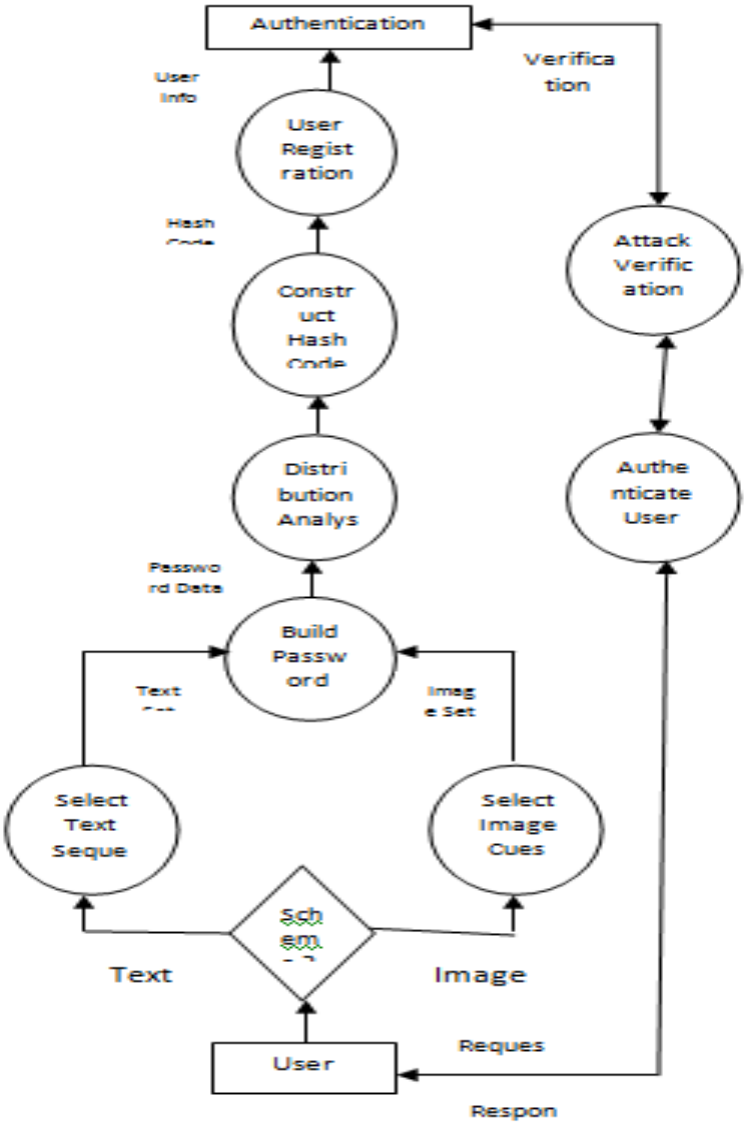

Fig. No: 6.1. An Efficient User Authentication Using CaRP

6.2. Authentication Server

The authentication server application is used to authenticate the users. User registration and password management operations are carried out under the server. Password verification is carried out under the server. Key and signature values are maintained under the server.

6.3. *Carp with Image Recognition Captcha*

Image objects are used in recognition-recall based CaRP Recognition CAPTCHA. Object recognition and click cue

identification mechanism are used in the system. Rectangular regions are used in the cued recall process. CAPTCHA-Zoo image object collection is used for the password construction process.

6.4. *Pattern Analysis*

Color and spatial patterns are analyzed in the system. Pixel color for click points are used in the color pattern analysis. Spatial patterns are extracted from location information. Password complexity is assessed with pattern information.

6.5. *Attack Handler*

Directory and shoulder surfing attacks are managed by the system. RSA algorithm is used to perform password encryption/decryption tasks. Image dimming mechanism is used to control shoulder surfing attacks. Mouse cursor size and location are automatically adjusted for attack handling process.

6.6. *Enhanced CaRP Scheme*

CaRP scheme and attack handling mechanism are integrated in the Enhanced CaRP scheme. Distribution, strength and pattern analysis schemes are integrated with CaRP scheme. The Secure hashing algorithm (SHA) is used to generate password signatures. Reusability level is analyzed.

6.7. *RSA Algorithm*

The domain name service sensitive attributes are secured using the RSA algorithm. The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

Key Generation

Select p,q

p and q both prime , $p \neq q$

Calculate $n = p \times q$

Calculate $\phi(n)=(p-1)(q-1)$

Select integer e

$\gcd(\phi(n),e) = 1; 1 < e < \phi(n)$

Calculate d

$d = e^{-1} \bmod \phi(n)$

Public key

$KU = \{e, n\}$

Private key

$KR = \{d, n\}$

Encryption

Plaintext

$M < n$

Cipher text

$C = M^e \pmod n$

Decryption

Cipher text

C

Plaintext

$M = C^d \pmod n$

6.8. Secure Hashing Algorithm

The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1 and the standard was no longer approved for most cryptographic uses after 2010.

CONCLUSION

Remote user authentication operations are carried out using the graphical password schemes to provide efficient security. CAPTCHA techniques are used to verify the source type of request. Captcha as Graphical Passwords scheme integrates the text and image captchas to construct graphical password scheme. CaRP scheme is enhanced with strength based password construction and attack resistant user authentication model. Password complexity prediction system is integrated to improve password construction process. The system increases the success and recall rates. User interface is upgraded to avoid capture attacks in password recall process. Efficient shoulder surfing attack controlling models are used to protect the system from attackers.

REFERENCES

[1] J. Thorpe. On the Predictability and Security of User Choice in Passwords. PhD thesis, Carleton University, 2008.

[2] S. Chiasson, A. Forget, R. Biddle and P.C. van Oorschot. Influencing Users towards Better Passwords: Persuasive Cued Click-Points. In Proceedings of HCI, British Computer Society, 2008

[3] S. Chiasson, A. Forget, R. Biddle and P.C. van Oorschot. User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords. International Journal of Information Security, 8(5), 2009.

[4] S. Chiasson, A. Forget, E. Stobert, P.C. van Oorschot and R. Biddle. Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. In 16th ACM Conference on Computer and Communications Security (CCS), 2009.

[5] P.C. van Oorschot and J. Thorpe. On Predicting and Exploiting Hot-Spots in Click-Based Graphical Passwords, 2008.

[6] K. Renaud. Guidelines for designing graphical authentication mechanism interfaces . International Journal of Information and Computer Security, 3(1):60–85, 2009.

[7] A. Salehi-Abari, J. Thorpe and P.C. van Oorschot. On Purely Automated Attacks and Click- Based Graphical Passwords. In Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), 2008

[8] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014

[9] B. B. Zhu et al., "Attacks And Design Of Image Recognition CAPTCHAs," in Proc. ACM CCS, 2010.

[10] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[11] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.

[12] Sonia Chiasson, Alain Forget, Robert Biddle and Paul C. van Oorschot, "Persuasive Cued Click-Points. Design, Implementation and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE Transactions On Dependable And

Secure Computing, Vol. 9, No. 2, March/April 2012

[13] P.C. van Oorschot and J. Thorpe. On Predictive Models and User-Drawn Graphical Passwords. ACM Transactions on Information and System Security, 10(4):1–33, January 2008.