Volume No:2, Issue No:8 (January-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Overcoming Security Attacks by Using Image Captcha and Sound Signature

Budarapu Sumalatha
PG Scholar,
Dept of CSE,
Mahaveer Instituteof Science and Technology,
Hyderabad, Telangana, India.

Konkapakat Srinivasa Rao
Professor,
Dept of CSE,
Mahaveer Instituteof Science and Technology,
Hyderabad, Telangana, India.

Abstract:
In this project, a graphical secret system with a validating sound signature to extend the remembrance of the secret is mentioned. In planned work a click-based graphical secret theme known as Cued Click Points (CCP) is bestowed. During this system a secret consists of sequence of some pictures within which user will choose one click-point per image. Additionally user is asked to pick a sound signature for every click purposeand this sound signature is going to facilitate the user in recalling the clicking purpose on a picture.

Keywords:
Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

Introduction:
The objective of this project is to produce the safety for any websites by victimization graphical passwords with read port and persuasive cued click-points. The purpose of this project is that the amount of predefined regions is little, maybe some dozens in every image. The Arcanum ought to be up to twelve clicks for adequate security, once more tedious for the user. Another drawback of this technique is that the want for the predefined regions must be without any acknowledgeable delay. Users usually produce unforgettable passwords that are simple for attackers to guess, however robust system-assigned passwords are troublesome for users to recollect. An Arcanum authentication system ought to encourage robust passwords whereas maintaining note ability. We have a tendency to propose that authentication schemes enable user selection whereas influencing users toward stronger passwords. We have a tendency to apply this approach to make the primary persuasive click-based graphical Arcanum system, Persuasive Cued Click-Points (PCCP), and conducted user studies evaluating usability and security.

EXISTING SYSTEM:
In CCP, users click one ==9
cures instead of on 5 points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they created a blunder once coming into their latest click-point (at that purpose they will cancel their try and try from the beginning).It conjointly makes attacks supported hotspot analysis tougher. Each click leads to showing a next-image, in impact leading users down a "path" as they click on their sequence of points. A wrong click leads down Associate in nursing incorrect path, with a definite indication of authentication failure solely when the ultimate click. Users will select their pictures solely to the extent that their click-point dictates succeeding image. While the sure thing downside will be resolved by disallowing user alternative and assignment passwords to users, this typically results in usability problems since users cannot simply keep in mind such random passwords. Number of graphical word systems is developed, Study shows that text-based passwords suffer with each security and usefulness issues.

DISADVANTAGES:
* The drawback with this theme is that the amount of predefined regions is tiny, maybe a number of dozens in a very image.
* The watchword could have to be compelled to be up to twelve clicks for adequate security, once more tedious for the user.
* Another drawback of this method is that they would like for the predefined regions to be promptly diagnosable.

PROPOSEDWORK:
In the planned work we've integrated sound signature to assist in recalling the watchword. No system has been developed up to now that uses sound signature in graphical watchword authentication.

Volume No:2, Issue No:8 (January-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Study says that sound signature or tone often recall facts like pictures, text etc. In existence we have a tendency to see numerous samples of recalling associate object by the sound associated with that object enters User ID and choose one sound frequency that he need to be selected at login time, a tolerance worth is additionally selected with can decide that the user is legitimate or associate receiver. To produce elaborated vector user needs to choose sequence of pictures and clicks on every image at click points of his alternative. Profile vector is made.

ADVANTAGE:

* To produce elaborated vector user needs to choose sequence of pictures and clicks on every image at click points of his alternative. Profile vector is made.
* Users most popular CCP to Pass Points, chosenlocation and memory only 1 purpose per image was easier and sound signature helps significantly in recalling the clicking points.
* System showed excellent Performance in terms of speed, accuracy, and easy use.

Architecture DIAGRAM:

RELATED WORK:

Grid Resource Abstraction, Virtualization, and Provisioning for Time-targeted Applications As a spread of science applications area unit integrated with large-scale HPDC (High Performance Distributed Computing) technologies, timely resource allocation is disclosed as an essential demand to be thought-about. This paper introduces a brand new HPDC resource management paradigm named resource slot that defines a network of logical machines across time and house. A resource slot isn't solely a resource programming target however conjointly a virtualized resource provisioning framework for a spread of resource management paradigms by encapsulating the resource management quality. Especially, we have a tendency to gift a resource provisioning technique named target-hunting redundant submission (GRS) that probabilistically guarantees a timely resource slot allocation. Experimental results performed against eight clusters in production show that concerning five redundant resources per slot will secure slot allocation with up to thirty six logical machines, every cluster having associate accessibility likelihood as low as zero.25 and therefore the target success likelihood of slot allocation is zero.95.

Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords:

The underlying problems regarding the usability and security of multiple passwords area unit for the most part undiscovered. However, we all know that individuals typically have problem basic cognitive process multiple passwords. This reduces security since users use a similar word for various systems or reveal different passwords as they fight to log in. we tend to report on a laboratory study comparison recall of multiple text passwords with recall of multiple click-based graphical passwords. In an exceedingly one-hour session (short-term), we tend to find that participants within the graphical word condition coped considerably higher than those within the text word condition. Especially, they created fewer errors once recalling their passwords, didn't resort to making passwords directly associated with account names, and didn't use similar passwords across multiple accounts. Once period, participants within the 2 conditions had recall success rates that weren't statistically completely different from one another, however those with text passwords created a lot of recall errors than participants with graphical passwords. In our study, click-based graphical words were considerably less at risk of multiple password interference within the short-run, whereas having comparable usability to text passwords in most different respects.

Comparing Passwords, Tokens, and Biometrics for User Authentication:

For decades, the positive identification has been the quality means used for user authentication on computers. However, as user's area unit needed to recollect additional, longer, and ever-changing passwords, it's evident that an additional convenient and secure resolution to user authentication is important. This paper examines passwords, security tokens, and biometrics—which we have a tendency to put together decision authenticators—and compares these authenticators and their mixtures. We have a tendency to examine their effectiveness against many attacks and suitableness for specific security specifications like compromise detection and non-repudiation. Samples of appraiser mixtures and protocols area unit delineate to indicate tradeoffs and solutions that meet chosen, sensible necessities. The paper endeavors to supply a comprehensive image of user authentication solutions for the needs of evaluating choices to be used and characteristic deficiencies requiring more analysis.

Volume No:2, Issue No:8 (January-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

MODULES:

Spatial Patterns:

The click-point distributions of PCCP on the x and y-axes fell among the vary for random distributions with ninety fifth chance, whereas those of Pass Points. Showed a transparent progression from top-left to bottom right supported the ordinal position of the click-points among the word. We have a tendency to believe that the distinction is users' choice strategy is predicated on whether or not the click points are hand-picked on one image, as in Pass Points, or distributed across many pictures. With one image, as in Pass Points, users tend to begin at one corner of the image and progress across the image with every ulterior click-point. However, with CCP and PCCP, users see a replacement image {for every for every} click-point and have a tendency to pick out each click-point severally, with no relation to its ordinal position among the word. Click-points among Pass Points were abundant nearer along (i.e., shorter segments between serial click-points), whereas CCP's segments were the longest and among vary of the random distributions. PCCP's segments were slightly shorter than CCP's. Provided that no different special patterns are apparent for PCCP, we have a tendency to suspect that these shorter segments are associate degree unit of the viewport positioning formula that slightly favored a lot of central areas of the image. With relevance angles and slopes shaped between adjacent line segments among passwords, analysis shows that PCCP passwords have massive angles and favor no explicit direction. In distinction, Pass Points passwords typically type straight horizontal or vertical lines. Similarly, the frequency distributions for the general shapes shaped by following the trail from the primary to last click-point for PCCP are among the vary of the random datasets. Pass Points passwords were rather more possible to make possible shapes.

Hotspots:

Hotspots square measure areas of the image that have higher chance of being select by users as word click-points. Attackers in any agency gain data of those hotspots through harvest sample passwords will build attack dictionaries and a lot of with success guess Pass Points passwords. Users additionally tend to pick out their click-points in predictable patterns(e.g., straight lines), which may even be exploited by attackers even while no data of the background image; so, strictly machine-driven attacks against Pass Points supported image process techniques and special patterns square measure a threat.

Click Patterns:

A precursor to PCCP, Cued Click-Points (CCP) was designed to cut back patterns and to cut back the quality of hotspots for attackers. Instead of 5 click-points on one image, CCP uses one click-point on 5 completely different pictures shown in sequence. Consequent image displayed relies on the situation of the antecedently entered click-point, making a path through a picture set. Users choose their pictures solely to the extent that their click-point determines consequent image. Making a replacement parole with completely different click-points leads to a unique image sequence.

Tolerance Range:

After creation of the login vector, system calculates the geometer distance between login vector and profile vectors keep geometric distance between 2 vectors p and alphabetic character is given by-Above distance is calculated for every image if this distance comes out but a tolerance price D. The worth of D is set in step with the appliance. In our system this price is chosen by the user. Tolerance level used for get coordinated pixels for our elite click points in our image.

Captcha Password:

It was introduced to use each Captcha and pay role in every user authentication protocol, that we tend to decision Captcha-based parole Authentication (CbPA) protocol, to counter on-line wordbook attacks. The CbPA-protocol in needs finding a Captcha challenge once inputting a sound try of user ID and parole unless a sound browser cookie is received. For associate degree invalid try of user ID and parole, the user includes a sure chance to resolve a Captcha challenge before being denied access.

Sound Signature:

Sound signature is especially further to resolve guesswork attack as we offer multiple click points from totally different pictures guesswork attack are going to be happened. Thus we tend to distribution a selected sound signature for cued click points that has been diagrammatical as graphical parole. In a very guesswork attack, a parole guess tested in Associate in nursing unsuccessful trial is decided wrong and excluded from later trials.

Volume No:2, Issue No:8 (January-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The amount of undetermined parole guesses decreases with a lot of trials, resulting in a higher probability of finding the parole. To counter guesswork attacks, ancient approaches in planning graphical paroles aim at increasing the effective password house to form passwords more durable to guess and so need a lot of trials. Regardless of however secure a graphical parole theme is, the parole will continuously be found by a brute force attack. During this paper, we tend to distinguish 2 varieties of guesswork. Attacks: automatic guesswork attacks apply Associate in nursing automatic trial and error method however S will be manually made whereas human guesswork attacks apply a manual trial and error method.

Secure Recovery:

If user forgets the press points or frequent dead reckoning attacks user was redirected to recovery part wherever user allowed resetting their graphical passwords of same pictures or they'll choose graphical passwords from new pictures in conjunction with sound signature. It principally protects users from parole re-usability.

CONCLUSION:

A common security goal in positive identification-based authentication systems is to maximize the effective password area. This impacts usability once user alternative is concerned. We've shown that it's possible to permit user alternative whereas still increasing the effective positive identification area. What is more, tools like PCCP's viewport (used throughout positive identification creation) can't be exploited throughout an attack. Users may be additional deterred (at some price in usability) from choosing obvious click-points by limiting the quantity of shuffles allowed throughout positive identification creation or by increasingly retardation system response in positioning the viewport with each shuffle past a particular threshold. The approaches mentioned during this paper gift a middle ground between insecure however unforgettable user-chosen passwords and secure system generated random passwords that square measure troublesome to recollect. We have projected CaRP, a brand new security primitive counting on unsolved arduous AI issues. CaRP is each a Captcha and a graphical positive identification theme. The notion of CaRP introduces a brand new family of graphical passwords, that adopts a brand new approach to counter on-line estimation attacks: a brand new CaRP image, that is additionally a Captcha challenge, is employed for each login conceive to build trials of a web estimation attack computationally freelance of every alternative. A positive identification of CaRP may be found solely probabilistically by automatic on-line estimation attacks together with brute-force attacks, a desired security property that alternative graphical positive identification schemes lack. Hotspots in CaRP pictures will not be exploited to mount automatic on-line estimation attacks, an inherent vulnerability in several graphical positive identification systems.

REFERENCES:

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords:Learning from the first twelve years," ACM Compute. Surveys, vol. 44,No. 4, 2012.

[2] (2012, Feb.). The Science Behind Passfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Pass Points: Design and longitudinal evaluation of a graphical password System," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, No. 4, pp. 1–33, 2008.

[7] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.

[8] A. E. Dirik, N. Memon, and J.-C.Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.

[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, pp. 103–118.

Volume No:2, Issue No:8 (January-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated Attacks on pass points-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[11] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click based Graphical passwords," J. Compute. Security, vol. 19, no. 4, pp. 669–702, 2011.

[12] T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/

[13] HP Tipping Point DVLabs, Vienna, Austria. (2010). Top Cyber SecurityRisks Report, SANS Institute and Qualys Research Labs [Online].Available: http://dvlabs.tippingpoint.com/toprisks2010

[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.

[15] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.

[16] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[17] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.

[18] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.

[19] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu.Conf. People Comput., Culture, Creativity, Interac tion, vol. 1. 2008, pp. 121–130.

[20] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in Proc. USENIX Security, 2004, pp. 1–11.

[21] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc. 9th USENIX Security, 2000, pp. 1–4.

[22] D. Weinshall, "Cognitive authentication schemes safe against spyware," inProc. IEEE Symp. Security Privacy, May 2006, pp. 300–306.

[23] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in Proc. ACM CCS, 2007, pp. 1–12.

[24] P. Golle, "Machine learning attacks against the Asirra CAPTCHA," in Proc. ACM CCS, 2008, pp. 535–542.

[25] B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs," inProc. ACM CCS, 2010, pp. 187–200.

[26] J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoft CAPTCHA," in Proc. ACM CCS, 2008, pp. 543–554.

[27] G. Mori and J. Malik, "Recognizing objects in adversarial clutter," InProc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognition., Jun. 2003, pp. 134–141.

[28] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23–28.

[29] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Computers beat humans at single character recognition in reading-based human interaction proofs," in Proc. 2nd Conf. Email Anti-Spam, 2005, pp. 1–3.

[30] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in Proc. 2nd Int. Workshop Human Interaction Proofs, 2005, pp. 1–10.

Volume No:2, Issue No:8 (January-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[31] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA That exploits interest-aligned manual image categorization," in Proc. ACM CCS, 2007, pp. 366–374.

[32] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new CAPTCHA interface design for mobile devices," in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8.

[33] N. Joshi. (2009, Nov. 29). Koobface Worm Asks for CAPTCHA [Online]. Available: http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor-CAPTCHA

[34] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs—Understanding CAPTCHA-Solving Services in an Economic Context," in Proc. USENIX Security, 2010, pp. 435–452.

[35] M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in Proc. ACSAC, 2007, pp. 375–384.

[36] G. Wolberg, "2-pass mesh warping," in Digital Image Warping. Hoboken, NJ, USA: Wiley, 1990.

[37] HP TippingPointDVLabs, New York, NY, USA. (2011). The Mid-Year Top Cyber Security Risks Report [Online]. Available:http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-7045ENW.pdf

[38] S. Kim, X. Cao, H. Zhang, and D. Tan, "Enabling concurrent dual views On common LCD screens," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 2175–2184.

[39] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayyam, A.-R. Sadeghi, And R. Schmitz, "Breaking e-banking CAPTCHAs," in Proc. ACSAC, 2010, pp. 1–10.

[40] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme Against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.

[41] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.

[42] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.