International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

A Survey of Comparative Analysis of Secure Passwords using CaRP by Different Techniques

Nanasaheb S. Pote [1], Prof. Deepali Javale[2]

[1] *Department of Computer Engineering, MIT COE Kothrud Pune, Maharashtra, India*
[2] *Department of Computer Engineering, MIT COE Kothrud Pune, Maharashtra, India*

Abstract - CAPTCHA is a graphical password scheme used for a user access authentication. It is mainly used for a security purpose to avoid the spyware attacks from website also to prevent bots from overrunning sites with spam, fraudulent registrations, fake sweepstakes entries, and other nefarious things. CAPTCHA is based on the image as a graphical password from the weak zone from the user. In this paper various techniques for CAPTCHA has been studies here we analysis the each and every scheme of CAPTCHA password like graphical password scheme and focus the security attitude and analysis the attack methods.

Key Words: *CAPTCHA, spyware attacks, spam, authentication, fake sweepstakes entries*

1. INTRODUCTION

CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". Since the dawn of the Internet, people have tried to abuse websites for both sport and profit. As the abuse became profitable, the scale of abuse grew using automated software (sometimes referred to as bots). To prevent bots from overrunning sites with spam, fraudulent registrations, fake sweepstakes entries, and other nefarious things, publishers responded by testing users to see if they were human or not.

Password is always more security and usability. The security password is access for authentication which has been used to access the password used through graphical aspects or CAPTCHA process. A key area in security research and practice is authentication, the determination of whether a user should be allowed to access to a given system or resource. Generally, the most common and convenient authentication method is the traditional alphanumeric password. However, their inherent security and usability problems led to the development of graphical passwords as an alternative.

2. LITERATURE SURVEY

2.1 Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems

Author proposed a framework called CaRP which is both a Captcha and a graphical password scheme. Here author introduced a new approach to encounter online guessing attacks which includes online guessing attacks also resistant to Captcha relay attacks.

Authors also done usability study of two CaRP schemes in which they had implemented system by taking more participants considered AnimalGrid and ClickText which is easier to use as compare to that of PassPoints and a combination of text password and Captcha. Author also stated that, if the proposed framework is combined with dual-view technologies it can be resilient to shoulder-surfing attacks and also help reduce spam emails sent from a Web email service.

2.1.1 Methodology used:

CaRP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image. It uses both Captcha and a graphical password scheme.

2.2 A new CAPTCHA interface design for mobile devices

This paper author has made two main contributions. The first is the proposal of an erosion-based CAPTCHA-breaking algorithm that successfully attacks the Drawing CAPTCHA for mobile devices and the second is a new CAPTCHA system for mobile devices called CAPTCHA Zoo, which is based on the parameterized 2D projection of 3D models of natural animals onto a natural background.

The second contribution represents a challenge for automated bot agents that author felt are presently insurmountable by CAPTCHA-breaking techniques. Author

mentioned that contributions improve the security of online systems that are accessed by mobile devices without having a negative impact upon the usability or accessibility of such systems.

2.2.1 Methodology used:

An image-processing technique is proposed in this system that breaks the Drawing CAPTCHA. A new CAPTCHA approach is then introduced here which is intended specially for mobile devices. Ex-perimental results suggest that this new CAPTCHA design is user-friendly as well as secure.

2.3 CAPTCHA: Using hard AI problems for security

In this paper author introduced a new technique for captcha, which automated test that humans can pass, but current computer programs can't pass them. Here author provided several novel constructions of captchas, author first studies many applications in practical security and with reference to that provided approach that introduces a new class of hard problems that can be exploited for security purposes.

Author believed that cryptography and artificial intelligence have much to contribute to one another so used both for the progress of algorithmic development.

2.3.1 Methodology used:

Author mainly focused on AI and introduced two families of AI problems that can be used to construct captchas and shown that solutions to such problems can be used for stenographic communication.

2.4 Purely Automated Attacks on PassPoints-Style Graphical Passwords

This paper introduced various methods for purely automated attacks against PassPoints-style graphical pass-words. For generating these attacks, author introduced a graph-based algorithm to create dictionaries based on heuristics such as click-order patterns.

Author also combine some methods with previous work, for example click-order heuristics with focus-of-attention scan-paths generated from a computational model of visual attention which yields significantly better automated attacks than previous work.

Author finally stated that generated attacks could be used to help inform more secure design choices in implementing PassPoints-style graphical passwords.

2.4.1 Methodology used:

Author basically combined some methods for example click-order heuristics with focus-of-attention scan-paths and used graph-based algorithm to create dictionaries based on heuristics such as click-order patterns.

3. CONCLUSIONS

The image based CAPTCHAs are effective way to counters bots and reduce spam. CAPTCHA help advance Artificial Intelligence Knowledge. The new form of CAPTCHA likely to be more robust against attacks by the spammers and machines. CaRP is also opposed to Captcha relay attacks and if combined with dual-view technologies shoulder-surfing attacks.

REFERENCES

[1] Zhu, B.B. Microsoft Res. Asia, Beijing, China Yan, J.; Guanbo Bao ; Maowei Yang ; Ning Xu, Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems, ieee transactions on information forensics and security, vol. 9, no. 6, june 2014.

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

[3] 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.

[4] Purely Automated Attacks on PassPoints-Style Graphical Passwords Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 3, SEPTEMBER 2010.

[5] 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.

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