Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

AN INTEGRATED ATTACK CONTROL MECHANISM FOR INTERNET/INTRANET SERVICES

Mr. K.GANESHAMOORTHI[1], Mrs. J.S. SUBHASHINI[2]
[1]M.Phil, Research Scholar, [2]MCA., M.Phil., Assistant Professor
Department of Computer Science,
SSM College of Arts & Science, Komarapaliyam, Tamilnadu, India

Abstract- Mail, messaging, data sharing and computational services are shared under the Intranet and Internet environment. User access on the services is allowed with reference to the user account information. User ID and passwords are applied in the user verification process. Graphical passwords are used to verify the users. Captcha techniques are employed to identify the request is received from the machine or human. Captcha as Graphical Passwords (CaRP) technique integrates the Captcha and Graphical passwords methods.

Recognition based method and recognition and recall based methods are adapted in the CaRP scheme. Text and image captchas are used in the CaRP scheme. Click points are selected by the user and verified by the authentication server environment. Guessing attacks, rely attacks and transmission attacks are raised against the CaRP scheme. An integrated attack controlling scheme is adapted to handle the attacks under the Internet and Intranet services.

Pixel location and color based pattern analysis methods are employed to control guessing attacks. Cryptography and data integrity verification methods are used to handle directory attacks and transmission attacks. Shoulder surfing attacks are also handled with image dimming and dynamic mouse cursor movements. Hash codes are used to maintain the password information. Password strength estimation mechanism improves the password construction process. The system protects the user authentication process with security ad attack control mechanism.

I. INTRODUCTION

Beginning around 1999, a multitude of graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. Where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches. Despite the large number of options for authentication, text passwords remain the most common choice for many reasons. They are easy and inexpensive to implement; are familiar to essentially all users; allow users to authenticate themselves while avoiding privacy issues that have been raised about biometrics; and have the advantage of portability without, for example, having to carry physical tokens. Text passwords also suffer from both security and usability disadvantages -- for example, passwords are typically difficult to remember and are predictable if user-choice is allowed.

One proposal to reduce problems related to text passwords is to use password managers [9]. These typically require that users remember only a master password. They store and send on behalf of

the user the appropriate passwords to web sites hosting user accounts. Ideally the latter are generated by the manager itself and are stronger than user-chosen passwords. Implementations of password managers introduce their own usability issues that can exacerbate security problems and their centralized architecture introduces a single point of failure and attractive target: attacker access to the master password provides control over all of the user's managed accounts. When text password users resort to unsafe coping strategies, such as reusing passwords across accounts to help with memorability, the decrease in security cannot be addressed by simply strengthening, in isolation, the underlying technical security of a system. Usability issues often significantly impact its real-world security. User interface design decisions may unintentionally sway user behavior towards less secure behavior. Successful authentication solutions must thus also include improved usability design based on appropriate research taking into account the abilities and limitations of the target users. In graphical passwords, human memory for visual information is leveraged in hope of a reduced memory burden that will facilitate the selection and use of more secure or less predictable passwords, dissuading users from unsafe coping practices.

The motivation is multi-fold. Knowledge-based authentication has increasing impact on society as its use expands from login to a single computer, to large numbers of remote computers hosting personal and corporate information, to authorizing online financial transactions via mobile devices. Some schemes such as PassFaces and grIDsure have commercial interests [7]. Because of the difficulty of typing on mobile devices, authentication schemes using alternatives to keyboard entry are receiving increased attention. This magnifies the importance of understanding usability and security implications of such schemes. PIN-level graphical schemes are used for unlocking Android smart phones. Besides providing specific authentication alternatives, graphical passwords allows for better understanding of knowledge-based authentication in general by looking at issues such as user choice in password selection, memory interference and the role of cueing in password memorability.

II. RELATED WORK

Most current graphical password schemes [5] require users to enter the password directly, typically by clicking or drawing. Hence, passwords are easily exposed to a third party who has the opportunity to record a successful authentication session. There have been a few graphical password schemes devoted to secure passwords against spyware attacks. In the following, several representatives will be described. Man, et al [10] proposed that users remember a number of text strings as well as several images as pass-objects. To pass the authentication, users should enter the unique codes corresponding to the displayed pass-object variants and a code indicating the relative location of the pass-objects in reference to a pair of eyes. It is relatively hard to crack this kind of password, but the complex memory requirement is an obstacle to its popularity.

In [6], users need to recognize pass-objects and click inside the convex hull formed by all of the pass-objects. If properly designed, this method can provide good security. From time to time the convex hull is either too small to click or too large, creating a guessing problem. Moreover, to provide a large password space may result in a crowed screen and indistinguishable objects. The method in [2] to resist shoulder-surfing is a trivial trick, where a user must click a group composed of both the pass-object and decoy-object rather than click the pass-objects directly. The prototype presented in [4] does not provide sufficient security, having only two objects in each group. In 2006, Weinshall proposed another challenge-response protocol that relied on a shared secret set of pictures [8]. To reduce the amount of information given out with each authentication session, the image set memberships are used to select a certain path on an image mosaic, with the user providing only a code that depends on the path's endpoint. This scheme was claimed to be so strong that an observer who fully records any feasible series of successful interactions could not compute the user's password. It was demonstrated by Golle and

Wagner [9] that the attacker can learn a user's secret key with a SAT solver after observing as few as six successful user logins. In essence, the above methods adopt a challenge-response protocol to confuse the spyware. They can prevent the passwords being cracked by the spyware and falling into the hand of an adversary, along with resisting replay attacks [1]. Taking the previous mechanisms for reference, our scheme also uses a challenge-response protocol to enhance security. But, unlike these methods, our scheme innovatively applies CAPTCHA to graphical passwords to create a highly secure authentication method.

III. SECURITY FOR INTERNET/INTRANET SERVICES

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. Using hard AI (Artificial Intelligence) problems for security, initially proposed is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots.

This new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open problem. The system uses a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which is called CaRP (Captcha as gRaphical Passwords). 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. 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 [3]. 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. It causes denial-of-service attacks and incurs expensive helpdesk costs for account reactivation. 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.

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 following drawbacks are identified from the existing system. Click point

relationship are not analyzed. Directory attacks are not handled. Device dependant shoulder surfing attack handling mechanism is employed in the CaRP scheme. Hash code security is not considered.

IV.AN INTEGRATED ATTACK CONTROL MECHANISM FOR USER VERIFICATION PROCESS

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 integrates the security and attack control mechanism for user authentication process.

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. 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.

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. Color and spatial patterns are analyzed in the system [7]. 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.

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. 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.

V. TECHNIQUES FOR DATA CONFIDENTIALITY AND INTEGRITY

5.1. 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≠q
Calculate n = p x 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	$M = C^d \pmod n$

5.2. 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.

VI. PERFORMANCE ANALYSIS

The user authentication system is designed with the graphical passwords and Captcha schemes. The Captcha as Graphical Passwords (CARP) scheme is constructed with the integration of the Captcha scheme and Graphical password techniques. The Captcha is applied to verify the request is initiated by the user or not. The graphical passwords are used to verify the correct user registered in the server. Recognition based scheme and Recognition and recall based schemes are used in the CARP scheme. Captcha text and images are used in the verification process. The password details are transferred as hash codes. The CARP scheme did not perform the strength analysis.

The Enhanced CARP scheme is constructed with the CARP scheme with strength and attack analysis mechanism. The pattern analysis mechanism is used to check the password strength levels. Three types of password strength analysis mechanism are used in the system. They are distribution analysis, color pattern analysis and spatial pattern analysis. The system also handles the directory attacks and transmission attacks. The RSA algorithm is used to secure the password transmission process. The digital signature scheme is used to verify the transmission errors. The Secure Hash Algorithm (SHA) is used in the system. The system also handles the shoulder surfing attacks. Image dimming, mouse cursor thinning and dynamic mouse curse movement techniques are used to control the shoulder surfing attacks.

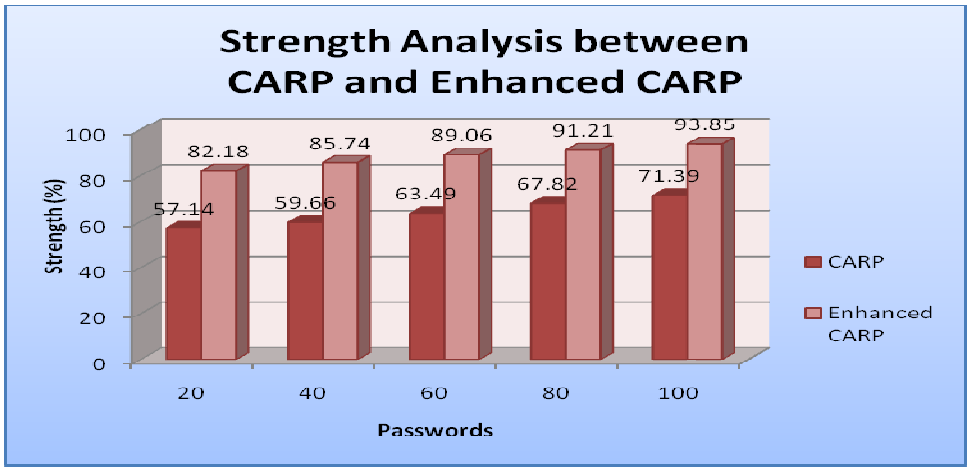

Figure No.6.1: Strength Analysis between PCP and EPCP

The CARP scheme and Enhanced CARP scheme are analyzed with different verification instances. The system analysis is carried out with strength analysis parameters. The strength analysis verifies the password strength level is each technique. The strength analysis between the CARP and Enhanced CARP schemes are shown in figure 6.1. The analysis results show that the Enhanced CARP scheme improves the password strength level 25% than the CARP scheme. The Enhanced CARP scheme produces better results than the CRP scheme in both strength and recall ratio factors.

VII. CONCLUSION AND FUTURE WORK

The Internet and Intranet services are secured with attack controlled user verification mechanism. Graphical password techniques are adapted to verify the user accounts. The system performs the user authentication with CAPTCHA and graphical passwords. Transmission attacks, directory attacks and guessing attacks are handled in the system. Shoulder surfing attacks are efficiently handled by the system. The system supports data integrity verification in the password verification process. The user verification system can be enhanced with the following features. The system can be integrated with Intrusion Detection Systems (IDS) to handle service request based attacks. The system can be adapted for the touch screen based devices with biometric authentication scheme.

REFERENCES

[1] Liming Wang, Xiuling Chang, Zhongjie Ren and Uwa Aickelin, “Against Spyware Using CAPTCHA in Graphical Password Scheme”, 2009.
[2] Z. Li, Q. Sun, Lian and D. Giusto. An association-based graphical password design resistant to shoulder-surfing attack. IEEE International Conference on Multimedia and Expo, 2005.
[3] Emin ˙Islam Tatlı, “Cracking More Password Hashes With Patterns”, IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, August 2015
[4] S. Wiedenbeck, J. Waters, A. Brodskiy and N. Memon. Authentication using graphical passwords: Basic results. In HumanCompute Interaction International. Las Vegas, NV, 2005.
[5] L. D. Paulson. Taking a Graphical Approach to the Password. Computer, 2002(35), pp. 19.
[6] S. Wiedenbeck. Design and Evaluation Of A Shoulder-Surfing Resistant Graphical Password Scheme. In Proceedings of the Working Conference on Advanced Visual Interface, New York, NY : ACM Press, 2006. pp. 177-184.
[7] Shiva Houshmand, Sudhir Aggarwal and Randy Flood, “Next Gen PCFG Password Cracking”, IEEE Transactions On Information Forensics And Security, August 2015
[8] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware. In Symposium on Security and Privacy, 2006.
[9] P. Golle and D.Wagner. Cryptanalysis of a Cognitive Authentication Scheme. In Symposium on Security and Privacy, 2007.
[10] D. Hong, S. Man, B. Hawes and M. Mathews. A Graphical Password Scheme Strongly Resistant To Spyware. In Proceedings of International conference on security and management. Las Vergas, NV, 2004.