Abstract graphical passwords, encouraging users to select

ABSTRACT Manysecurity primitives are based on hard mathematical problems. Using hard AI (ArtificialIntelligence) problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present a new security primitivebased on hard AI problems, namely, a novel family of graphical password systemsbuilt on top of Captcha technology, which we call Captcha as graphicalpasswords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRPaddresses a number of security problems altogether, such as online guessingattacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found onlyprobabilistically by automatic online guessing attacks even if the password isin the search set. CaRP also offers a novel approach to address the well-knownimage hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices.

CaRP is not a panacea, but itoffers reasonable security and usability and appears to fit well with somepractical applications for improving online security. INTRODUCTIONThe main aim of this project is an integrated evaluation of the Captcha as Graphical Passwords scheme(CaRP) is both a Captcha and agraphical password scheme., including usability and securityevaluations, and implementation considerations. An important usability goal forknowledge-based authentication systems is to support users in selecting passwordsof higher security, in the sense of being from an expanded effective securityspace. We use persuasion to influence user choice in click-based graphicalpasswords, encouraging users to select more random, and hence more difficult toguess, click-points. Using hard AI

(Artificial Intelligence) problems for security, Under this paradigm, the most notable primitive invented is Captcha, whichdistinguishes human users from computers by presenting a challenge, i. e.

, apuzzle, beyond the capability of computers but easy for humans. Captcha is nowa standard Internet security technique to protect online email and otherservices from being abused by bots. we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captchatechnology, which we call CaRP (Captcha as graphical Passwords). CaRP isclick-based graphical passwords, where a sequence of clicks on an image is usedto derive a password.

Unlike other click-based graphical passwords, images usedin CaRP are Captcha challenges, and a new CaRP image is generated for everylogin attempt. The notion of CaRP is simple but generic. CaRP can have multipleinstantiations. In theory, any Captcha scheme relying on multiple-objectclassification can be converted to a CaRP scheme. We present exemplary CaRPsbuilt on both text Captcha and image-recognition Captcha. One of them is a textCaRP wherein a password is a sequence of characters like a text password, butentered by clicking the right character sequence on CaRP images. 1. 1 GraphicalPasswordsA large number of graphical password schemes have been proposed.

They can be classified into three categories according to the task involved inmemorizing and entering passwords. ü Recognitionü Recallü Cued-recall 1. 1. 1 RecognitionBased SchemeA recognition-based schemerequires identifying among decoys the visual objects belonging to a passwordportfolio.

A typical scheme is Passfaces whereina user selects a portfolio of faces from a database in creating a password. During authentication, a panel ofcandidate faces is presented for the user to select the face belonging to herportfolio. This process is repeated several rounds, each round with a different panel. A successful login requirescorrect selection in each round.

The set of images in a panel remains the samebetween logins, but their locations are permuted. Cognitive Authentication requiresa user to generate a path through a panel of images as follows: starting fromthe top-left image, moving down if the image is in portfolio, or rightotherwise. The user identifies amongdecoys the row or column label that the path ends. This process is repeated, each time with a different panel. A successful login requires that thecumulative probability that correct answers were not entered by chance exceedsa threshold within a given number of rounds. 1. 1.

2 RecallBased SchemeA recall-based schemerequires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) was the firstrecall-based scheme proposed. A user draws password on a 2D grid. The systemencodes the sequence of grid cells along the drawing path as a user drawn password. Pass-Go improves DAS’s usability by encoding the grid intersection pointsrather than the grid cells. BDAS addsbackground images to DAS to encourage users to create more complex passwords. Typical application scenarios for CaRPinclude: 1)CaRP can be applied on touch-

screen devices whereon typing passwords iscumbersome, esp. for secure Internet applications such as e-banks.

Manye-banking systems have applied Captchas in user logins. 2)CaRP increases spammer’s operating cost and thus helps reduce spam emails. Foran email service provider that deploys CaRP, a spam bot cannot log into an emailaccount even if it knows the password. Instead, human involvement is compulsoryto access an account. If CaRP is combined with a policy to throttle the number ofemails sent to new recipients per login session, a spam bot can send only alimited number of emails before asking human assistance for login, leading toreduced outbound spam traffic.

1. 1. 3 Cued-RecallBased SchemeIn a cued-recall scheme, an external cue is provided to help memorize and entera password. PassPoints is a widely studied click-based cued-recallscheme wherein a user clicks a sequence of points anywhere on an image increating a password, and re-clicks the same sequence during authentication.

Cued Click Points (CCP) is similar to PassPoints but uses one image per click, with thenext image selected by a deterministic function. Persuasive Cued Click Points (PCCP) extends CCP by requiring a user toselect a point inside a randomly positionedviewport when creating a password, resulting in more randomly distributedclick-points in a password. 1. 2 CaptchaCaptcha relies on the gap of capabilities between humans and bots in solving certain hard AIproblems.

There are two typesof visual Captcha: ü Text Captchaü Image-Recognition Captcha (IRC). 1. 2. 1 Text CaptchaThe former relies on character recognition while the latter relies on recognitionof non-character objects. Security of text Captchas has been extensively studied.

The following principle has been established: Text Captcha should rely on the difficultyof character segmentation, whichis computationally expensive and combinatorialhard. 1. 2.

2 Image-RecognitionCaptchaMachine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty ofobject identification or classification, possibly combined with the difficulty of object segmentation. Asirra relieson binary object classification: a useris asked to identify all the catsfrom a panel of 12 images of cats and dogs. Security of IRCs has also been studied. Asirra wasfound to be susceptible to machine-learning attacks. IRCsbased on binary object classificationor identification of one concrete type of objectsare likely insecure. Multi-label classification problems are considered much harder than binary classification problems. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed tohuman solvers, whose answersare fed back to the targeted application.

1. 3 Captcha inAuthenticationIt was introduced intouse both Captcha and password in auser authentication protocol, which we call Captcha-based Password Authentication (CbPA)protocol, to counter onlinedictionary attacks. TheCbPA-protocol in requires solvinga Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookieis received. For an invalidpair of user ID and password, the user has a certain probability to solve a Captchachallenge before being denied access. An improved CbPA-

protocol is proposed in by storing cookies only on user-trustedmachines and applying aCaptcha challenge only when the number of failed login attempts for the account has exceededa threshold.

It is further improvedin by applying a small threshold for failedlogin attempts from unknown machines but a large threshold for failed attempts from knownmachines with a previous successfullogin within a given time frame. Captcha was also used with recognition-based graphical passwords to address spywarewherein a text Captcha is displayed below each image; a user locates her own pass-imagesfrom decoy images, and enters the characters atspecific locations of the Captcha below each pass-image as her password during authentication. These specific locations wereselected for each pass-image during password creation as a part of the password. Literature Survey   Title – Security in Graphical Authentication Authors – Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee Abstract Graphical Authentication Systems are a potential replacement orsupplement for conventional authentication systems. Several studies havesuggested graphical authentication may offer greater resistance to guessing andcapture attacks but there are other attacks against graphical authenticationincluding social engineering, brute force attacks, shoulder surfing, intercepted communication and spyware. In this paper we give a briefdescription and classification of different graphical password schemes followedby information about vulnerabilities in the various schemes and recommendationsfor future development. Keywords: graphical userauthentication, graphical password Introduction Authenticationis the primary gatekeeper for computer systems.

It both verifies authorizedusers of a system and distinguishes between different users. Halting anddetecting intruders is only possible with a strong authentication mechanism andefficient access control. However, users dislike inconvenient authorizationmethods and may compromise them to make their lives easier. Thetraditional and most common authentication method employs usernames andpasswords composed of alphanumeric text.

This method has proven to be insecurein practice. For example, users may choose easily guessed passwords or, if apassword is hard to guess, users may find it too difficult to remember leadingto increased support issues, users writing down their passwords where they canbe easily found or users using the same password for multiple sites. Thereforewe need substitutes or supplements for traditional authentication methods tohave more secure and reliable authentication. Recently several new methods forauthentication such as token-based authentication, biometric-based andgraphical authentication have been developed. All of these can be used togetherwith conventional usernames and passwords. The most commonly used approaches toauthentication are knowledge-based techniques which include text andpicture-based passwords.

Since it is easier for humans to remember picturesthan text, graphical authentication schemes have been proposed as an alternativeto text-based schemes. With graphical authentication there is no need toremember long sequences of characters. Instead, a user can pass the authenticationstep by recognizing or recreating the graphical password. When the number ofpictures is large enough graphical authentications may be superior totext-based methods.

Title – A Graphical Password Based System forSmall Mobile Devices Authors-Wazir Zada Khan, Mohammed Y Aalsalem and Yang

Xiang AbstractPasswordsprovide security mechanism for authentication and protection services against unwantedaccess to resources. A graphical based password is one promising alternativesof textual passwords. According to human psychology, humans are able toremember pictures easily. In this paper, we have proposed a new hybridgraphical password based system, which is a combination of recognition andrecall based techniques that offers many advantages over the existing systemsand may be more convenient for the user.

Our scheme is resistant to shouldersurfing attack and many other attacks on graphical passwords. This scheme isproposed for smart mobile devices (like smart phones i. e. ipod, iphone, PDAs etc)which are more handy and convenient to use than traditional desktop computersystems. Keywords: Smart Phones, Graphical Passwords, Authentication, NetworkSecurity. Introduction Computersecurity systems must also consider the human factors such as ease of a use andaccessibility.

Current secure systems suffer because they mostly ignore theimportance of human factors in security. All current security systems haveflaws which make them specific for well trained and skilled users only. Weakpasswords are vulnerable to dictionary attacks and brute force attacks where asStrong passwords are harder to remember. To overcome the problems associatedwith password based authentication systems, the researchers have proposed theconcept of graphical passwords and developed the alternative authenticationmechanisms.

Graphical passwords systems are the most promising alternative toconventional password based authentication systems. Graphical passwords (GP) use pictures insteadof textual passwords and are partially motivated by the fact that humans canremember pictures more easily than a string of characters. An importantadvantage of GP is that they are easier to remember than textual passwords. Human beings have the ability to remember faces of people, places they visitand things they have seen for a longer duration. Thus, graphical passwordsprovide a means for making more user-friendly passwords while increasing thelevel of security. Another common problem with graphical passwords is that ittakes longer to input graphical passwords than textual passwords.

The loginprocess is slow and it may frustrate the impatient users. Graphical passwordsserve the same purpose as textual passwords differing in consisting ofhandwritten designs (drawing), possibly in addition to text. The exploitationof smart phones like ipod and PDA’s is increased due to their small size, compact deployment and low cost. Title – TheEffect of Baroque Music on the PassPoints Graphical PasswordAuthors – Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin AbstractGraphical passwords have beendemonstrated to be the possible alternatives to traditional alphanumericpasswords. However, they still tend to follow predictable patterns that areeasier to attack. The crux of the problem is users’ memory limitations.

Usersare the weakest link in password authentication mechanism. It shows thatbaroque music has positive effects on human memorizing and learning. Weintroduce baroque music to the Pass Points graphical password scheme andconduct a laboratory study in this paper. Results shown that there is nostatistic difference between the music group and the control group withoutmusic in short-term recall experiments, both had high recall success rates.

Butin long-term recall, the music group performed significantly better. We alsofound that the music group tended to set significantly more complicatedpasswords, which are usually more resistant to dictionary and other guessattacks. But compared with the control group, the music group took more time tolog in both in short-term and long-term tests. Besides, it appears thatbackground music does not work in terms of hotspots. IntroductionThere have been three dominanttechniques available of graphical passwords which can be defined as: Drawmetrics, Locimetrics and Econometrics. PassPoints is a representative Locimetric scheme of particular interest andworthy of extensive study. In PassPoints, passwords consist of a sequence ofseveral click-points on a given image, and hotspot is a primary security problem.

Literatures reveal thatusers are the ‘ weakest link’ in password authentication, probably due to theirmemory limitations. Psychological and studies indicate that baroque music haspositive effects of great importance on human memorizing and learning. In this paper, we investigate the novel idea of introducing background baroque music to thePassPoints graphical password scheme with the purpose of alleviating users’memory burden and improving usable security. An aboratory study was conducted toexplore the efficiency of background baroque music on memorizing graphicalpasswords. We are also interested in whether the background music has othereffects on graphical password, like the login time and the password complexity. The results of our empirical study are very encouraging in PassPoints scheme. The music group coped significantly better than the group without music whenrecalling passwords after one week. The music group also tended to set significantlymore complicated passwords.

This appeared to suggest that the applied musiccould improve memorability of PassPoints password. Besides, the backgroundmusic had no significant influence on login times. Title – A Proposal to Improve the Usability of Graphical PasswordsAuthors – Hai Tao and Carlisle Adams AbstractInspired by an old Chinese game, Go, we have designed a new graphical password scheme, Pass-Go, in which a user selects intersections on a grid as a wayto in-put a password. While offering an extremely large full password space(256 bits for the most basic scheme), our scheme provides acceptable usability, as empirically. Our scheme supports mostapplication environments and input devices, rather than being limited to smallmobile devices and can be used to derive cryptographic keys. We study thememorable password space and show the potential power of this scheme byexploring further improvements and variation mechanisms.

Keywords: Dictionary attack, graphical password,

Pass- IntroductionConventional textual passwords use astring of alphanumeric characters (or printable ASCII characters) to identify auser. However, it is well known that textual passwords are vulnerable to smalldictionary attack in which an attacker exhaustively searches candidate passwordsfrom a “ small dictionary”. This “ small dictionary” attack is so successful thatin Klein’s case study, about 25% of14, 000 passwords were cracked by a dictionary with only 3 million entries (thesize of the dictionary is 21. 5 bits). Therefore, it is widely believed that thesecurity of a password scheme is related more closely to the size of itsmemorable password space, rather than that of its full password space. Graphical passwords, which require auser to remember and repeat visual information, have been proposed to offerbetter resistance to dictionary attack.

Psychological studies support thehypothesis that humans have a significant capability to recognize and to recallvisual images. If users are able to remember more complex graphical passwords, anattacker has to build a bigger dictionary, thus spend more time or deploy morecomputational power to achieve the same success as for textual passwords. In 1999, Jermyn et al suggested agraphical password scheme called DAS(draw-a-secret), which requires a user to draw a secret design on a grid asa way to input a password. Surprisingly, they found that DAS could offer verylarge password space for reasonable parameters. On a 5 × 5 grid, the totalnumber of passwords of length 12 or less is larger than that of textualpasswords composed of 8 printable ASCII characters (958 = 6. 6 × 1015).

Theystudied the memorable password space of DAS and introduced the concept of asymmetric graphical dictionary, based on psychological theories that peopleprefer images that exhibit (especially mirror) symmetric patterns. Theyclassified symmetric passwords into several subclasses according to the axesconsidered. Title – A Free Drawing Graphical Password SchemeAuthors – Alice J. Lin and Fuhua(Frank) Cheng AbstractThis paper presents a method forfreely drawing a graphical password. The new method achieves better securitythan conventional textual passwords and other graphical password schemes. Withthis method it is also easier for a user to remember the password. The basicidea of the new method is to use a number of the user's representative sampledrawings to predict the user's future drawing prediction interval. Thepredicted values are obtained by conducting the least squares method to thepolynomial regression model.

Based on the predicted values and deviation of theuser's sample drawings, a prediction interval for the signature/picture isgenerated. This prediction interval is used as the password and, subsequently, if the signature/picture drawn by a user lies within the prediction interval, the user is authenticated into the application. Keywords: graphical password, security, free drawing, signature, prediction. IntroductionAuthenticating users in network-basedand Internet-based environments has been a challenge for network administratorsand end users. The most popular computer authentication method is for a user tosubmit a user name and a textual password. The vulnerabilities of this methodare well known.

One of the main problems is the difficulty of rememberingpasswords. Unfortunately, these passwords can also be easily figured out orbroken. Despite their vulnerabilities, textual passwords are still the mostcommonly used authentication mechanism. Alternative authentication solutions, such as token-based or biometric authentication, do not rely on the users' memoryand introduce an increased level of security at the expense of increasedhardware and software costs and usability, and are therefore not used asfrequent means of user authentication. Graphical password schemes have beenproposed as a possible alternative to text-based schemes, motivated partiallyby the fact that humans can remember pictures better than texts; psychological studiessupport such assumption, Pictures are generally easier to remember or recognizethan texts. In addition, if the number of possible pictures is large enough, the possible password space of a graphical password scheme may exceed that of text-basedschemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical passwords. In addition to workstation and web log-in applications, graphical passwordshave also been applied to ATM machines and mobile devices.