ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

Remote Desktop Access Using Cued Clicked Points and SMS Authentication

B.B.Gite[1], Hariharan Swaminathan[2], Dipali Kalambe[3], Deepti Pawar[4], Jyoti Sarode[5]

Assistant Professor, Department of Computer Engineering, STES's Sinhgad Academy of Engineering,
University of Pune, Pune, Maharashtra,India[1]

Department of Computer Engineering, STES's Sinhgad Academy of Engineering,
University of Pune, Pune, Maharashtra,India[2]

(Department of Computer Engineering, STES's Sinhgad Academy of Engineering,
University of Pune, Pune, Maharashtra,India[3]

Department of Computer Engineering, STES's Sinhgad Academy of Engineering,
University of Pune, Pune, Maharashtra,India[4]

Department of Computer Engineering, STES's Sinhgad Academy of Engineering,
University of Pune, Pune, Maharashtra,India[5]

Abstract--We propose an elegant method called Cued Click Points (CCP) to solve the authentication problem in a ubiquitous manner. The fundamental idea of CCP is based on premise that "humans are good at identifying remembering and recollecting graphical patterns than text patterns, the core idea of CCP is that, instead of remembering a sequence of characters as a secret user's have to remember a shape (which is internally stored as sequence of positions as the secret)"
Due to wireless networks feature of being open and the deficiency of wireless protocol; more and more means of attack have been offered, therefore it is important to share secret password between sender and recipient securely,a mobile authentication scheme using SMS in which a password kept as secret with our expectations.
Remote desktop is an application that allows user to control the desktop and the entire content of one computer from mobile devices. When it is difficult and impractical to be physically near a system in order to use it, or in order to access it, we can use this application. Desktop screen will be displayed on the android phone and you can pretty much do whatever you want to do.

Keywords--Cued Click Points (CCP), SMS, Remote desktop

I. INTRODUCTION

Phishing, a serious security threat to Internet users is an e-mail fraud in which the perpetrator sends out an email which looks like legitimate, in an order to gather personal and financialinformation of the receiver. It is important to prevent such phishing attacks. One of the ways to prevent the password theft is to avoid using passwords and to authenticate a user without a text password. In this paper, we are proposing an authentication service that is image based and which eliminates the need for text passwords. The image based authentication method relies on the user's ability to recognize pre-chosen categories from a grid of pictures. Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures. There are mainly two types of passwords:

1. Static password.
2. Dynamic password

Static password is the traditional password which is usually changed only when it is necessary: it is changed when the user has to reset the password, i.e., either the user has forgotten the password or the password has expired. Static passwords are highly susceptible to cracking, because passwords used will get cached on the hard drives.To solve this we developed One Time Password Token. Unlike a static password, dynamic password is a password which changes every time the user logs in.

We have developed Image Based Passwords using Cued Click Points. Image based authentication is included to provide additional security integrated with OTP. With IBA, when the user performs first time registration on a website, he makes a choice of five secret categories of images that are easy to remember, such as pictures of natural scenery, automobiles, etc. Every time the user logs in, an image from among his selected images is presented to the user. The user clicks on correct point of the image. Only on clicking the correct point on the first image the user is directed to the next image where he again has clicks on the correct point of the image. This process continues till the fifth image. An OTP will be generated following the submission and will be sent to the users registered mobile through SMS. If OTP get verified then he will be given access to the remote machine to perform the various desired operations.

If an unauthorized person is trying to gain access, he is unaware of the correct points on each image. As a result, during the selection process if he selects a wrong point on the first image, the next image shown to him is totally different from the ones selected by the user during the registration process and this continues up till the very last image, thus forcing the unauthorized person to select from among the wrong set of images.

Moreover, this password authentication is done from a remote machine, thus ensuring the user of complete security although he is accessing from a remote machine which as we know is more susceptible to attacks. In this paper we are also discussing the use of the AES Algorithm which serves in the encryption process.

II. CUED CLICK POINTS

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, usersclick one point on each of c = 5 images rather than on five points on one image. Itoffers cued-recall and introduces visual cues that instantly alert valid users if theyhave made a mistake when entering their latest click-point (at which point theycan cancel their attempt and retry from the beginning). It also makes attacksbased on hotspot analysis more challenging, as we discuss later. As shown inFigure 1, each click results in showing a next-image, in effect leading users downa "path" as they click on their sequence of points. A wrong click leads down anincorrect path, with an explicit indication of authentication failure only after thefinal click. Users can choose their images only to the extent that their click-point4 Cued Click Pointsdictates the next image. If they dislike the resulting images, they could create anew password involving different click-points to get different images. Figure 1 CCP passwords can be regarded as a choice-dependent path of images. We envision that CCP fits into an authentication model where a user hasa client device (which displays the images) to access an online server (whichauthenticates the user). We assume that the images are stored server-side withclient communication through SSL/TLS and encryption is obtained by AES. For implementation, CCP initially functions like PassPoints. During password creation, a discretization method is used to determine aclick-point's tolerance square and corresponding grid. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whetherthe click-point falls within tolerance of the original point. With CCP, we furtherneed to determine which next-image to display.

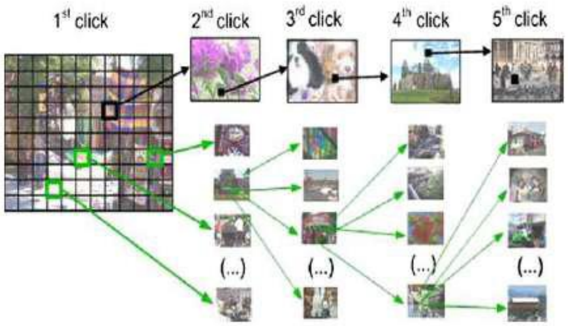


Figure 1: CCP passwords can be regarded as a choice-dependent path of images

Similar to the PassPoints studies, our example system had images of size451x331 pixels and tolerance squares of 19x19 pixels. If we used robust discretization [1], we would have 3 overlapping candidate grids each containingapproximately 400 squares and in the simplest design, 1200 tolerance squaresper image (although only 400 are used in a given grid). We use a functionf(username, currentImage, currentToleranceSquare) that uniquely maps eachtolerance square to a next-image. This suggests a minimum set of 1200 imagesrequired at each stage. One argument against using fewer images, and havingmultiple tolerance squares map to the same next-image, is that this could potentially result in misleading implicit feedback in (albeit rare) situations whereusers click on an incorrect point yet still see the correct next-image.Each of the 1200 next-images would have 1200 tolerance squares and thusrequire 1200 next-images of their own. The number of images would quicklybecome quite large. So we propose re-using the image set across stages. By reusing images, there is a slight chance that users see duplicate images. Duringthe 5 stages in password creation, the image indices i1, ..., i5 for the images inthe password sequence are each in the range 1 _ ij _ 1200. When computingthe next-image index, if any is a repeat (i.e., the next ij is equal to ik for someCued Click

Points 5k < j), then the next-image selection function f is deterministically perturbedto select a distinct image.A user's initial image is selected by the system based on some user characteristic (as an argument to f above; we used username). The sequence isre-generated on-the-fly from the function each time a user enters the password.If a user enters an incorrect click-point, then the sequence of images from thatpoint onwards will be incorrect and thus the login attempt will fail. For an attacker who does not know the correct sequence of images, this cue will not behelpful.We expect that hotspots [6, 16] will appear as in PassPoints, but since thenumber of images is significantly increased, analysis will require more effortwhich increases proportionally with the configurable number of images in thesystem. For example, if attackers identify thirty likely click-points on the firstimage, they then need to analyze the thirty corresponding second images (oncethey determine both the indices of these images and get access to the imagesthemselves), and so on, growing exponentially.A major usability improvement over PassPoints is the fact that legitimateusers get immediate feedback about an error when trying to log in.When they seean incorrect image, they know that the latest click-point was incorrect and canimmediately cancel this attempt and try again from the beginning. The visualcue does not explicitly reveal "right" or "wrong" but is evident using knowledgeonly the legitimate user should possess. As with text passwords, PassPoints canonly safely provide feedback at the end and cannot reveal the cause of error.Providing explicit feedback in PassPoints before the final click-point could allowPassPoints attackers to mount an online attack to prune potential passwordsubspaces, whereas CCP's visual cues should not help attackers in this way.Another usability improvement is that being cued to recall one point on each offive images appears easier than remembering an ordered sequence of five pointson one image.

III. THREATS AND ATTACKS

In cases where attackers are not in aposition to capture information from the user, they are limited to what they candeduce through image analysis.Hotspots are specific areas in the image that have a higher probability ofbeing selected by users as part of their passwords. If attackers can accuratelypredict the hotspots in an image, then a dictionary of passwords containingcombinations of these hotspots can be built. Hotspots are known to be problematic for PassPoints [6, 16]; further analysis is needed to determine whetherprecautions such as carefully selecting images can minimize this threat.Our example system had 400 tolerance squares per grid for a given image.Because the chosen grid is stored during password creation, the correct grid isalways retrieved by the system during login so the fact that there are severalgrids (and 1200 images) does not come into play. This means that for eachimage, there is a 1/400 chance of clicking within the correct tolerance square.However, due to hotspots some of these have a much higher probability of beingcorrect than others. Knowing the hotspots would allow an attacker to modify anattack dictionary to test passwords with higher probability first. For example, re-examining the data from our larger PassPoints-style study [3] we found that, as a general result across 17 images used, the 30 largest hotspots on an image cover approximately 50% of user-chosen click-points. Assuming that attackers are first able to extract the necessary images and perform hotspot analysis, there is approximately a 3% (.55) chance that a password is contained in a dictionary of 225 entries built entirely from hotspots. A key advantage of CCP over PassPoints is that attackers need to analyze hotspots on a large set of images rather than only one image since they do not know the sequence of images used for a given password. Secondly, using different subsets of images for different users means that an attacker must somehow gather information about the specific subset assigned to the current user. Further testing is required to gather a larger sample of click-points per image for CCP, but preliminary analysis provides evidence that users are no more likely to select a popular hotspot as their click-point in CCP than with PassPoints. When presented with the same images, users selected similar points in both our CCP and PassPoints-style [3] user studies.

IV. AES ALGORITHM

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. The main loop of AES performs the following functions:

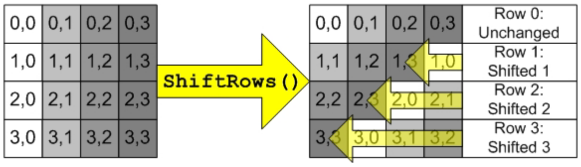
- **SubBytes()**
- **ShiftRows()**
- **MixColumns()**
- **AddRoundKey()**

A simpler way to view the AES function order is:
1. Scramble each byte (SubBytes).
2. Scramble each row (ShiftRows).
3. Scramble each column (MixColumns).
4. Encrypt (AddRoundKey).

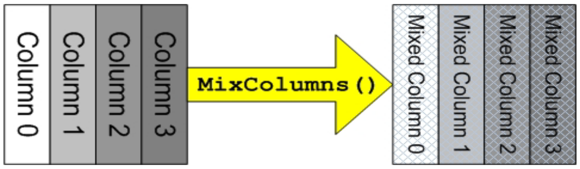
A term associated with AES is "the State," an 'intermediate cipher,'11 or the ciphertext before the final round has been applied. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially `MixColumns()` and `Shiftrows()`.

`SubBytes()` adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

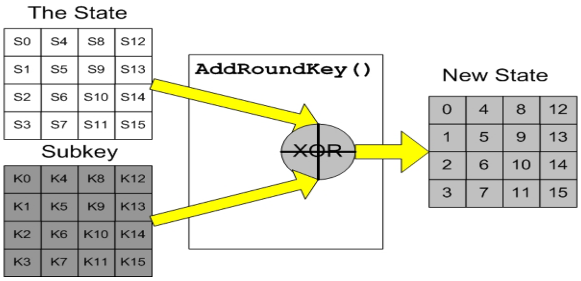
`ShiftRows()` provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes, as shown in the *FIPS* illustration that follows:



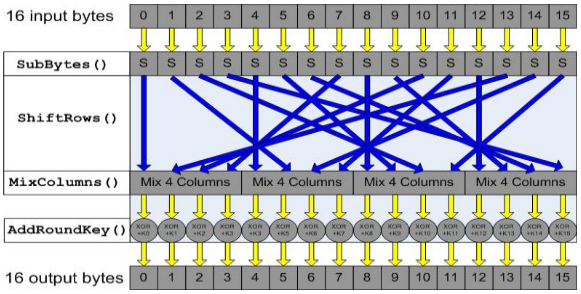
`MixColumns()` also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics, as shown in the *FIPS* illustration that follows:



The actual 'encryption' is performed in the `AddRoundKey()` function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule, as shown in the *FIPS* illustration that follows:



Here is one round of AES encryption, shown in the *FIPS* publication two dimensionally:



ALGORITHM

1. One time initialization

a. Expand the 16-byte key to get the actual Key Block to be used.

b. Do one time initialization of the 16-byte plain text block (called as State).

c. XOR the state with the key block.

2. For each round do the following:

a. Apply S-box to each of the plain text bytes.

b. Rotate row k of the plain text block by k bytes.

c. Perform a mix column operation

d. XOR the state with the key block.

V. CONCLUSION

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over PassPoints in terms of usability. Being cued as each image is shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. In our small comparison group, users strongly preferred CCP. We believe that CCP offers a more secure alternative to PassPoints. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. Furthermore, the system's flexibility to increase the overall number of images in the system allows us to arbitrarily increase this workload. Future work should include a thorough assessment of the viability of CCP as an authentication mechanism, including a long term study of how these passwords work in practice and whether longer CCP passwords would be usable. The security of CCP also deserves closer examination, and should address how attackers might exploit the emergence of hotspots.

VI. REFERENCES

1. Sonia Chiasson, Paul C. van Oorschot, Robert Biddle: Graphical Password Authentication Using Cued Click Points. ESORICS 2007: 359-374
2. Sonia Chiasson, Alain Forget, Robert Biddle, Paul C. van Oorschot: Influencing users towards better passwords: persuasive cued click-points. BCS HCI (1) 2008: 121-130
3. Chippy.T,R.Nagendran,Defence Against Large Online Password Guessing Attacks By Using Persuasive Click Points, IJCE 2012
4. Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd Stanford University,Reducing Shoulder-surfing by Using Gaze-based Password Entry (SOUPS) 2007,Pittsburgh, PA, USA.
5. Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, THE DESIGN AND ANALYSIS OF GRAPH CAL PASSWORDS, 8th USENIX Security Symposium Washington USA, August 1999
6. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of9th USENIX Security Symposium, 2000.
7. XiaoyuanSuo,YingZhu,G. Scott.Owen,Graphical Passwords: A Survey,Computer Security Applications Conference, 21st Annual 2005
8. AnkeshKhandelwal,ShanshankSingh,NirajSatnalikaInformation and Telecommunication Technologies, 2008. APSITT. 7th Asia-Pacific Symposium
9. HimikaParmar,NancyNainan,SumaiyaThaseen, Generation Of Secure One Time Password Based On Image Authentication,airccj.org/CSCP/vol2/csit2417.
10. Shuhaib K P,Sobin C CAn Efficient Method for Graphic Password Authentication,Dept Of I.T. MES College