INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 479-483
RECEIVED : 18/02/2016. PUBLISHED : 3/03/2016
March 3, 2016

AN IMPROVED PRIVACY POLICY INFERENCE OVER THE SOCIALLY SHARED IMAGES IN SOCIAL WEBSITES

Vanitha.A, PG Scholar Department of Computer Science Engineering
Paavai Engineering College, Namakkal,
Magendiran.N, Asso.Prof, Department of Computer Science Engineering
Paavai Engineering College, Namakkal.

Abstract:

In this project, we discuss how to prevent users' passwords from being stolen by adversaries in online environments and automated teller machines. We propose differentiated virtual password mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure users passwords. The tradeoff is that the stronger the scheme, the more complex the scheme may be. Among the schemes, we have a default method, system recommended functions, user-specified functions, user-specified programs, and so on. A function/program is used to implement the virtual password concept with a tradeoff of security for complexity requiring a small amount of human computing. We further propose several functions to serve as system recommended functions and provide a security analysis. For user-specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions/algorithms.

Key words- Adversaries, Virtual password, Secret algorithm.

1. INTRODUCTION

Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images, due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed. The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following, when a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P- social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be displayed to the user. If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can choose to revise the policy. The actual policy will be stored in the policy repository of the system for the policy prediction of future uploads.

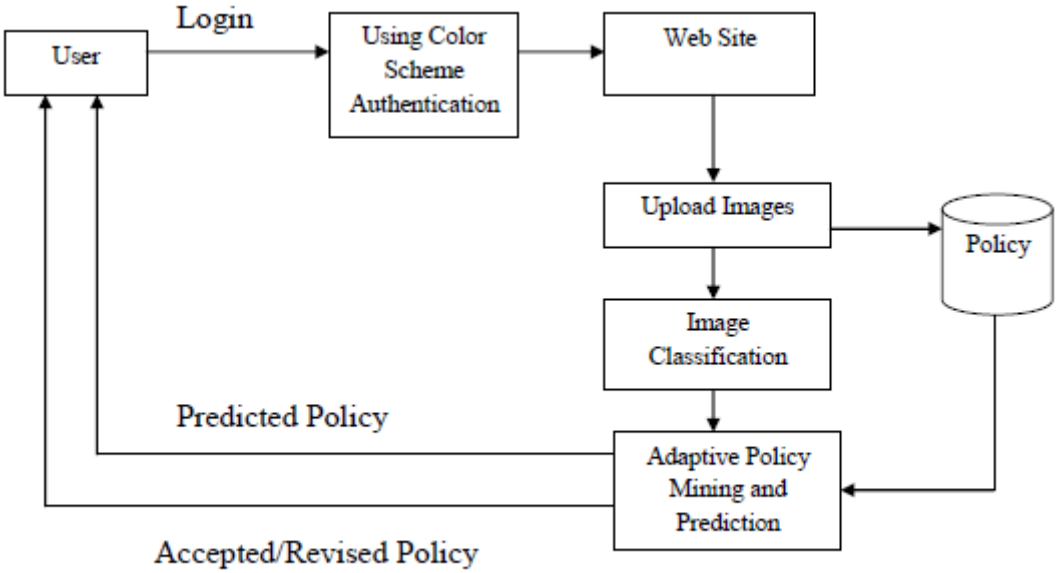
2. EXISTING SYSTEM

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 479-483
RECEIVED : 18/02/2016. PUBLISHED : 3/03/2016
March 3, 2016

Most content sharing websites allow users to enter their privacy references but users struggle to set up and maintain such privacy settings. Existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images. Privacy-Aware Image Classification and Search to automatically detect private images, and to enable privacy-oriented image search. It combines textual meta data images with variety of visual features to provide security policies. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. Consider a photo of a student's 2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students B Apos family members and other friends. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations. Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

3. PROPOSED SYSTEM

An Adaptive Privacy Policy Prediction (A3P) system using color Scheme authentication which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. A policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features.



Fg.1. Block diagram of proposed system

Adaptive Privacy Policy Prediction (A3P) system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person's personal characteristics and images content and metadata. A Color Scheme Authentication system figure 1 in which authentication is done using colors and numbers. Users can give values from 0 to 7 for the given 8 colors. Users can even give same value for two different colors. This makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc.

4. PROBLEM DESCRIPTION

With the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. Privacy-aware image classification using a mixed set of features, both content and meta-data. This is however a binary classification (private versus public), so the classification task is very different than ours. Also, the authors do not deal with the issue of cold-start problem. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction. Adopting a two -stage approach is more suitable for policy recommendation than applying the common one -stage data mining approaches to mine both image features and policies together. Recall that when a user uploads a new image, the user is waiting for a recommended policy. The two-stage approach allows the system to employ the first stage to classify the new image and find the candidate sets of images for the subsequent policy recommendation. As for the one -stage mining approach, it would not be able to locate the right class of the new image because its classification criteria need both image features and policies whereas the policies of the new image are not available yet. Moreover, combining both image features and policies into a single classifier would lead to a system which is very dependent to the specific syntax of the policy. If a change in the supported policies were to be introduced, the whole learning model would need to change.

5. RIJNDAEL'S ALGORITHM

Rijndael (pronounced rain-dahl) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). It was selected from a list of five finalists that were themselves selected from an original list of more than 15 submissions. Rijndael will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years in many cryptography applications. The algorithm was designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name. Rijndael has its origins in Square, an earlier collaboration between the two cryptologists. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. The blocks can be interpreted as unidimensional arrays of 4-byte vectors. The exact transformations occur as follows: the byte sub transformation is nonlinear and operates on each of the State bytes independently - the invertible S-box (substitution table) is made up of 2 transformations. The shift row transformation sees the State shifted over variable offsets. The shift offset values are dependent on the block length of the State. The mix column transformation sees the State columns take on polynomial characteristics over a Galois Field values.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 479-483
RECEIVED : 18/02/2016. PUBLISHED : 3/03/2016
March 3, 2016

6. RESULT ANALYSIS

The login interface having the color grid and number grid of 8x8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session passwords. The first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element. The same method is followed for other pairs of

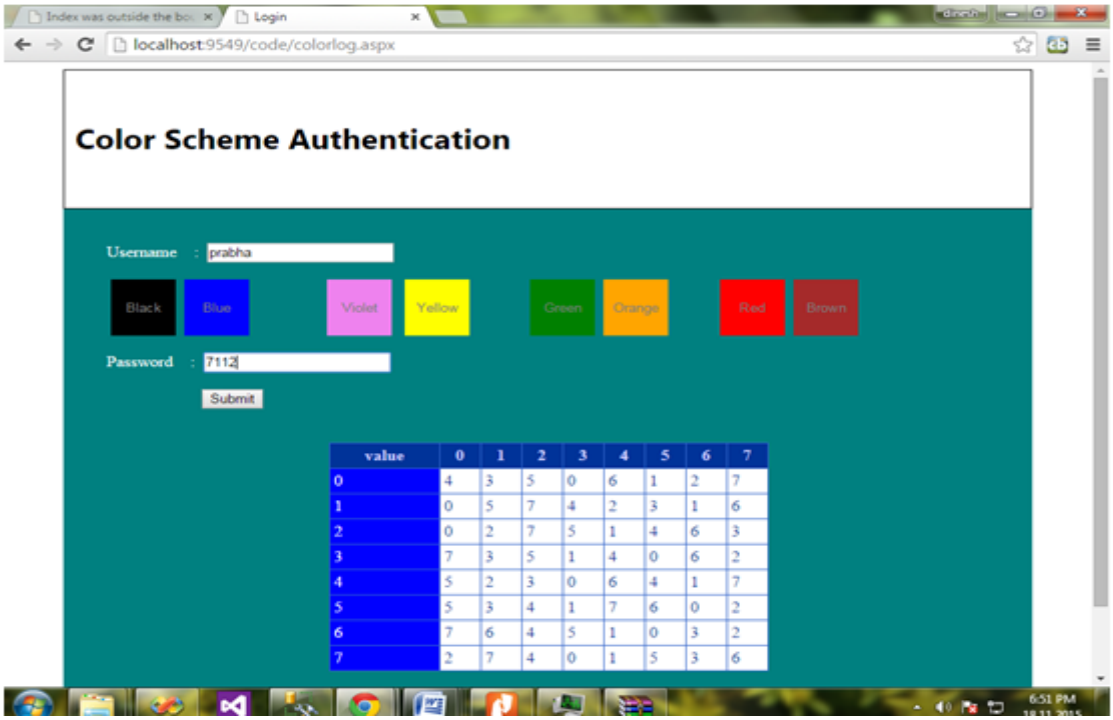


Fig.2.Output result

colors. So the password is "3573". For every login, both the number grid and the color grid get randomizes so the session password changes for every session. The key schedule helps the cipher key determine the round keys through key expansion and round selection. Overall, the structure of Rijndael displays a high degree of modular design, which should make modification to counter any attack developed in the future much simpler than with past algorithm designs.

CONCLUSION

An Adaptive Privacy Policy Prediction system with Color Scheme Authentication that helps users automates the privacy policy settings for their uploaded images. This makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold-start, leveraging social context information. Our

experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

REFERENCES

[1].Dan Lin,Sundareswaran.S,Wede.J, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites" in Proc. IEEE Int.Volume.27, Issue.1Jan. 1 2015.
[2]. H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.
[3]. N. Zheng, Q. Li, S. Liao, and L. Zhang, "Which photo groups should I choose? A comparative study of recommendation algorithms in flickr," J. Inform. Sci., vol. 36, pp. 733–750, Dec. 2010. [4]. J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1464–1467.
[5]. C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, "Personalized photograph ranking and selection system," in Proc. Int. Conf. Multimedia, 2010, pp. 211–220. [Online]. Available: http://doi.acm.org/10.1145/1873951.1873963.
[6]. K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.
[7]. R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
[8]. J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal.Mining., 2009, pp.249–254.