BYOP: BRING YOUR OWN PICTURE FOR SECURING GRAPHICAL PASSWORDS

AUTHOR: U.POZHILAN, K.VINOD KUMAR, SHAM KRISHNAN, P.SRUVITH
Mrs. J.SAKUNTHALA M.E (ASP/IT)

ABSTRACT:

BYOP is a new graphical password scheme for public terminals that replaces the static digital images typically used in graphical password systems with personalized physical tokens, herein in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users present these images to a system camera and then enter their password as a sequence of selections on live video of the token. Highly distinctive optical features are extracted from these selections and used as the password. We present three feasibility studies of BYOP examining its reliability, usability, and security against observation. The reliability study shows that image-feature based passwords are viable and suggests appropriate system thresholds—password items should contain a minimum of seven features, 40% of which must geometrically match originals stored on an authentication server in order to be judged equivalent. The usability study measures task completion times and error rates, revealing these to be 7.5 s and 9%, broadly comparable with prior graphical password systems that use static digital images. Finally, the security study highlights BYOP's resistance to observation attack—three attackers are unable to compromise a password using shoulder surfing, camera based observation, or malware. These results indicate that pass-BYOP shows promise for security while maintaining the usability of current graphical password schemes.

INTRODUCTION:

However, graphical passwords present their own problems. One issue is their susceptibility to intelligent guessing, and shoulder-surfing attacks. Such attacks are effective because the sections of images that users select as password items are both easy for an attacker to observe by snooping over shoulders or setting up a camera to record input and also relatively predictable users tend to choose *hotspots* such as the eyes in a facial portrait. This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers and readily presented to attackers in response to input of easily accessible user identity information.

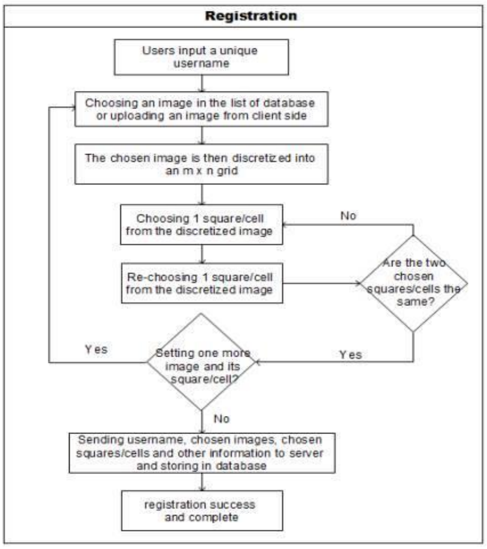
To address this issue, we present a new point-click graphical password system, *BYOP—Bring Your Own Picture,* that increases resistance to observation attack by coupling the user's password to an image or object physically possessed. This is achieved by using live video of a physical token, such as an object, a photograph, or even an image of a body part (e.g., a palm), as the canvas for entering a graphical password. This physical object replaces easily accessible server-based images, and we argue that attackers will struggle to capture useful replicas of this content. We present an implementation for the scheme based on SIFT image features and a demonstration of its viability through three feasibility studies covering: 1) the reliability and robustness of BYOP feature based input; 2) participant task performance times and error rates using BYOP; and 3) the security of BYOP against observation attack.

EXISTING SYSTEM:

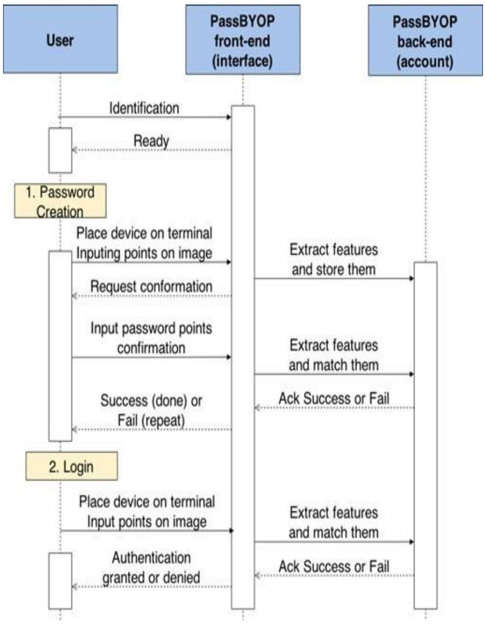
Graphical password systems are knowledge-based authentication techniques that leverage peoples' ability to memorize and recognize visual information more readily than alphanumeric information. Researchers have explored three broad types of graphical passwords: recall-based *draw metric* schemes based on sketching shapes on screen, recognition-based *cogno metric* schemes based on selecting known items from large sets of options, and cued-recall *locimetric* schemes based on selecting regions of prechosen images . locimetric schemes are discussed as is multifactor authentication, as it relates to pass-BYOP and its combination of a token, or something you have, on which a password, or something you know, is entered.

PROPOSED SYSTEM:

BYOP seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks .we argue these weaknesses stem from the ease with which both password contents and password canvases can be observed or, in the case of canvases, directly accessed from a server. BYOP tackles this problem by introducing a physical token into the authentication process. This way, BYOP transforms a graphical password, which is traditionally a single factor authentication mechanism, to a more secure multifactor authentication method. We argue that this makes BYOP *resilient-to-internal-observation*, meaning that an attacker cannot impersonate a user simply by intercepting input on the authentication device or by eavesdropping on the communication between the authentication device and verification system. Assuming users have previously created a password, login involves users identifying themselves at a BYOP terminal in a manner fitting the system and use context. For example, systems such as office door locks may assume all users are valid, while a user id might be used on a public computer, and higher security applications, such as a bank ATM, will likely rely on a physical token such as an ATM card. BYOP could be integrated into any of these scenarios. Second, users place a pre-chosen password image or object they possess on top of a camera unit in the terminal. This is captured and displayed live on an adjacent touch screen. Third, they tap on the image locations that correspond to their password. This way, authentication requires both the physical token and the password simultaneously. We argue this raises the resistance of BYOP to attacks based on password observation and guessing as attackers need to possess a user's genuine token or a high fidelity copy.


Registration
Users input a unique username
Choosing an image in the list of database or uploading an image from client side
The chosen image is then discretized into an m x n grid
Choosing 1 square/cell from the discretized image
Re-choosing 1 square/cell from the discretized image
Are the two chosen squares/cells the same?
No
Yes
Setting one more image and its square/cell?
Yes
No
Sending username, chosen images, chosen squares/cells and other information to server and storing in database
registration success and complete

SYSTEM FLOW:


User
PassBYOP front-end (interface)
PassBYOP back-end (account)
Identification
Ready
1. Password Creation
Place device on terminal Inputing points on image
Extract features and store them
Request conformation
Input password points confirmation
Extract features and match them
Ack Success or Fail
Success (done) or Fail (repeat)
2. Login
Place device on terminal Input points on image
Extract features and match them
Ack Success or Fail
Authentication granted or denied

CONCLUSION:

In summary, this paper proposed improving the security of graphical password systems by integrating live video of a physical token that a user carries with them. It first demonstrates the feasibility of the concept by building and testing a fully functional prototype. It then illustrates that user performance is equivalent to that attained in standard graphical password systems through a usability study assessing task time, error rate, and subjective workload. Finally, a security study shows that BYOP substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes. Ultimately, we argue this paper demonstrates that BYOP conserves the beneficial properties of graphical passwords while increasing their security.

REFRENCES:

[1] a. adams and m. sasse, “users are not the enemy,” *commun. acm*, vol. 42, pp. 40–46, 1999.

[2] m. adham, a. azodi, y. desmedt, and i. karaolis, “how to attack twofactor authentication internet banking,” in *proc. 17th int. conf. financial cryptography*, 2013, pp. 322–328.

[3] artigo, http://www.artigo.org/.

[4] f. aloul, s. zahidi, and w. el-hajj, “two factor authentication using mobile phones,” *proc. comput. syst. appl.*, 2009, pp. 641–644.

[5] r. biddle, s. chiasson, and p. van oorschot, “graphical passwords: learning from the first twelve years,” *acmcomput. surveys*vol. 44, no. 4, p. 19, 2012.

[6] g. e. blonder, “graphical passwords,” u.s. patent 5 559 961, 1996.

[7] j. bonneau, c. herley, p. c. van oorschot, and f. stajano, “the quest to replace passwords: a framework for comparative evaluation of web authentication schemes,” in *proc. ieeesymp. security privacy*, 2012, pp. 553–567.

[8] s.chiasson, r. biddle, and p. van oorschot, “asecond look at the usability of click-based graphical passwords,” in *proc. 3rd symp. usable privacy security*, 2007, pp. 1–12.

[9] s. chiasson, p. c. van oorschot, and r. biddle, “graphical password authentication using cued click points,” in *proc. 12th eur.symp. res. comput. security*, 2007, pp. 359–374.

[10] s. chiasson, a. forget, r. biddle, and p. c. oorschot, “user interface design affects security: patterns in click-based graphical passwords, *int. j. inf. security*, vol. 8, no. 6, pp. 387–398, 2009.