Survey Paper Onlive Object for Securing Graphical Password

Pooja Kale[1], Ankita Pansare[2], Vikky D. Jambhulkar[3]
[1, 2] Dept of Computer
[3]Assistant Professor, Dept of Computer
[1, 2, 3] P K Technical Campus,Chakan, Pune, Maharashtra, INDIA.

Abstract- *To provide security to the cloud system, Bring your own picture for a securing graphical password is a new graphical password scheme for public terminals that replaces the constant digital images typically used in graphical password systems with personalized physical tokens, here in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users represent 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 Live Object for a securing graphical password 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, Usability study measures task completion times and error rates, revealing these to be broadly comparable with graphical password systems that use static digital images. The study of highlights Live Object for a securing graphical password resistance to observation attack 3 attackers are unable to compromise a password using shoulder surfing, camera based observation, or malware*

Keywords- PassByOp, Seft, ORB, Cloud

I. INTRODUCTION

Secure access to information underpins modern digital systems and services. We keep our communications, financial data, work documents, and personal media safe by providing identity information and then authenticating to that identity. Text passwords and personal identification numbers (PINs) are the dominant authentication method as they are simple and can be deployed on systems including public terminals, the web, and mobile devices.

A. Locimetric Password Schemes

1) Cued-recall (locimetric) password schemes involve users se-lecting regions on one or more images. Blonder's [6] U.S. patent is the earliest example. A seminal example is PassPoints [30]. During login, users are shown a previously selected image, and they enter a password by clicking on a sequence of locations on the image. Authentication is successful if the XY coordinates of these clicks match a previously stored set of password points. A longitudinal study resulted in login times of 8.78–24.25 s and a failed authentication rate of 7–13% [30]. Read already published work in the samefield.

II. PASSBYOP OVERVIEW

Live Object For to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks [27], [30]. 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 [30]. PassBYOP tackles this problem by introducing a physi-cal token into the authentication process. This way, PassBYOP transforms a graphical password, which is traditionally a single-factor authentication mechanism, to a more secure multifactor authentication method. We argue that this makes PassBYOP

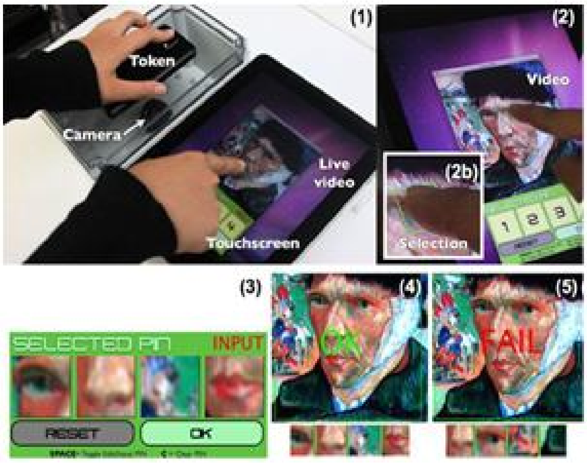
Resilient-to-Internal-Observation [7], meaning that an attacker cannot impersonate a user simply by intercepting input on the authentication device or by eavesdropping on the communica-tion between the authentication device and verification system.

Live Object authentication takes place as follows (see Fig. 1).

Assuming users have previously created a password, login in users identifying themselves at a Live Object 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. PassBYOP could be integrated into any of these scenarios. 2, users place a 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 live Object to attacks based on password observation and guessing as attackers need to possess a user's genuine token or a high fidelity copy.

III. IMPLEMENTATION

The PassBYOP prototype consists of a 13.5-cm-wide × 22.5-cm-long × 12-cm-high plastic box with a transparent cover and containing an upward-facing Logitech QuickCam E3500 webcam with a resolution of 640×480 pixels and a speed of 30



wirelessly to the PC via a screen-sharing application [see (1) in Fig. 2] and fixed to the surface of a desk. The video resolution on the iPad is 450×600 pixels or approx-imately 8.5 cm × 14 cm. All input to the system is made on the iPad touchscreen. Specifically, as illustrated in (2) in Fig.2, users makeselections by tapping the screen to visually highlight 70 × 70 pixel (approximately 1.5 cm2 The webcam is connected to a PCrunningPassBYOP. The PassBYOP interface and video feed are shown on anApple iPad that is connected) portions of the displayed image, drag to move this region and release to select it.

IV. CONCLUSION

To improve the security of cloud access by graphical password systems by integrating live object 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 thenuser performance is equivalent to standard graphical password systems through a usability study assessing task time, error rate,and subjective workload. Finally, a safety study shows that live object for securing graphical password substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes.

V. ACKNOWLEDGMENT

The authors would like to thank all their experimental partic-ipants for their time

REFERENCES

[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 two-factor authentication internet banking,"in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322–328.