Defeat Spyware With Anti-Screen Capture Technology Using Visual Persistence

Johnny Lim
Netrust
10 Collyer Quay, #09-05
Ocean Building, Singapore 049315
johnny.lim@netrust.net

ABSTRACT

In this paper, we describe a novel web-based method to generate an on-screen keypad with anti-screen capture technology for secure data entry. Our method protects against spying via keyboard, mouse and screen on a compromised computer.

1. INTRODUCTION

The online entry of sensitive data like PIN and credit card number using textboxes is extremely vulnerable to keylogger. One bank [1] is using on-screen keyboard to thwart key and mouse-click logging. However, this is useless against spyware that takes snapshots of the user's mouse clicks.

2. METHOD DESCRIPTION

2.1 Visual Persistence

A user of our method shall see an on-screen keypad like Figure 1 in his browser. Unknown to him, the keypad is constructed by fusing several images (see Figure 2) into a single image using the visual persistence of the human vision system. The browser cyclically displays these images at a fast refresh rate on the screen. By visual persistence, the cyclic pattern of images is integrated into a strobed display of the keypad. This integration is illustrated in Figure 3 for the formation of the number "4" using one empty and two partial images.

The browser does not display a complete keypad image at any one instance. Consequently, the spyware can capture merely an empty or partial image in a screenshot that does not reveal the user's selection.

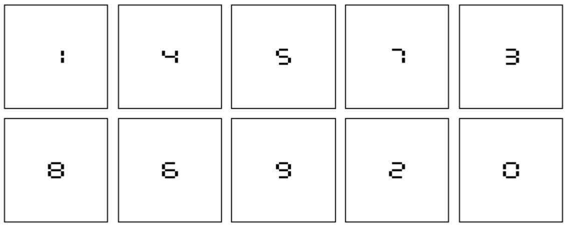

Figure 1. On-screen Keypad with Random Number Layout

Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

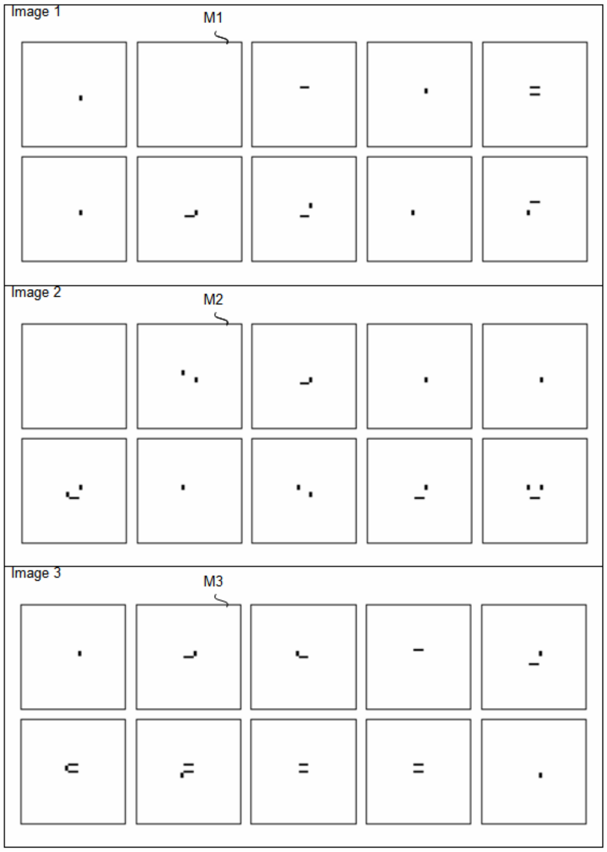

Figure 2. Partial Images of Keypad

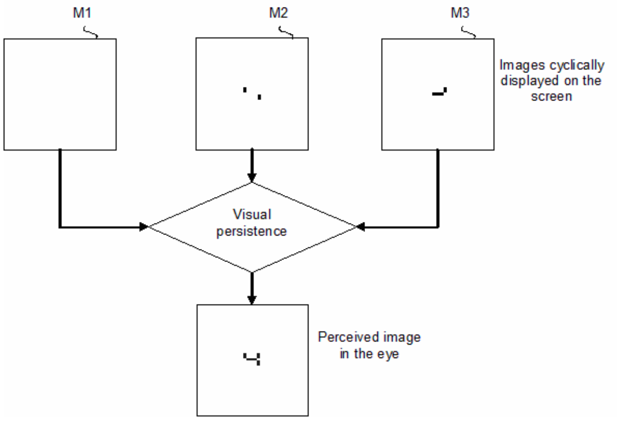
M1
M2
M3
Images cyclically displayed on the screen
Visual persistence
Perceived image in the eye

Figure 3. Formation of Number "4"

2.2 Image Generation

To increase the security of our method, the set of images is generated using an algorithm [2] that is designed to make it statistically difficult for a hacker to guess the user's number by examining one or more screenshots of the keypad.[1]

The algorithm takes the pixels required to form a number and randomly distributes them among the images while ensuring that infrequently-used pixels are not placed in the same image. The usage frequency of a pixel is the number of times the pixel is used when all the numbers from "0" to "9" are considered. Infrequently-used pixel gives more information about the number. Hence, by keeping them separate, we make it statistically hard to guess a number based on partial images. In Figure 3, if the spyware captures the image M2, it obtains 50% information about the number "4". However, this is insufficient for the hacker to determine the number as there is more than one possible number that shares the same pixel pattern, like number "6" and "5".

In addition, a newly generated set of images is used to display the keypad after each mouse click. Therefore screenshots captured over time across mouse clicks have no correlation. This further enhances our anti-screen capture technology.

2.3 Image Set Size

The number of images in one image set used to construct the keypad is dependent on the human vision system's integration time and the monitor's refresh rate.

$$Set\ Size = \lfloor \frac{Integration\ Time}{Refresh\ Rate} \rfloor + 1$$

Images seen within the integration time are fused into a single image by our eye. To minimize perceived flicker, we use an integration time of about 30-40ms. In Figure 2, we assume the monitor's refresh rate is 16ms, meaning we can use 3 images to give an integration time of 32ms.

Current monitors have a refresh rate of 2ms. This allows us to fit in 16 images with an integration time of 30ms. As a result of this large image set size, many of the images are empty. For example, Figure 1 uses a seven-segment numeric font type, and we see in Figure 3 that we require 4 segments to form the number "4". Generating the 16 images, we get 4 partial and 12 empty images.

A large image set size results in more empty images. Thereby the spyware is more likely to capture an empty useless screenshot.

2.4 Random Layout

The layout of the numbers on the keypad in Figure 1 is random and changes after each mouse click. Consequently, faithful reproduction of mouse clicks captured by spyware is useless. This defeats mouse-click logging.

2.5 Server-Driven

Our method is web-based and server-driven. The server is responsible for generating the random number layout and the partial images. Only the images are sent to the browser for display. This prevents in-memory hacking as the browser has no knowledge of the user's number. The server then receives and deciphers the mouse click to obtain the user's number.

Being server-driven, the enterprise is able to enforce security in restrictive client environments wherein installation is prohibited (e.g. public computers in internet cafes) or unfeasible (e.g. customers' computers outside the enterprise's control).

3. APPLICATION & LIMITATION

Online entry of credit card numbers, which is currently left unprotected, can be easily secured by our method. Credit card issuers and merchants realize that it is impractical to use 2FA devices given the varied and large number of stakeholders involved in credit card processing. Our method can be easily integrated to the existing entry process.

The security of our method comes from the fact that it is non-trivial for the spyware to capture all the partial images. To capture the whole image set every time, the spyware has to take screenshots at the same high rate as the monitor's refresh rate. This greatly increases its resource consumption and risk of discovery [3].

4. CONCLUSION

Our method is able to defeat key, mouse-click and screenshot logging on a compromised computer. It gives the user a familiar and easy-to-use interface. It enables the enterprise to provide security without hardware or download. Details of our method are in [2].

We would like to integrate our method with mutual authentication. We would also like to license our technology to other partners to benefit future work in this area.

5. REFERENCES

[1] Citibank Singapore. *Login page.* http://www.citibank.com.sg.

[2] Lim, Y., and Tan, M. *Method for Protecting a Character Entered at a Graphical Interface.* WO/2005/083638, PCT Database, WIPO, 2005.

[3] Florencio, D., and Herley, C. *How to login from an Internet café without worrying about keyloggers.* SOUPS, 2006.

[1] This does not hold true if the hacker captures the whole image set. See Section 3.