# Secure Authentication using Anti-Screenshot Virtual Keyboard

**Ankit Parekh[1], Ajinkya Pawar[2] , Pratik Munot[3] and Piyush Mantri[4]**

**[1,2,3] Department of Computer Engineering,
MIT College of Engineering,
Pune University, India**

**[4] Department of Computer Engineering,
Trinity College of Engineering and Research,
Pune University, India**

### Abstract

With the development of electronic commerce, a lot of companies have established online trading platforms of their own such as e-tickets, online booking, online shopping, etc. Virtual Keyboard is used for authentication on such web based platform. However Virtual Keyboard still suffers from numerous other fallacies that an attacker can take advantage of. These include click based screenshot capturing and over the shoulder spoofing. To overcome these drawbacks, we have designed a virtual keyboard that is generated dynamically each time the user access the web site. Also after each click event of the user the arrangement of the keys of the virtual keyboard are shuffled. The position of the keys is hidden so that a user standing behind may not be able to see the pressed key. Our proposed approach makes the usage of virtual keyboard even more secure for users and makes it tougher for malware programs to capture authentication details.

***Keywords:*** *Virtual Keyboard, Keylogging, Online Banking, Trojan Horse, Security, Efficiency*

## 1. Introduction

Today, the Internet has melted into our daily lives with more and more services being moved online. Besides reading news, searching for information and other risk free activities online, we are also accustomed to other risk related work such as paying using credit cards, online banking, etc. We enjoy the convenience but at the same time we are putting ourselves at risk. More and more Trojan Horses have developed which have been the huge trouble to security of e-commerce and makes businesses and customer suffer huge economic losses.

Virtual Keyboard is a mechanism used by many banks to solve the problem of their bank account and password being stolen by these Trojans. However the Virtual Keyboard is not foolproof and has its own fallacies. Hence, a new Anti-Screenshot Virtual Keyboard is proposed in the paper, which can protect bank accounts and passwords from stealing due to the screen capture of Trojan Horses.

## 2. Password Stealing Schemes

In this section various methods in which passwords are been stolen have been discussed. These methods are Shoulder Surfing, Phishing, Attacks using hardware and Attacks using Trojan Horses. These methods have been discussed in detail in Sections 2.1, 2.2, 2.3 and 2.4 respectively.

### 2.1 Shoulder Surfing

Shoulder Surfing is a well known method of stealing others passwords and other sensitive information by looking over victims shoulders while they are sitting in front of terminals. This attack is most likely to occur in insecure and crowded public environments such as Internet Café, shopping malls, etc. It is possible for an attacker to use hidden camera to record all keyboard actions of a user. Video of the users actions on the keyboard can be studied later to figure out users ID and Password.

### 2.2 Phishing

Phishers attempt to fraudently acquire sensitive information, such as passwords and credit card details, by disguising as a trustworthy person or business in an electronic communication. For example, a phisher may set up a fake website and send emails to potential victims and persuade them to access the fake website. This way, the phisher can get a clear text of victims password. Phishing attacks are proven to be effective.

### 2.3 Using Hardware

Hardware Keyloggers are used for keylogging by means of a hardware circuit attached somewhere between computer keyboards and the computer. All the keystroke activities are logged into the internal memory which can later be accessed. A Hardware keylogger has an advantage over software solution because it is not dependent on installation on target computer operating system, it will not interfere with any program running on the target machine and also cannot be detected by any software. However its physical presence can be detected.

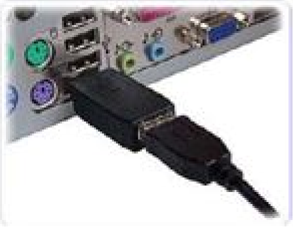


Fig. 1 Hardware Keylogger

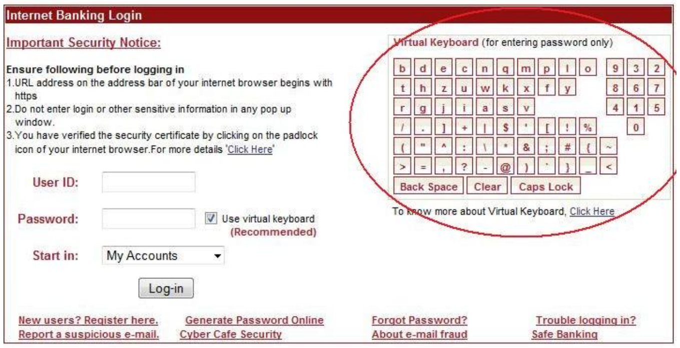
### 2.4 Using Trojan Horses

Trojan is a program that contains or installs malicious code. There are many such Trojans available online today. Trojans capture the keystrokes and store them somewhere in the machine and send them back to the adversary. Once a Trojan is activated, it provides the adversary with a string of characters that a user might enter online, consequently putting personal data and online account information at risk. They work in the background without the user coming to know about them. Chances of computer being affected by such malicious software is 70% even if the computer is up-to-date. A Trojan Horse typically contains two files: DLL file end EXE file. The DLL file does all the recording in some file in the computer while the EXE installs the DLL and triggers it to work. The file in which all the recording is done is mailed to the adversaries mail account.

## 3.Virtual Keyboard

Virtual Keyboard is a software technology that is used to mitigate the attack of password stealing Trojans. It is an on-screen keyboard which uses mouse to enter sensitive details such as an credit card pin number or password.

Fig 2 shows a virtual keyboard. The user has to use the mouse to click on the key on virtual keyboard he wants to press. The corresponding key will be typed into the selected textbox. Hence in this way using the virtual keyboard the use of traditional keyboard can be nullified. Thus sensitive and personal information can be protected.



Internet Banking Login

Important Security Notice:

Ensure following before logging in

1.URL address on the address bar of your internet browser begins with https
2.Do not enter login or other sensitive information in any pop up window.
3.You have verified the security certificate by clicking on the padlock icon of your internet browser.For more details 'Click Here'

User ID:

Password: ☑ Use virtual keyboard (Recommended)

Start in: My Accounts

Virtual Keyboard (for entering password only)

To know more about Virtual Keyboard, Click Here

Fig. 2 Virtual Keyboard

## 4. Problems of Virtual Keyboard

The virtual keyboard has a number of fallacies that the attacker can take advantage of. There are advanced Trojans which take screenshots on the Mouse Click event. All these screenshots are uploaded to the hackers website or mail account. Hence in this way even a virtual keyboard is made susceptible to attacks. Also the virtual keyboard is susceptible to shoulder surfing.

## 5. Anti-Screenshot Virtual Keyboard (ASVK)

In order to overcome the fallacies of the virtual keyboard, such as susceptibility to screenshot capturing and shoulder surfing, the anti-screenshot virtual keyboard is proposed in this paper.

In the anti-screenshot virtual keyboard, when the mouse move to one key, all the keys on that particular row of the keyboard are changed to some special symbol like an asterisk(*) or a hash(#). Figure 3 shows the position of the anti-screenshot virtual keyboard when the mouse cursor moves on a particular key.

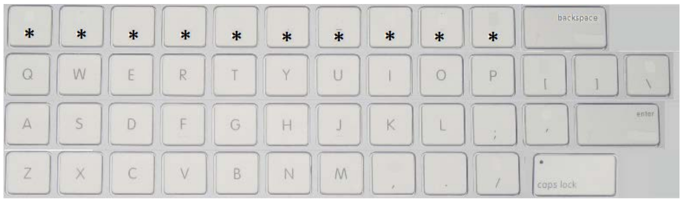


Fig. 1 : Position of the virtual keyboard on mouse move event

When the user clicks a particular button all the keys on the virtual keyboard are changed to some special symbol, say asterisk(*). Hence even if the Trojan takes a screenshot on the mouse click event, all that will be captured is asterisk(*). Figure 4 shows the position of ant-screenshot virtual keyboard when a particular key is pressed.

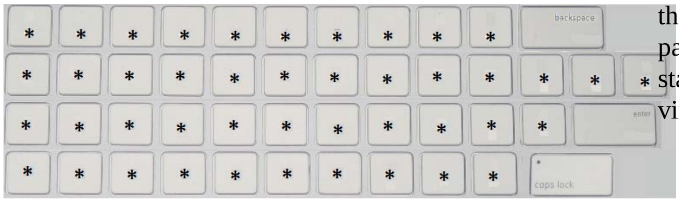


Fig 2: Position of the virtual keyboard on mouse click event

When the user releases the key, the keyboard is retained back to as shown in Figure 3.

However, in the above approach, if the Trojan Horse takes the screenshot of the virtual keyboard layout, then it is possible to identify the password. Hence in order to overcome this problem, real time refreshing can be done i.e when the user releases a key, instead of bringing the keyboard back to the original position, its keys can be randomized. However total randomization of the keyboard will make the user uncomfortable.

Hence in anti-screenshot virtual keyboard, the keyboard is divided into 15 areas as shown in Figure 5. The keyboard areas are as follows:

- 11 keyboard areas which consist of 3 keys.
- 3 keyboard areas which consist of 4 keys.
- 1 keyboard area which consists of 1 key.

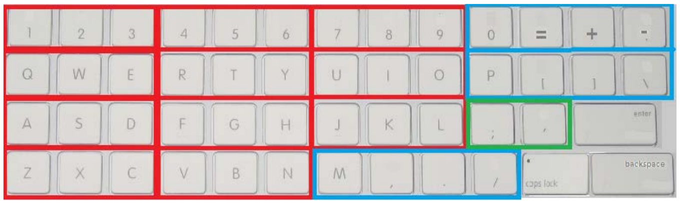

1 2 3 4 5 6 7 8 9 0 = + -
Q W E R T Y U I O P [ ] \
A S D F G H J K L ; , enter
Z X C V B N M , . / caps lock backspace

Fig 3 : Division of Virtual Keyboard for randomization

Each time the page is loaded or a key is pressed by the mouse, the order of keys in each area is rearranged. Because of this randomization the Trojan cannot find the input content even though they have captured one or two pictures of virtual keyboard layout. Let us assume that the user has 8-bit password consisting of only characters, then the Trojan Horse will require two million attempts to get the password. The bank account is blocked after three unsuccessful attempts. Hence the level of security provided by the anti-screenshot virtual keyboard is very high.

## 6. Analysis of Anti-Screenshot Virtual Keyboard

The anti-screenshot virtual keyboard requires some delayed time of say 0.2 seconds after the mouse button is released to show the values of keys and they are refreshed by areas on the virtual keyboard. Thus it is obvious that efficiency of virtual keyboard is less than that of traditional keyboard. But it is worthy to make the account secure at the cost of efficiency. With the inputting of a 8–bit password the comparison of consumed time between standard traditional keyboard and the anti-screenshot virtual keyboard is as shown in Figure 6.

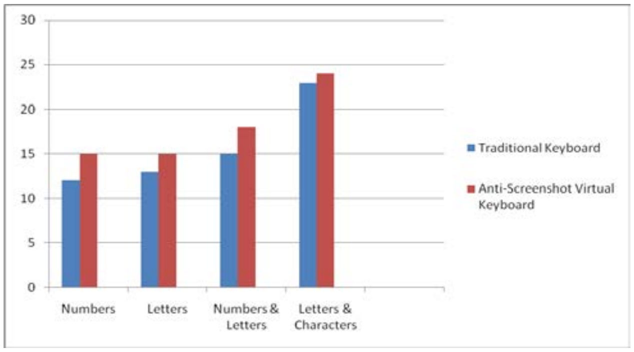


Fig. 4 : Efficiency Comparison

Results show that efficiency of virtual keyboards is 10.6% less than the traditional keyboards. When the customers input their accounts and passwords, the average time consumed is 20 seconds then 10.6% means 2 seconds slower than traditional keyboard. This 2 second delay will not make much difference to the customers because it is at the cost of security of account.

## 7. Advantages of Anti-Screenshot Virtual Keyboard

The anti-screenshot virtual keyboard is capable of solving the problem of screen capture by advanced Trojans. Also because of the change of caption of keys to some special symbols such as asterisk(*) or hash(#) its vulnerability to shoulder surfing is less as compared to the traditional virtual keyboards. Also the implementation of anti-screenshot virtual keyboard is simple. JavaScript can be used for its implementation.

## 8. Disadvantages of Anti-Screenshot Virtual Keyboard

The anti-screenshot virtual keyboard is less efficient as compared to the traditional keyboard. It is 10.6% less efficient as compared to the traditional keyboard. This makes the operation on anti-screenshot virtual keyboard slower. But it is worthy to make the account secure at the cost of efficiency.

## 9. Conclusion

The new design method of virtual keyboard presented in this paper to solve the problem of accounts of users are stolen because of Trojan Horses monitors the keyboards or captures the screen of internet payment is foolproof and improves the security and has an ability of becoming escort of online banking.

## References

[1] Analysis of New Threats to Online Banking Authentication Schemes by Oscar Delgado, A. Fuster-Sabater and J.M.Sierra

[2] UCAM.CL.TR-731 ISSN 1476-2986 : A new approach to Online Banking by Matthew Johnson

[3] Matthew Pemble. Evolutionary trends in bank customer – targeted malware. Network Security, 2005(10):4–7, October 2005

[4] M.AlZomai, B.Al Fayyadh, A.J sang, and A.McCullagh .An experimental investigation of the usability of transaction authorization in online bank security systems. In Proceedings of the Australasian Information Security Conference(AISC'08), Wollongong, Australia, January 2008.

[5] Zhang Zhanjun, Xu Jialiang. Online virtual keyboard and intelligent input system, Tsinghua University Press, 1998.

[6] Video demonstrating a Trojan Attack against Caja Murica Bank of spain
http://www.hispasec.com/laboratorio/cajamurcia_en.swf

[7] Demo of Attack against Citi Bank India
www.tracingbug.com/index.php/articles/view/23.html

[8] Hyunjung Kim, Minjung Sohn, Seoktae Kim, Jinhee Pak, Woohun Lee , Springer. Button Keyboard: A Very Small Keyboard with Universal Usability for Wearable Computing. In Maria Cecília Calani Baranauskas, Philippe Palanque, Julio Abascal, Simone Diniz Junqueira Barbosa, eds. Human-Computer Interaction – INTERACT 2007, 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part I. Lecture Notes in Computer Science 4662 Springer 2007. 343-346