Robust Virtual Keyboard for Online Banking

Chinmohan Nayak
Security Test Engineer
Tata Consultancy Services
Bhubaneswar, Odisha 751024

Manoranjan Parhi
Assistant Professor
SOA University
Bhubaneswar, Odisha 751030

Sujit Ghosal
Senior Security Researcher
Juniper Networks
Bangalore, Karnataka 560103

ABSTRACT
Current authentication practices suffer from many loopholes. To access an online banking facility, a customer with Internet access would need to register with the institution for the service, and set up some password for authentication process. Basically there are two types of password inputs allowed by banking websites these days. The first one is the traditional input in which we enter the password using keyboards and the second one is the virtual input in which the system accepts password using a virtual keyboard available in login pages of all bank websites. Virtual keyboards are considered as additional security steps for accessing online banking websites but this paper will describe how weak this implementation can be and what security measures can be adopted to maintain the confidentiality.

General Terms
Social Engineering Attack, Shoulder Surfing, Virtual Keyboard, Security, Algorithms

Keywords
Virtual Keyboard, Shoulder Surfing, Displacement Factor, Traversal, Trojan

1. INTRODUCTION
As online transactions are faster and exact almost no man power, people these days prefer transacting over internet. Though this makes life easier, at the same time this also puts you at risk. Security of a customer's financial information is very important, without which online banking is impossible to operate. Many attackers use different techniques to takeover an account but the easiest method is the shoulder surfing attack in case of a bank account. This is because of the implementation flaw associated with the Virtual Keyboard in the login page of every bank web application. Online banking is a riskier job until and unless implemented properly. Advanced Trojan horse like NetBus, ZeuS are designed to run in Microsoft Windows operating system and steal banking information by keystroke, form grabbing and screen capturing. In this paper we will consider the visual methods of stealing password like traditional shoulder surfing and screenshot capture by Trojans and the proposed methods to prevent these attacks.

2. VIRTUAL KEYBOARD ATTACKS
There are a lot of techniques used by hackers to steal credentials but for password theft from virtual keyboards there are two most successful techniques which are easy to execute. They are social engineering and Trojan horse attacks. Both of the techniques are briefly explained below.

2.1 Social Engineering Attack
Social Engineering attack is a technique to manipulate people to steal confidential information. Shoulder surfing is a form of social engineering attack. In this method an attacker can look over the victim's shoulder while they are typing their secure credentials to login into a website. This doesn't only happen when a user is sitting in front of a machine rather this attack can be exploited when users enter their PIN at an automated teller machine or a POS terminal, uses a telephone card at a public payphone, enters a code for a rented locker in a public place such as a swimming pool or airport and now-a-days public transport is also an area of concern. However if someone is able to steal credentials by this method to login into a bank account, this will result in a huge loss because of the high risk associated with the monetary transactions. A shoulder surfing attack can be demonstrated in Fig 1.

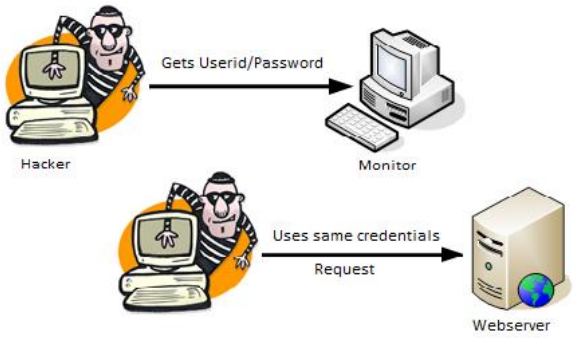

Fig 1: Shoulder Surfing Attack

2.2 Trojan horse Attack
A Trojan horse is a computer malware which contains malicious code. Once this is executed in a system, it behaves as it is programmed. This kind of malwares is usually spread as an email attachment disguised to be unsuspected. Trojans are designed to steal sensitive information from computers, slow down systems due to heavy network usage. Moreover they are not easily detectable.

3. VIRTUAL KEYBOARDS
Virtual keyboards were designed to ease the life of users. Disabled users who are not able to use the physical keyboard will easily be able to login using the virtual keyboard. While considering the security aspects this was designed to reduce the risk of key logger strokes. Though this technique succeeded to reduce key logging, it increased the risk in many other ways.

We can see a snapshot of a virtual keyboard in Fig 2.

Fig 2: A virtual keyboard

4. BLIND KEYBOARD

Blind keyboard is an obfuscation technique which will disguise the hackers. The integration of Blind keyboard will help overcome the weakness that the current virtual keyboard holds. Depending on the Displacement Factor and Traversal Direction, the proposed blind keyboard will function. There are two actions which will take place in this proposed algorithm. The front end action which can be seen by users will just act as an illusion where as the backend process is something different and that is the actual action which will be processed further for log in.

Displacement Factor (DF) is a numerical value which determines the number of box to be displaced for selecting the actual character. DF follows a rotational pattern.

Traversal Direction (TD) is the direction in which the DF will jump. This can be two ways.

1. Horizontal.

2. Vertical.

Both the traversal directions will follow a clockwise movement. The application will allow you to save the DF and TD value which will be stored in the database. We will consider horizontal as well as vertical traversal in our proposed algorithm.

4.1 Horizontal TD

In this type of traversal, the DF will move in a horizontal direction to select the actual character. The technique is demonstrated below.

Fig 3 explains how blind keyboard functions when it implements a horizontal traversal direction.

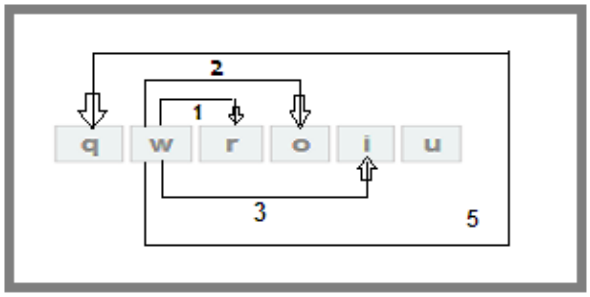

Fig 3: Example of Horizontal TD

Consider that DF is set to 3 and the traversal is horizontal. So to select the character "**w**" we should click on "**i**". To click the actual box we should move 3 positions towards right.

Similarly let the DF is set to 5 and the traversal is horizontal, to select the character "**w**" we should click on "**q**". The DF will follow a rotational pattern in this case.

4.2 Vertical TD

In this type of traversal, the DF will move in vertical direction to select the actual character. This technique is demonstrated below.

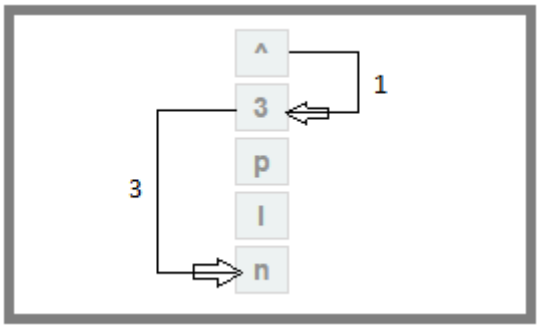

Fig 4: Example of Vertical TD

Fig 4 explains how blind keyboard functions when it implements a vertical traversal direction.

Consider that DF is set to 1 and the traversal is vertical. So to select the character "^" we should click on "**3**".

Similarly let the DF is set to 3 and the traversal is vertical, to select the character "**3**" we should click on "**n**". In this case also the DF will follow a rotational pattern.

5. ALGORITHM FOR BLIND KEYBOARD

We have proposed an algorithm to properly implement this keyboard. The steps are as follows

1. Fetch DF value from console
2. Fetch TD value from console
3. Set the default virtual keyboard
4. Actual key = Disguised Key *+ Shift(DF)

*Disguised key is the key shown to the user

6. DEMONSTRATION OF BLIND KEYBOARD

In this section we will illustrate a complete example of Blind Keyboard. Let us consider we will select a password '**ep0int**'.

Let's say we have already saved our preference for DF and TD in the database as shown below.

DF = 4

TD = Horizontal

Now we set the default virtual keyboard as shown in Fig 5

Fig 5: Default virtual keyboard

Using the blind keyboard, the password "ep0int" will instead be selected as "**iu5|; y**" as shown in Fig 6

- To select "e" we should move right till 4 box and select "i"
- To select "p" we should move right till 4 box and select "u"
- To select "0" we should move right till 4 box in a rotational fashion and select "5"
- To select "i" we should move right till 4 box and select "|"
- To select "n" we should move right till 4 box and select ";"
- To select "t" we should move right till 4 box and select "y"

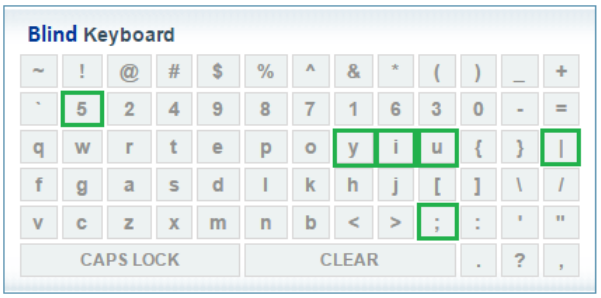

Fig 6: Blind keyboard

7. ADVANTAGES OF BLIND KEYBOARD

Blind keyboard helps in avoiding the damage caused by shoulder surfing and the most advanced Trojans. It ensures you that the sensitive information will be safe and secure. The password which someone enters using the blind keyboard will not be the actual password. Different processes will be running in the background to frame the actual password. There will be various combinations for a single password sequence that was just entered using the virtual keyboard. It can be horizontal TD or vertical TD sequence making the hacker to guess the password more difficult. So if an attacker tries to frame all the combinations and login with each one of them, it will be impossible because banking website allow only thrice entering a correct password. Moreover framing a password is itself tedious and takes a huge amount of time.

8. CONCLUSION

This paper presents an enhanced virtual keyboard known as Blind Keyboard which improves the security of online services. The proposed keyboard will hinder the success of different advance hacking techniques. This will not have any impact on the users with physical disabilities as they will be using the same virtual keyboard with just a simple calculation. The model used in this paper is thoroughly analyzed and found that it is very easy and simple to implement. However users who are illiterate will find it challenging to use this advanced keyboard. Two algorithms facilitating blind keyboard are introduced in this paper. They are for horizontal and vertical traversal directions. This approach can greatly improve the user's security over internet. We are trying to modify this technique as a part of future work so that the illiterate users can also use the blind keyboards. This keyboard can be implemented and used by various online banking websites.

9. REFERENCES

[1] White paper on"Threats to Online Banking- Symantec Security Response", Dublin

[2] "Online Banking: threats and Countermeasures Revised Version: 1.3", AhnLab, Inc., June, 2010.

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

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

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

[6] 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.

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

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

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

[10] Authentication in an Internet Banking Environment by Federal Financial Institutions Examination Council, June 29,2011[online]http://www.fdic.gov/news/news/financial/2010/index.html

[11] Adams, A., Sasse, M.A., Lunt, P. (1997). Making passwords secure and usable. Proceedings of HCI on People and Computers XII, 1-19.