The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 8||Pages|| 19-22||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

Random Number Based Dynamic Anti-Screenshot Virtual Keyboard for Securer Web Login

Afolayan A. Obiniyi[1] and Mohammed Aminu Umar[2]
[1, 2] Department of Mathematics, Ahmadu Bello University, Zaria, Kaduna, Nigeria.

--***ABSTRACT***--

Virtual Keyboards have for long been employed by online bank portals and other Internet web portal to mitigate threats of key loggers, this has now being made inefficient by use of screen capture technologies to steal user credentials. Thus, these have made the quest for a newer approach eminent.

KEYWORDS: *Virtual Keyboard, Keyloggers, Anti-Screenshot, Trojan, Online Banking.*

Date of Submission: 24 July2013, ⟷ Date of Publication: 12Aug2013,

I. BACKGROUND OF STUDY

With the rise in Internet access and E-commerce web application has increasingly become popular. Virtual Keyboard has been used as a medium of login to such sensitive financial portals like, Internet Banking, etc. but the emergency of screen capture enable Trojans have since dwarfed this approach. Several anti-screen capture keyboards have being developed recently but with careful evaluation all seem to be lacking one thing or the other.

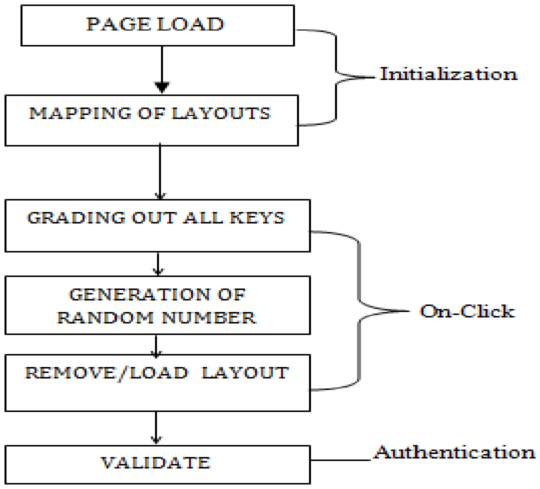
II. MATERIAL AND METHODS

The propose design will leverage on the early anti-screen capture keyboard designs and will try to correct their weakness.

The propose system is going to be a random number based dynamic anti-screen virtual keyboard (RASVK) and will composed of the following components:-

- Initialization
- On-Click
- Authentication

Figs 2.1 below are components of the proposed system.



3.1: Proposed System Components

2.1 Propose System Description

Below is the step by step description of the proposed keyboard.

a. There should be Five (5) distinct keyboard layout with the QWERTY layout been the default layout at page load or a CLEAR button click.

b. Screen size should be intermediary so as to be compatible with mobile browsers like Safari mini, Google Chrome etc.

c. An Unbiased random Integer Number Generator (1 -5) is to be design with 1- assign to the QWERTY layout and rest layout attached to the remaining numbers i.e. 2-5.

d. On each Key click on the propose keyboard all keys on the keyboard are graded to asterisk (*)

e. The random number generator is activated depending on the number generated the current layout is removed and replaced with the layout attached to that number. This process continues till all characters of the password are keyed in.

2.3 Implementation of RDASVK

In order to create the propose design we use JavaScript (Jquery) version 1.9.0 which is a client-side scripting language for broader compatibility across browsers. We also use PHP version 5.4.3 for the server-side scripting, MySQL Database Server version 5.5.24 and Apache Web Server Version 2.2.22.

The UML activity diagram of the proposed system as follows:

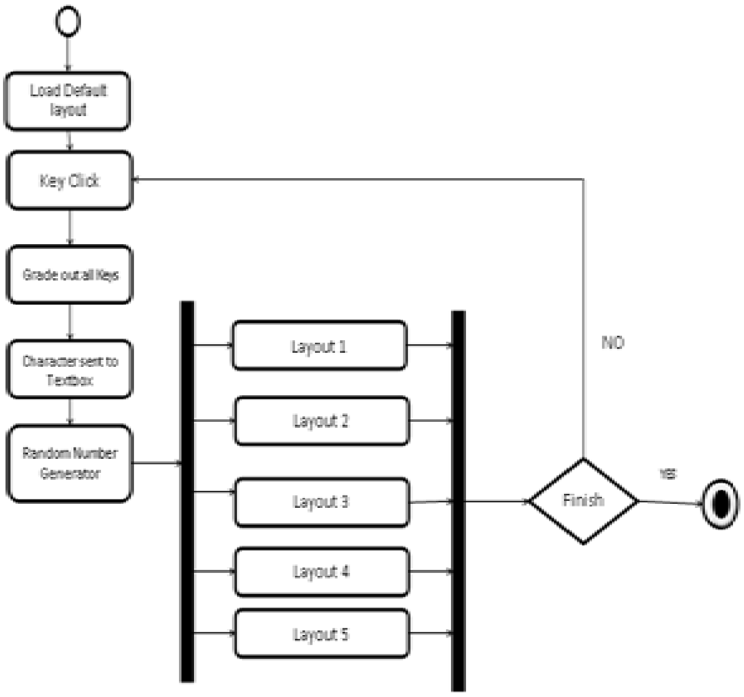
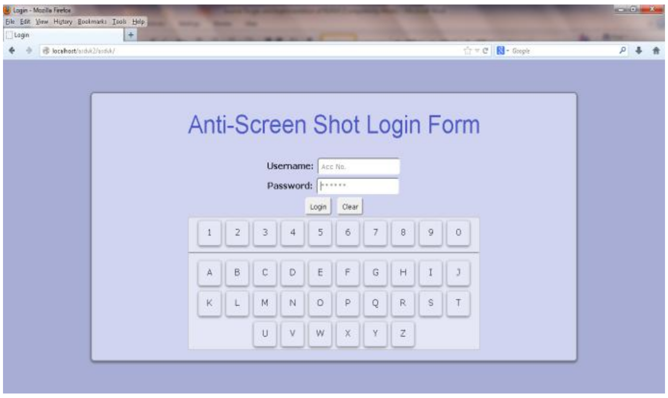


Fig 2.2 Propose System Diagram

III. RESULT AND DISCUSSION

Following the successful design, implementation and testing of the proposed system. Below are screenshot of it interface:

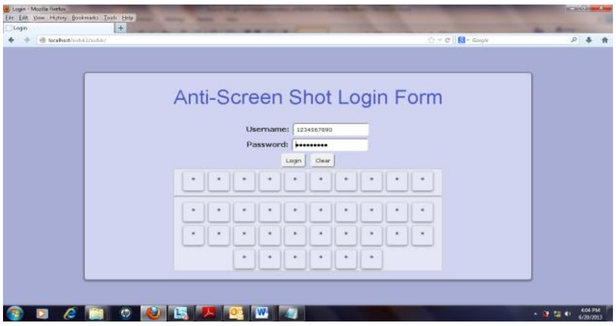


Anti-Screen Shot Login Form

Username: Acc No.

Password: ******

Fig 3.1 Interface with one of 5 Layout

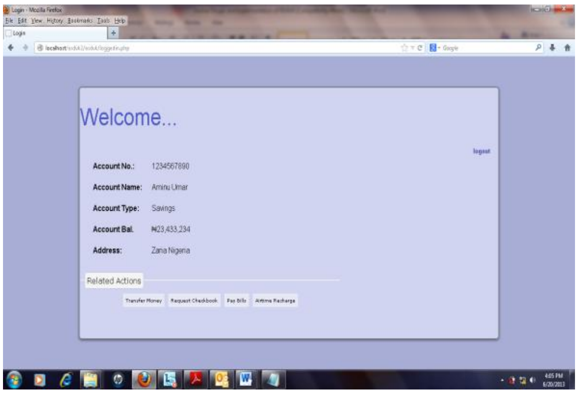


Anti-Screen Shot Login Form

Username: 1234567890

Password: ••••••••••

Fig 3.2 Click event Activity



Welcome...

Account No.: 1234567890

Account Name: Aminu Umar

Account Type: Savings

Account Bal. ₦23,433,234

Address: Zaria Nigeria

Fig 3.3 Interface After sucessfully logon

3.1 Evaluation

The goal of software evaluation according to (Gediga et al, 2010) is but not limited to;

a) Compare alternative software systems, e.g. to choose the best fitting software tool for given application, e.g. several versions of a software system.

b) Determination of the degree of desired qualities of a finished system. The evaluation of the system with respect to “Usability-Goals” is one of the applications of this goal.

c) Determine the weaknesses of software such that the result generates suggestions for further development.

Method of Evaluation

The Evaluation is going to be carried out based on the 3.1b above using the criteria based assessment model.
And the assessment measures are:

1) **Usability:** this checks if the application is useful for the purpose intended.
2) **Portability:** this measure checks if the application can be implemented across several platforms e.g. Browsers, OS, mobile
3) **Guard against all known of identity Theft:** Checks if the application mitigates more forms of Identity theft. E.g. Shoulder Surfing
4) **Decipherability:** this checks the ease the security provided by the application is not easily cracked.

Based on the above listed criteria’s the new designed have shown to be very solid as against earlier ones. As shown in the table 4.1 below:

	Usability	**Portability**	**Guard against Known Forms Identity Theft**	**Decipherability**
***VP**	✓	×	×	×
****ASVK**	✓	✓	✓	×
RASVK	✓	✓	✓	✓

Table 4.1: Evaluation Table

***** Visual Persistence Model Proposed by (4)
** Anti-Screen Shot Model by (5)

IV. CONCLUSION AND RECOMMENDATION

The propose design has indeed provided an additional security for the Anti-screenshot Virtual Keyboard technology. Anti-screenshot keyboard technology will keep evolving as the need for secure web applications grows.One of the main drawback to this design is typing character through this keyboard is slower compared to the regular online keyboard as a result of the layout interchange going on. However, this can be tolerated given the level of security it gives.

REFERENCES

[1]. Ali, A. (2010). *A study of security in wireless and mobile payments.* Stockholm: Linköping Institute of Technology.

[2]. Baloch, R. (2011). *An Introduction To Keyloggers, RATS And Malware.* http://rafayhackingarticles.blogspot.com.

[3]. Foss, J.-M., & Ingvaldsen, N. (2005). *Web Application Security.* Oslo: Norwegian University of Science Technology.

[4]. Lim, J. (2010). *Defeat Spyware with Anti-Screen Capture technology using visual Persistence.* Singapore: Univeristy of Singapore.

[5]. Parekh, A., & Pawar, A. (2011). *Secure Authentication using Anti-ScreenShot Virtual keyboard.* Pune: Pune University, India.

[6]. Schratt, M. (2012, 03 13). *MFS.* Retrieved 09 12, 2012, from http://mfs-enterprise.com/wordpress/2012/03/13/virtual-keyboard-sniffer/: http://mfs-enterprise.com/wordpress/2012/03/13/virtual-keyboard-sniffer/

[7]. Symantec Security Response. (2008). *Symantec Internet Security Threat Report: Trends for July–December 07.*

[8]. Weymes, B. (2012). *Recognising Botnets in Organisations.* Netherlands: Department of Computer Science,Radboud University.

[9]. Wüeest, C. (2006). *Threats to Online Banking.* Dublin: Symantec Security Response.

First Author Obiniyi, A. Afolayan is a doctorate degree holder in Computer Science with over two decades of lecturing experience. He is presently a Senior lecturer at the Mathematics department of the Ahmadu Bello University, Zaria – Nigeria.

Second Author Mohammed Aminu Umar is the Regional IT Coordinator, Mainstreet Bank Limited. Kaduna. He obtained a BSc. Degree in Computer Science at the University of Abuja, Nigeria and currently, he is undergoing a master's degree program in Computer Science at ABU, Zaria - Nigeria.