ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Grid Based Authentication System

Yogesh Mali[1]
Department of Computer Engineering
Dr. D. Y. Patil SOET
Lohegaon, Pune – India

Viresh Chapte[2]
Assistant Professor, Department of Computer Engineering
Dr. D. Y. Patil SOET
Lohegaon, Pune – India

Abstract: ***The twenty-first century is filled with many new gadgets and innovations. At first glance, our society may appear to be rather advanced. However, looks can be deceiving .In reality we are only at the forefront at what is in store for the near future. With the passing of each day, we may not know it, but our lives are becoming more and more digitized. A fully paperless society is on the horizon .As the digital world ushers itself in it will become important for one is protect his/her identity and from them those lurking in the distance.***

This paper will focus on the solution to the attacks namely 'Shoulder Surfing', 'Keystroke Logging' and 'Duplicate Login Pages'. The solution is the problem stated above will be discussed in the paper. The Proposed 'Grid Based Authentication System 'will improve the login security mechanism.

Keywords: Duplicate Login Pages, Grid Based Authentication System, Keystroke logging and Shoulder Surfing.

I. INTRODUCTION

What truly happens to data that is required into a computer system? It is true that the data is computed. However, it is also possible that something or someone else within close proximity to the computer read the information as well. That something or someone else could most likely be a Shoulder surfer. Dr. Fred Cohen, a respected leader in computer security and information protection classifies shoulder surfing as an attack that involves 'watching over people's shoulder as they use information or information systems'. With the advent of many technological innovations that require the inputting of information, shoulder surfing has become a new tool for attackers who want to exploit the vulnerable within their immediate reach. In some cases keystroke logging and duplicated login pages are also used to get passwords and misuse them.

Now we move to the solution to the problems mentioned above. Well the main problem is the attackers try to get access to the password which the user types. What if the user does not know the password which will allow him to access? Sounds a bit strange but this is what our system does.

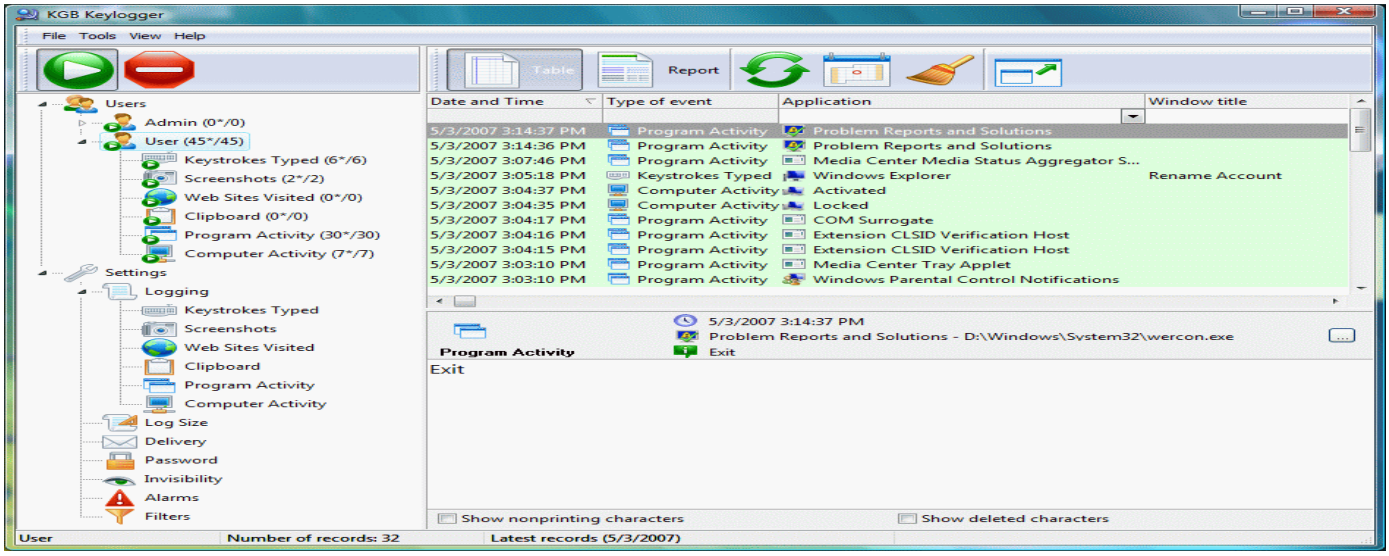
II. SHOULDER SURFING

Shoulder Surfing is particularly effective in crowded places because it is relatively easy to observe someone as they:

- Fill out a form
- Enter their pin at an automated teller machine or a POS terminal
- Use a telephone card at public payphone
- Enter a password at a cybercafé, public and university libraries.
- Enter a code for a rented locker in a public place such as swimming pool or airport.

Shoulder surfing can also be done at a distance using binocular or other vision enhancing device. Inexpensive, miniature closed circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paper word or keypad from view by using one's body hand.

Shoulder surfing is a form of attack that can strike at anytime and anywhere people ant technology meet. As time passes, our lives will become more and more digitized. We still have a name but a special signature, code or number may also help to positively identify us.



Many new technological innovations are slowly being introduced into today's society. Large majorities of people are embracing all the new gadgets and gizmos coming onto the market. Things are becoming more convenient and less time consuming. However, it also brings about an increase in vulnerabilities.

No matter how advanced society we become, one thing is certain, we must always remember to protect our identity, privacy and integrity. Shoulder surfers are individuals who pick a vulnerable target and exploit the information obtained from the person whose shoulder they looked over. They have the potential to steal someone's identity or disrupt someone's identity or right to privacy. Technological innovations can be great, however, one must be extra cautious when utilizing them.

Experts in the field can always attempt to improve on technology and make things safer to use. However, improvements and such are not always the answer. In regards to attack such as shoulder surfing, Vincent Vongo says it best: "User education is the means to combat these types of information gathering, to block the leaking of information before it's too late". Technology will always continue to advance. Unfortunately, it is up to the user of that technology to use it responsibly and protect him/her while doing so.

III. KEYSTROKE LOGGING

Keystroke logging (more often called as "key logging or key loggers") is the action of tracking (or logging) the keys struck on a keyboard, typically in a convert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous key logging methods, ranging from hardware and software based approaches to electromagnetic and acoustic analysis.

1) Software based key loggers

These are software programs designed to work on the target computer's operating system. From a technical perspective there are five categories:

a) Hypervisor based: The key logger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. Ineffectively becomes a virtual machine. Blue pill is a conceptual example.

b) Kernel based: This method is difficult both to write and combat. Such key logger resides at kernel level and is thus difficult to detect, especially for user-mode application. They are frequently implemented as root kits that subvert the operating system kernel and g**a**in unauthorized access to any information typed on the keyboard as it goes on to operating system .

c) API-based: These key loggers hook keyboard API's the operating system the notifies the key logger each time the key is pressed and the key logger simply records it.

a. Windows API such as Get a sync Key State (),Get Foreground Window () etc. are used to poll the state of the keyboard or to subscribe to keyboard events. These types of key loggers are easiest to write, but where constant polling of each key is required, they can cause a noticeable increase in CPU usage. A more recent example simply polls the BIOS for pre-boot authentication PIN's that has not been cleared form memory.

d) **Form grabbing based**: Form grabbing –based key loggers log web form submissions by recording the web browsing o submit event functions. This records form data before it is passed over the internet and bypasses HTTPS encryption.

e) **Memory injection based**: Memory injection (MitB)-based key loggers alter memory tables associated with the browser and other system functions to perform their logging functions. By patching the memory tables, this can be used by malware authors who are looking to bypass windows UAC (user account control). The Zeus and spy eye Trojans use this method exclusively.

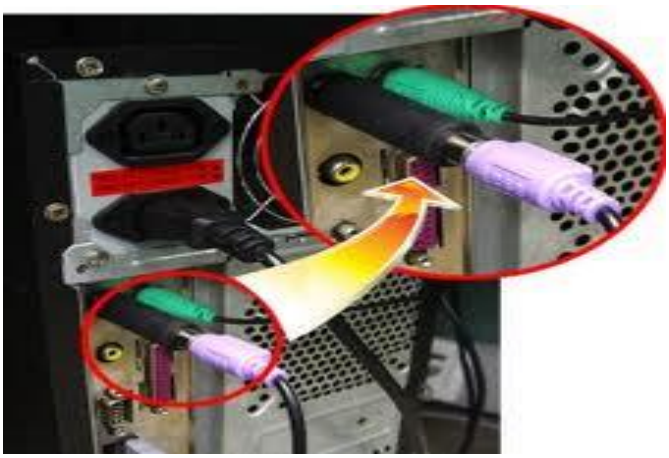
1) **Packet analyzers**: This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords.

2) **Remote access software key loggers**

These are local software key loggers with an added feature that allows access to the locally recorded data from a remote location. Remote communication may be achieved using one of these methods.

- Data is uploaded to a website, database or an FTP server.
- Data is periodically emailed to a pre-defined email address.
- Data is wirelessly transmitted by means of an attached hardware system.
- The software enables a remote login to the local machine from the internet or the local network, for data logs stored on the target machine to be accessed.

Hardware based key loggers do not depend upon any software being installed as they exist at a hardware level in a computer system.



- **Firmware based:** BIOS-level firmware that handles keyboard events can be modified to record these events as they are processed. Physical and/or root-level access is required to the machine, and the software loaded in the bios needs to be created for the specific hardware that it will be running on.
- **Keyboard hardware**: hardware key loggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer and the computer. More stealthy implementations can be built into standard keyboards, so that no device is visible on external cable. Both types log all keyboard activities to their internal memory, which can be subsequently accessed. For example, by typing in a secret key sequence. A hardware key logger is an advantage over software solution: it is not dependent on being installed on the target's computer's operating system and therefore will not interface with any program running on the target machine or be detected by any software. However its physical presence may be detected if, for example it is installed outside the case as an inline device between the computer and the keyboard. Some of the have the ability to be controlled and monitored remotely by means of a wireless communication standard.
- **Wireless keyboard sniffers**: This passive sniffer collects packets of being transferred from a wireless keyboard and its receiver. As encryption may be used to secure the wireless communications between the two devices, this may needs to be cracked beforehand if the transmissions are to be read.
- **Keyboard overlays**: Criminals have been known to use keyboard overlays on ATM'S to capture people's PIN's. Each key press is registered by the keyboard of the ATM as well as criminal's keypad that is placed over it.
- **Acoustic key logger**: Acoustic cryptanalysis can be used to monitor the sound created by typing on the computer. Each key on the keyboard makes a subtly different acoustic signature when struck. It is then possible to identify which keystroke signature relates to which keyboard character via statistical methods such as frequency analysis. The repetition frequency of similar acoustic keystroke strokes and the other context information such as the probable language in which the user is writing are used in this analysis to map sounds to letters. A fairly long recording (1000 or more keystrokes) is required so that a big enough sample is collected.
- **Electronic emissions**: It is possible to capture the electromagnetic emissions of a wired keyboard from up to 20 meters away, without being physically wired to it. In 2008, Swiss researches tested 11 different USB, PS2 and laptop keyboards in a semi-anechoic chamber and found them all vulnerable, primarily because of the prohibitive cost of adding shielding during manufacture. The researchers used a wide band receiver to tune into the specific frequency of the emissions radiated from the keyboard.

- **Optical surveillance**: Optical surveillance, while not a key logger in the classical sense, is nonetheless an approach that can be used to capture password or PIN's. A strategically placed camera at an ATM, can allow a criminal to watch a PIN or password being entered.

- **Physical Evidence:** For a keypad that is used only to enter a security code, the keys which are in actual use will have evidence of use from many fingerprints. A pass code of four digits in question are known, is reduced from 10,000 possibilities to just 24 possibilities. These could then be used on separate occasions for a manual "brute force attack".

IV. Grid Based Authentication System

We use a 6x6 grid which consists of 26 alphabets and 10 numbers. So we have 36 characters. We use the matrix as the login mechanism. While registering the user we ask the user to give a private key, which will be his primary keyword. The user needs to use this keyword but very indirectly. The keyword won't be written anywhere so there is no chance of it getting misused.

V. Procedure

So the characters will be arranged in a random manner in to the grid. Every time the user sees the grid with different character mapping. He has to click the matrix element corresponding to a particular row and column.

Let's say the private keyword has 6 letters. So the user will click the matrix element corresponding to the row in which the 1st letter exists and the column in which the 2nd letter exists. Similar steps will be followed for the corresponding letters. If the keyword has odd letters then last letter which will have partner to group with, will be clicked as it in the matrix.

Let's assume that user keyword is "NATURE" then his password will be of 3 characters. And password will be 'QUK'

W	2	F	3	H	8
C	N	Q	E	G	B
Z	T	U	0	1	O
6	D	A	P	J	9
M	X	R	K	S	Y
I	L	5	4	V	7

Next time during password input he will get different grid. So the keyword will be same but password will be different. Now for the same keyword 'NATURE' password will be NUE.

Z	T	U	K	1	A
3	B	O	5	2	N
8	C	S	V	Q	W
X	J	9	6	I	D
Y	F	L	H	G	7
P	4	M	R	E	0

VI. Advantages and Disadvantages

Advantages: As the grid will be random every time the password generated will be different. The part played by the keyboard will be cancelled so the key logging problem will be solved. The problem of duplicate website will be solved as eve if it is a fake website one does not have to worry as the password will be different each time and the captured one is useless next time. Now let's move on to problem of Shoulder surfing , here even if the person watches the matrix elements which are pressed he will not be able to guess the keyword. Let's give a fair chance to the attacker and say he knows the matrix. Still there are 6 row elements and 6 column elements. So even after knowing the grid and the elements pressed the password is still hard to decipher.

Disadvantages: Well the only disadvantage is that it could be little time consuming to find the letters in the grid. But the main purpose of enhancing the security and solving the problems mentioned above is achieved.

VII. Relevant Mathematics

1 Resistance to Accidental Login:-

Probability of Same grid to be appeared again.

$$\alpha + \beta = \Sigma T$$

Where

α - Number of Alphabets present in the Grid (A,B..Z)

β - Number of Numbers in Grid (0,1….9).

Σ T-Total Number of Alpha & Numbers will be 36

Thus the probability of same grid to appear will be 1/36!

This calculation is nearly equal to 3.719933^41 showing a very huge number.

2 Resistance to Possible Attack:-

Probability of hacker trying to attack in respective column and respective row.

$$P_{ra} = 1 - \frac{C_6^{36}}{C_6^{36}}$$

Where ,

Pra= Probability of Resistance to Attack

C= For Rows & for Column

Number of possible combinations in Rows and combinations in column

VIII. Conclusion and Future Scope

The proposed "Grid Based Authentication" system provides the solution to the problems like "Shoulder Surfing", "Keystroke logging" & "Duplicate login pages".

It enhances the security of the web based system and makes it difficult for the attackers to decipher the keyword of the user. These use of one time password through email or sms and obtaining a special character in grid will make system more Secure an complex as grid size will also increases and as a result combinations increases.

References

1. Mun-Kyu Lee "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry" IEEE Transaction 2014.
2. Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme" IEEE Conference 2014.
3. D.Aarthi, Dr.K.Elangovan "A Survey on Recall-Based Graphical User Authentications Algorithms" IJCSMA Feb 2014.
4. Dr Harsh Kumar Sarohi, Farhat Ullah Khan,"Graphical Password Authentication Schemes: Current Status and Key Issues" IJCSI March 2013.
5. Devika S, Backiyalakshmi R,"Design and Analysis of User Identification for Graphical Password System" IJCSIT March 2014.
6. A.R.Johnson Durai, V .Vinayan, " A Novel Crave-Char Based Password Entry System Resistant to Shoulder-Surfing" IMECS May 2014.

AUTHOR(S) PROFILE

Yogesh Mali received the B.E. degree in Computer Science & Engineering in 2013 and now pursuing M.E. degree in Computer Engineering from Dr. D. Y. Patil School of Engineering and Technology in current academic year 2014-15. He is now studying for the domain Information Security as research purpose on Grid Based Authentication System in his academic year.

Prof. Viresh Chapte (M.Tech CSE) now assistant professor in department of computer engineering Dr. D. Y. Patil School of Engineering and Technology Lohegaon , Pune. He is now in the research field of area of Information Security domain.

