I. J. Computer Network and Information Security, 2012, 5, 13-21
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.05.02

Battering Keyloggers and Screen Recording Software by Fabricating Passwords

Nairit Adhikary[1], Rohit Shrivastava[2], Ashwani Kumar[3], Sunil Kumar Verma[4], Monark Bag[5], Vrijendra Singh [6]
Cyber Law and Information Security Division, Indian Institute of Information Technology, Allahabad-211012, India
nairit.adhikary@yahoo.com[1], rshrivastav04@gmail.com[2], ashwanik@hotmail.com[3], contact.sunil86@gmail.com[4], monark@iiita.ac.in[5], vrij@iiita.ac.in[6]

Abstract — The keyloggers are covert security threat to the privacy and identity of users. The attackers are exploring different techniques of keylogging using hardware keyloggers, software keyloggers and screen capturing software to steal the user sensitive data. The Incognizance of the user is imposing greater risk. To overcome this problem, we have proposed a model. In this model solution to Keylogger and Screen Recording Software has been proposed by using the concept of fabricated password on untrusted machine. It deceives the untrusted system's key logging and video capturing software. The concept used here is "WYSINT What You See Is Not True". The main feature of this model is that it has a hardware recognition to retrieve the key .This key is required by the Temporary Filter layer (TFL) as an intermediary to change into the trusted password after bypassing all the capturing techniques and returning the original password to the required website.

Index Terms — Onscreen Keyboard, Screen Recording, Key logger, Anti-key logger, Thumb drive

I. Introduction

The threats of keyloggers are increasing day by day and the threat is becoming potent as people are unable to detect the presence of keyloggers in the system. Moreover the threat has taken a severe form after the introduction of screen recording software which paralyze the anti keylogging [1], [2], [3] mechanisms like the virtual keyboards which are pertinent today. The various modes of larceny of critical data are explained below:

Key loggers, may it be in the form of Hardware or Software are very common these days which stores every key press and hence steals very critical information of user. It is a major threat because most of the access control such as login ids which are entered through keyboard gets stored or recorded. Hence makes the control mechanisms ineffective. Keyloggers are mainly classified into two categories: Hardware Keyloggers and Software Keyloggers.

A. Hardware Keyloggers

Hardware keylogger is mainly a small electronic device used for capturing the data in between a keyboard device and I/O port [4]. When they are mounted in a computer system they start capturing the keystrokes in their inbuilt memory. At present various number of hardware keylogger are available in market [5]. These keyloggers can be plugged inside the keyboard port, or directly inside the keyboard or at the end of the keyboard cable. The main privilege of hardware keylogger is that it does not use any computer resource so it becomes quite infeasible for the anti-viral software or scanners to detect. The keystrokes logs are stored in encrypted form in its own memory instead of the computer's hard disk .The major disadvantage of hardware keylogger is that they necessitate physical installation in the keyboard or Computer case.

B. Software Keyloggers

Software keyloggers logs and monitors the keystrokes and data within the target operating system, store them on hard disk or in remote locations, and send them to the attacker. Software keylogger [1], [6] monitoring is mainly based on the operating-system.

The Major Problem of Data Theft due to use of the key loggers were minimized by the use of various anti-key logging mechanisms. Virtual keyboard is one very popular among them. Since virtual keyboard only operates through mouse clicks so the key strokes are not captured [7]. The virtual keyboard uses the concept of random shuffling of keys; hence it is not having a definite structure. Therefore the key presses if captured cannot be used because of the random changing of the key locations. There is a bigger threat residing that is the screen recording software which is present and undetected.

C. Screen Recording Softwares

Screen Recording Softwares are prevalent because they are used to capture whatever is happening on the screen for monitoring [8] purpose or for the purpose of the Educational Demonstrations. This could be used negatively because the software could be used to capture the screen and mouse movement, so whosoever is using the virtual keyboard to avoid keyloggers are no more safe. This software records the screen activities which includes key presses trough virtual keyboards. Whatever activities are done on the screen is recorded and hence the passwords could be easily be captured.

The model we have proposed deceives the keyloggers and screen recording software and thereby bypassing the malicious techniques and help the access control techniques to work properly. The model is solution to such a problem which includes bypassing of hardware and software keyloggers as well as the screen recording

softwares. This also includes the solution to shoulder surfing, or capturing the screen activities through camera or other devices while secure access codes are entered. The rest of the paper is organized as follows: Section II consists of a brief literature review. In Section III the details of online survey conducted prior to development of the model is provided. Section IV have terms and basic concept used along with purpose of our proposed model while Section V explains implementation methodology from requirements to Algorithms along with illustrative examples of our model .The Section VI have advantages and disadvantages of our model .At last the Section VII consist of conclusion and future scope of our model.

II. LITERATURE REVIEW

In the current scenario ,security concerns are priority for any organization .Attackers are using various key logging techniques to gain sensitive data especially user login credentials .Once attacker gets these credentials ,they can easily authenticate themselves as authentic user.

In [7], the author has proposed a new pattern of virtual keyboard .The solution in this paper emphasizes on login credential protection from screen capture software by using the concept of reordering of the keys. This is providing solution to only screen capturing software. But this captures the screen only when an event occurs. While in case of screen recording software there is no need of event occurrence. Keystrokes can easily be guessed by analyzing the recorded video. In [9], the author has proposed a solution to the screen capturing keylogger by using a color coding mechanism and dynamic keyboard layout .The major flaw of this solution is that an attacker can identify the keys clicked on virtual keyboard. This can be done by analyzing the pattern of screen shot captured from the first appearance of the keyboard when no color coding mechanism is induced in it . In [4], this paper discuss about the increasing threats to computer security and the privacy. It explains various techniques of key logging and describe detail working of keyloggers .There are different places to put the keylogger. It can be anywhere between any virtual keyboard and windows procedure .The thorough study shows that the right place to add anti-keylogging mechanism is just before the window procedure.

The existing models does not provide full-fledged solution to key logging and screen recording software .They provide security to some extent to key logging and screen capturing software .So there needs to be a solution for the same.

III. ONLINE SURVEY PRIOR TO DEVELOPMENT OF THE MODEL

Solution regarding the screen recording softwares and keyloggers is must which has been confirmed from an online survey we conducted. Initially we had a survey to estimate the level of awareness existing among people regarding these unlawful data capturing techniques. we found a very positive result as shown in the Figure 1 (92.9% people were knowing about keyloggers) and (80% of people knew about screen capturing softwares). Next we asked how many of them knew how to check presence of keyloggers and screen recording softwares installed on a machine being used. The response to this question was a concern as most of them did not bother to check or does not know how to check them (74% were saying this) as shown in Figure 2. As per our survey 93.3% people needs a solution to this problem. Hence finally we thought to propose a model which can be a reasonable solution to this problem.

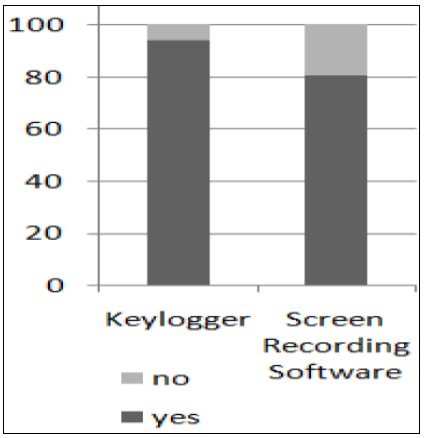

Figure 1. Level of awareness about Keylogger and Screen Recording Software.

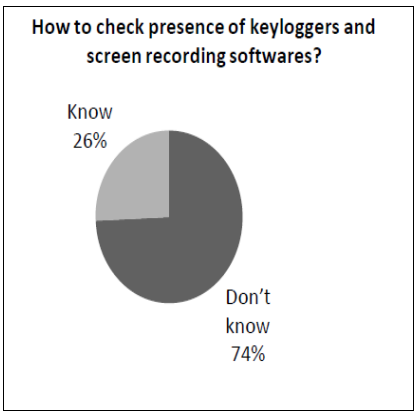

Figure 2. Presence of keyloggers

For the purpose of research work we used various tools to capture key logs and screen recording by ethical means and ethical use only.

The model which we have proposed consists of four phases which one needs to follow. After the customer receives the critical user details from the banks till the customer first time uses the username and password.

IV. PROPOSED MODEL

The main purpose of the model is to bypass the Keyloggers and Screen recording software by Two Factor Authentication and hence securely use password in un-trusted machines.

A. Terms Used in the Model

Following terms used in our model:

Trusted Systems

Trusted systems are systems with proper security configuration, updated patches, updated antivirus, configured firewall etc. These systems are those which are accessed by only one user or the persons trusted by him like his family members, for example personal Computer, laptop etc.

Un-trusted System.

Un-trusted systems are systems which are accessed not only by the user but by many other persons like computer system in cyber cafes, computer in public places. These systems are termed as untrusted systems which may have keyloggers, screen recording software or other malicious programs. The Un-trusted system has been divided into the following two zones:

a. Trusted Zone.
This is the zone which is considered free from presence of any malicious software like keylogger. The trusted zone is considered a safe place where the windows procedure operates and where the web-browser is present. This zone is represented in green color in the Figure 3.

b. Un- trusted Zone.
All the malicious activities such as existence of keyloggers and screen recording software are operational here in this zone. This is considered unsafe for the critical data as it might get captured. This is the zone where protection of the critical data is required. The un-trusted zone is represented by red color in Figure 3

Onscreen Keyboard:

An onscreen keyboard is a software component that allows a user to enter characters. The onscreen keyboard is generally a visual representation of the real keyboard on the standard output. An onscreen keyboard can usually be operated with multiple input devices, which may include an actual keyboard, a computer mouse, an eye mouse, and a head mouse.[Secure Authentication using Dynamic Virtual Keyboard Layout] .A typical onscreen keyboard is shown in Figure 3

Temporary Filter Layer:

This is a layer which is only operational when needed by user in the un-trusted machine. It is present in between the un-trusted and the trusted zone in the Un-trusted System as shown in Figure 3. This is the main operational layer which converts the fabricated password to the original password before reaching the window procedure. The existence of this layer will only be during the critical data transfer such as the password transfer.

Hooks:

An application can register (hook) itself into a point so that any message flowing in windows message mechanisms is passed to the hooked application before going to the original target that receives the message.[4] The two types of hooks as shown in Figure 3 are:

a. Global Hook: Global hooks monitor system-wide message.

b. Local Hook: Local hooks monitor application specific messages.

Window procedure:

It is the active window for which the key press is intended to.[4] Here for our purpose the active window will be the web-browser with the webpage where the user requires the access codes and credentials to be reached safely which is in the trusted zone in the Figure 3

WYSINT:

What you see is not true is the concept used in this model where the recording and capturing agents are deceived by making them capture something what is not useful.

Original Password:

The password which is used in trusted systems.

Fabricated Password:

The password used in un-trusted systems.

Pendrive/Thumb drive/USB Mass Storage Device Unique id:

This is the key used for identification of the Hardware Device.

B. Basic Concept of the Model

The paradigm of banking services has shifted from traditional to online for the ease of accessibility. Ease of operation had been a boon to both the bankers and the clients but online use of banking services requires certain security access codes to verify the identity and authenticity of the user. Hence confidentiality is very important for such critical data. This proposed model has been built keeping in mind the confidentiality factor with two layer authentication mechanism to make the operation safe.

When both keylogger in hardware form or in software form and screen recording software are present together then most of the existing solutions fail to protect the security access codes from being captured or stored. In this model we come up with a concept of fabricating password and bypassing all the unauthorized techniques and help in safe transmission of the password to the required web page.

The Figure 3 shows the working of the model in an un-trusted system where keyloggers and Screen recording software are present. The various methods of capturing can be present in the red zone so we use a fabricated password which is generated in the trusted machine by the concept of WYSINT. The user has to provide his original password and the fabricated password he wants to use in the un-trusted machine. This fabricated password is memorized by the user to use on all the un-trusted machines. This process of password generation also requires a USB storage device as per the two factor authentication.

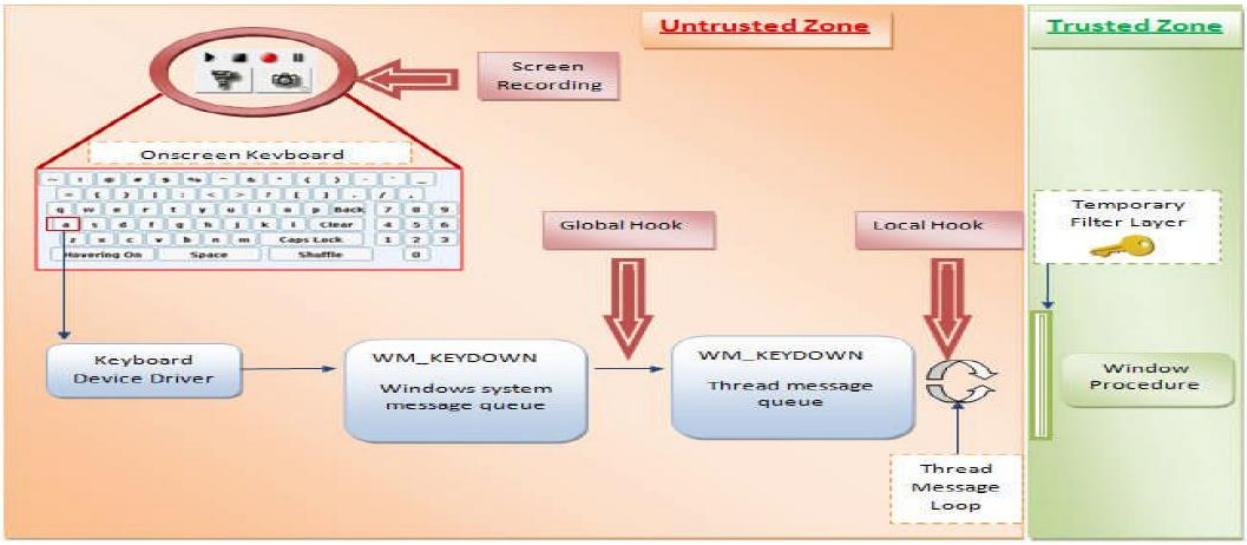

Figure 3.Proposed Model with separation of zone

This process will be carried out by the user through application software which will take the required inputs and then generate the fabricated password. The application also needs to store the key along with the codes required for the activation of the Temporary filter layer(TFL) on the Un trusted System in the connected USB storage drive which acts as a hardware recognition device in the Un-trusted machine.

On the Un-trusted machine the USB Storage Drive possessing the key and the required TFL creation package for the activation of the Temporary Filter Layer (TFL) needs to be connected which has been explained in Figure 4. Once it gets connected the TFL starts operating similar to the auto run functionality. Here it needs to be taken care that prior entering the fabricated password the user should plug USB Storage drive and unplug the same while entering the other details because it is considered that the TFL is active immediately after the plugging of the USB Storage Drive and it deactivates after the USB Storage Device is Unplugged. As soon as the password is entered through the keyboard the pressed key goes to the Operating System and then the keyboard driver of the operating system translates those keystrokes into a Windows message called WM_KEYDOWN. This message is pushed into the system message queue. The Operating System in turn puts this message into the message queue of the thread of the application related to the active window on the screen. The thread polling this queue sends the message to the window procedure of the active window [4]. As we know that just before the window procedure fabricated password is changed into original password which requires an operation performed by the TFL. To perform this operation TFL needs to extracts the PID, Transformation Key stored in the Thumb drive and fabricated password provided by the user. TFL is primarily implementing the Key Retrieval Algorithm. This algorithm performs the identification of the USB Storage Drive which is the first layer of authentication and then the fabricated password which is the second layer of authentication. Finally the TFL filters the entered values and pass it on to the browser which is trusted zone represented by green color in Figure 3 which gets the trusted password.

V. IMPLEMENTATION METHODOLOGY AND PROCESS

A. Requirement

Two things required in our model are:

a. USB Pendrive

A pendrive is uniquely identified by the combination of Vendor ID (Vid), Product ID (Pid) and the serial Number, where Vid and Pid are of four characters each and Serial Number is of variable length. *This can be view in Appendix 1*

The combination of these three, gives a variable length key to uniquely identify the pen drive [10]. A key generator application installed on the trusted system will fetch the pendrive's unique id and apply operation P to generate the intermediary PKEY which will lead to formation of final key i.e. TKEY.

b. Password

Two passwords are required by the model , one which is used on the trusted machine i.e. the original password and other on the untrusted machine opted by the user i.e.

the fabricated password. These two passwords are provided by user through a key generator application installed on the trusted system to generate the intermediary CKEY which will lead to formation of final key i.e. TKEY.

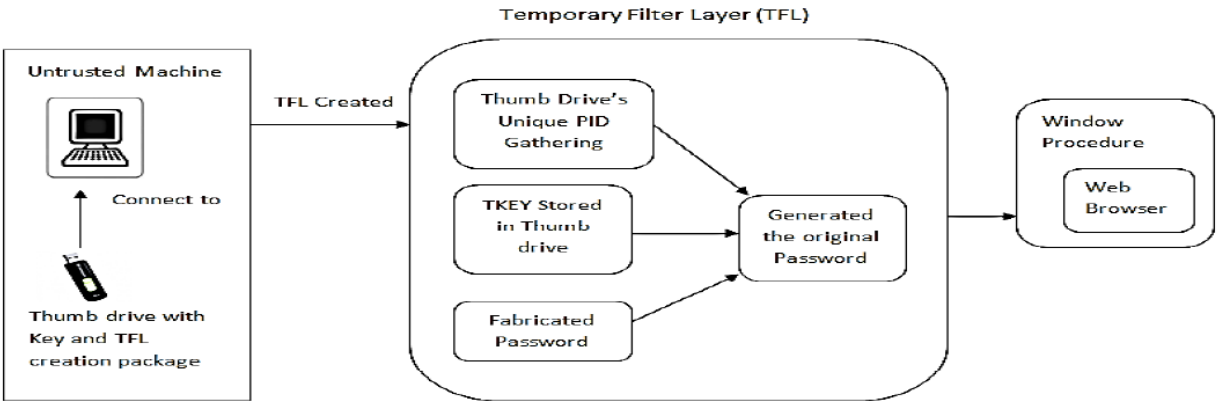

Figure 4. Creation and Operation of Temporary Filter Layer (TFL) in Un-trusted Machine

B. Algorithm

a. Key generation

In this phase a unique key is generated for each user based on its original password , fabricated password and pen drive's unique ID , this key will be used to login on un-trusted machine .The variable length key is generated. The key generated will be random in nature. The key generated by this algorithm is a combination to two strings CKEY and PKEY.

CKEY is stored in an array, which stores difference in ASCII value of OPASS and FPASS.

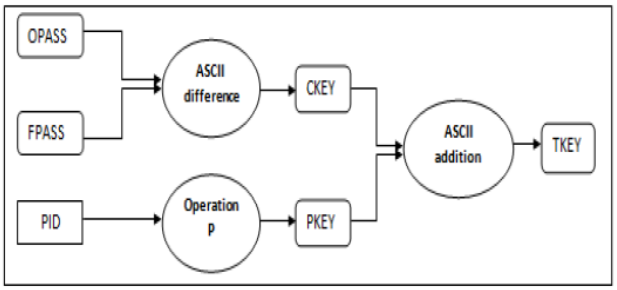

Figure 5. Key Generation Algorithm

PKEY is stored in an array, which is obtained by applying operation P on ASCII value PID of pendrive . Required key TKEY is stored in an array which is the sum of corresponding elements of CKEY and PKEY.

i. Creation of CKEY

The original password varies from user to user. The users are required to select a new password which will be considered as the fabricated password of same length as that of original password. Then the ASCII difference of two passwords i.e. of OPASS and FPASS is taken as CKEY.

1. OPASS – Stores the ASCII value of the original password

2. FPASS – Stores the ASCII value of the fabricated Password

3. CKEY – Difference of corresponding elements of OPASS and FPASS.

ii. Creation of PKEY(Operation P)

The PID is a combination of Vendor id, product id and the serial number of pen drive , it is a string, and the length of this string varies from pen drive to pen drive.

b. Key retrieval

In this phase, the CKEY is retrieved on untrusted system, the CKEY is obtained by subtracting the corresponding elements of TKEY and PKEY.

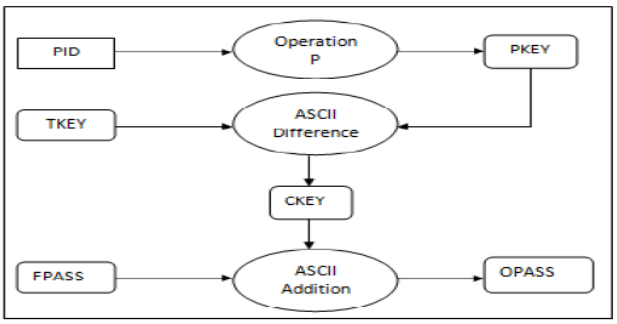

Figure 6. Key Retrieval Algorithm

i. Obtain TKEY

This key is obtained from the plugged pen drive in the un-trusted machine.

ii. Creation of PKEY

The same Operation P which was performed on the trusted machine will be applied on unique ID of the plugged in pen drive ASCII value i.e. on PID to get PKEY.

C. Example

i. Key generation

As shown in the Figure 7 ,Unique ID of the Plugged in Pen drive is converted into the corresponding ASCII value i.e. PID which is further divided into two sub array. These two sub arrays are added to form PKEY. Now, the difference between ASCII value of original password i.e. abhi_123 and fabricated password i.e. abhishek results in the CKEY. The corresponding element of CKEY is added to the PKEY to get the final key TKEY.

ii. Key retrieval

As shown in Figure 8, Unique ID of the Plugged in Pen drive is converted into the corresponding ASCII value i.e. PID which is further divided into two sub array. These two sub arrays are added to form PKEY. This PKEY is subtracted from the TKEY, which is retrieved by the application from pen drive, it will result in CKEY. This CKEY is added to FPASS to get the OPASS. The FPASS is the ASCII value corresponding to fabricated password i.e. abhishek. The OPASS is the ASCII value corresponding to original password. This ASCII value is converted back to character to get original password i.e. abhi_123.

VI. ADVANTAGES AND DISADVANTAGES

1. Shoulder surfing fails in the un-trusted machine as one can only get the fabricate password.
2. The model is only effective at the time of entering the critical information.
3. The Un-trusted machine must have an USB port enabled where the mass storage device could get connected.
4. The Temporary Filter layer which is created in between the window procedure and the browser, needs to be deactivated when the USB mass storage device is disconnected.
5. The USB mass storage device used in this model cannot be used for any other purpose.

VII. CONCLUSION

The issue of key-loggers and screen recording software are addressed and a new USB mass storage device authenticated anti key-logging technique is proposed. This new technique not only provides the protection against screen recording software, keyloggers but also help to protect from shoulder surfing and protecting the critical data of the users. The model we developed will help in increasing the client side security in a client – server architecture and help in battering keylogger and screen recording software in any of its forms. The model follows two factor authentication

These factors are:

- Something the user knows (fabricated password);and
- Something the user has (USB mass storage device with the key);

Hence this increases the security of this model to a great extent making it difficult for any sort of security breach.

This model could be implemented in the windows operating system platform and further it could be used in the other platforms as well. The model could replace the virtual keyboard technology used in banking portals by integrating the temporary filter layer and applying the two factor authentication so that the clients could securely enter the critical information. Further research could be carried out to design a single password solution. In which user has to remember a single simple password for multiple websites to keep the critical information secure.

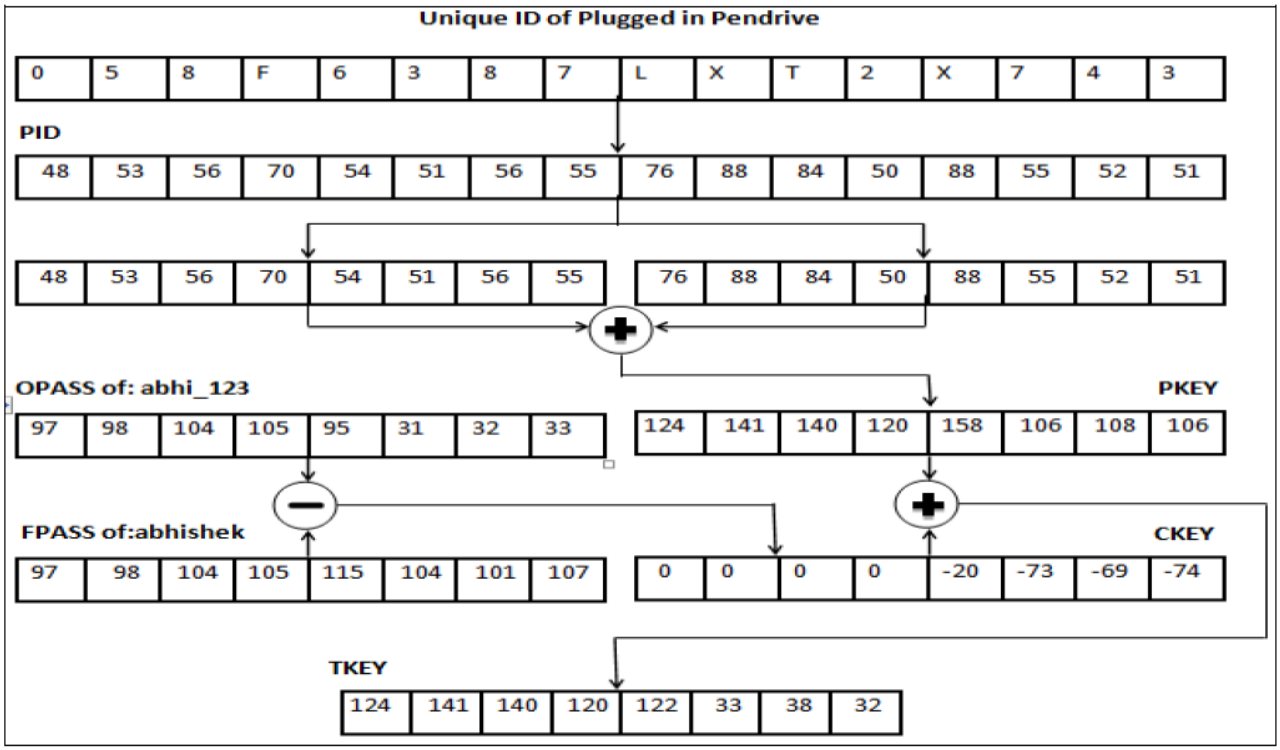

Figure 7. Key Generation Algorithm Example

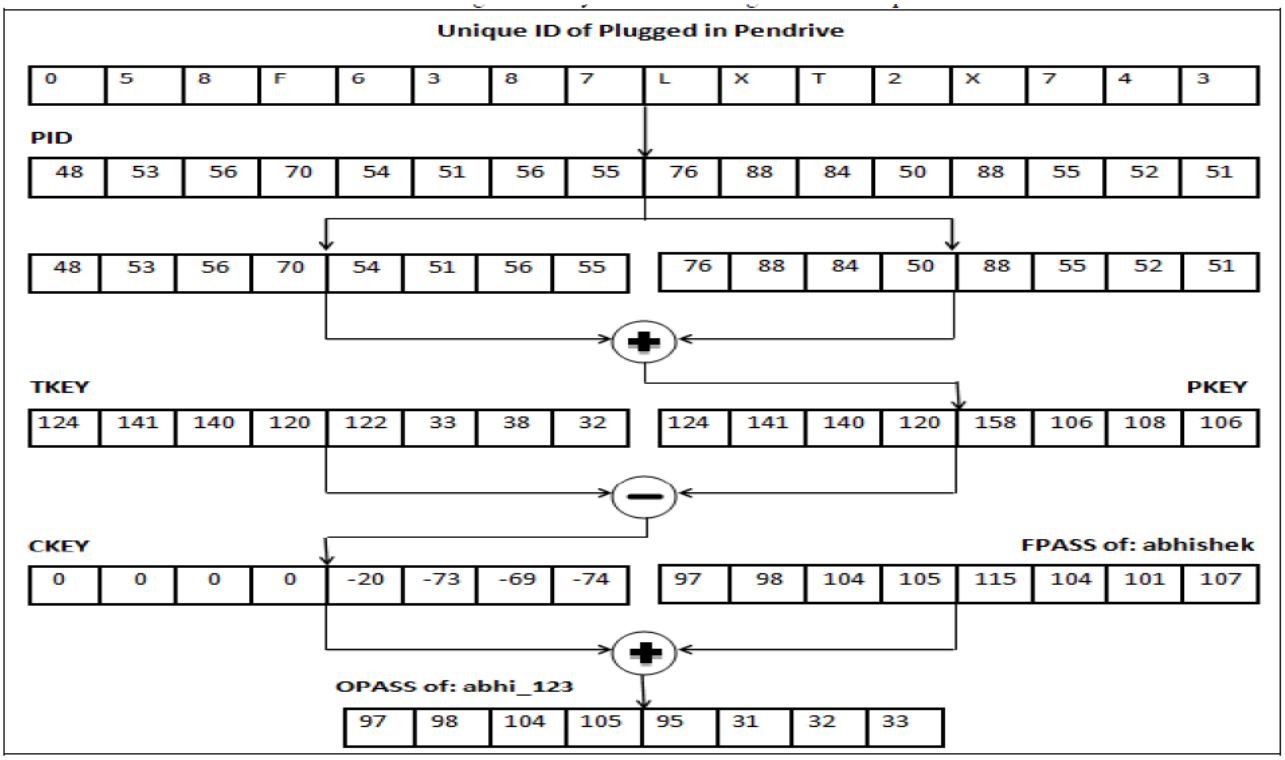

Figure 8. Key Retrieval Algorithm Example

REFERENCES

[1] G. Canbek, "Analysis, design and implementation of keyloggers and anti-keyloggers" Gazi University, Institute Of Science And Technology, M.Sc. thesis (in Turkish), Sept. 2005, pp. 103

[2] Williams, "I know what you did last logon: Monitoring software, spyware, and privacy," microsoft Security News., vol. 4, no. 6, June 2007.

[3] M. Kotadia, "Keylogger spying at work on the rise, survey says," CNET News.com, May2006; http://news.com.com/Keylogger+spying+at+work+on+the+rise,+survey+says/2100-7355_3-6072948.html accessed on 27 Jan 2012.

[4] S. Seref and C. Gurol "Keyloggers increasing threats to computer security and privacy" IEEE Technology and society magazine,2009,pp.10-17.

[5] www.keylogger.org accessed on 9 Dec 2011

[6] F.S. Lane, "The naked employee: How technology is Compromising workplace privacy" AMACOM Div American Mgmt. Assn.,2003, pp.128-130.

[7] S. Gong "Design and Implementation of Anti-Screenshot Virtual Keyboard Applied in Online Banking "E-Business and E-Government (ICEE), 2010 International Conf., 7-9 May 2010,pp-1320-1322

[8] L. Valeri "Screen Recording System For Windows Desktop" Russian-Korean International Symposium Science and Technology conf., 2004, pp.107-109

[9] M Agarwal , M Mehra "Secure Authentication using Dynamic Virtual Keyboard Layout" ICWET – TCET, Mumbai, India, 2011

[10] L. Keun-Gi ,"USB PassOn: Secure USB Thumb Drive Forensic Toolkit" , Future Generation Communication and Networking, 2008. FGCN '08. Second International Conf., 13-15 Dec. 2008,pp- 279 – 282

Nairit Adhikary received his B.A.-L.L.B. degree from University of Calcutta, Kolkata, India in 2008. He also received his B.C.A. degree from Indira Gandhi National Open University, New Delhi, India in 2011. These days he is pursuing his MS in Cyber Law and Information Security Post Graduate degree at Indian Institute of Information Technology, Allahabad, India. His research interest includes information security relating to banking sector and network security.

Rohit Shrivastava received his Bachelor degree of engineering in Information Technology from Madhav Institute of Technology and Science ,Gwalior ,India in 2008. He is pursuing his postgraduate study in Cyber Law and Information Security at Indian Institute of Information Technology , Allahabad ,India since 2010. His research interests include information security ,virtualization

Ashwani kumar received the B.Tech in Computer Science & Engineering from UPTU India in 2010. He is pursuing MS in Cyber Law & Information Security at Indian Institute of Information Technology. His research interests include network security and operating system security

Sunil Kumar Verma received the B.Tech in Computer Science & Engineering from UPTU India in 2009. He is pursuing MS in Cyber Law & Information Security at Indian Institute of Information Technology. His research interests include web application security and network security.

Monark Bag is a Lecturer in MBA (IT) and MS (CLIS) Division of Indian Institute of Information Technology, Allahabad. He holds a B.Tech (Computer Science and Engineering), MBA (Information Technology Management) and PhD (Engineering). He is highly engaged in teaching and research. His research interest includes expert system, control chart pattern recognition, quality control, optimization techniques, *intrusion detection Systems*. He has published many papers in reputed journals, conferences and book chapters.

Vrijendra Singh has received his Ph. D. from Dayalbagh Educational Institute, Agra, India. These days, he is designated as Assistant Professor in the Indian Institute of Information Technology, Allahabad, India. His research interests include Information Security and Digital Signal Processing.

APPENDIX 1

The snapshot of USBdeview software , the yellow highlighted line shows the unique id of pen drive