IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Keylogging: A Malicious Attack

Sonal Shinde[1], Ujwala H. Wanaskar[2]

Student, Department of Computer Engineering, Padmabhooshan Vasantdada Patil College of Engineering, Pune, India[1]

Asst Professor, Dept of Computer Engineering, Padmabhooshan Vasantdada Patil College of Engineering, Pune, India[2]

Abstract: Keylogging, one of the harmful malware, is the activity of recording the keys struck on a keyboard such that the person using the keyboard is unknown about the fact that their actions are being observed. It has authentic use in investigation of human-computer interaction and is considered as the main threat for business and personal activities. It can be used to intercept passwords and other confidential information entered via the keyboard. Hence, prevention of keylogging is important and strict authentication is required for it. Designing of secure authentication protocols is quite challenging, considering that various kinds of root kits reside in Personal Computers to observe user's behaviour. There are various keylogging techniques, extending from hardware and software based methodologies to acoustic examination. Human involvement in authentication protocols, though guaranteeing, is not simple. This paper reviews various research areas which cover protocol authentications used securely preventing the visualization of keylogging attacks.

Keywords: Keylogging; Authentication; Protocol; Acoustic examination; Visualization.

I. INTRODUCTION

Traditional authentication systems used to protect access to online services (such as passwords) are vulnerable to attack by the introduction of a keystroke logger to the service user's computer.[1] In the current Internet environment, most consumer computers are infected with one or more forms of spyware or malware.[2,3] The loss and steal of devices is getting a big problem because the data are not secured properly.[4] Keylogging or keystroke logging is a harmful malware in which an activity of recording the keys struck on a keyboard, normally in a secretive way, is performed so that the person using the keyboard is unknown about the fact that their actions are being observed.[5] The widespread distribution of keylogger functionality in malware is not surprising when you think about the number of situations in which entire digital identities can be stolen merely by capturing keyboard input.[6] Growing machine use for essential business and individual activities using the Internet has made feasible treatment of keylogging basic. The data caught can incorporate report content, passwords, user ID's, and other potentially touchy bits of information. Using this approach, an assailant can get essential data without breaking into a cemented database or file server.[7]

Keylogging attacks or those that utilize session hijacking, phishing and pharming and visual fraudulence, cannot be addressed by simply enabling encryption.[8] Keyloggers malignantly track customer information from the comfort attempting to recuperate individual and private information.[9] Nowadays, there are many threats against electronic and financial services which can be classified into two major classes: credential stealing and channel breaking attacks. Credential stealing is nothing but username, password and pin number which can be stolen by the attacker if they are poorly managed. Channel breaking attacks is nothing but eavesdropping on communication between users and a financial institution.[8,10,11]

There are two types of keyloggers, hardware keylogger and software keylogger. Hardware keylogger used for keystroke logging is a method of recording victim's keystrokes which will include ATM PIN, login password etc.

Fig 1: Hardware-based keylogger

They can be implemented by BIOS-level firmware or may be used through a device plugged in line between a computer keyboards and a computer. 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 monitoring is mainly based on the operating-system.[12]

A keylogger is a software designed to capture all of a user's keyboard strokes and then make use of them to impersonate a user in financial transactions. The threat of such keyloggers is pervasive and can be present both in personal computers and public kiosks. The weakest link in software-based full disk encryption is the authentication procedure today.[13] The worst part is that, keyloggers,

DOI 10.17148/IJARCCE.2016.5661

often root kitted, are hard to detect since they will not show up in the task manager process list. To mitigate the keylogger attack, virtual or onscreen keyboards with random keyboard arrangements are widely used in practice. Both techniques, by rearranging alphabets randomly on the buttons, can frustrate simple keyloggers. Unfortunately, the keylogger, which has control over the entire PC, can easily capture every event and read the video buffer to create a mapping between the clicks and the new alphabet. Another mitigation technique is to use the keyboard hooking prevention technique by perturbing the keyboard interrupt vector table. However, this technique is not universal and can interfere with the operating system and native drivers. It is not enough to depend only on cryptographic techniques to prevent attacks which aim to deceive user's visual experience while residing in a PC. Human user's involvement in the security protocol is sometimes necessary to prevent this type of attacks but humans are not good at complicated calculations and do not have a sufficient memory to remember cryptographically strong keys and signatures.[8]
The protection against keylogger addresses the problem of programs being able to read the global key state or the actual key buffer of a window. It does so by installing a filter driver in the kernel which receives every keystroke before it is sent to the Windows driver. This enables keystrokes to be filtered out as if they had never occurred. The result is that the keystroke appears in neither the global key state nor the key buffer, thus preventing malware from intercepting the input data. However, so that the keystrokes are not simply filtered out, the keys that have been pressed are obviously then added back into the system by sending them directly to the foreground window. This side channel ensures that Windows cannot determine that a particular key has been pressed. Windows simply knows that input has occurred in the foreground window.[6]
The concept behind keylogger protection is shown in fig 2;

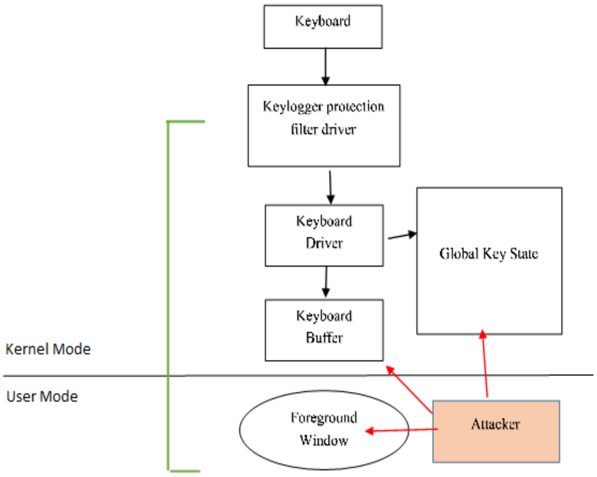

Fig 2: Processing keyboard input in Windows and the concept behind Keylogger Protection[6]

In this paper we focus on the literature survey which is related to keylogger, its working, prevention detection of keylogger attacks and its various applications.

II. LITERATURE SURVEY

Extensive work was performed dealing with the authentication protocols. Notable some among them were closely related to trust establishment for group communication like SPATE, GAnGS, Seeing-is-Believing (SiB), and SafeSlinger which deals with the issue of client authentication and connection of e-banking money. It is noteworthy that none of these works use visualization, although they provide primitives for authentication users and establishing trust.
Daehung et al and Bharadwaj et al have proposed two visual authentication protocols: One-Time-Password protocol and Password-based authentication protocol to show how visualization can enhance usability and security. Daehung et al studied that how these protocols utilize simple technologies available in most out-of-box smart phone devices and developed android application of a prototype of protocol and demonstrated its feasibility and potential in real-world deployment and operational settings for user authentication. Bharadwaj et al developed enhancement through offline transaction with IMI security. The main purpose of this was to avoid malicious transaction. The future plan was to implement this protocol on smart glasses such as Google glass to investigate the design of other protocols with more stringent performance requirements using the same tools.[7,8]

Cheng et al in his research proposed a novel password input protection system, KGuard, composed of novel user-hypervisor interaction channel, a keyboard stroke interception mechanism, and a hypervisor-based SSL client. This method does not require specialized hardware and is fully transparent to the operating system and the browser. A security-conscious user can conveniently and securely activate or deactivate the password protection by using key combinations. Implementation of KGuard and experimentation of prototype on Windows with Firefox shows that there is no significant performance loss induced by this protection mechanism when a user authenticates to commercial web servers. Moreover, the prototype implementation and testing have demonstrated that the protection system incurs insignificant overhead on the platform and maintains the user-friendliness of password authentication in web services.[14]

Chia et al proposed GAnGS, a protocol for the secure exchange of authenticated information among a group of people. GAnGS resists Group-in-the-Middle and Sybil attacks by malicious insiders, as well as infiltration attacks by malicious bystanders. In GAnGS, the physical interaction or Physical Articulation to Authenticate Legitimate Parties (PAALP) enables group members to collect and distribute authentic information while achieving resiliency to counting and comparison errors [Enumeration Error Proof (EEP) and Comparison Error Proof (CEP)]. Resilience to user errors presents a trade-off between usability, efficiency and security. With pairwise exchanges, users can collect group information in $O(n^2)$ total interactions with 100% attack detection and no

DOI 10.17148/IJARCCE.2016.5661

counting or comparison. In GAnGS, use of randomly assigned subgroups to balance these goals was performed. Subgroups with 5 members achieved a balance such that: users have to perform at most O(log(n)) operations, counting and comparison which is less susceptible to errors, and probability of attack detection is 95% or greater. Chia have implemented and evaluated GAnGS on Nokia N70 phones and the GAnGS system was viable and achieved a good balance between scalability, security and ease of use.[15]

Farb et al proposed SafeSlinger as a secure basis for online communication. It is a system for leveraging the proliferation of smartphones to enable people to securely and privately exchange their public keys. It also provides an API for importing application public keys into a user's contact information. It was proposed that by slinging entire contact entries to others, secure introductions were made, as the contact entry includes the SafeSlinger public keys as well as other public keys that were imported. Farb et al also presented the design and implementation of SafeSlinger for Android and iOS. The goal of this invention was to provide immediate utility through the robust exchange of contact list information between different smartphone platforms, which does not require any location information or leakage of private information outside the participating phones.[16]

Mannan et al proposed a simple approach to counter the attacks during transactions which may be due to keylogging, phishing and pharming. The proposed approach cryptographically separates a user's long-term secret input (typically low-entropy password) from the client PC. He also provided a comprehensive survey of web authentication techniques that use an additional factor of authentication such as a cell phone, PDA (personal digital assistant) or hardware token. A proof sketch of MP-Auth using the Protocol Composition Logic (PCL) was also provided. MP-Auth primarily focuses on online banking but can be used for general web authentication systems as well as at ATMs. In MP-Auth implementation, cryptographic computations and bluetooth communications took less than a second for login (excluding the user input time), which was believed to be an acceptable delay for the added security. Despite a main objective of preventing phishing and keylogging attacks, MP-Auth remains one-factor authentication and thus an attacker who nonetheless learns a user password can impersonate that user. MP-Auth has yet to be user-tested for usability.[2]

Matthias et al in his research focussed on the biometric authentication through virtual keyboards for smartphones. He presented a new implemented keyboard layout to show differences between a 12-key layout and a QWERTZ-layout. In addition, he compared a numerical (PIN) and alphabetic (password) input for mobile phones. For this, he added new features for a keystroke authentication with a capacitive display. With the knowledge of the fault rates, he discussed the improvement of the security for keystroke dynamics with different virtual keyboard layouts. The results show that even with new hardware factors, an authentication via keystroke dynamics was possible.[4]
Nair et al studied an enhanced authentication mechanism against untrusted access and phishing attacks using Unstructured Supplementary Service Data (USSD). He proposed a simple approach to overcome attacks like keylogging, phishing and pharming. This approach provides two modes of authentication, low mode and high mode. In low mode, normal text password is used and thereby user indicates the server that user is in an untrusted environment which restricts the user's action. In high mode, the user's text password input is separated cryptographically from the client PC and the user has full access to all the services. The user's secret key is input through an independent personal trusted device such as a cell phone which makes it available to the PC using a telecommunication facility called Unstructured Supplementary Service Data (USSD). The USSD is a session oriented GSM service which is much faster than SMS and is used to send messages between a mobile phone and an application server in the network. This proposal was intended to safeguard passwords from attacks such as password stealing attack, phishing attack and also provide transaction security to foil session hijacking.[3]

Parekh et al designed a virtual keyboard to overcome the drawbacks which is still suffered by virtual keyboards which include but not limited to click based screenshot capturing and over the shoulder spoofing. The designed virtual keyboard, in this paper, is generated dynamically each time the user access the website. Also, after each click event of the user the arrangement of the keys of the virtual keyboard are shuffled. The position of the keys was hidden so that a user standing behind may not be able to see the pressed key. Thus, the proposed approach may make the usage of virtual keyboard even more secure for users and may make it tougher for malware programs to capture authentication details.[17]

Stuart et al studied the malicious programs having keystroke logging capabilities using an example of real online banking system. He mentioned that if any of the features of the system were incorrectly implemented, they can potentially allow an attacker to gain access to a user's bank account. He also mentioned that the vulnerability of the attacks can be easily removed if the system always ask for a new set of characters whether or not login is successful. Because the analysis depended on character positions and not on the specific types of character that are allowed in the authentication code, allowing codes to consist of a wider variety of characters would not remove the vulnerability, although it might improve security in other respects. He also proposed that increasing the permissible lengths of authentication codes would slow down the attack, but would not alter the basic situation. In summary, the key point is that anti-keylogging systems implemented in this particular way effectively negate their entire intent.[1]
Tilo et al proposed STARK, a tamperproof authentication scheme that mutually authenticates the computer and the

DOI 10.17148/IJARCCE.2016.5661

user in order to resist keylogging during boot. STARK combined two ideas in a novel way: (a) Stark implemented trust bootstrapping from a secure token (a USB flash drive) to the whole PC. (b) In Stark, users can securely verify the authenticity of the PC before entering their password by using one-time boot prompts that are updated upon successful boot.[13]

Yan et al proposed a user authentication scheme, CoverPad, for password entry on touchscreen mobile devices. This research was mainly focused on improving the leakage resilience of password entry on mobile devices which are not sufficiently addressed due to small screen size. Also, additional features of mobile devices such as touch screen were not utilized, as they are not available in the traditional settings. Hence, Yan et al proposed a user authentication scheme named CoverPad for password entry on touchscreen mobile devices. CoverPad improved leakage resilience by safely delivering hidden messages, which break the correlation between the underlying password and the interaction information observable to an adversary. It was also designed to retain most benefits of legacy passwords, which is critical to a scheme intended for practical use. The usability of CoverPad was evaluated with an extended user study which included additional test conditions related to time pressure, distraction and mental workload. These test conditions simulated common situations for a password entry scheme used on a daily basis, which was not evaluated earlier. The results of user study showed that CoverPad improved leakage resilience while preserving most benefits of legacy passwords.[18]

III. KEYLOGGER APPLICATIONS

As illustrated from above literatures, it is evident that most of the times keyloggers are used for the malicious purpose. But apart from it there are affirmative and positive uses of keyloggers also. In IT organizations for troubleshooting technical problems with computers and business networks keyloggers are used. Other legal uses include family or business people using them to monitor the network usage without their user's direct knowledge. However, malicious individuals may use keyloggers on public computers to steal passwords or credit card information.

From a technical perspective there are several categories as follows.

- Hypervisor-based: For effective virtual machine keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. Example: Blue Pill
- Kernel-based: A program on the machine obtains root access to hide itself in the OS and starts intercepting keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as root kits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A keylogger using this method can act as a keyboard device driver and thus gain access to any information typed on the keyboard as it goes to the operating system.
- API-based: These keyloggers hook keyboard APIs inside a running application. The keylogger registers for keystroke events, as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it. Windows APIs such as GetAsyncKeyState(), GetForegroundWindow(), are used to poll the state of the keyboard or to subscribe to keyboard events.
- Form grabbing based: Form grabbing based keyloggers log web form submissions by recording the web browsing on submit events. These happen when the user finishes filling in a form and submits it usually by clicking a button or hitting enter. This records form data before it is passed over the Internet.
- Memory injection based: Memory Injection based keyloggers alter memory tables associated with the browser and other system functions to perform their logging functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors who are looking to bypass Windows UAC (User Account Control). The Zeus and Spyeye Trojans use this method exclusively. Non-Windows systems have analogous protection mechanisms that need to be thwarted somehow by the keylogger.
- Packet analyzers: This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords. This is made more difficult when connecting via HTTPS, which is one of the reasons HTTPS was invented.
- Remote access Software keyloggers: 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.
  - Most of these aren't stopped by HTTPS encryption because that only protects data in transit between computers to the keyboard.[12]

IV. CONCLUSION & FUTURE SCOPE

This review article attempts to an insight on the recent advancements on the attempts to mitigate the risks of keylogging attacks. The author realizes that the literature survey revealed in this article may have few loose ends on the virtue of inventions related to keylogging attacks and hopes that there may be more advancements in this area. The author also propose that much there is still scope to

DOI 10.17148/IJARCCE.2016.5661

perform inventory work in the area of keylogging attacks which needs to be addressed and worked upon in the coming years.

ACKNOWLEDGMENT

The author wishes to acknowledge Asst. Professor **Ms. Ujwala Wanaskar** and other contributors who had helped during the course of this work.

REFERENCES

[1] S. P. Goring, J. R. Rabaiotti and A. J. Jones, "Anti-keylogging measures for secure internet login: an example of the law of unintended consequences", Computers & Security, Page 1-9, Feb 2007

[2] M. Mannan and P. C. van Oorschot, "Leveraging personal devices for stronger password authentication from untrusted computers", Extended version of paper appeared in the proceedings of Financial Cryptography and Data security 2007, Version 6, Page 1-29, Oct 2008

[3] A. A. Nair and S. T. D., "An enhanced authentication mechanism against untrusted access and phishing attacks using USSD", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, Page 1188-1193, Aug 2013

[4] M. Trojahn and F. Ortmeier, "Biometric authentication through a virtual keyboard for smartphones", International Journal of Computer Science & Information Technology, Vol. 4, No. 5, Page 1-12, Oct 2012

[5] D. Bhave, P. Bhavsar, S. Chavan and K. Gore, "Keylogging-resistant visual authentication protocol", International Journal of Advanced Research in Computer and communication Engineering, Vol 5. Issue 2, Page 520-524, Feb 2016

[6] Keylogger protection-System security research, GData, Whitepaper, Page 1-8, Mar 2014

[7] S. Bharadwaj, R. Prathyusha and Rajeesh Kumar, "Attack resistant visually authenticated and secured system", International Journal of Research and Engineering, Vol. 2, Issue 2, Page 16-19

[8] D. Nyang, A. Mohaisen and J. Kang, "Keylogging-resistant visual authentication protocols", IEEE Transactions on Mobile Computing, Vol. 13, No. 11, Page 2566-2579, Nov 2014

[9] P. K. Veni and B. Naresh, "A novel visual authentication protocols implementation based on keylogging-resistant", International Journal of Scientific Engineering and Technology Research, Vol. 4, Issue 28, Page 5470-5477, Jul 2015

[10] R. Sangeetha, N. H. Vinodha and A. V. Kalpana, "QR code based encrypted matrix representation for eradication hardware and software keylogging", International Journal of Engineering Sciences and Research Technology, Page 642-647, Apr 2015

[11] R. Saraswathi, G. Shanmathi, P. Preethi and U. Arul, "Secure internet banking with visual authentication protocol", International Journal of Scientific Research in Science, Engineering and Technology, Vol. 1, Issue 1, Page 351-353, Jan-Feb 2015

[12] H. Pathak, A. Pawar and B. Patil, "A survey on keylogger-A malicious attack", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 4, Issue 4, Page 1465-1469, Apr 2015

[13] T. Muller, H. Spath, R. Mackl and F. C. Freiling, "STARK-Tamperproof authentication to resist keylogging", Chapter: Financial Cryptography and Data Security, Volume 7859 of the series lecture notes in Computer Science, Page 295-312

[14] Y. Cheng and X. Ding, "Virtualization Based Password Protection against Malware in Untrusted Operating Systems", Chapter: Trust and trustworthy computing, Volume 7344 of the series lecture notes in computer science, Page 201-218

[15] C. O. Chen, C. Chen, C. Kuo, Y. Lai, J. M. McCune, A. Studer, A. Perrig, B. Yang and T. Wu, "GAnGS: Gather, Authenticate 'n Group Securely", (http://www.iis.sinica.edu.tw/papers/byyang/6942-F.pdf)

[16] M. Farb, Y. Lin, T. H. Kim, J. McCune and A. Perrig, "SafeSlinger: Easy-to-Use and Secure Public-Key Exchange", Carnegie Mellon University, CMU-CyLab-11-021, Rev. 03 Oct 2013

[17] A. Parekh, A. Pawar, P. Munot and P. Mantri, "Secure authentication using anti-screenshot virtual keyboard", International Journal of Computer Science, Vol. 8, Issue 5, Page 534-537, Sep 2011

[18] Q. Yan, J. Han, Y. Li, J. Jhou and R. H. Deng, "Designing leakage-resilient password entry on touchscreen mobile devices", Singapore Management University, May 2013

BIOGRAPHIES

Ms. Sonal Shinde, Student, Department of Computer Engineering, Padmabhooshan Vasantdada Patil Institute of Technology, Pune.

Ms. Ujwala Wanaskar, Assistant Professor, Department of Computer Engineering, Specialization in Web Mining and Data Mining, Padmabhooshan Vasantdada Patil Institute of Technology, Pune.

DOI 10.17148/IJARCCE.2016.5661