https://doi.org/10.2352/ISSN.2470-1173.2017.6.MOBMU-313

The strange world of keyloggers - an overview, Part I

Reiner Creutzburg

Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, P.O.Box 2132, D-14737 Brandenburg, Germany

Email: creutzburg@th-brandenburg.de

Abstract

In this article we give a bibliographic overview of keyloggers and review the relavant hard- and software and mobile keyloggers that are available and in use. The functionalities, availability, detection possibilities of keyloggers are described and reviewed.

In a future Part II keyloggers for mobile devices and the ethical and legal aspects are reviewed.

Keylogger – Introduction

Keystroke logging, often referred to as keylogging [1] or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Keylogging can also be used to study humancomputer interaction. Numerous keylogging methods exist: they range from hardware and software-based approaches to acoustic analysis.

Software-based keyloggers

These are computer programs designed to work on the target computer's software [2]. Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Families and business people use keyloggers legally to monitor network usage without their users' direct knowledge. However, malicious individuals can use keyloggers on public computers to steal passwords or credit card information.

From a technical perspective there are several categories:

- **Hypervisor-based:** The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which thus remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example.
- **Kernel-based:** A program on the machine obtains root access to hide itself in the OS and intercepts keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the kernel level, which makes them difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as rootkits that subvert the operating system kernel to gain unauthorized access to the hardware. This makes them very powerful. A keylogger using this method can act as a keyboard device driver, for example, 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 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(), etc. are used to poll the state of the keyboard or to subscribe to keyboard events [3]. A more recent example simply polls the BIOS for pre-boot authentication PINs that have not been cleared from memory [4].
- **Form grabbing based:** Form grabbing-based keyloggers log web form submissions by recording the web browsing on submit events. This happens when the user completes a form and submits it, usually by clicking a button or hitting enter. This type of keylogger records form data before it is passed over the Internet.
- **Memory injection based:** Memory Injection (MitB)-based keyloggers perform their logging function by altering the memory tables associated with the browser and other system functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors to bypass Windows UAC (User Account Control). The Zeus and SpyEye trojans use this method exclusively [5]. Non-Windows systems have analogous protection mechanisms that the keylogger must thwart.
- **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:** These are local software keyloggers with an added feature that allows access to locally recorded data from a remote location. Remote communication may be achieved when one of these methods is used: + 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.

Most of these keyloggers aren't stopped by HTTPS encryption because that only protects data in transit between computers. This is a threat in your own computerthe one connected to the keyboard.

Keystroke logging in writing process research

Keystroke logging is now an established research method for the study of writing processes [6,7] Different programs have been

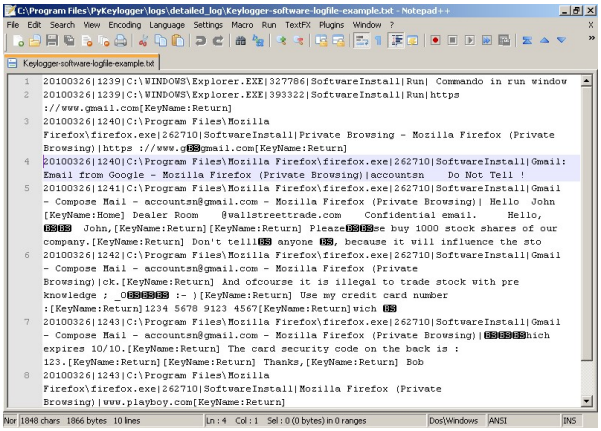

Figure 1. *Illustration of pedagogical philosophy concepts [??]*

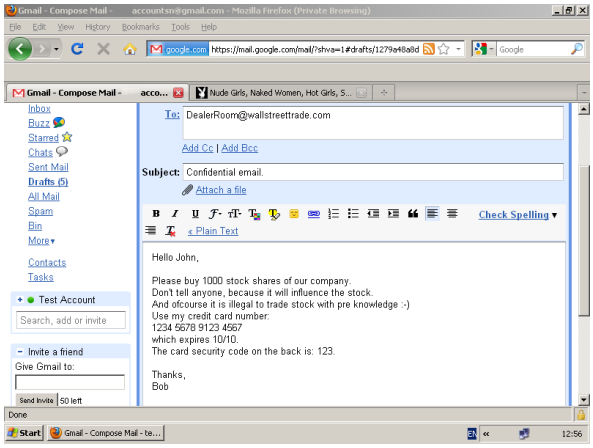

Figure 2. *Illustration of pedagogical philosophy concepts [??]*

developed to collect online process data of writing activities [8], including Inputlog, Scriptlog, and Translog.

Keystroke logging is legitimately used as a suitable research instrument in a number of writing contexts. These include studies on cognitive writing processes, which include

- descriptions of writing strategies; the writing development of children (with and without writing difficulties),
- spelling,
- first and second language writing, and
- specialist skill areas such as translation and subtitling.

Keystroke logging can be used to research writing, specifically. It can also be integrated in educational domains for second language learning, programming skills, and typing skills.

Figure 3. *Illustration of pedagogical philosophy concepts [??]*

Figure 4. *Illustration of pedagogical philosophy concepts [??]*

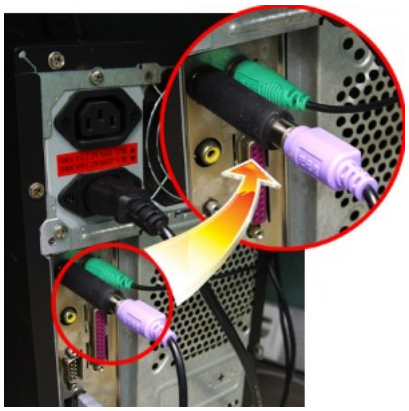

Figure 5. *Platforms of blended learning and 21st Century Learning [??]*

Related features

Software keyloggers may be augmented with features that capture user information without relying on keyboard key presses as the sole input. Some of these features include:

- Clipboard logging: Anything that has been copied to the clipboard can be captured by the program.
- Screen logging. Screenshots are taken to capture graphics-based information. Applications with screen logging abilities may take screenshots of the whole screen, of just one application, or even just around the mouse cursor. They may take these screenshots periodically or in response to user behaviours (for example, when a user clicks the mouse). A practical application that is used by some keyloggers with this screen logging ability, is to take small screenshots around where a mouse has just clicked; thus defeating web-based keyboards (for example, the web-based screen keyboards that are often used by banks), and any web-based on-screen keyboard without screenshot protection.
- Programmatically capturing the text in a control. The Microsoft Windows API allows programs to request the text 'value' in some controls. This means that some passwords may be captured, even if they are hidden behind password masks (usually asterisks).
- The recording of every program/folder/window opened including a screenshot of each and every website visited. - The recording of search engines queries, instant messenger conversations, FTP downloads and other Internet-based activities (including the bandwidth used).

Hardware-based keyloggers

Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer

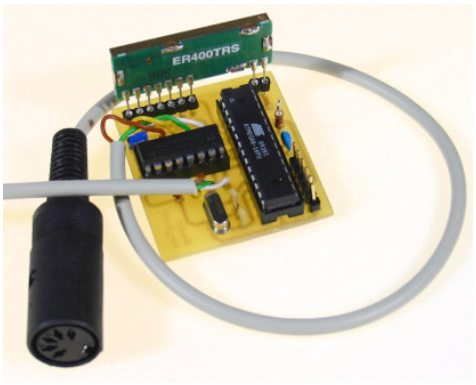

Figure 6. *Illustration of pedagogical philosophy concepts [??]*

Figure 7. *Illustration of pedagogical philosophy concepts [??]*

Figure 8. *Illustration of pedagogical philosophy concepts [??]*

system.

From a technical perspective there are several categories:

- **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 into the BIOS needs to be created for the specific hardware that it will be running on [10].
- **Keyboard hardware:** Hardware keyloggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer keyboard and the computer, typically inline with the keyboard's cable connector. There are also USB connectors based Hardware keyloggers as well as ones for Laptop computers (the Mini-PCI card plugs into the expansion slot of a laptop). More stealthy implementations can be installed or built into standard keyboards, so that no device is visible on the external cable. Both types log all keyboard activity to their internal memory, which can be subsequently accessed, for example, by typing in a secret key sequence [10]. A hardware keylogger has an advantage over a software solution: it is not dependent on being installed on the target computer's operating system and therefore will not interfere 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 these implementations have the ability to be controlled and monitored remotely by means of a wireless communication standard [12].
- **Wireless keyboard and mouse sniffers:** These passive sniffers collect packets of data 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 need to be cracked beforehand if the transmissions are to be read. In some cases this enables an attacker to type arbitrary commands into a victim's computer [13].
- **Keyboard overlays:** Criminals have been known to use keyboard overlays on ATMs to capture people's PINs. Each keypress is registered by the keyboard of the ATM as well as the criminal's keypad that is placed over it. The device is designed to look like an integrated part of the machine so that bank customers are unaware of its presence [14].
- **Acoustic keyloggers:** Acoustic cryptanalysis can be used to monitor the sound created by someone typing on a 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 signatures, the timings between different keyboard strokes and other context information such as the probable language in which the user is writing are used in this analysis to map sounds to letters [15]. A fairly long recording (1000 or more keystrokes) is required so that a big enough sample is collected [16].
- **Electromagnetic emissions:** It is possible to capture the electromagnetic emissions of a wired keyboard from up to 20 metres (66 ft) away, without being physically wired to it [17]. In 2009, Swiss researchers tested 11 different USB, PS/2 and laptop keyboards in a semi-anechoic chamber and found them all vulnerable, primarily because of the prohibitive cost of adding shielding during manufacture [18]. The researchers used a wide-band receiver to tune into the specific frequency of the emissions radiated from the keyboards.
- **Optical surveillance:** Optical surveillance, while not a keylogger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINs. A strategically

Figure 9. *Illustration of pedagogical philosophy concepts [??]*

placed camera, such as a hidden surveillance camera at an ATM, can allow a criminal to watch a PIN or password being entered [19,20].

- **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 passcode of four digits, if the four digits in question are known, is reduced from 10,000 possibilities to just 24 possibilities (10^4 versus 4!=24). These could then be used on separate occasions for a manual "brute force attack".
- **Smartphone sensors:** Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity accelerometer found in smartphones [21]. The attack is made possible by placing a smartphone nearby a keyboard on the same desk. The smartphone's accelerometer can then detect the vibrations created by typing on the keyboard, and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy. The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys. It models "keyboard events" in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard. Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way [22]. Similar techniques have also been shown to be effective at capturing keystrokes on touchscreen keyboards [23,24,25] while in some cases, in combination with gyroscope [26,27].

Hardware keylogger

Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer. They log all keyboard activity to their internal memory.

Hardware keyloggers have an advantage over software keyloggers as they can begin logging from the moment a computer is turned on (and are therefore able to intercept passwords for the BIOS or disk encryption software).

All hardware keylogger devices have to have the following:

- A microcontroller - this interprets the datastream between the keyboard and computer, processes it, and passes it to the non-volatile memory
- A non-volatile memory device, such as flash memory - this stores the recorded data, retaining it even when power is lost

Generally, recorded data is retrieved by typing a special password into a computer text editor. The hardware keylogger plugged in between the keyboard and computer detects that the password has been typed and then presents the computer with "typed" data to produce a menu. Beyond text menu some keyloggers offer a high-speed download to speed up retrieval of stored data; this can be via USB mass-storage enumeration or with a USB or serial download adapter.

Typically the memory capacity of a hardware keylogger may range from a few kilobytes to several gigabytes, with each keystroke recorded typically consuming a byte of memory.

Types of hardware keyloggers

- A Regular Hardware Keylogger is used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer keyboard and the computer. It logs all keyboard activity to its internal memory which can be accessed by typing in a series of pre-defined characters. A hardware keylogger has an advantage over a software solution; because it is not dependent on the computer's operating system it will not interfere with any program running on the target machine and hence cannot be detected by any software. They are typically designed to have an innocuous appearance that blends in with the rest of the cabling or hardware, such as appearing to be an EMC Balun. They can also be installed inside a keyboard itself (as a circuit attachment or modification), or the keyboard could be manufactured with this "feature". They are designed to work with legacy PS/2 keyboards, or more recently, with USB keyboards. Some variants, known as wireless hardware keyloggers, have the ability to be controlled and monitored remotely by means of a wireless communication standard.
- Wireless Keylogger sniffers - Collect packets of data being transferred from a wireless keyboard and its receiver and then attempt to crack the encryption key being used to secure wireless communications between the two devices.
- Firmware - A computer's BIOS, which is typically responsible for handling keyboard events, can be reprogrammed so that it records keystrokes as it processes them.
- Keyboard overlays - a fake keypad is placed over the real one so that any keys pressed are registered by both the eavesdropping device as well as the legitimate one that the customer is using [2].

Countermeasures

Denial of physical access to sensitive computers, e.g. by locking the server room, is the most effective means of preventing hardware keylogger installation. Visual inspection is the easiest way of detecting hardware keyloggers. But there are also some techniques that can be used for most hardware keyloggers on the market, to detect them via software. In cases in which the computer case is hidden from view (e.g. at some public access kiosks where the case is in a locked box and only a monitor, keyboard, and mouse are exposed to view) and the user has no possibility

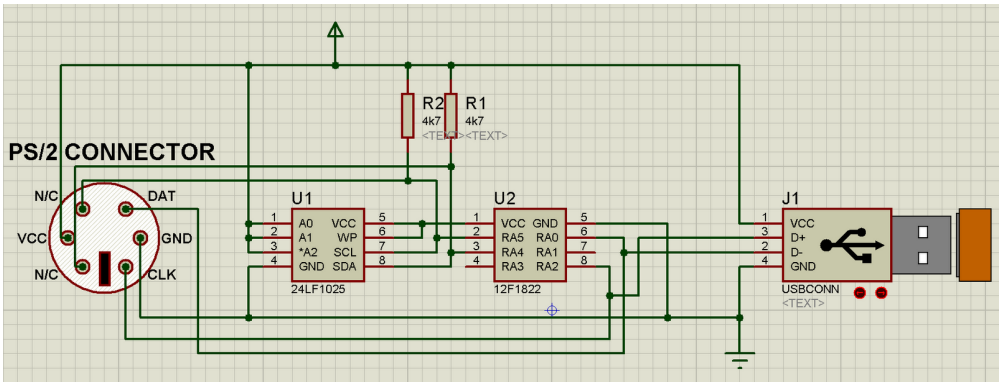

Figure 10. *Illustration of pedagogical philosophy concepts [??]*

to run software checks, a user might thwart a keylogger by typing part of a password, using the mouse to move to a text editor or other window, typing some garbage text, mousing back to the password window, typing the next part of the password, etc. so that the keylogger will record an unintelligible mix of garbage and password text [3].

The main risk associated with keylogger use is that physical access is needed twice: initially to install the keylogger, and secondly to retrieve it. Thus, if the victim discovers the keylogger, they can then set up a sting operation to catch the person in the act of retrieving it. This could include camera surveillance or the review of access card swipe records to determine who gained physical access to the area during the time period that the keylogger was removed.

Historical Remarks

An early keylogger was written by Perry Kivolowitz and posted to the Usenet news group net.unix-wizards,net.sources on November 17, 1983 [28]. The posting seems to be a motivating factor in restricting access to /dev/kmem on Unix systems. The user-mode program operated by locating and dumping character lists (clists) as they were assembled in the Unix kernel.

In the 1970s, spies installed keystroke loggers in the US Embassy and Consulate buildings in Moscow and St Petersburg [29,30]. They installed the bugs in Selectric II and Selectric III electric typewriters [31].

Soviet embassies used manual typewriters, rather than electric typewriters, for classified informationapparently because they are immune to such bugs [31]. As of 2013, Russian special services still use typewriters [30,32,33].

Cracking

Writing simple software applications for keylogging can be trivial, and like any nefarious computer program, can be distributed as a trojan horse or as part of a virus. What is not trivial for an attacker, however, is installing a covert keystroke logger without getting caught and downloading data that has been logged without being traced. An attacker that manually connects to a host machine to download logged keystrokes risks being traced. A trojan that sends keylogged data to a fixed e-mail address or IP address risks exposing the attacker.

Trojans

Researchers devised several methods for solving this problem. They presented a deniable password snatching attack in which the keystroke logging trojan is installed using a virus or worm [34,35]. An attacker who is caught with the virus or worm can claim to be a victim. The cryptotrojan asymmetrically encrypts the pilfered login/password pairs using the public key of the trojan author and covertly broadcasts the resulting ciphertext. They mentioned that the ciphertext can be steganographically encoded and posted to a public bulletin board such as Usenet.

Use by police

In 2000, the FBI used FlashCrest iSpy to obtain the PGP passphrase of Nicodemo Scarfo, Jr., son of mob boss Nicodemo Scarfo [36]. Also in 2000, the FBI lured two suspected Russian cyber criminals to the US in an elaborate ruse, and captured their usernames and passwords with a keylogger that was covertly installed on a machine that they used to access their computers in Russia. The FBI then used these credentials to hack into the suspects' computers in Russia in order to obtain evidence to prosecute them [37].

Countermeasures

The effectiveness of countermeasures varies, because keyloggers use a variety of techniques to capture data and the countermeasure needs to be effective against the particular data capture technique. For example, an on-screen keyboard will be effective against hardware keyloggers, transparency will defeat somebut not allscreenloggers and an anti-spyware application that can only disable hook-based keyloggers will be ineffective against kernel-based keyloggers.

Also, keylogger program authors may be able to update the code to adapt to countermeasures that may have proven to be effective against them.

Anti keyloggers

An anti keylogger is a piece of software specifically designed to detect keyloggers on a computer, typically comparing all files in the computer against a database of keyloggers looking for similarities which might signal the presence of a hidden keylogger. As anti keyloggers have been designed specifically to detect keyloggers, they have the potential to be more effective than conven-

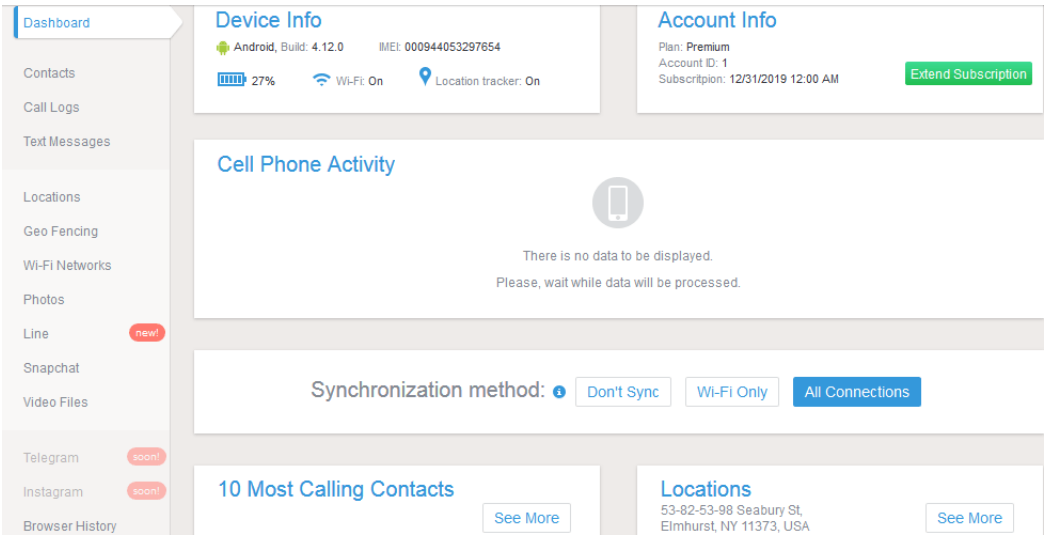

Figure 11. *Variety of E-Learning instructional methods and activities [??]*

tional anti virus software; some anti virus software do not consider a virus, as under some circumstances a keylogger can be considered a legitimate piece of software [38].

An anti-keylogger (or antikeystroke logger) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on your computer. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware); all keystroke-logging programs are flagged and optionally removed, whether they appear to be legitimate keystroke-logging software or not.

Use of anti-keyloggers

Keyloggers are sometimes part of malware packages downloaded onto computers without the owners' knowledge. Detecting the presence of a keylogger on a computer can be difficult. So-called anti- keylogging programs have been developed to thwart keylogging systems, and these are often effective when used properly.

Anti-keyloggers are used both by large organizations as well as individuals in order to scan for and remove (or in some cases simply immobilize) keystroke logging software on your computer. It is generally advised the software developers that anti-keylogging scans be run on a regular basis in order to reduce the amount of time during which a keylogger may record your keystrokes; for example, if you scan your system once every three days, there is a maximum of only three days during which a keylogger could be hidden on your computer and recording your keystrokes.

Public computers

Public computers are extremely susceptible to the installation of keystroke logging software and hardware, and there are documented instances of this occurring [1]. Public computers are particularly susceptible to keyloggers because any number of people can gain access to the machine and install both a hardware keylogger and a software keylogger, either or both of which can be secretly installed in a matter of minutes [2]. Anti-keyloggers are often used on a daily basis to ensure that public computers are not infected with keyloggers, and are safe for public use.

Gaming usage

Keyloggers have been prevalent in the online gaming industry, being used to secretly record a gamer's access credentials, user name and password, when logging into an account, this information is sent back to the hacker. The hacker can sign on later to the account and change the password to the account, thus stealing it.

World of Warcraft has been of particular importance to game hackers and has been the target of numerous keylogging viruses. Anti-keyloggers are used by many World of Warcraft and other gaming community members in order to try to keep their gaming accounts secure.

Financial institutions

Financial institutions have become the target of keyloggers, particularly those institutions which do not use advanced security features such as PIN pads or screen keyboards [4]. Anti-keyloggers are used to run regular scans of any computer on which banking or client information is accessed, protecting passwords, banking information, and credit card numbers from identity thieves.

Personal use

The most common use of an anti-keylogger is by individuals wishing to protect their privacy while using their computer; uses range from protecting financial information used in online banking, any passwords, personal communication, and virtually any other information which may be typed into your computer. Keyloggers are often installed by people you know, and many times have been installed by an ex-partner hoping to spy on their ex-

partner's activities, particularly chat [5].

Types

Signature-based

This type of software has a signature base, that is strategic information that helps to uniquely identify a keylogger, and the list contains as many known keyloggers as possible. Some vendors make some effort or availability of an up-to-date listing for download by customers. Each time you run a 'System Scan' this software compares the contents of your hard disk drive, item by item, against the list, looking for any matches.

This type of software is a rather widespread one, but it has its own drawbacks The biggest drawback of signature-based anti-keyloggers is that, while using them you can only be sure that you are protected from keyloggers found on your signature-base list, thus staying absolutely vulnerable to unknown or unrecognized keyloggers. A criminal can download one of many famous keyloggers, change it just enough and your anti-keylogger won't recognize it.

Heuristic analysis

This software doesn't use signature bases, it uses a checklist of known features, attributes, and methods that keyloggers are known use.

It analyzes the methods of work of all the modules in your PC, thus blocking the activity of any module that is similar to the work of keyloggers. Though this method gives better keylogging protection than signature-based anti-keyloggers, it has its own drawbacks. One of them is that this type of software blocks non-keyloggers also. Several 'non-harmful' software modules, either part of the operating system or part of legitimate apps, use processes which keyloggers also use, which can trigger a false positive. Usually all the non signature-based keyloggers have the option to allow the user to unblock selected modules, but this can cause difficulties for inexperienced users who are unable to discern good modules from bad modules when manually choosing to block or unblock.

Live CD/USB

Rebooting the computer using a Live CD or write-protected Live USB is a possible countermeasure against software keyloggers if the CD is clean of malware and the operating system contained on it is secured and fully patched so that it cannot be infected as soon as it is started. Booting a different operating system does not impact the use of a hardware or BIOS based keylogger.

Anti-spyware / Anti-virus programs

Many anti-spyware applications are able to detect some software based keyloggers and quarantine, disable or cleanse them. However, because many keylogging programs are legitimate pieces of software under some circumstances, anti spyware often neglects to label keylogging programs as spyware or a virus. These applications are able to detect software-based keyloggers based on patterns in executable code, heuristics and keylogger behaviours (such as the use of hooks and certain APIs).

No software-based anti-spyware application can be 100% effective against all keyloggers. Also, software-based anti-spyware cannot defeat non-software keyloggers (for example, hardware keyloggers attached to keyboards will always receive keystrokes before any software-based anti-spyware application).

However, the particular technique that the anti-spyware application uses will influence its potential effectiveness against software keyloggers. As a general rule, anti-spyware applications with higher privileges will defeat keyloggers with lower privileges. For example, a hook-based anti-spyware application cannot defeat a kernel-based keylogger (as the keylogger will receive the keystroke messages before the anti-spyware application), but it could potentially defeat hook- and API-based keyloggers.

Network monitors

Network monitors (also known as reverse-firewalls) can be used to alert the user whenever an application attempts to make a network connection. This gives the user the chance to prevent the keylogger from "phoning home" with his or her typed information.

Automatic form filler programs

Automatic form-filling programs may prevent keylogging by removing the requirement for a user to type personal details and passwords using the keyboard. Form fillers are primarily designed for web browsers to fill in checkout pages and log users into their accounts. Once the user's account and credit card information has been entered into the program, it will be automatically entered into forms without ever using the keyboard or clipboard, thereby reducing the possibility that private data is being recorded. However someone with physical access to the machine may still be able to install software that is able to intercept this information elsewhere in the operating system or while in transit on the network. (Transport Layer Security (TLS) reduces the risk that data in transit may be intercepted by network sniffers and proxy tools.)

One-time passwords (OTP)

Using one-time passwords may be keylogger-safe, as each password is invalidated as soon as it is used. This solution may be useful for someone using a public computer. However, an attacker who has remote control over such a computer can simply wait for the victim to enter his/her credentials before performing unauthorised transactions on their behalf while their session is active.

Security tokens

Use of smart cards or other security tokens may improve security against replay attacks in the face of a successful keylogging attack, as accessing protected information would require both the (hardware) security token as well as the appropriate password/passphrase. Knowing the keystrokes, mouse actions, display, clipboard etc. used on one computer will not subsequently help an attacker gain access to the protected resource. Some security tokens work as a type of hardware-assisted one-time password system, and others implement a cryptographic challenge-response authentication, which can improve security in a manner conceptually similar to one time passwords. Smartcard readers and their associated keypads for PIN entry may be vulnerable to keystroke logging through a so-called supply chain attack where an attacker substitutes the card reader/PIN entry hardware for one which records the user's PIN.

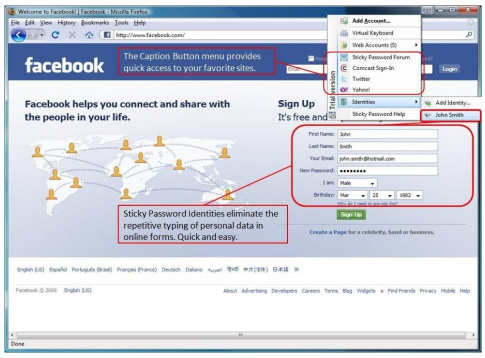

Figure 12. *Variety of E-Learning instructional methods and activities [??]*

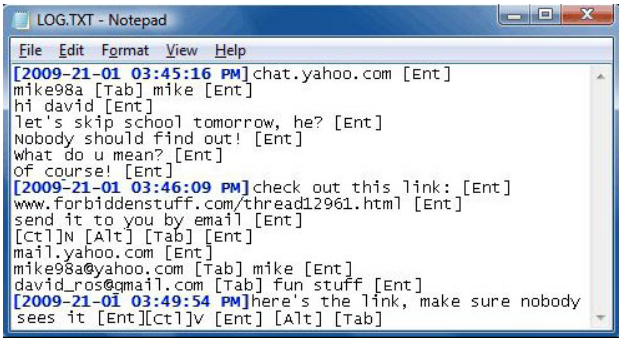

Figure 13. *Variety of E-Learning instructional methods and activities [??]*

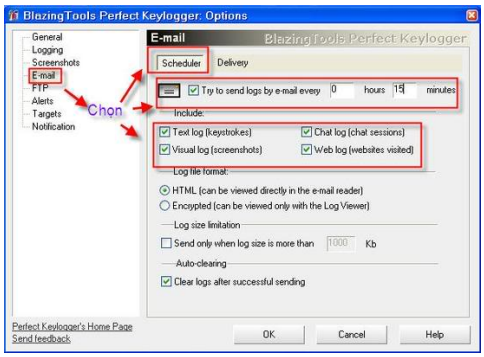

Figure 14. *Variety of E-Learning instructional methods and activities [??]*

On-screen keyboards

Most on-screen keyboards (such as the on-screen keyboard that comes with Windows XP) send normal keyboard event messages to the external target program to type text. Software key loggers can log these typed characters sent from one program to another [40]. Additionally, keylogging software can take screenshots of what is displayed on the screen (periodically, and/or upon each mouse click), which means that although certainly a useful security measure, an on-screen keyboard will not protect from all keyloggers.

Keystroke interference software

Keystroke interference software is also available [41]. These programs attempt to trick keyloggers by introducing random keystrokes, although this simply results in the keylogger recording more information than it needs to. An attacker has the task of extracting the keystrokes of interestthe security of this mechanism, specifically how well it stands up to cryptanalysis, is unclear.

Speech recognition

Similar to on-screen keyboards, speech-to-text conversion software can also be used against keyloggers, since there are no typing or mouse movements involved. The weakest point of using voice-recognition software may be how the software sends the recognized text to target software after the recognition took place.

Handwriting recognition and mouse gestures

Also, many PDAs and lately tablet PCs can already convert pen (also called stylus) movements on their touchscreens to computer understandable text successfully. Mouse gestures use this principle by using mouse movements instead of a stylus. Mouse gesture programs convert these strokes to user-definable actions, such as typing text. Similarly, graphics tablets and light pens can be used to input these gestures, however these are less common everyday.

The same potential weakness of speech recognition applies to this technique as well.

Macro expanders/recorders

With the help of many programs, a seemingly meaningless text can be expanded to a meaningful text and most of the time context-sensitively, e.g. ”en.wikipedia.org” can be expanded when a web browser window has the focus. The biggest weakness of this technique is that these programs send their keystrokes directly to the target program. However, this can be overcome by using the ’alternating’ technique described below, i.e. sending mouse clicks to non-responsive areas of the target program, sending meaningless keys, sending another mouse click to target area (e.g. password field) and switching back-and-forth.

Non-technological methods

Alternating between typing the login credentials and typing characters somewhere else in the focus window [42] can cause a keylogger to record more information than they need to, although this could easily be filtered out by an attacker. Similarly, a user

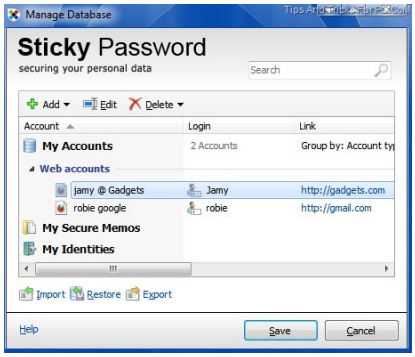

Figure 15. *Variety of E-Learning instructional methods and activities [??]*

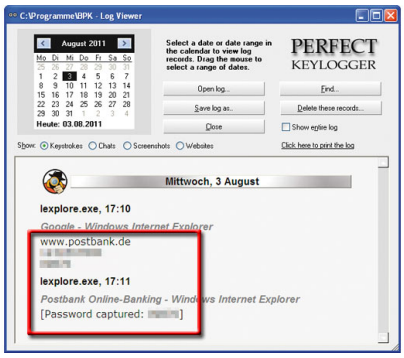

Figure 16. *Variety of E-Learning instructional methods and activities [??]*

can move their cursor using the mouse during typing, causing the logged keystrokes to be in the wrong order e.g., by typing a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter. Lastly, someone can also use context menus to remove, cut, copy, and paste parts of the typed text without using the keyboard. An attacker who is able to capture only parts of a password will have a smaller key space to attack if he chose to execute a brute-force attack.

Another very similar technique uses the fact that any selected text portion is replaced by the next key typed. e.g., if the password is ”secret”, one could type ”s”, then some dummy keys ”asdfsd”. Then, these dummies could be selected with the mouse, and the next character from the password ”e” is typed, which replaces the dummies ”asdfsd”.

These techniques assume incorrectly that keystroke logging software cannot directly monitor the clipboard, the selected text in a form, or take a screenshot every time a keystroke or mouse click occurs. They may however be effective against some hardware keyloggers.

Summary

In this article a bibliographic overview of keyloggers is given and relevant hardware, software in use is described.

The functionalities, availability, detection possibilities of keyloggers are described and reviewed.

References

[1] ”Keylogger”. Oxford dictionaries.

[2] ”What is a Keylogger?”. PC Tools.

[3] ”The Evolution of Malicious IRC Bots” (PDF). Symantec. 2005-11-26: 2324. Retrieved 2011-03-25.

[4] Jonathan Brossard (2008-09-03). ”Bypassing pre-boot authentication passwords by instrumenting the BIOS keyboard buffer (practical low level attacks against x86 pre-boot authentication software)” (PDF). Iviz Technosolutions. Retrieved 2008-09-23. External link in —publisher= (help)

[5] ”SpyEye Targets Opera, Google Chrome Users”. Krebs on Security. Retrieved 26 April 2011.

[6] K.P.H. Sullivan & E. Lindgren (Eds., 2006), Studies in Writing: Vol. 18. Computer Key-Stroke Logging and Writing: Methods and Applications. Oxford: Elsevier.

[7] V. W. Berninger (Ed., 2012), Past, present, and future contributions of cognitive writing research to cognitive psychology. New York/Sussex: Taylor & Francis. ISBN 9781848729636

[8] Vincentas (11 July 2013). ”Keystroke Logging in SpyWareLoop.com”. Spyware Loop. Retrieved 27 July 2013.

[9] Microsoft. ”EM-GETLINE Message()”. Microsoft. Retrieved 2009-07-15.

[10] ”Apple keyboard hack”. Apple keyboard hack. Digital Society. Retrieved 9 June 2011.

[11] ”Keyghost”. keyghost.com. Retrieved 2009-04-19. External link in —publisher= (help)

[12] ”Keylogger Removal”. Keylogger Removal. SpyReveal Anti Keylogger. Retrieved 25 April 2011.

[13] ”Keylogger Removal”. Keylogger Removal. SpyReveal Anti Keylogger. Retrieved 26 February 2016.

[14] Jeremy Kirk (2008-12-16). ”Tampered Credit Card Terminals”. IDG News Service. Retrieved 2009-04-19.

[15] Andrew Kelly (2010-09-10). ”Cracking Passwords using Keyboard Acoustics and Language Modeling” (PDF).

[16] Sarah Young (14 September 2005). ”Researchers recover typed text using audio recording of keystrokes”. UC Berkeley NewsCenter.

[17] ”Remote monitoring uncovered by American techno activists”. ZDNet. 2000-10-26. Retrieved 2008-09-23.

[18] Martin Vuagnoux and Sylvain Pasini (2009-06-01). ”Compromising Electromagnetic Emanations of Wired and Wireless Keyboards”. Lausanne: Security and Cryptography Laboratory (LASEC).

[19] ”ATM camera”. snopes.com. Retrieved 2009-04-19. External link in —publisher= (help)

[20] Maggi, Federico; Volpatto, Alberto; Gasparini, Simone; Boracchi, Giacomo; Zanero, Stefano (2011). A fast eavesdropping attack against touchscreens. 7th International Conference on Information Assurance and Security. IEEE. doi:10.1109/ISIAS.2011.6122840.

[21] Marquardt, Philip; Verma, Arunabh; Carter, Henry; Traynor, Patrick (2011). (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. Proceedings of the 18th ACM conference on Computer and communications security. ACM. pp. 561562. doi:10.1145/2046707.2046771.

[22] ”iPhone Accelerometer Could Spy on Computer Keystrokes”. Wired. 19 October 2011. Retrieved August 25, 2014. External link in —publisher= (help)

[23] Owusu, Emmanuel; Han, Jun; Das, Sauvik; Perrig, Adrian; Zhang, Joy (2012). ACCessory: password inference using accelerometers on smartphones. Proceedings of the Thirteenth Workshop on Mobile Computing Systems and Applications. ACM. doi:10.1145/2162081.2162095.

[24] Aviv, Adam J.; Sapp, Benjamin; Blaze, Matt; Smith, Jonathan M. (2012). Practicality of accelerometer side channels on smartphones. Proceedings of the 28th Annual Computer Security Applications Conference. ACM. doi:10.1145/2420950.2420957.

[25] Cai, Liang; Chen, Hao (2011). TouchLogger: inferring keystrokes on touch screen from smartphone motion (PDF). Proceedings of the 6th USENIX conference on Hot topics in security. USENIX. Retrieved 25 August 2014.

[26] Xu, Zhi; Bai, Kun; Zhu, Sencun (2012). TapLogger: inferring user inputs on smartphone touchscreens using on-board

motion sensors. Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. ACM. pp. 113124. doi:10.1145/2185448.2185465.
[27] Miluzzo, Emiliano; Varshavsky, Alexander; Balakrishnan, Suhrid; Choudhury, Romit Roy (2012). Tapprints: your finger taps have fingerprints. Proceedings of the 10th international conference on Mobile systems, applications, and services. ACM. pp. 323336. doi:10.1145/2307636.2307666.
[28] "The Security Digest Archives". Retrieved 2009-11-22.
[29] "Soviet Spies Bugged World's First Electronic Typewriters". qccglobal.com.
[30] Geoffrey Ingersoll."Russia Turns To Typewriters To Protect Against Cyber Espionage". 2013.
[31] Sharon A. Maneki."Learning from the Enemy: The GUNMAN Project". 2012.
[32] Agence France-Presse, Associated Press. "Wanted: 20 electric typewriters for Russia to avoid leaks". inquirer.net.
[33] Anna Arutunyan."Russian security agency to buy typewriters to avoid surveillance".
[34] Young, Adam; Yung, Moti (1997). "Deniable Password Snatching: On the Possibility of Evasive Electronic Espionage". Proceedings of IEEE Symposium on Security and Privacy. IEEE: 224235. doi:10.1109/SECPRI.1997.601339.
[35] Young, Adam; Yung, Moti (1996). "Cryptovirology: extortion-based security threats and countermeasures". Proceedings of IEEE Symposium on Security and Privacy. IEEE: 129140. doi:10.1109/SECPRI.1996.502676.
[36] John Leyden (2000-12-06). "Mafia trial to test FBI spying tactics: Keystroke logging used to spy on mob suspect using PGP". The Register. Retrieved 2009-04-19.
[37] John Leyden (2002-08-16). "Russians accuse FBI Agent of Hacking". The Register.
[38] Theron, Kristen (19 February 2016). "What is Anti Keylogger".
[39] Austin Modine (2008-10-10). "Organized crime tampers with European card swipe devices". The Register. Retrieved 2009-04-18.
[40] Scott Dunn (2009-09-10). "Prevent keyloggers from grabbing your passwords". Windows Secrets. Retrieved 2014-05-10.
[41] Christopher Ciabarra (2009-06-10). "Anti Keylogger". Networkintercept.com.
[42] Cormac Herley and Dinei Florencio (2006-02-06). "How To Login From an Internet Cafe Without Worrying About Keyloggers" (PDF). Microsoft Research. Retrieved 2008-09-23.
[43] "Keyloggers found plugged into library computers". SC Magazine. Retrieved 25 April 2011.
[44] "Anti Keylogging & Public Computers". Anti Keylogging & Public Computers. Archived from the original on 22 May 2011. Retrieved 10 May 2011.
[45] "Cyber threat landscape faced by financial and insurance industry". Dr Kim-Kwang Raymond Choo. Retrieved 21 February 2011.
[46] "Privacy Watch: More Criminals Use Keystroke Loggers". Privacy Watch: More Criminals Use Keystroke Loggers. PC World About.
[47] "Is someone you know spying on you?". USA Today. 4 March 2010. Retrieved 25 April 2011.
[48] "Keyloggers, pros and cons". BCS.
[49] Jeremy Kirk (2008-12-16). "Tampered Credit Card Terminals". IDG News Service. Retrieved 2009-04-19.
[50] Hardware Keylogger Detection, SpyCop.