Keyloggers

Increasing Threats to Computer Security and Privacy

SEREF SAGIROGLU AND GUROL CANBEK

Digital Object Identifier 10.1109/MTS.2009.934159

In the early days, idealistic hackers attacked computers because they could, or to show off to each other. But today, cracking computers has become an industry. In spite of recent improvements in computer hardware and software security, attacks on computer systems have increased in both frequency and complexity.

Community Emergency Response Team Coordination Center (CERT/CC) Statistics in 2007 indicated that total cataloged vulnerabilities increased to over 8000, almost 8 times more than in 2000 [39]. The Information Security Breaches Survey 2006 reported that viruses and malicious software (malware) together caused the highest breaches ever in U.K. businesses [40]. Cyveillance trending data shows that the average number of URLs detected with malware averaged less than 20 000 per day in December 2006. By February 2007, this average had grown to approximately 60 000 [46]. The Microsoft Security Intelligence Report in December 2007 demonstrated an in-depth perspective on the recent threats including software vulnerability disclosures and exploits, malware, and potentially unwanted software, especially a rising number of Trojan based attacks [32]. In 2008, F-Secure reported malware growth at a higher level than ever before. The number of different malware threats reached 900 000 at the end of June 2008 [33]. Spyware is reportedly the fourth greatest threat to enterprise security [44]. New malware is emerging at a frightening rate, and there are over a thousand new malicious code threats coming out every day [45].

Unfortunately, existing techniques for detecting malware and analyzing unknown code samples have significant shortcomings [34]. We focus on a particular kind of malware, keyloggers. Keyloggers have become an increasingly serious problem because they are largely undetectable by most antiviral solutions [2], [5], [7], [9], [12], [32].

Keyloggers are known variously as tracking software, computer activity monitoring software, keystroke monitoring systems, keystroke recorders, keystroke loggers, keyboard sniffers, and snoopware [1]–[8]. Although the main purpose of keyloggers is to monitor a user's keyboard actions, they now have capabilities that extend beyond that function. They can track virtually anything running on a computer. Some keyloggers, known as "screen scrapers," enable the visual surveillance of a target computer by taking periodic snapshots of the screen. The captured images can then be used to gather valuable information about the user. Advanced keyloggers can track such things as cut, copy, and paste operations, Internet usage, file operations (executing, creating, renaming, modifying, and deleting), and printouts. Keyloggers are also used for monitoring users' behaviors, and for gathering information such as personally-identifiable or otherwise private or critical information [4].

Keyloggers are different from other types of spyware or malware such as viruses and worms. They share the system resources (e.g., CPU and memory) with legitimate programs, stay resident on the system invisibly for as long as is required, and are carefully and simply designed to do their tasks without attracting the attention of users.

The Symantec Internet Security Threat Report stated that keystroke logging threats in 2006 made up 79% of all confidential information threats, up from 57% in the first half of 2006 and from 66% in the second half of 2005 [6]. Despite organizations having anti-virus software, anti-spyware, and firewalls, instances of corporate spyware based on keystroke logging also recorded significant growth. The Websense Web@ Work Survey 2006 showed that the growth in instances of keyloggers had increased [7], and the survey also demonstrated that websites hosting keyloggers in 2005–2006 had also increased from 260 to 2157.

There are some legitimate uses of keyloggers, some of which are discussed later in this article. But keyloggers are currently a favorite tool of hackers. iDefense, the cyber-security intelligence provider and a VeriSign company, released data indicating that in 2005, hackers were on pace to unleash a record-setting 6191 keyloggers, a 65% increase since the 3753 keyloggers reported in 2004 [5].

Most of the studies on attack prevention focus on machine-to-machine interface security. The security of man-to-machine interfaces is usually ignored or overlooked [1]. Indeed, ensuring a secure channel of data communication in local or wide-area networks and the Internet is crucial.

Keyloggers monitor many different computer-based activities. Users' keystrokes or other activities within operating systems are stored and/or transferred in local or remotely accessed disks via keyloggers. In most cases, keyloggers send the keystroke logs to the attackers by email. Even though keyloggers were originally surveillance tools, today's keyloggers are more sophisticated and have complicated functionality including concealment, data gathering, communicating, surviving, reporting, and monitoring.

A recent study in Security and Cryptography Laboratory (LASEC/EPFL) in Switzerland has reported four different ways to fully or partially recover keystrokes from wired keyboards at distances up to 20 m, even through walls [11]. The work was based on acquiring the signal directly from the antenna and works on the whole captured electromagnetic spectrum. Twelve different wired and wireless keyboard models including PS/2, USB, and laptops were tested. The study reported and demonstrated in a videoclip that

all the models are vulnerable to at least one of four attacks. The study concluded that wired and wireless computer keyboards are not safe to transmit information.

Keyloggers can be mainly classified into two categories: hardware and software.

Hardware Keyloggers

Hardware keyloggers are small electronic devices used for capturing the data in between a keyboard device and I/O port. They store the keystrokes in their built-in memory after being mounted in a computer system. There are a number of commercial hardware keylogger products available [41]. Most models are plugged into the end of the keyboard cable while others are installed inside the computer case, inside the keyboard port, or directly inside the keyboard itself. This hardware does not use any computer resource. It cannot be detected by anti-viral software or scanners since it works on the hardware platform. It also does not use the computer's hard disk to store the keystroke logs. The captured keystrokes can be stored in encrypted form in its own memory, which generally exceeds 2MB. A hardware keylogger costs about $50–150. Some keyboards are even designed with built-in hardware keylogger functionalities [10], and even though it has not yet been reported, it would be possible to design special keylogger hardware that is supported by Bluetooth technologies as well. Compared to software keyloggers, the major disadvantage of hardware keyloggers is that they require physical installation in the keyboard or computer case.

An acoustic keylogger, a kind of hardware keylogger, was introduced to transmit keystrokes using the enhanced encoding scheme [36]. This is achieved by analyzing the repetition frequency of similar acoustic keystroke signatures, the timing between different keyboard strokes, and other context information. This keylogger is potentially more conspicuous than a traditional keylogger since it consumes a computer's processor resources during data transmission, and because it causes the machine's internals to emit faint, structured sounds. It is demonstrated in [36] how this can be achieved with an inexpensive and easily-concealed microphone.

Software Keyloggers

Software keyloggers track systems that collect keystroke data within the target operating system, store them on disk or in remote locations, and send them to the attacker who installed the keylogger.

A total of 540 keyloggers, mostly software-based, were reported in a project dedicated to the removal of spyware parasites [8]. Commercial software keyloggers are readily available on the Internet market while the parasitical ones are produced or used by hackers. There are many real-life cases in which keyloggers have been involved [9].

Monitoring methods for software keyloggers are operating-system-specific [2] and [13]. Windows operating systems (WOS) contain an event mechanism. When a user presses a key in the WOS, the keyboard driver of the operating system translates a keystroke into a Windows message called WM_KEYDOWN. This message is pushed into the system message queue. The WOS 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. This kind of messaging mechanism works for other events like mouse messages.

There are four main methods for developing keylogger systems [2]: the Keyboard State Table method, the Windows Keyboard Hook method, the Kernel-Based Keyboard Filter Driver method, and Creative methods.

Keyboard State Table Method

In WOS, every application that uses a window interface refers to a table showing the status of 256 virtual keys. This table is normally used by applications for determining the other key states at the same time. For example, a key may be pressed with Ctrl or Shift key. A keylogger can use the GetKeyboardState API function to reveal the keystroke information as shown in Fig. 1, by attaching its thread to the top-level window's thread message loop using AttachThreadInput API.

Windows Keyboard Hook Method

Hook-based keyloggers monitor the keyboard with functions provided by the operating system (OS). The OS warns any time a key is pressed and it records the action. Windows hooks are unique to Windows message mechanisms. Fig. 2 shows a block diagram of this method. An application can register (hook) itself into this point so that any message flowing in this mechanism is passed to the application before going to the original target that receives the message. WOS maintains these mechanisms as a hook chain for each hook type. Today, most keyloggers use this technique to capture keystrokes.

Hooks have robust capabilities related to Windows messages and can be classified into two distinct types. Global hooks monitor system-wide messages, and local hooks monitor application-specific messages. A keyboard hook can:

- read all keyboard messages and pass them to the next hook procedure in a chain,
- modify the original message and pass it to the next hook procedure,
- interrupt the message flow by not passing it to the next hook procedure.

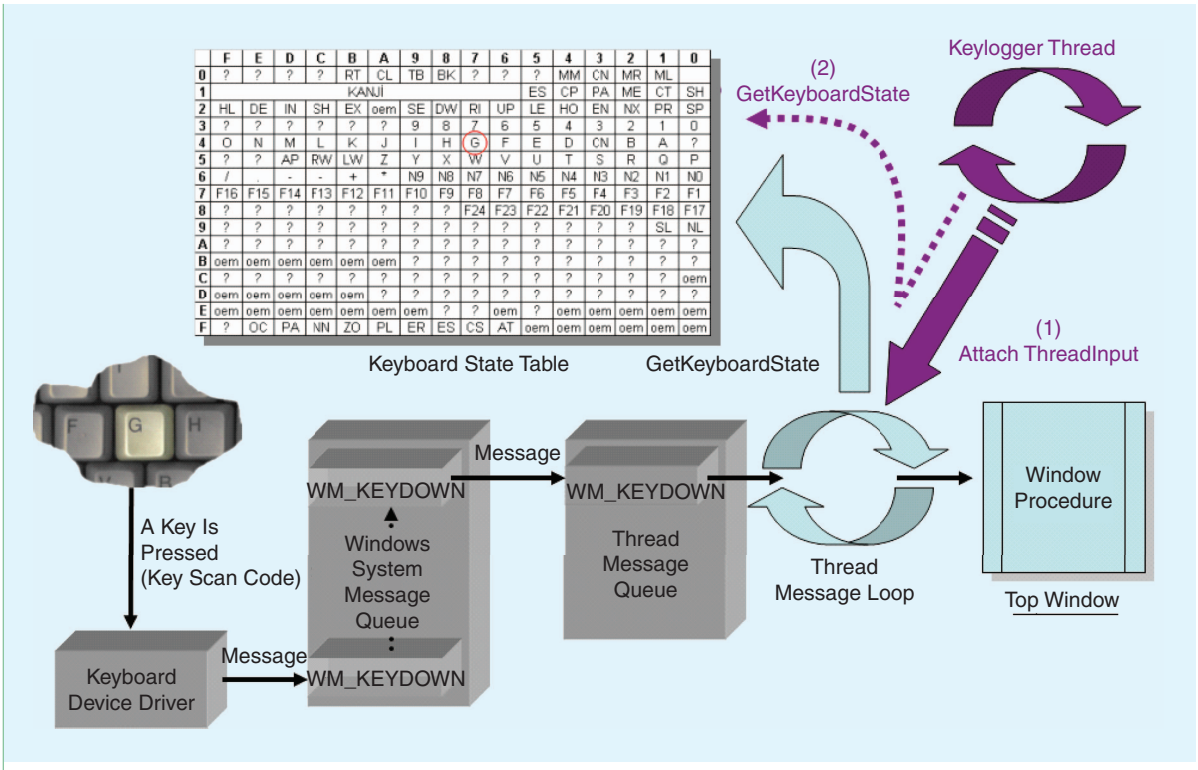

Fig. 1. Block representation of keyboard state table method.

Generally, keyloggers using a Windows monitoring mechanism capture keystroke messages by monitoring the keyboard hook chain and passing the message to the next hook procedure in the chain.

Kernel-Based Keyboard Filter Driver Method

The keyloggers using this method reside at the kernel level and are thus practically invisible. It is more advanced than the two methods introduced earlier. These keyloggers are difficult to implement, difficult to detect, and administrator privileges are required to install them on a target machine. In this method, a keyboard filter driver is installed

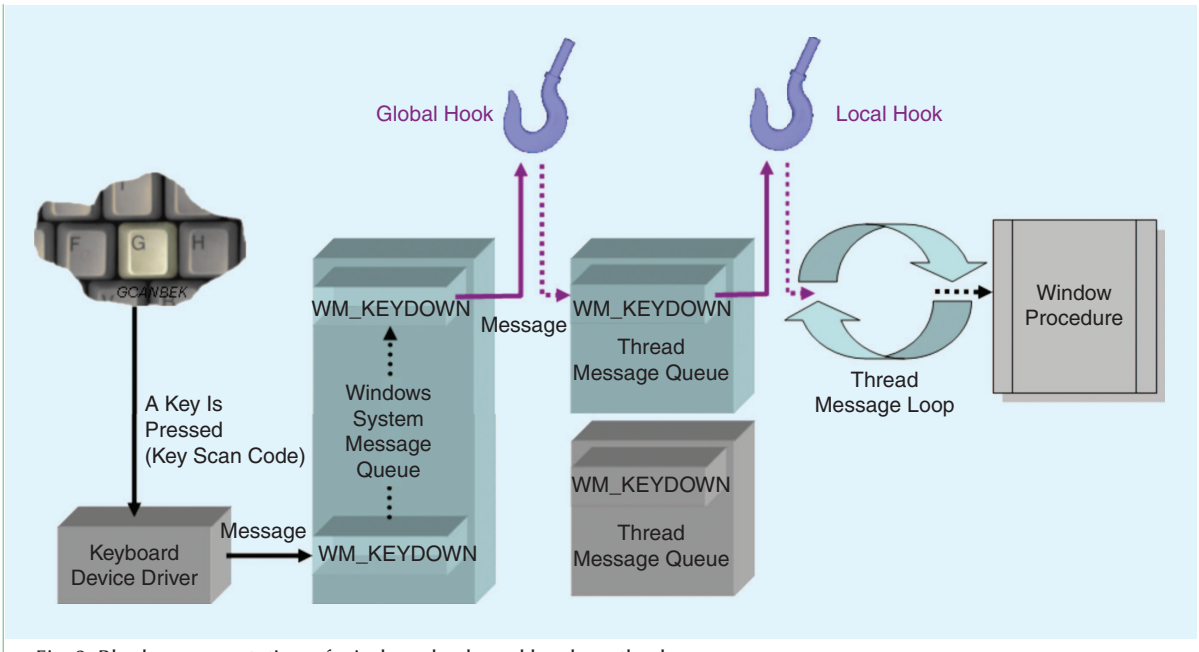

Fig. 2. Block representation of windows keyboard hook method.

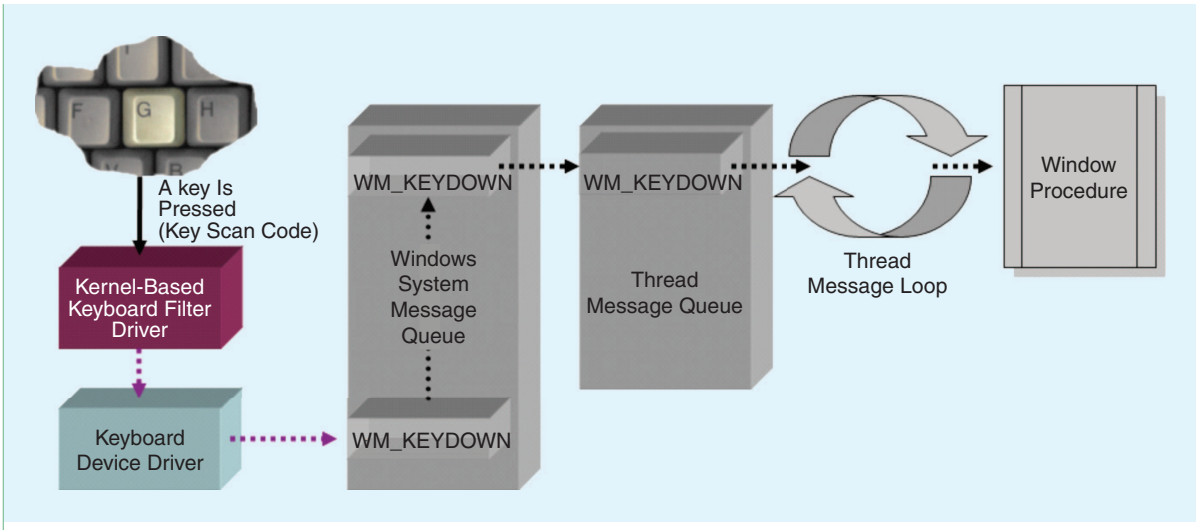

Fig. 3. Kernel-based keyboard filter driver method.

by a keylogger before the system's keyboard device driver, as shown in Fig. 3. This kind of keylogger captures the keystrokes even before the operating system.

Creative Methods

In addition to the three methods introduced earlier, creative keylogger coders are constantly developing keyloggers requiring less memory space, less CPU usage, and less interference with other software. The development of these new methods is ongoing, and will not be discussed further here.

Software keyloggers have a number of functionalities [12]. Here is only a partial list of some of the information keyloggers sense, record, and transmit:

- any keystroke typed by the user;
- mouse actions (clicks and movements);
- title of windows opened or focused;
- periodic or event-triggered screen snapshots;
- applications run and usage statistics;
- file system operations (create, rename, modify, access, and delete);
- internet usage (visited pages and per-page duration of visit);
- emails sent, received, and even unsent;
- both side of chats and instant message conversations;
- programs installed and uninstalled;
- clipboard operations (text and image copied);
- modifications within the system registry;
- document printouts;
- windows operating system session start dates, end dates and times (logon/logoff);
- sound record using the system microphone;
- video record using Web Cam if it is installed;
- CD, DVD, USB media usage;
- MAC, IP addresses; or
- keyword and password capturing including system logon password.

Keyloggers in Action

Keyloggers can be used for many purposes to meet different requirements of different users including officials from governmental, military, and law-enforcement organizations, computer security experts, employers, managers, parents, teachers, and couples [13]–[18]. Most keyloggers are used for gathering secret information and for identity theft, and these uses are illegal. But there are also legitimate uses such as intrusion detection, computer forensics by the police, parental monitoring, workplace monitoring and surveillance, and disaster recovery.

Spying and Gathering Secret Information

Software keyloggers are an instance of spyware. Since keystrokes are the basic communication tool between a user and a computer, keystroke monitoring systems are effective for information spying on employees, children, spouses, teachers, and students. The availability of such technology may be extremely harmful [19]. Outsiders or insiders might use a keylogger to steal credit card information. Corporate espionage can be facilitated by using keyloggers as a secret information-gathering tool for companies. In fact, it is quite common for some companies to use technology such as this to gather important information about their competitors [20]. Keyloggers can be effectively used by companies to reveal trade secrets, tactics, costumer records, and business contacts. Family members can use keyloggers in the home to secretly monitor other family members' computer use.

Identity Theft

Electronic or online identity theft is defined as gathering personal information using the Internet or

computer systems in order to use it for illegal actions such as economic fraud. Identity theft can be extremely damaging and is on the increase. It is reported in [21] that identity theft cost the U.S. $52.6 billion in 2005 alone. Although a large percentage of these thefts resulted from traditional methods such as lost or stolen checkbooks and credit cards, spyware-generated theft was reported as 5.2%. The information required for identity theft includes bank account information, online banking passwords, credit card information, and social security numbers [12], all of which is vulnerable to keylogger attacks.

Intrusion Detection and Computer Forensics

It is possible to use keystroke monitoring systems to detect physical intrusion on computer systems [22]. The records logged by the systems can reveal all the activities that took place during the intrusion. We know that law enforcement agencies are successfully using keystroke monitoring techniques to fight crime [23] and to capture forensic-quality evidence in order to support their cases [24].

Parental Monitoring

Shields and Behrman note that many children spend more than four hours per day using their home computers [25]. Even though some people consider it unethical for parents to use keyloggers to monitor their children, the need for parental monitoring is acute because of the risk in online environments including inappropriate material (sexual, violent, illegal, dangerous), communicating with malicious people, physical abuse, and negative legal and financial consequences [26], [27].

Workplace Monitoring and Surveillance

Even though there are objections to monitoring employees [42], employers and managers are constantly looking for ways to control and monitor employees for efficiency, success, and security. They are concerned about everything from personal emails, game playing, and web-browsing during office hours, to protecting intellectual property. In general, they are keen on increasing productivity and profits. Several technologies are designed and used for workplace surveillance including entry access, electronic badge tracking, video surveillance, phone and email accounting systems, and phone-call recorders [28]. A survey on workplace surveillance conducted by the American Management Association shows that the use of different workplace surveillance technologies had increased in 2005 to 76% in comparison to 2001, as shown in Table I [29].

Keystroke monitoring systems can be modified to meet different workplace surveillance requirements. They also can be also used for the electronic performance-monitoring of employees using computer systems. However, there are many ethical issues related to electronic workplace surveillance, such as privacy, disclosure, and consent. This kind of surveillance may also affect the health of employees and contribute to a growth in employee psychological problems [13].

CERT-CC first issued advice on keystroke monitoring in 1992, based on legal advice from the U.S. Department of Justice [18]. According to CERT, legitimate keystroke monitoring systems must show a banner advising users that logging into and using the system constitutes consent to monitoring. Any decision to use high-level electronic surveillance systems such as keystroke monitoring systems must therefore be made only after comprehensive analysis of the possible effects, both positive and negative.

Personal Use of Keyloggers Can Be Beneficial

The use of a keylogger may help a private computer owner to enhance daily productivity and security. A keylogger makes it possible to recover text typed into word processors, spreadsheets, and computer programming environments after an application or system crash. The text can be accessed even after the original files have been deleted either deliberately or accidentally. The keylogger works like an automatic diary in your computer. Valuable information can be retrieved such as forgotten passwords for websites and forgotten Internet addresses recently visited. With a personal keylogger installed on a computer,

Table I
Forms of Electronic Monitoring and Surveillance [29]

Workplace Surveillance	2001 (%)	2005 (%)
Recording & reviewing telephone conversations	11.9	19
Storing & reviewing voicemail messages	7.8	15
Storing & reviewing computer files	36.1	50
Storing & reviewing email messages	46.5	55
Monitoring Internet connections	62.8	76
Video recording of employee job performance	15.2	20
Telephone usage (time spent, numbers called)	43.3	51
Computer usage (duration, keystroke counts, etc.)	18.9	21
Video surveillance for security purposes	37.7	51
Total, all forms of e-monitoring and/or surveillance	82.2	N/A

> Standard security measures for machine-to-machine interfaces do not protect computer systems from keylogger attacks.

it is possible for the computer owner to detect whether someone else has used that computer and what the intruder did.

Protecting Computers from Keyloggers

Measures to detect keyloggers are essential to protect personal or institutional information assets. Computer users should know how to recognize the existence of keyloggers installed in their computers. Some of general indicators are [2]:

- Alerts from firewalls, anti-spyware, anti-keyloggers, and anti-virus programs.
- Some keys don't work properly.
- It takes time for a character to appear on the screen after a key is pressed.
- Mouse clicks don't always function.
- Double clicks and drag-drop operations behave strangely.

If any of these signs appear even after restarting a system, it is likely that a keylogger exists in the computer system. Users should always keep in mind the threats of keyloggers while entering critical information through a keyboard. Even if applications such as online banking or online shopping present virtual keyboards to enter personal information, virtual keyboards do not completely protect the users's personal information. It should not be forgotten that some advanced keyloggers can take screenshots based on mouse clicks to reveal critical information [2].

It is crucial to install anti-spyware and anti-keylogger software. Anti-keylogger software uses Application Programming Interface (API) monitoring techniques such as proxy DLL and Import Address Table (IAT) patching. These methods can detect keyloggers using the Windows Hook and Keyboard State Table methods. Driver signing and Integrity Protection Driver (IPD) can be used against keyloggers using the Kernel-Based Keyboard Filter Driver method [2].

Users can learn more about keyloggers by visiting web sites such as OnGuardOnLine [37] or www.keylogger.org. The preventive steps given in [2], [30], [35], [37], [42]–[44] are summarized as:

- Audit computer logs from time to time, and don't let anybody else view them.
- Always be aware of any activity on your computer.
- Use other prevention techniques such as firewalls, anti-virus, anti-spyware and anti-spam tools.
- Never leave others alone with your computer.
- Always be aware of signs of keyloggers and activity monitoring systems.
- Use on-screen keyboards.
- Keep security patches up to date.
- Only download programs from trusted websites.
- Read all security warnings, license agreements, and privacy statement pop-ups.
- Use one or more anti-spyware tools to detect and remove spyware, malware, and viruses.
- Only use licensed software.
- Always keep up-to-date about new threats.
- Explicitly Restrict OS privileges.
- Have a strong password policy.
- Do not connect to the Internet or even to an internal network while logged in to the computer as an administrator.
- Inspect your computer's keyboard port to see if a hardware keylogger is attached.
- Monitor the PS/2 keyboard timeout bit (BIT6 at port 100).
- Use alternative keyboard layouts supported by keyboard layout creator.
- Use smart cards if possible.
- Use one-time passwords (OTP) if possible.
- Use an automatic form filler program.
- Monitor the legal status of spyware.

Other measures that have been suggested to help protect users from some keylogger vulnerabilities include using wireless, infrared, Bluetooth, or laser keyboards, virtual keyboards, and touch-screen monitors. However, these measures may incur their own risks.

Computer users should also consider using technologies such as BlueGem Security as introduced in *Computer News Briefs*, October 2005 [31]. This technology uses LocalSSL encryption to prevent hackers from using keylogger tools to intercept and view user keystrokes. LocalSSL protects transmissions with 128-key encryption by bypassing the operating system. Another suggestion was introduced by Baig and Muhammad that a virtual keyboard application could bypass the system message queue and to post the keyboard messages directly to a specific application message queue using an application-level hook [38]. After receiving these keyboard messages, the application performs the appropriate actions as if it received the actual hardware interrupt through the system message queue. The system-level message queue is bypassed through this, and no known software keylogger will be able to capture the strokes [38].

Powerful Tools

Keyloggers are powerful tools that can perform many tasks. Although

some keylogger uses are legitimate, many (perhaps most) keyloggers are used illegally.

Standard security measures for machine-to-machine interfaces do not protect computer systems from keylogger attacks. Human-to-machine interfaces must be considered to combat keylogger intrusions.

It is expected that the threats of keyloggers will arise more and more. Users should be aware of this high risk of using computers and follow preventive steps.

Even though there are documents, materials, and websites about keyloggers, unfortunately there is not enough information, especially about emerging threats.

The most effective way to reduce security risks is to use a complete security solution dealing with a wide range of threats.

The judicious use of keyloggers by employers and computer owners could, in some situations, improve security, privacy, and efficiency. But the possible positive effects must be balanced against the possible negative effects on employees, users, and children.

Author Information

The authors are with the Department of Computer Engineering, Faculty of Engineering & Architecture, Gazi University, Maltepe 06570, Ankara, Turkey; email: ss@gazi.edu.tr.

References

[1] W. Fabian, "Beyond cryptography: Threats before and after," in *Proc. Int. Carnahan Conf. on Security Technology*, 1998, pp. 97–107.

[2] 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.

[3] J. Wurtzel, "Bugging your keyboard," *BBC News, Science/Nature*; http://news.bbc.co.uk/1/hi/sci/tech/1638795.stm, accessed Sept. 2006.

[4] Anti-Spyware Coalition, "Spyware definitions and supporting documents," *ASC, working rep.*, June 29, 2006; http://www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf; accessed Sept. 2007.

[5] "iDefense tracks dramatic growth in password-stealing keyloggers," *VeriSign*; http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_036258.html, accessed Sept. 2007.

[6] Symantec, "Trends for July–December 06," *Symantec Internet Security Threat Report*, vol. XI, Mar. 2007; http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

[7] M. Kotadia, "Keylogger spying at work on the rise, survey says," *CNET News.com*, May 2006; http://news.com.com/Keylogger+spying+at+work+on+the+rise,+survey+says/2100-7355_3-6072948.html.

[8] "List of keyloggers parasites," *Dedicated 2 Spyware*, http://www.2-spyware.com/keyloggers-removal; accessed Sept. 2007.

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

[10] M.A. Caloyannides, "Privacy protection and computer forensics," Artech House, p. 57, 2004.

[11] M. Vuagnoux, and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," Security and Cryptography Laboratory (LASEC); http://lasecwww.epfl.ch/keyboard/, accessed Mar. 2009.

[12] T. Claburn, "Identity-theft keylogger identified," *InformationWeek*, Aug. 11, 2005; http://informationweek.com/story/showArticle.jhtml;?articleID=168600805.

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

[14] T.A. Peters, *Computerized Monitoring and Online Privacy*. McFarland, 1999, pp. 46.

[15] J.B. Hansen and S. Young, *The Hacker's Handbook*. CRC, 2003, pp. 151.

[16] R.S. Gaines, W. Lisowski, J. S. Press, and S. Norman, "Authentication by keystroke timing: Some preliminary results," RANS, Tech. rep. R-2526-NSF, May 1980.

[17] L. Zhuang, F. Zhou, and J.D. Tygar, "Keyboard acoustic emanations revisited," *presented at 12th ACM Conf. Computer and Communications Security*, Alexandria, VA, 2005.

[18] G. Mohay, B. Collie, O. Vel, R. McKemmish, and A. Anderson, *Computer and Intrusion Forensics*. Artech, 2003, p. 227.

[19] J. Bennett, *Digital Umbrella: Technology's Attack on Personal Privacy in America*. Boca Raton, FL: Brown Walker, 2004, pp. 51-52, 64.

[20] J.K. Tudor, *Information Security Architecture*. CRC, 2000, pp. 141-146.

[21] 2005 Identity Fraud Survey Report, Javelin Strategy & Research, 2005, pp. 4-8.

[22] A.B. Sterneckert, *Critical Incident Management*. CRC, 2003, p. 227.

[23] J. Weckert, *Electronic Monitoring in the Workplace*. Idea Group Inc (IGI), 2004, pp. 7-8.

[24] H.F. Tipton and M. Krause, *Information Security Management Handbook*. CRC, 2003, p. 1891.

[25] M.K. Shields and R.E. Behrman, "Children and computer technology: Analysis and recommendations," *Children J.*, vol. 10, no. 2, pp. 3-29, 2000.

[26] L.J. Magid, "Child safety on the information highway," National Center for Missing and Exploited Children (NCMEC), 2003; http://www.safekids.com/child_safety.htm.

[27] "Child safety on the information superhighway," *SpyArsenal.com*; http://www.spyarsenal.com/child-safety.html, accessed Feb. 1, 2006.

[28] J.K. Petersen, *Understanding Surveillance Technologies*. CRC, 2000, pp. 161-166.

[29] *Electronic Monitoring & Surveillance Survey*, American Management Association, 2005.

[30] "Anti-spyware coalition definitions and supporting documents," http://www.antispywarecoalition.org/documents/20051027definitions.pdf. accessed Aug. 12, 2009.

[31] L.D. Paulson, "New products fill gap in encryption protection," *IEEE Computer*, pp.21-23, Oct. 2005.

[32] *Microsoft, Security Intelligence Report July through December 2007*, http://download.microsoft.com/download/f/f/d/ffd1f8b8-afcc-4ed1-a635-2caa8b96ac2f/MS_Security_Report_Jul-Dec07.pdf

[33] "Malware report," F-Secure 2008; http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080624_1_eng.html, accessed Mar. 2009.

[34] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing system-wide information flow for malware detection and analysis," in *Proc. 14th ACM Conf. Computer and Communications Security*, pp. 116-127, 2007.

[35] K. Subramanyam, C.E. Frank, and D.F. Galli, "Keyloggers: The overlooked threat to computer security," *keylogger.org*; http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html, accessed Aug. 12, 2009.

[36] M. LeMay and J. Tan, "Acoustic surveillance of physically unmodified PCs, *keylogger.org*; http://www.keylogger.org/articles/Acoustic_Surveillance_of_Physically_Unmodified_PCs/8, accessed July 2009.

[37] On Guard Online, U.S. Federal Trade Commission; http://www.onguardonline.gov, accessed July 2009.

[38] M.M. Baig and W. Mahmood, "A robust technique of anti key-logging using key-logging mechanism," in *Proc. IEEE-IES Digital EcoSystems and Technologies Conf.*, Feb. 21-23, 2007, pp. 314-318.

[39] Community Emergency Response Team Coordination Center (CERT/CC), "2007 statistics," Software Engineering Institute, Carnegie Mellon University, 2007; http://www.cert.org/stats/.

[40] *Information Security Breaches Survey* DTI, 2006; http://www.pwc.co.uk/pdf/pwc_dti-fullsurveyresults06.pdf.

[41] www.keylogger.org, accessed July 2009.

[42] G.B. Garrie, F. A. Blakley, and M.J. Armstrong, "The legal status of spyware," *Federal Communications Law J.*, pp. 161-218, Dec. 2006.

[43] A. Young and M. Yung, "Deniable password snatching: On the possibility of evasive electronic espionage," in *Proc. IEEE Symp. Security & Privacy*, May 4-7, 1997, pp. 224-235.

[44] S. Gordon, "Fighting spyware and adware in the enterprise," *EDPACS*, June 2005, Taylor and Francis, vol. 32, no. 12, pp.14-18, June 2005; http://dx.doi.org/10.1201/1079/45242.32.12.20050601/88294.2.

[45] BERR, *The Information Security Breaches Survey, Tech. rep.*, 2008; http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf

[46] "Online financial fraud and identity theft 2007," *Cyveillance*, 2007; http://www.cyveillance.com/web/news/press_rel/2007/2007-03-27.asp, accessed Mar. 2009.