Keystroke Logging: The Next Sherlock Holmes in Cyberspace

Francis Lee

February 25, 2013

Computer Science 205 F-Format

Banks, law firms, trading companies, corporates big and small all have one thing in common: they have important and secret information that need to be protected from outsiders; some even from their own employees. Most of these companies store their information in a large database. Information stored in these mass databases tend to range from documents that do not require high level of security to the most top secret, 'chief-level (C-level) executives' eyes only' documents. These top-secret documents are heavily guarded with firewalls, encryptions, and other defense mechanisms so that no one who is not supposed to may lay his or her eyes on these information. Yet there are those who still wish to gain access to them, through one way or another, and since directly hacking into the heavily guarded system is way too difficult, many of them try to pick off information that will give them access to the 'big stuff' that they are seeking, such as log in information. In order to pick these things off, many of them use a fairly recent method known as keystroke logging.

Keystroke logging is "the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored."[1] Through keystroke logging, a person can record and log emails sent, passwords, IDs, chat conversations, and anything else that involves typing using a keyboard.

[1] "Keystroke Logging," Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/Keystroke_logging#History (February 20, 2013).

Key loggers are the actual tools that perform the keystroke logging. Depending on its specific design and intended purpose, what it records may be different, but generally, it functions as a recorder, logging user inputs (whatever is typed on the keyboard) and user commands (what the computer is told to do through direct user input). Key loggers can be generally categorized as either software based key logger or hardware based key logger.[2]

Software based key loggers can be summed up into these categories: hypervisor-based loggers, kernel-based loggers, API-based loggers, form grabbing loggers, and packet analyzers.

A hypervisor is a "computer, software, firmware, or a hardware that can create and run virtual machines."[3] A computer can host and run multiple operating systems (defined as virtual machines), which a hypervisor manages the execution of. A hypervisor-based key logger can theoretically run in a malware (software being used for malicious intent) hypervisor that operates under the radar and therefore, unbeknownst to the user and most likely, the computer. There, the key logger tracks and records user's keyboard inputs.

Kernel-based loggers operate at the "kernel-level," which is the highest level of access points in the computer's security system. Access levels of a computer are divided into rings, the outer one being the least secure and the kernel level being the most guarded. Programs and other operations are classified into these rings, which give them access to certain parts of the computer, but restrict them from other parts.[4] A program at the kernel level has access to most, if not all of the computer's files, programs, and machinery. A kernel-based key logger enjoys the virtually unlimited access to the computer and performs its programmed tasks. These are the most difficult to detect as it is at the very core of the operating system where it is rather difficult to censor and check for malware once a malware

---

[2] "Keystroke Logging," online.
[3] "Hypervisor," Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/Hypervisor (February 20, 2013).
[4] "Ring (Computer Security)," Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/Ring_(computer_security) (February 20, 2013).

infiltrates it.[5] At the kernel level, the key logger remains in a stealth satus and continues to track and record user inputs whilst acting as a keyboard "device driver," software that is used to control a specific hardware that is attached to the computer.[6]

Application Programming Interface (API) is a software that helps the operating system receive signals from the keyboard, process it, and perform the user-inputted command. An API-based key logger hooks the keyboard API and reroutes the keyboard API's function so that in addition to performing its originally designated task, it would also send a signal to the key logger so that every time a key is pressed (a command is sent through), the key logger can record it.[7]

Form grabbing key logger records user's web browsing history and browsing commands. Before the input or the signal to browse something is executed, the computer first processes the signal internally. Then it sends the signal through to the Internet. Form grabbing key loggers record and track these signals whilst they are being processed in the computer.[8]

Packet analyzers intercept and record all network traffic coming in and out of the computer. The key logger intercepts and records all data, decodes them, processes them, and logs the information. This is often used to decode and log passwords or PINs.[9]

Hardware based key loggers can be generalized into the following: firmware-based, keyboard hardware, wireless keyboard sniffers, acoustic key loggers, electromagnetic emission loggers, optical surveillance loggers, and physical evidence based loggers.

BIOS level firmware that handles keyboard functions can be altered in a way so that it could record all keyboard inputs / events as they are processed inside the computer.[10] BIOS (Basic Input and Output System) is the basic firmware interface that is employed in all IBM

[5] "Keystroke Logging," online.
[6] "Keystroke Logging," online.
[7] "Keystroke Logging," online.
[8] "Keystroke Logging," online.
[9] "Packet Analyzer," Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/Packet_sniffing (February 20, 2013).
[10] "Keystroke Logging," online.

PC compatible computer that boots, tests, and initializes a computer's operating system, essential programs, and activates memory devices.)[11] This altered function of the firmware acts as the physical logger of all transactions between the keyboard and the computer.

A keyboard hardware based key logger is an actual piece of hardware that is attached somewhere between the keyboard and the computer, usually on the cable that connects the keyboard to the computer. It can be attached at the end of the cable, which would normally be directly plugged into the computer, or it can be built into the keyboard so that no hardware is actually visible. Regardless of where it is installed, this key logger stores every signal that the keyboard sends to the computer in its internal memory, which can be easily accessed.[12]

A wireless keyboard sniffer intercepts the communication between a wireless keyboard and a computer. When intercepted, the information may be encrypted in some sort of a secure language in order to make sure the wireless communication between the two devices is secure and not interfered with. Because of this, the data collected by the key logger may need to be decoded before it can be read.[13] A sniffing logger performs the same function as the keyboard hardware based logger.

Acoustic key loggers use the unique sound that each key on the keyboard makes in order to pick up on which key is being pressed. It bases its data collection off of a massive sample collection of what each key sounds like and statistical analysis of the order in which keys are pressed to figure out and record what is being typed into the keyboard.[14] The key logger then either stores the collected information in its internal memory, or sends the information to another computer or database for storage.

Electromagnetic emission based key loggers functions on electromagnetic waves produced by the keyboards. Most keyboard emit electromagnetic waves when the keys are

---

[11] "BIOS," Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/BIOS (February 20, 2013).
[12] "Keystroke Logging," online.
[13] "Keystroke Logging," online.
[14] "Keystroke Logging," online.

pressed. This key logger captures the electromagnetic waves through a wide-band receiver and translates the waves into an understandable language in order to figure out which keys are emitting the electromagnetic waves and thus, are being pressed.[15]

An optical surveillance based key logger is not the typical key logger, in that it involves nothing technologically challenging in order to track and record user inputs. Optical surveillance, as its name suggests, involves a video camera of some sort being installed in a strategically convenient location so that someone can monitor what the user is typing.[16] This type of key logger is difficult to be considered a type of a key logger as it ironically serves the function of a simple security camera except with a completely opposite purpose.

Lastly, physical evidence based key logging is even less technologically advanced or challenging. Frequently used keys have marks on them from wear and tear. For example, a four digit passcode or a PIN is easily decodable because the keys that correspond to the numbers in the passcode or the PIN would have wear marks on them. Once the four digits are determined, it is only a matter of time until it can be pieced together into the right combination. This type of key logging, which is hardly a 'logger,' is used most frequently for brute force (non-technologically challenging nor involving) attacks.[17]

Keystroking has been used for mostly malicious purposes and criminal pursuits. Thousands of personal bank accounts, personal emails, PINs (Personal Identification Number), IDs and passwords, corporate databases, and other protected accounts have been compromised by malicious use of this technology.

In 2005, an unknown band of cyber criminals tried to steal 423 million dollars from the London offices of Sumitomo Mitsui, a Japanese bank. An Israeli man was arrested after he had attempted to transfer nearly 27 million dollars into an Israeli account. Police reports say that the culprits were planning on distributing the 423 million dollars to 10 different bank

[15] "Keystroke Logging," online.
[16] "Keystroke Logging," online.
[17] "Keystroke Logging," online.

accounts. The perpetrators infiltrated the bank's system and used key loggers to log and record customer PINs, employee ID numbers, and other security-related information in order to access the bank's transaction system and heist the 423 million dollars.[18]

In 2008, hundreds of card swipe devices were found to have been bugged with key loggers, which logged and sent card information to computers in Pakistan through mobile networks. Hardware based key loggers were thought to have been installed in card swipe devices either during production or shortly after coming off the production line, right before distribution. According to *The Telegraph,* the scam is thought to have caused the loss of tens of millions of British pounds through the creation of copied credit cards, Internet transactions, or cash withdrawal.[19]

As seen in the above two cases, keystroke logging has been used for mostly criminal intents, and most of the time, culprits have succeeded or nearly succeeded in their attempts because of keystroke logging. However, keystroke logging holds great potential to be used for the opposite purpose: law enforcement.

In 2000, the FBI arrested two Russians, Vasily Gorshkov and Alexy Ivanov, on charges of fraud, conspiracy, theft, and other computer related crimes. Both were convicted and each faced a maximum of a hundred years in prison. Having no legal jurisdiction in Russia where the two were based out of, and therefore, unable to conduct and sufficient search and investigation to bring the two to court, the FBI lured the pair into the United States claiming to be a fictional security firm offering them "good jobs" if they could prove their skills. The FBI gave them a computer rigged with a key logger to prove and requested that they prove their skills through certain tasks. The two used the computer to access their personal computer back home. The FBI later retrieved the key logger and gained access to a

[18] Gregg Keizer. "Keyloggers Foiled In Attempted $423 Million Bank Heist," Bank Systems & Technology, http://www.banktech.com/keyloggers-foiled-in-attempted-423-milli/159902118 (February 21, 2013).
[19] Austin Modine. "Organized Crime Tampers with European Card Swipe Devices," The Register, http://www.theregister.co.uk/2008/10/10/organized_crime_doctors_chip_and_pin_machines/ (February 21, 2013).

wealth of information including the two's computer account IDs, passwords, and other log in information, which they used to log into their accounts and conduct investigation. Using the evidence they gathered through this method, they were able to charge and convict the two for their crimes.[20]

As seen in this case, keystroke logging holds much potential to be used for legal purposes such as criminal investigation. Furthermore, it holds potential to be used for monitoring national security by tracking activities of suspected individuals deemed possible to pose a threat to national security. A kernel-level logger can be instrumental in tracking dangerous individuals' activities which can provide the government with crucial and necessary information and details regarding those individuals and what they are up to.

Keystroke logging, though it has been and is currently used mostly for criminal purposes and unlawful pursuits, holds tremendous potential for use in countering those criminal pursuits. As seen with the FBI case and the national security hypothetical, key loggers can be used in law enforcement as a tool for thorough investigation when direct access to and investigation of suspects is difficult, especially if there are no hard enough evidence to issue a search warrant or justify a search when asked to testify. It holds too great a potential to be ignored and deemed irretrievable into the light of law enforcement and legal activities. Keystroke logging may open the doors to a new age of cyber policing, national security, and law enforcement: the three very things that does not have an end to development and needs to continue to grow and strengthen.

[20] John Layden, "Russians Accuse FBI Agent of Hacking," The Register, http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (February 21, 2013).