Max Varner

COSC 356

April 10, 2012

Keylogging

**Introduction:**

Keystroke logging, also known as keylogging, is simply tracking the keys that are struck on a keyboard. This can be done in multiple ways using a wide variety of hardware devices or software. The reason for its large threat to networks and their security is due to its covertness nature. Most keyloggers show no signs of any intrusion within the system allowing for them to gain typed information without anyone having knowledge of its actions except for the user who installed it. With the proper keylogger installed on the correct machine a person could easily gain access to a company’s entire network infrastructure. In terms of system critical data or extremely privileged information this could cause problems for a vast amount of people very quickly. Throughout the remainder of this paper I will continue to give a background description of keyloggers, provide you with methods for using them, compare different types of keyloggers, and analyze any issues that may arise from keylogger usage.

**Background and Description:**

The only thing we can know for sure is that we will never know an exact date or an exact person to pinpoint the invention of keyloggers on. They have existed and have been used for many years. Keyloggers first appeared on the scene in the late 80’s and early 90’s. One of the earliest keyloggers was writing by a man named Perry Kivolowitz. He posted his source code to net.unix-wizards, net.sources on November 17, 1983. The program basically operated by locating character lists, or clists, as they were being built by the Unix kernel.

Keyloggers have a wide variety of uses and can be either hardware-based or software-based. The main purpose is to log everything that is typed on a keyboard and store it in text files for later assessment. Everything that is typed will be logged; this includes sensitive information such as passwords, names, pin numbers, and even credit card numbers. While keyloggers have many acceptable uses they also have many malicious uses.

Acceptable uses:

* Parent monitoring child’s computer usage
* Boss monitoring employee’s computer usage
* Government retrieving information pertinent to a crime

Malicious uses:

* Cracking passwords
* Gaining unauthorized information
* Stealing credit card numbers
* Reading sent emails or messages not intended for public viewing
* Retrieving secret names
* Stealing account numbers

Most associations with keyloggers are much like those with hackers. Even though there are many beneficial uses to keyloggers the only ones the public seems to associate with them are the malicious ones.

**Types of keyloggers:**

There are two basic types of keyloggers, hardware and software. The first ones I’ll talk about are the hardware-based keyloggers.

Hardware keyloggers can be implemented via BIOS-level firmware or via a device that can be plugged inline between a wired computer keyboard and a computer. All of the information that is logged by a hardware-based keylogger is stored to its own internal memory leaving no trace of its existence on the machine itself. One of the main advantages to using a hardware key logger over a software based one is that it can begin recording keystrokes from the moment the computer is turned on. This gives it the ability to capture passwords related to the BIOS and system encryption. All hardware keyloggers must have both a microcontroller and non-volatile memory. The microcontroller processes the data stream between the computer and the keyboard while the non-volatile memory stores the information collected even after power to the computer is lost. Hardware keyloggers non-volatile memory can range anywhere from a few kilobytes to several gigabytes. With each key stroke taking typically only one byte of space most hardware keyloggers can hold millions of character strings. Typical hardware keyloggers are designed to blend in with the rest of the computer cabling system. They either resemble a PS/2 connection or more recently a USB interface that simply plugs into the end of the keyboard cable and then into the computer, hence the inline description. The pictures below depict both a PS/2 (left) and a USB (right) inline keylogger.



In the event a person would need to be even more covert with their hardware keylogger a circuit attachment installed inside of the keyboard is also available. With this type of modification to the naked eye nothing will appear to have changed with the computer system while still given access to the data collected by the keylogger. The picture below is an example of a circuit keylogger that can be soldered within the keyboard’s circuitry. To be even more inconspicuous the BIOS, which handles all of the events of the keyboard, could also be reprogrammed to retain keystrokes for later assessment. This type of modification would be done strictly to the computers firmware requiring no extra hardware since the collected data could be stored directly to the computer’s hard drive.



Another type of logger that is considered to be hardware based is an Acoustic Keylogger. Every time a key is pressed on the keyboard it has a unique sound signature. With the proper frequency analyzer a person would be able to find a repetition frequency of similar acoustic keystroke signatures. A few things become necessary for this to work. The timing between the keystrokes and the language the user is typing in can be combined to create a so called map of sounds to letters. A fairly long string of about 1000 or more typed characters is required to ensure that a proper map is created.

Lastly, in a world today where most every peripheral device such as keyboards and mice are becoming wireless, there are hardware keyloggers that can attempt to capture this information as well. Wireless keyloggers simply collect the data that is transmitted between the wireless keyboard and the receiver and attempt to crack the encryption between the two devices. With wireless keyloggers the information collected can be retrieved by the user from any computer with the supplied software within range of the wireless keyloggers transmitter. This is the best option when it comes to hardware keyloggers because it only requires the installer to gain access to the system once. With the ability to retrieve the logged information wirelessly the installer will have no need to recover the keylogger risking getting caught by someone in the process.

**Software Keyloggers:**

Software keyloggers fall into basically five main categories, hypervisor-based, API-based, Form grabbing based, Memory injected based, and Kernel-based. Hypervisor- based loggers can be embedded in a malware hypervisor running behind the operating system. The essentially become a virtual machine that is undetected by the computer user. A good example of this is a program called Blue Pill. API-based loggers are simple programs that hook the keyboard’s API allowing for windows to notify the program each time a key is pressed. Even though these are the simplest to write they may be easily detected in the event there is a great amount of keystrokes to pull. The increased amount of key pulling will also increase the CPU usage which can be seen by the computer user via task manager or some other 3rd party software that displays CPU usage. A form grabbing based logger is confined only to web based forms. These loggers record data that is input into forms and captured when the user clicks the submit button. Because this is done on the host side of the machine it can bypass any security set up by a HTTPS website such as Bank account web pages and those alike. Memory injection based loggers do just as the name states; they inject directly into memory and alter memory tables to capture keystrokes in web forms and other system functions. This method is commonly used when the user wants to bypass Windows UAC (User Access Control). Finally, Kernel based loggers are the most difficult to program and implement but also allow for the greatest amount of discrepancy. These loggers can act as a keyboard driver giving it the ability to capture any and all information typed on the keyboard. They are typically implemented using rootkits that can bypass the operating system kernel and give the user unauthorized access to the system hardware.

**Prevention methods:**

Even though most keyloggers are difficult to detect there are a few ways to prevent them from gaining data that can be used. Many software based keyloggers will have a malware signature type to them that can sometimes be picked up by virus/malware protection programs. Running these scan periodically can help to prevent a keylogger from residing on a user’s computer for too long. Typing half of a password into the password field then typing a few random characters into a notepad document and then finishing the password back at the password field can also prevent the logger from retrieving usable information. Another good measure they may work against most keyloggers would be choosing a different keyboard layout that is not common to most loggers. By using a different layout when the user types the letter ‘e’ on the keyboard it would type the letter ‘f’ instead on the screen. This prevents the logger from recording the actual character string that the user is typing in the text fields. Say the password being entered is ‘bighouse’ the keylogger would record the keys type on the modified keyboard layout and record them as ‘johexiuw’. Even though the user was able to access their system properly the logger only records what appears to be random characters.

One of the most full proof ways to prevent keylogging is to prevent unauthorized access to computer and network systems. Keeping server rooms locked, limiting access to software changes on employee and personal computers, and installing software on client machines that detect when new devices are attached and software is installed.

**Causes for Network Security concern:**

Due to the fact that network keyloggers are so easily available and most require little computer background to operate it poses a great risk to sensitive data on computer systems. In the even a person were able to can access to a server room within a company and install a keylogger the installer would then be able to gain unauthorized access to the computer system. Once the passwords and usernames are available to the installer they can essentially do anything with the system whether the intent is malicious or not. Sensitive company data is typically protected by passwords that are typed over and over each day, if a keylogger is installed on the system the installer of said keylogger would also have access to this sensitive data giving them the ability to do with it as they may.

**Conclusion:**

There are a multitude of keyloggers from hardware based to software based. Each of them has their advantages and disadvantages. Keyloggers prose one of the largest threats to computer and network systems. Most everything that users protect on computers is protected by usernames and passwords. Keyloggers basically bypass these setup safety protocols making their data completely vulnerable. In order to prevent keyloggers from recording sensitive data such as passwords, usernames, bank account number, and others alike it is pertinent that administrators follows the steps of prevention described above. Software programmers could also use this information to write future programs that look for keylogging and work in ways to prevent information like this from being kept alive any longer than needed. Keylogging is a serious threat and the only one who can insure that it doesn’t happen to them is the end user. It is their reasonability to watch for keylogging signs and remove software and hardware devices from their systems.