Keyloggers

Chelsea Edwards & Matthew Krieger

Spring 2017

Computer Security

Group 11

Among the vast array of topics belonging beneath the umbrella of computer security, the issue of computer surveillance rises with importance in parallel to our society’s continual advancement in communication with technology. As a whole, much of computer surveillance as a field is dedicated to monitoring the traffic and transferal of data between users on the Internet. This has led to ethical controversy over the importance of an individual’s right to privacy versus a government or authority figure’s right to determine the existence of illegal activity within their own legal boundaries, leading to what some may call a fear of mass surveillance. The methods in which computer surveillance can be carried out are many—since there are a multitude of ways in which data can be shared, the same can be said for how it can be collected. Packet sniffing is one example of this under network surveillance, where keywords can be filtered out and examined by certain computers automatically, and the captured data can later be analyzed as seen fit. Corporate surveillance is another area geared toward marketing field, and is often used to find a preferred audience by tracking a specific individual’s preferences. By following a user’s digital footsteps on the Internet, an algorithm can be modified to change content they may see through advertisements on web pages or sold to other businesses so that they can tailor a product to that individual. Google is a prominent example of this, storing information from each search made by a user, including their IP address. “Many websites, such as news sites and blogs, partner with Google to show ads to their visitors… we may use cookies for a number of purposes, such as to stop you from seeing the same ad over and over again, to detect and stop click fraud, and to show ads that are likely to be more relevant…These [server logs](https://www.google.com/intl/en/policies/privacy/key-terms/#toc-terms-server-logs) typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. “ Another method of surveillance, one that this paper will focus on, is that of the use of malicious software. This software, whether it be through the form of spyware, a virus, Trojan, or keylogger, generally depend on the user to install software that covertly houses this malware within its contents. Once installed, the malware can begin extracting data from the computer’s hard drive and actively monitoring computer usage. Keylogging, in particular, holds unique interest in the scope of computer surveillance because of its direct approach in actively recording keyboard strokes to collect the data needed from a particular user.

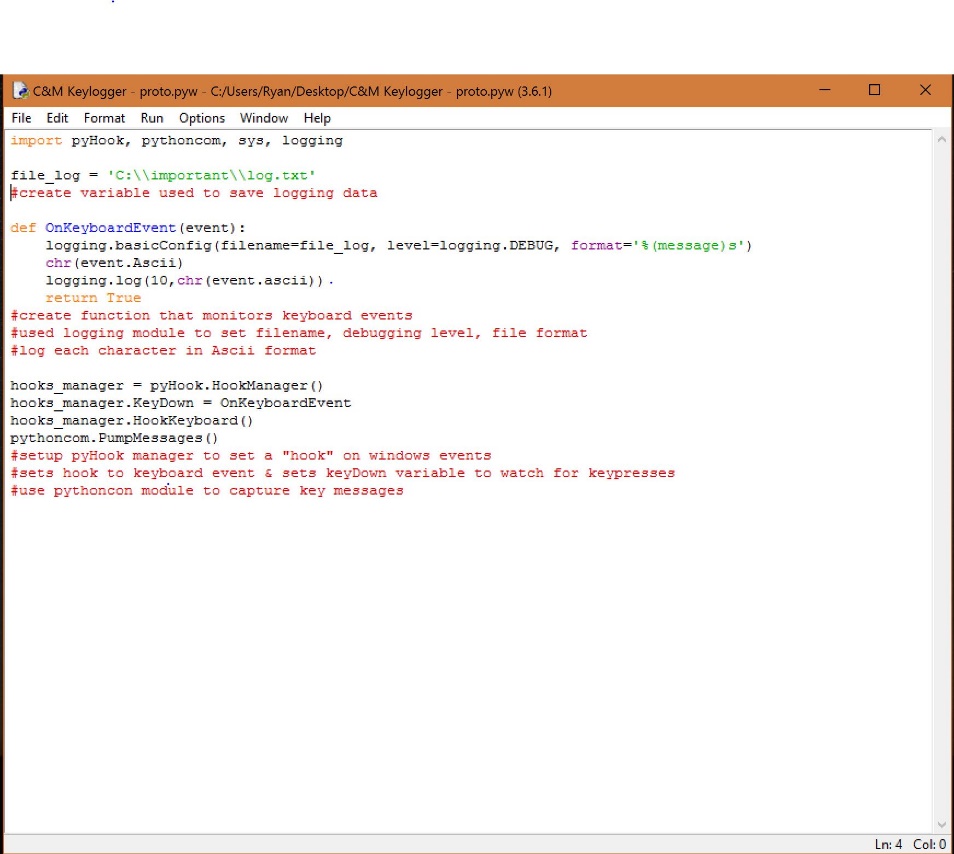
According to webopedia, a keylogger is “a type of surveillance software [often considered spyware] that has the capability to record every keystroke you make to a log file, usually encrypted.” Potentially, it can capture credit card numbers, passwords, personal messages, etc. It is because of this intimacy with unlawful surveillance and embezzlement of private and financial information that keyloggers possess a somewhat negative reputation in the tech community. However, much but not all this reputation is warranted. Keyloggers also have honorable applications that deserve to be acknowledged. One of the most effective ways to keep young children safe from the potential dangers of the internet on the internet is by monitoring their internet activity. In addition, keyloggers can potentially save a company thousands of dollars if not more by tracking the computer activities of employees who pose a threat to the company by selling confidential information or simply wasting the company’s money by not working when are expected to be. There are two distinct types of keyloggers: hardware & software. The hardware keylogger is a small device that plugs inline between a computer keyboard and a computer. These devices have onboard memory so they must be retrieved to access the desired data. Two advantages of hardware keyloggers are that they can begin logging data as soon as the computer is turned on and they are invisible to anti-virus software. On the other hand, software keyloggers are a piece software that is installed on a target computer where every keystroke is recorded and usually emailed to the person tracking the data. One of the advantages to using a software keylogger is that the keylogger can run indefinitely and does NOT have to be physically retrieved like it would if a hardware keylogger is utilized. For this project we will create, execute, and demonstrate a customized software keylogger.

Even though the history of key logging is rather murky, it is known to have been practiced for at least fifty years. It is widely believed keylogging was first used in a governmental capacity about fifty years ago despite there being no date to support this. However, the 1970’s formally introduced to the world the concept of keylogging. From 1976 to 1984, Soviet spies installed primitive “keyloggers” in dozens of IBM Selectric typewriters that were used in the United States embassy in Moscow and the United States Consulate in Leningrad. The Soviet’s objective at the time was to monitor classified information being shuffled into and out of these two important bureaucratic institutions. (Goodin) For the most part, during the twentieth-century keylogging remained a government activity. However, since the advent of the twenty-first century, they have become one of the most popular technology devices used for surveillance.

The implementation of software keyloggers can vary in three ways and each way has pros and cons. The most popular method for constructing keyloggers is by utilizing the SetWindowsHook API function. This occurs when the “system hook intercepts the keypress notifications and is installed using the abovementioned API function for messages transmitted by the windows procedure ”. (Dimov) This talks about implementation of keyloggers

Our prototype keylogger targets the Internet Explorer application process in the targeted computer. This talks about OUR implementation

Conclusion

Works Cited

Bass, Steve, and Steve Bass,PCWorld|Dec 13, 2006 12:00 AMPT. "Have Kids? Try a Keylogger." *PCWorld*. PCWorld, 13 Dec. 2006. Web. 26 Mar. 2017. <http://www.pcworld.com/article/128085/security/article.html>.

Beal, Vangie. "Keylogger." *What Is Keylogger? Webopedia Definition*. IT Business Edge, n.d. Web. 26 Mar. 2017. <http://www.webopedia.com/TERM/K/keylogger.html>.

Goodin, Dan. "How Soviets Used IBM Selectric Keyloggers to Spy on US Diplomats." *Ars Technica*. N.p., 13 Oct. 2015. Web. 26 Mar. 2017. <https://arstechnica.com/security/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats/>.

KALPA. "Keyloggers." *Security Research*. N.p., 19 Mar. 2011. Web. 26 Mar. 2017. <http://securityresearch.in/index.php/projects/malware\_lab/malware-keyloggers/>.

https://www.google.com/policies/technologies/ads/