OS PROJECT REPORT
ON
IMPLEMENTATION OF KERNEL SPACE KEYLOGGER

BY

GOVIND S
JERIN JOSE
HARIKRISHNAN K R

Keyloggers are software or hardware tools that capture a computer user's keystrokes.A kernel-level keylogger can act as a keyboard driver or replace some functions of an original driver to obtain any information from a keyboard.Keyloggers are frequently implemented as rootkits that subvert the operating system kernel to gain unauthorized access to the hardware.

When you press a key on the keyboard,the keyboard will send corresponding scancodes to keyboard driver.A single key press can produce a sequence of up to six scancodes.

The handle_scancode() function in the keyboard driver parses the stream of scancodes and converts it into a series of keypress and keyrelease events called keycode by using a translation table via kbd_translate().It is this keycode that we receive in our program.

Each key is provided with a unique keycode k in the range 1-127.Pressing a key k produces a keycode k while releasing it produces key code k+128.

Keyloggers can be implemented by writing an interrupt handler,function hijacking or through a notifier block and a callback function.

Our initial attempt to implement keylogger using the function hijacking method failed as it required intercepting sys_read/sys_write system calls and our multiple attempt to achieve this failed.Our subsequent attempt was to implement the

keylogger using the third method using a callback function in a kernel module.

Our program runs by registering a notifier_block with the keyboard using register_keyboard_notifier(). This notifier_block's .notifier_call is set to the keylogger_callback() function that receives the keycode value along with other params and converts it to the required form and then log it to the debugfs directory in a "keys" file. Only root or sudoers can read this log.

Debugfs is a special file system available in the Linux kernel since version 2.6.10-rc3. It was written by Greg Kroah-Hartman. debugfs is a simple-to-use RAM-based file system specially designed for debugging purposes. It exists as a simple way for kernel developers to make information available to user space.

Our keylogger can log keys with keycodes in the range 0-119 and also identify the shift modifier.It logs the output to debufs's log which can be transferred to any other file using a simple script.

References:

Books:

1. https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf

Other links:

1. https://github.com/vanhauser-thc/THC-Archive/blob/master/Papers/writing-linux-kernel-keylogger.txt
2. https://github.com/arunpn123/keylogger