CAPTURE

SYNOPSIS

Submitted by

VISHAL RAWAT -19BCS1770

in partial fulfillment for the award of the degree of

BACHLOR OF ENGINEERING

IN

COMPUTER SCIENCE ENGINEERING

CHANDIGARH UNIVERSITY
NOV 2022

BONAFIDE CERTIFICATE

Certified that this project report **"CAPTURE"** is the bonafide work of "**VISHAL RAWAT (19BCS1770)**"who carried out the project work under my/our supervision

SIGNATURE

Dr. Navpreet Kaur

HEAD OF DEPARTMENT

Computer Science Engineering

Chandigarh University

SIGNATURE

Saurav Budhiaraja

SUPERVISOR

Computer science Engineering

Chandigarh University

Submitted for the project viva -voce examination held on

INTERNAL EXAMINER

EXTERNAL EXAMINER

TABLE OF CONTENTS

List of Figures

List of Tables

Abstract

This is python based-project, This program called Capture. Capture is an application used to track keys as the user presses the keyboard. Keyword strokes are captured in a transformed way, so users are unaware that their activity is being monitor .ultimately saving it to a hidden log file that only administrators can see. increase. Only administrators have access. It can be accessed by administrator only. This technology can be used for finding out all the sites and files which are being accessed by any person in the administrator's absence.

This is a monitoring application used to track users who are recording their keystrokes. using the log file Getting information. This application helps you remember forgotten emails and URLs. In my project, when the user types something on the keyboard, the keystrokes are captured and

Without the user's knowledge, it will be sent to the administrator's email id within the set time The project can be used for proper identification and authentication. Typing dynamics can be used for different user profiles. This makes it a valid means of determining an individual's identity.

Graphical Abstract

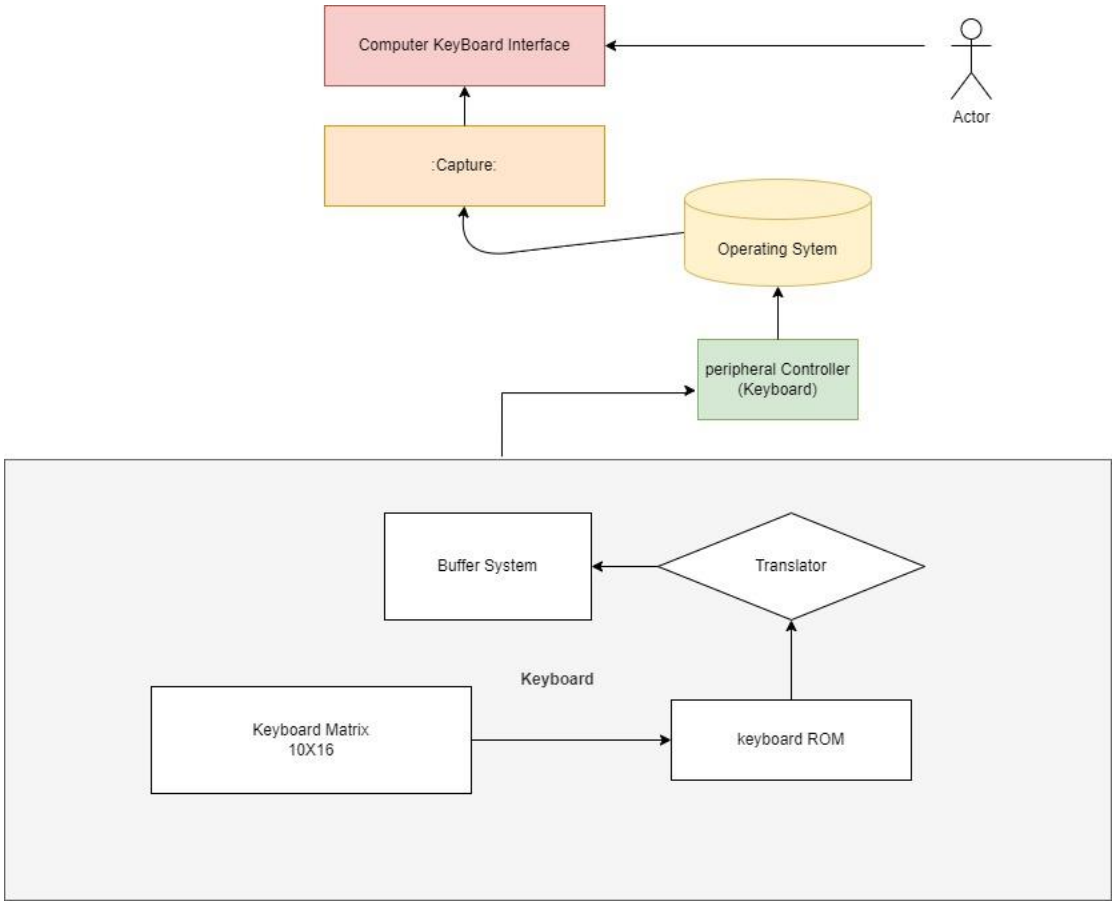

Fig 1.1

Abbreviation

First, Key-Logger is an acronym that means "keystroke logging".

Remember everything you type on your keyboard.

CHAPTER 1.

INTRODUCTION

Data security are top priorities for many IT infrastructure organizations today. A key factor used in computer forensics. computer forensics is Techniques for examining digital media to effectively store, retrieve, and analyze data. There are many cases where data security is essential. So using a capture application Data can be retrieved in the event of a disaster such as a power outage or when a work file is damaged. Key-loggers are particularly effective at monitoring crimes in progress. This is a monitoring application Used to track who logged keystrokes, capture information using log files, and collect records All keys entered. Collected information is stored in the system as a hidden file or emailed Administrator or forensic analyst. Cybercriminals have come up with many ways to get sensitive information terminal. However, few are as effective as recording keystrokes. Keystroke logging, also known as key-logging, is the “Capture” of typed characters. Or The data collected may include document content, passwords, user IDs, and other potential information.
Confidential information. Using this approach, an attacker can obtain valuable data
No need to break into hardened databases and files her server. Key-logging poses particular challenges for security managers. unlike traditional worms Viruses and certain types of key-loggers are almost undetectable. In this article, we will explore how key-loggers work. Examine different types of key-loggers and how they differ. Finally, we'll look at how to prevent key-logging and how to react to it. A key-logger has been detected.

1.1 [Client Identification]

Work on Company equipment or via Company digital networks is subject to monitoring as long as the activity is part of the "normal course of business." Both the Electronic Communications Privacy Act and the Stored Communications Act allow companies to track employee activity without prior notice, but the extent of permissible monitoring varies considerably from state to state. Many of the regulations governing workplace surveillance apply at the state level, and there are significant differences in permissible responsibilities and legal precedents governing such conduct.

In some places, companies can use keylogger software on company devices. Personal information can be revealed to managers when employees mix personal and business

activities on company devices. According to Matt Pinsker, Associate Professor of Homeland Security and Criminal Justice at Virginia Commonwealth University, "Employees typically have little expectation of privacy when using company property or company property.

It can also be used by parents to keep track of their children. There is no doubt that in today's modern era, how children live in things, what they do. That is why it is also necessary to take full care of their children, but a working parent cannot even take care all the time and check their laptop all the time to see what they are doing which will have a bad effect on them too. There is also a truth that in today's time no one can survive without a phone, even a small child needs a laptop to do his work, that's why (Capture) can become such a solution, you can keep an eye on your children. Can also keep what he is searching for, what message is he sending to someone

1.2 [identification of problem]

The most fundamental type of cybercriminal who is normal but could be the most dangerous is insider threat . Insider threats are security risks that originate from within the organization being attacked. This typically involves a current or former employee or business partner who is accessing and misusing sensitive information or privileged accounts within the organization's network.

Traditional security measures typically focus on external threats and cannot always detect internal threats originating from within an organization.

Insider threats include:

Malicious Insider - Also known as Turn-cloak, someone who maliciously and intentionally misuses legitimate credentials, usually stealing information for financial or personal incentive. For example, someone who holds a grudge against a former employer, or an opportunistic employee who sells confidential information to a competitor. Turncloaks have an advantage over other attackers due to their familiarity with an organization's security policies and procedures and vulnerabilities.

Careless Insider - An innocent pawn who unwittingly exposes the system to outside threats. This is the most common type of insider threat due to bugs. B. If your device is left unprotected or you become a victim of fraud. For example, a harmless employee who clicks on an unsafe link can infect your system with malware.

Moles – technically outsiders, but crooks who have managed to gain insider access to privileged networks. This is someone outside your organization posing as an employee or partner.

Hackers and other third parties are constantly looking for system vulnerabilities. In order to know what they want from your organization, they can access sensitive data stored on your system, compromising data integrity or causing data loss. Another problem is that cybercrime is increasing day by day. With the victim's laptop chat logs or keystroke logs, we can easily analyze the victim's entire plan and provide the best solution to eliminate or fix the problem.

Best Practices :

Protect critical assets

Enforce policies

Using Key-logger

Increase visibility

Promote culture changes.

1.3[Task Identification]

Permitted use of a keylogger is using such software with the knowledge and consent of the PC. Owner or security administrator. Licensed monitoring software products typically have physical Computer access and administrative privileges for configuration and installation (or The (at least minimized) risk of program abuse. By convention, such software products may receive and configure "packaged" executable installation files that are delivered to users. In some places, companies can use keylogger software on company devices. Personal information can be revealed to managers when employees mix personal and business activities on company devices Computers using various ethical and sanctioned systems. Other than during installation Display a message on the screen or create a window.

Modules used in the Keylogger project:

1. smtplib:

A module included in Python defines an SMTP client session object.

Used to send email to any Internet machine using the SMTP listener daemon.

2. Threading:

This is one of the modules provided by Python and easy to implement.

A locking mechanism that allows thread synchronization.

3. Pynput:

This library allows users to control and monitor input devices. for example. ;

pynput.mouse, pynput.keyboard

1.4 [Project Timeline]

		Week															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Phase 1	Project finalization and understanding																
	Title																
	Abstract																
	Deciding Tools/Software																
	Literature Review																
Phase 2	Basic design and undertaking																
	Simulation																
	Stimulating various model changes																
	Gathering results and analysis																
	Report and PPT Review by management																

1.5 [Timeline]

Since I am doing this project myself, I think I can finish this project in 16 weeks. I've found this project to be pretty easy and good, so I'll try to give it to you in advance. That way I get the result I'm trying to see . In the first three weeks I will read about

each model that will help you create this project, then in a week or two you will understand how to use this model and then define the algorithm for the time complexity of your project. . This work will take two weeks. After that, I spend the rest of my time writing projects and preparing reports.

1.6 [Organisation of Report]

The main purpose of this document is to describe the requirements of a keylogger project. Today, IT business infrastructure primarily requires computers as a cyber security element. forensics. Keyloggers can effectively assist computer forensic scientists in their investigations.

digital media. Keystroke loggers are available in software and hardware form and are used for capture and compilation. A record of all keys entered. Information collected by keyloggers The system is saved as a hidden file or emailed to a forensic analyst or administrator. Generic keyboard shortcuts Loggers typically record keystrokes associated with keyboard input. Extended keystroke Loggers have many additional features. The project keylogger has the following features:

- Monitor keystrokes
- Send an email to the administrator's email id
- Records keystrokes including special keys

Keyloggers have the advantage of being able to collect information before it is encrypted. do like this Facilitates the work of forensic analysts. Most keyloggers show no signs of system intrusion This allows you to receive typed information without others being aware of your actions. users who use it. Keyloggers span a wide range of cybersecurity issues, A hands-on approach to understanding topics such as attacker targets, malware types, and their types implementation, the role of malware in infection, and how stealth is archived on infected systems..

CHAPTER-2

LITERATURE REVIEW

2.1 [Timeline of reported problem]

The use of keyloggers dates back to the 1970s, when the Soviet Union developed hardware keylogging devices for electric typewriters. Called the Selectric Bug, the keylogger tracked the movement of the printhead by measuring the magnetic fields emitted by the movement of the printhead. The Selectric bug targeted IBM Selectric typewriters and spied on US diplomats in the US Embassy and Consulate buildings in Moscow and St. Petersburg. The Selectric keylogger was found in 16 typewriters and was in use until 1984 when another US ally targeted in this operation discovered the intrusion.

Another early keylogger is a software keylogger created by Perry Kivolowitz in 1983. A user-mode keylogger found and dumped a character list in the Unix kernel.

In particular, he has expanded his use of keyloggers since the 1990s. More keylogger malware was developed. This meant that the attacker didn't need to install a hardware her keylogger and could steal personal data, such as credit card numbers, from remote unsuspecting victims. The use of keyloggers began targeting home his users for fraudulent purposes and various industries for phishing purposes.

According to an IBM and Observe IT analysis from 2020, insider risks cost businesses $11.5 million on average. This represents a 30% increase from 2018, demonstrating the growing prevalence of insider threats in industry.

Keyloggers may be used by high-security businesses, such as those in the national defence sector, to keep an eye on its staff members for indications of insider threats. A keylogger can be used to identify unusual behavior , such as a WPM cadence that is significantly higher than normal (perhaps an indication that a malicious script is being executed), or the inclusion of high-risk phrases.

According to the UK Information Commissioner's Office, 90% of all reported breaches in 2019 were due to end-user error. This is an aggrandize ahead of 61% and 87% over the last two years.

According to a 2018 white paper, 53% of companies surveyed had experienced an insider attack against their organization in the past 12 months, and 27% said insider attacks were becoming more common.

The US Financial Sector's July 2012 Insider Threat Report provides statistics on insider threat incidents. 80% of malicious acts took place in the workplace during working hours. 81% of perpetrators planned their crimes in advance. 33% of offenders were described as 'difficult' and 17% were described as 'angry'. Insiders identified him with a 74% chance. Financial gain was the motive in 81% of incidents, 23% of incidents were revenge, and 27% of perpetrators were in financial difficulty at the time.

The US Department of Defense's Center for Human Resources Security Research has released a report detailing an approach to detecting insider threats. We previously published 10 case studies of insider attacks by IT professionals.

A cybersecurity expert believes that he 38% of careless insiders fall victim to phishing attacks, receiving emails that appear to come from legitimate sources such as companies. These emails usually contain malware in the form of hyperlinks

Data Stolen Case by security officer :

Yovan Garcia, a former security officer, was found guilty in 2017 by a California court of hacking the networks of his former employer in order to take data, destroy servers, deface the website, and duplicate proprietary software in order to start a competing business.

Garcia apparently got fired for faking his timesheet, which launched a cybercrime spree. Garcia was penalised more than $316,000 for a variety of violations.

It's truly astounding how much harm this one irate employee actually did. Garcia destroyed backups, stole client information, secret business information, and even shared humiliating images of his former employer to the corporate website.

Through an internal customer relationship management system, a Bupa employee gained access to client information in 2017. The employee downloaded the data, removed it from the database, and then attempted to sell it on the Dark Web. Following an ICO investigation, which resulted in a breach that affected 547,000 consumers, Bupa was fined £170,000 in 2018.

2.2 [proposed solution]

Tools that might assist organisations increase productivity and network security are continually being examined by businesses. In most firms, productivity monitoring is a top priority. Businesses who wish to keep an eye on productivity can track idle time,

record keystrokes, screenshot desktops, and monitor internet traffic. For instance, a keystroke log entry that includes the sentence "what would you like to do tonight? "Want to see a movie?" might suggest that the employee was chatting with a friend via social media. Employers are frequently motivated to prohibit this activity given that up to 64% of employees access websites that are unrelated to their jobs every day while at work. Nevertheless, the corporation runs the risk of obtaining private messages and passwords when it records individual keystrokes. A technique that should not be done lightly is consulting with professionals to help align on components of software and hardware that will work together to generate the most successful plan.

Many companies may come to the conclusion that keyloggers are a useful instrument to aid in achieving their corporate objectives during this process. Keyloggers, nevertheless, present a number of issues and worries, and there are numerous choices that are readily available and will offer more insightful information. while suggesting keylogger substitutes that will boost company productivity and security without the privacy and security hazards connected with recording individual keystrokes. Keyloggers allow companies to monitor every keystroke that their employees type. A keylogger is a bad idea for employee productivity tracking even if it might be used to track employee productivity due to the huge volume of data and the possibility to record sensitive information. The ideal solution for keeping track of the websites that employees visit, monitoring the apps they use, and determining how much time is spent on tasks that are deemed productive for your business is employee internet monitoring software. When monitoring productivity, companies frequently look for actions that are deemed unproductive, such as spending time playing games, using social media, or doing other online activities that do not directly advance the company's goals.

2.3 Bibliometric Analysis

Key Features

1. Businesses can monitor what other activities their employees are doing while working at their computers.
2. To know what kind of activities students are doing at the university.
3. Parents can monitor their children whether they are doing something wrong.

There are many other benefits as well.

1. Easy to deploy at scale. Unobtrusive monitoring of user activity.
2. It can be deployed without physical access to the device that records keystrokes.

Effectiveness :

Full Transparency If you pick out to install keyloggers throughout your commercial enterprise' community, it's crucial to reveal this statistics to personnel. New workforce contributors and present personnel will admire your transparency approximately the usage of this type of software program. When your personnel understand they are being monitored, it creates a set of complete transparency and honesty amongst employees and management. Top Benefits of using a Keylogger With Employees More Productivity a advantage maximum employers see without delay after putting in a keylogger is a upward thrust in worker productivity. Staff contributors who employment on computer systems all day with out tracking regularly have many downtimes. Unfortunately, this means the capacity to waste time on different webweb sites throughout the net, like social media or gaming spots. This time-losing even as at the clock prices your commercial enterprise money. Keylogger tracking steers personnel aloof from time wasters and returned to their paintings agenda. A clearer expertise of Performance Monitoring your personnel with a keylogger additionally enables you apprehend their overall performance extra accurately. Many keyloggers, like pcTattletale, provide display recording. this gives you a real-time view of precisely what your workforce is performing on at some stage in the day. Seeing their extra development enables you find out and apprehend workforce contributors who're going above and beyond. It additionally enables you notice employees who want extra route and management. Less Risk of expertise Theft Companies can also be extra proactive approximately shielding themselves from a big danger in today's world, statistics theft. If you want to keep away from being the following goal for hackers with touchy or treasured organization statistics, it's crucial to require motion and steps to guard yourself. Keylogger Windows 10 software program can help you live earlier than criminals and hold your statistics in which it belongs, secure interior your community. Top Benefits of using a Keylogger With Employees Photo through Annie Spratt on Unsplash Better Password Access one a number of the hassles in IT, particularly if you have got an outsized workforce of personnel, is coping with hundreds of consumer passwords and login credentials. It's anticipated that workforce contributors are going to be accountable for their consumer

statistics and hold song in their passwords and expertise inside the first-rate-case scenario. In reality, matters appear and sometimes, personnel lose song in their statistics. as opposed to spending hours reassigning passwords and login names, you will virtually reminisce at your keylogger statistics and get better misplaced credentials quickly. Tougher Deterrent Against Phishing and Viruses Businesses are also annoyed with the upward thrust in phishing and virus assaults on their networks inside the current decade. Today, it's not unusualplace for malware to be by accident mounted through workforce contributors establishing their emails and clicking on volatile links. Keylogger software program, like pcTattletale, can help you positioned an stop to the contemporary careless behavior. If a person does disclose your organization's community to malware, you may be capable of go back and test pcTattletale's video log to training session who the perpetrator was. Clearer Protection Against Liability Finally, a keylogger software enables your organization guard itself in opposition to capacity liabilities. Viewing your worker's paintings sports can help you spot on any risk-takers or irresponsible employees. It's crucial to keep in mind to constantly divulge that you're using a keylogger and to in no way use your keylogger to get right of entry to your workforce member's statistics. A keylogger is the first-rate desire for employers who need to personal higher manipulate over how their workforce works at some stage in the day. Choosing a product like most appropriate pcTattletale can help you spot of capacity regions of development and praise extra effective personnel in order that your commercial enterprise can bounce and attain better goals.

Some Drawbacks :

Monitoring individual keystrokes is highly invasive. Because these employee monitoring methods carry the risk of directly collecting sensitive personal information, employers should justify using them over less invasive methods such as computer activity tracking software. There are very few Of course, the legality of recording individual keystrokes varies by jurisdiction. As a best practice, employers should consider other options to determine if they really need to monitor keystrokes, or if a less invasive method of monitoring can accomplish their goals. Even in jurisdictions that allow keyloggers, dealing with logs can raise legal concerns. Because keylogging technology can capture sensitive information such as user passwords, private messages, or other forms of personal information,

this data must be adequately protected from misuse by administrative and technical safeguards .For example, if an employee is unaware of a keylogger, it can reveal personal information through chats and emails with family and friends. This kind of information can be very sensitive and mishandling could lead to legal consequences for the administrator.

Data overload

Stressed and confused man using laptop His average typing speed is about 40 words per minute (WPM). If a particular user writes for her one hour at a time, he spends an average of 2400 words per hour written. Add this to the number of employees in your organization and it's immediately apparent that keyloggers generate a very large amount of data. Much more than useful in most cases.

The actual storage required for a keyloggerhis space is negligible, but from a logistical point of view, the sheer amount of information is overwhelming for an administrator to manage and interpret effectively.

Artificial intelligence can be trained to interpret this data, but this level of complexity is far beyond what the average business really needs in an employee monitoring solution. For example, if a company wants to know how much time they spend browsing the internet, they can simply use internet monitoring software to create a report of their employees' internet activity.

cyber security risk

From an insider threat management perspective, a disgruntled administrator with access to logs is a significant threat. They may choose to sell the records to outside threat actors, or simply scrutinize the logs for passwords and other sensitive information.

2.4 [Literature Review]

In the current scenario, security issues are a priority for all organizations. Attackers use various keylogging techniques to obtain sensitive data, especially user credentials. Once an attacker obtains these credentials, they can easily authenticate themselves as a legitimate user. The author proposed a new pattern for virtual keyboards. The

solution in this document emphasizes using the concept of key remapping to protect credentials from screen capture software. It only provides a solution for screen recording software. However, this only captures the screen when the event occurs. In the case of screen recording software, events do not have to occur. Keystrokes can be easily guessed by analyzing the recorded video. the author proposed a screen recording keylogger solution using a color coding mechanism and a dynamic keyboard his layout. The main drawback of this solution is that an attacker can identify which keys were clicked on the virtual keyboard. This can be done by analyzing patterns in screenshots captured when the keyboard first appears when no color-coding mechanism has been induced in the keyboard. This white paper discusses the growing threats to computer security and privacy. We will discuss various keylogger techniques and explain the detailed work of keyloggers. There are various places where you can place your keylogger. It can be placed anywhere between any virtual keyboard and any Windows procedure. After thorough research, the right place to add an anti-keylogging mechanism is just before the window procedure. Existing models do not offer a complete solution for keylogging and screen recording software. These provide some degree of security for keylogging and screen recording software. So there should be a solution for this.

2.5[Problem Definition]

SANS Advanced Threats report attributed to lack of basics of normal user behaviour and poor access control management of privileged user accounts making them attractive targets for brute force attacks and social phishing. identified major gaps in defense against insider threats.

Even the best security teams struggle to spot insider threats. Insiders, by definition, have legitimate access to organizational information and assets. It is difficult to distinguish between normal activity and malicious activity. This problem is exacerbated by the fact that role-based access management is ineffective, as insiders typically know where sensitive data is stored and may make legitimate access requests. As a result, data breaches by insiders are much more costly than those by outside attackers. In the Ponemon Institute's 2019 Cost of Data Breach Report, researchers found that the average cost per record for a malicious or criminal attack is $166, compared to $132 for system disruption, was found to be $133. For more information, read our full post on the cost of a data breach Combine this with the fact that insider threats account for 60% of cyberattacks(IBM) and nearly one-third of data breaches

(Verizon), and developing an insider threat program is a worthwhile investment. I can see why. It's important to note that these numbers include an increase in reports of internal bugs and malicious intent. Either way, security teams have shown that they need to develop insider threat detection methods that prevent sensitive information from being exposed by threat actors or negligent insiders. Use implementation of key-logger as best practises

2.6[Goals/Objectives]

Objective:

To provide the confidentiality to the companies data, In such way so that it is used by authentic person The purpose of this application is to keep tracks on every key that is typed through the keyboard and send it to the admin through the mail server in the time set or given.

Keywords: Python, Capture (key-Logger), Security, Applications, Challenges