Bandaru Ravi Amrutha

Final Project

KEYLOGGER SECURITY

KEYLOGGER SECURITY

- A key logger, sometimes called a keystroke logger, is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone. It can be either hardware- or software-based

- **Types of key loggers.**
- There are two types of key loggers
- Hardware key logger
- Software key logger
- A key logger is a program or tool designed to monitor and keep a tab on the“keystrokes” made on a user’s keyboard. This enables in compromising sensitive data like, bank details, passwords etc.

AGENDA

Key loggers security is the main one to secure the data

- Hardware key logger
- A Hardware key logger works much like its software counterpart. The biggest difference is hardware key loggers have to be physically connected to the target computer to record the user's keystrokes.
- Software key logger

. a software key logger., it transmits information to the hacker or hacking organization, which they will then use to compromise your computer, network, or anything else that requires authentication to access.

PROBLEM STATEMENT

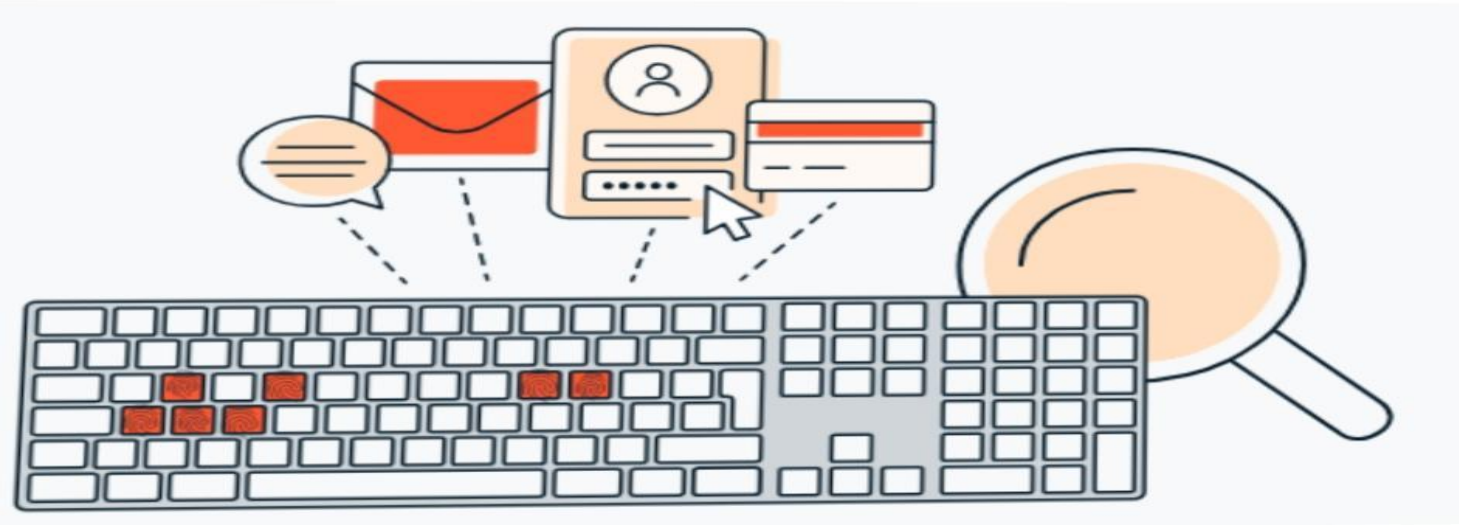
- The problem statement is that the key loggers can be detected using antiviruses
- . Installation of hardware key loggers is difficult without the knowledge of the owner of the system
- . The solution to the above existing problem is that we can build a software key loggers instead of hardware key loggers.

PROJECT OVERVIEW

- Keylogging is the action of capturing and recording keys struck on a keyboard.
- A key logger is a program which captures and monitors all key logs.
- Key loggers can be both in the form of a built software program or directly
- downloaded onto a hardware module.
- Key logger or keystroke logger/keyboard capturing is a form of malware or hardware that keeps track of and records your keystrokes as you type
- . It takes the information and sends it to a hacker using a command-and-control (C&C) server
- The hacker then analyzes the keystrokes to locate usernames and passwords and uses them
- to hack into otherwise secure systems.

WHO ARE THE END USERS?

- Key loggers aren't always used for illegal purposes. Consider the following examples of legal uses for keylogging software:
- Parents might use a key logger to monitor a child's screen time.
- Companies often use key logger software as part of employee monitoring software to help track employee productivity.
- Information technology departments can use key logger software to troubleshoot issues on a device.



YOUR SOLUTION AND ITS VALUE PROPOSITION

Key loggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Key loggers are a form of spyware where users are unaware their actions are being tracked. Key loggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some key loggers can also capture your screen at random intervals; these are known as screen recorders. Key logger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions.

THE WOW IN YOUR SOLUTION

"The easiest protection against any key logger scam is to never type you account name. That is easy, because World of Warcraft has a useful "Remember Account Name" checkbox on the login page, and as long as you don't run several accounts on the same computer, you only need to type in your account name once, and then never again. A key logger can't gather information you don't type. Thus a similar trick is to create a text file on your desktop with you password in it, and using copy and paste to enter the password, again invisible to key loggers

MODELLING

Teams cam add wireframes

User mode key loggers use a Windows application programming interface (API) to intercept keyboard and mouse movements.
GetAsyncKeyState or GetKeyState API functions might also be captured. These key loggers require the attacker to actively monitor each key press.
Kernel mode key loggers are a more powerful and complex software keylogging method. They work with higher privileges and can be harder to locate in a system.
In addition, they can modify the internal Windows system through the kernel.

RESULTS

- Key loggers are a erent threat to both individuals and enterprises, with the potential to cause significant harm if left undetected.
- Understanding the nature of key loggers, their methods of infiltration, and the dangers they pose is crucial for maintaining a secure digital environment.
- Antivirus techniques cannot catch these
- Work on all computer platform
- Can be deployed remotely via software Vulnerability attack
- Are fairly easy to write
- Are hard to detect the errors