KEYLOGGER AND SECURITY

Presented By:

S.Jeya Subha-Holy cross engineering college-CSE

OUTLINE

☒ Problem Statement

☒ Proposed System/Solution

☒ System Development Approach

☒ Required libraries and software

☒ Result

☒ Conclusion

☒ Future Scope

☒ References

PROBLEM STATEMENT

☒ Problem statement : In today's digital age, where cybersecurity threats loom large, one of the significant concerns is the proliferation of keyloggers, stealthy software tools designed to monitor and record keystrokes on a user's computer without their knowledge.Keyloggers pose a severe threat to individuals and organizations as they can capture sensitive information such as passwords,credit card details,and other personal data,leading to identify theft,financial loss,and privacy breaches.

PROPOSED SOLUTION

- The proposed system aims to address the challenge of keylogger security system. This involves requirement analysis ,. The solution will consist of the following components:

- Requirement analysis:

  - The timing of the email and the email address can be changed later in the settings.

  - The daily report will be mailed to the PC owner on his/her email.

- Keyboard monitoring:

  - Python 3 library pynput is used for on screen keyboard.

  - These keystrokes saved in text file will be maintained for 7 days.

- Maintaing the log file :

  - The keylogger will maintain the files containing the keystrokes for a maximum of 7 days.

  - The program will then automatically delete the past files.

  - This settings can also be changed later.

- Prevention:

  - Antivirus

  - Automatic form fillers

  - On screen Keyboard

edunet
foundation

SYSTEM APPROACH

The "System Approach" section outlines the overall strategy and methodology for developing and implementing the keylogger and security system. Here's a suggested structure for this section:

- System requirements

- Library required to build the model

REQUIRED LIBRARIES & SOFTWARE

python idle

pip install pynput

pip install jsonlib

RESULT

Attack tactics and social engineering are
some of the common ways keyloggers are installed in
a malicious scenario. But there is another way this
software can find its way to your computer. Imagine a
scenario where you make your way to a file-sharing site
or software marketplace and choose a software download.
While doing so, you get something extra – your software
comes bundled with a keylogger. This way, a keylogger
can infiltrate your "safe" computer.


```
access.log - Notepad
File  Edit  Format  View  Help
2019-07-09 16:06:30,045› New Tab - Google Chrome› Key.caps_lock
2019-07-09 16:06:30,361› New Tab - Google Chrome› 't'
2019-07-09 16:06:30,523› New Tab - Google Chrome› 'h'
2019-07-09 16:06:30,571› New Tab - Google Chrome› 'i'
2019-07-09 16:06:30,750› New Tab - Google Chrome› 's'
2019-07-09 16:06:32,439› New Tab - Google Chrome› Key.space
2019-07-09 16:06:35,576› YouTube - Google Chrome› 'i'
2019-07-09 16:06:35,733› YouTube - Google Chrome› 's'
2019-07-09 16:06:35,813› YouTube - Google Chrome› Key.space
2019-07-09 16:06:36,220› YouTube - Google Chrome› 'a'
2019-07-09 16:06:36,522› YouTube - Google Chrome› Key.space
2019-07-09 16:06:39,713› Facebook - Google Chrome› 'k'
2019-07-09 16:06:39,804› Facebook - Google Chrome› 'e'
2019-07-09 16:06:39,943› Facebook - Google Chrome› 'y'
2019-07-09 16:06:40,129› Facebook - Google Chrome› 'l'
2019-07-09 16:06:40,277› Facebook - Google Chrome› 'o'
2019-07-09 16:06:40,482› Facebook - Google Chrome› 'g'
2019-07-09 16:06:40,585› Facebook - Google Chrome› 'g'
2019-07-09 16:06:40,703› Facebook - Google Chrome› 'e'
2019-07-09 16:06:40,866› Facebook - Google Chrome› 'r'
2019-07-09 16:06:41,306› Facebook - Google Chrome› '.'
```

CONCLUSION

☒ Keyloggers are a potent threat to both individuals and enterprises ,with the potential to cause significant harm if left undetected . Understanding the nature of keyloggers , their methods of infiltration , and the dangers they pose is crucial for maintaining a secure digital environment.

FUTURE SCOPE

☒ The development of more advanced encryption methods to protect against keyloggers.Additionally,there could be advancements in behavioral analysis techniques to detect and prevent keylogging attempts . Some potential areas of focus include developing machine learning algorithms to detect unusual typing patterns ,enhancing real-time monitoring systems, and improving user education about the risks and prevention of keyloggers.

REFERENCES

☒ REFERENCES [1] Working of Keyloggers available at http: //securelist.com/analysis/publications/36138/keyloggers-how-theywork-and-how-todetect-them-part-1. [2] C.a.Rajendra."Keylogger in Cybersecurity Education". Rechester Institute of Technology,Rechester,New York,USA. [3] M. Aslam, R. N. Idrees, M. M. Baig, and M. A.Arshad, "Antihook shield against the software key loggers," in Proceedings of the National Conference of Emerging Technologies,2004. [4] E. S. L. Martignoni, M. Fredrikson, S. Jha, and J. C. Mitchell, "A layered architecture for detecting malicious behaviors, ".Heidelberg.2008 [5] C. Y. D. Le, T. Smart, and H. Wang,, "Detecting kernel level keyloggers through dynamic taint analysis," College of William & Mary, Department of Computer Science, illiamsburg,,2008. [6] C. G. S.Ortani, and Crispo."Bait your Hook: A novel Detection technique for keylogger". University of Trento, Via Sommarive.Trento, Italy.2010. [7] S.S.a.Anith.

edunet
foundation

THANK YOU