


Chapter 8

Advanced Encryption– Based Keylogger for System Security

V. R. Balasaraswathi


Vellore Institute of Technology, Chennai, India

Ashiq Noor Sudheer

 <https://orcid.org/0009-0008-9647-0002>


Vellore Institute of Technology, Chennai, India

Gautham Vidyashankar

 <https://orcid.org/0009-0002-7253-1006>


Vellore Institute of Technology, Chennai, India

Kevin Sebastian

 <https://orcid.org/0009-0003-6255-3073>

Vellore Institute of Technology, Chennai, India

Priyanshu Pattanaik

 <https://orcid.org/0009-0007-5542-8644>

Vellore Institute of Technology, Chennai, India

ABSTRACT

Our research presents a paradigm shift in network security, combining advanced technology to transcend conventional keyloggers. This software aims to revolutionize monitoring capabilities, specifically targeting keystrokes, while concurrently implementing text encryption mechanisms for log files. Our primary objective is to transform the traditionally perceived risks associated with keyloggers into practical benefits. This keylogger, designed to capture keystrokes, extends its functionality to

DOI: 10.4018/979-8-3693-8014-7.ch008

collect crucial system data, screenshots, and audio recordings—all meticulously recorded in their respective log files which are then encrypted for security purposes. The key focus of our project is to harness the logging capabilities of the keylogger for positive outcomes, enabling users to access encrypted log files in the event of a system crash. This unconventional yet effective approach demonstrates the versatility of research, showcasing how a tool with potential dangers can be repurposed to enhance system diagnostics and improve overall security.

I. INTRODUCTION

Keyloggers are software tools capable of logging every keystroke entered on a computer or mobile device keyboard. As users predominantly interact with devices through keyboards, keyloggers can capture extensive information about their activities (Sagiroglu & Canbek, 2009). Keyloggers represent a highly concerning form of malware that covertly record keyboard inputs and often transmit the collected data to external entities. Despite extensive research and commercial endeavours (Le, Yue, Smart, & Wang, 2008) (Kruegel, Robertson, & Vigna, 2006) (Ortolani & Crispo, 2012), keyloggers continue to present a significant risk, potentially compromising personal and financial data. This includes tracking input such as credit card details, visited websites, and passwords utilized during online sessions.

In 2005, more than eight hackers were accused of trying to steal over 423 million dollars from a Japanese bank by putting keyloggers in its systems. Reports (Hung et al., 2012) say that around 12% of leaked data came from insiders, and 96% of the leaked information was personal data. This shows how serious keyloggers can be in causing data breaches, with both external hackers and insiders posing significant risks to security. This incident underscores the grave implications of keylogger infiltration, revealing the vulnerabilities within organizational security frameworks and the severity of potential data breaches orchestrated by both external threat actors and internal breaches.

When keyloggers operate, they systematically monitor and record each keystroke, storing the data in a file. Keyloggers are specifically designed to record keystrokes by disrupting the flow of information between the moment a key is pressed and when the corresponding keystroke is displayed on the screen. This can be achieved through a range of techniques, including video surveillance, exploiting hardware weaknesses in keyboards or computers, intercepting input/output, modifying keyboard or filter drivers and interfering with kernel functions (Ruhani & Zolkipli, 2023). Early Usage of keyloggers in applications by the year is shown in Table 1. The plot is displayed in Figure 1.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/advanced-encryption-based-keylogger-for-system-security/378750

Related Content

Comprehensive Study on Incorporation of Blockchain Technology With IoT Enterprises

Ashok Kumar Yadav (2021). *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles* (pp. 22-33).

www.irma-international.org/chapter/comprehensive-study-on-incorporation-of-blockchain-technology-with-iot-enterprises/262693

The Role of Quantum Computing in Software Forensics and Digital Evidence: Issues and Challenges

Sandeep Kumar Sharma and Mazhar Khaliq (2021). *Limitations and Future Applications of Quantum Cryptography* (pp. 169-185).

www.irma-international.org/chapter/the-role-of-quantum-computing-in-software-forensics-and-digital-evidence/272370

Threats Classification: State of the Art

Mouna Jouini and Latifa Ben Arfa Rabai (2016). *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 368-392).

www.irma-international.org/chapter/threats-classification/153084

A Pairing-based Homomorphic Encryption Scheme for Multi-User Settings

Zhang Wei (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 295-305).

www.irma-international.org/chapter/a-pairing-based-homomorphic-encryption-scheme-for-multi-user-settings/244920

H0NEY4LOG: A Comprehensive Tool for SSH Honeypot and Log4j Vulnerability Scanner

Sujatha Gurunathan (2025). *Cryptography, Biometrics, and Anonymity in Cybersecurity Management* (pp. 317-342).

www.irma-international.org/chapter/h0ney4log/378756