

Mitra: Real-time Behavior-based Anomaly Detection
for Secure SSH Sessions*

Hyunjong Moon, Juyong Shin, and Jaehyun Nam

Dankook University, Yongin, Gyeonggi-do, 16890, Republic of Korea
 {moonhj, juyongshin, namjh}@dankook.ac.kr

Abstract

This paper introduces Mitra, an innovative eBPF-based real-time SSH monitoring system designed to overcome the limitations of traditional system log-based approaches, which are prone to high overhead and susceptible to vulnerabilities, such as log deletion and omission. Mitra operates independently of system logs, providing efficient, lightweight SSH session monitoring in both kernel and user spaces and detects malicious activities by leveraging this comprehensive monitoring. These contributions enhance the security posture of Linux environments, offering a robust alternative to conventional SSH monitoring methods.

1 Introduction

Secure Shell (SSH) monitoring plays a crucial role in maintaining the security and integrity of systems, as unauthorized access and malicious activities can severely compromise sensitive data and operations. However, traditional SSH monitoring approaches, which rely on system logs, suffer from significant limitations, such as the risk of log modification or deletion by attackers and the ability to bypass logging using specific SSH options (such as `ssh -T`). To address these challenges, we present Mitra, an eBPF-based real-time SSH monitoring system. Mitra provides lightweight SSH session monitoring and effectively detects various malicious activities (e.g., brute-force attacks, stealth access attempts, and log tampering), providing a more efficient and reliable alternative to conventional SSH monitoring methods.

2 Our Approach

Figure 1 illustrates the overall architecture of Mitra system that consists of two main components: *Intrusion and Behavior Detectors*. These components utilize eBPF to perform kernel-level

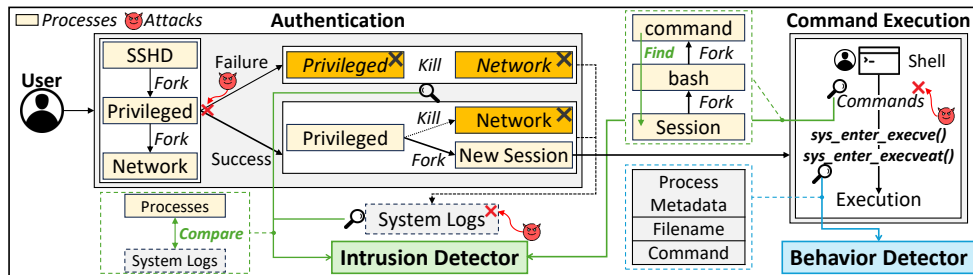


Figure 1: The Overall Architecture and Workflow of Mitra System

*Proceedings of the 8th International Conference on Mobile Internet Security (MobiSec'24), Article No. P-71, December 17-19, 2024, Sapporo, Japan. © The copyright of this paper remains with the author(s).

monitoring of SSH session lifecycles, detecting potential threats such as brute-force attacks, stealth access attempts, and log evasion at various stages of the session.

The **Intrusion Detector** begins by monitoring the SSH authentication process. It tracks the creation and termination of 'Privileged' and 'Network' processes, forked by SSHD during authentication, to detect authentication anomalies. Continuous authentication failures—exceeding one per second over a 10-second period—are flagged as brute-force attacks [1]. After successful authentication, it cross-checks system logs to detect stealth access attempts and monitors the process hierarchy to identify the ownership of executed commands and activities, ensuring comprehensive tracking of user sessions.

The **Behavior Detector** then focuses on post-authentication activities, particularly command executions. It traces system calls, such as `sys_enter_execve`, to gather metadata such as filenames and command details, enabling real-time user action tracking. Also, it monitors for malicious behaviors, including attempts to delete or alter system logs, ensuring that suspicious activities during sessions are quickly detected.

Figure 2 presents the results of CPU and memory usages, and latency variations on an SSH server equipped with an Intel Xeon Gold 5220R (8 vCPUs) and 16GB of RAM during high-frequency login simulations (over 100 attempts per second for one minute, repeated five times) [2]. The results indicate minimal overhead, with all metrics showing less than a 5.7% increase in resource utilization.

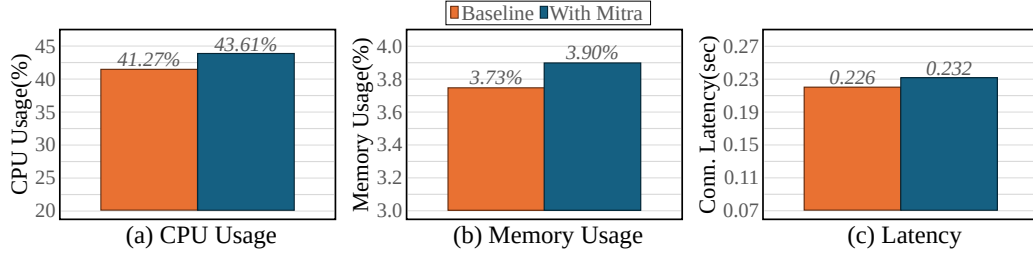


Figure 2: Performance Measurements with and without Mitra Systems

3 Conclusion

In this paper, we introduced Mitra, an eBPF-based real-time SSH monitoring system. By leveraging kernel-level monitoring that operates independently of system logs, Mitra effectively mitigates log manipulation and evasion attempts while maintaining minimal overhead, with CPU utilization staying below 5.7%. Future work will focus on improving detection mechanisms for more advanced attack vectors, such as SSH key compromise attempts, and expanding the monitoring framework to support additional remote access protocols, including VNC and RDP.

Acknowledgement: This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICAN (ICT Challenge and Advanced Network of HRD) support program (IITP-2024-RS-2023-00259867) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

- [1] Jim Owens and Jeanna Matthews. A study of passwords and methods used in brute-force SSH attacks. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats*, 2008.

- [2] Anna Sperotto, Ramin Sadre, Pieter-Tjerk de Boer, and Aiko Pras. Hidden Markov Model modeling of SSH brute-force attacks. In *IFIP/IEEE International Workshop on Distributed Systems: Operations and Management*, 2009.