Masterarbeits

Structure embeddings for OpenSSH heap dump analysis

A report by

Lahoche, Clément Claude Martial

Prüfer

Prof. Dr. Michael Granitzer

Christofer Fellicious

Prof. Dr. Pierre-Edouard Portier

August 17, 2023

Abstract

Acknowledgements

Contents

List of Figures

List of Tables

1 Introduction

Digital forensics stands as a cornerstone of cybersecurity and investigation. It provides the means to retrieve crucial evidence from devices, including personal computers. Such evidence is instrumental in identifying malware or tracing the digital footprints of potential intruders. A predominant technique in this domain involves analyzing the contents of a device's primary memory. The integration of machine learning offers a promising avenue to enhance and refine these analysis processes.

Moreover, As the demand for secure communication channels grows, protocols like Secure Shell (SSH) have become ubiquitous. However, these very channels, designed for security, can sometimes obscure malicious activities, making traditional investigative methods less effective. Recent research has highlighted innovative approaches to address these challenges. For instance, the study on „SmartKex: Machine Learning Assisted SSH Keys Extraction From The Heap Dump“ [1] underscores the potential of machine learning in enhancing the extraction of session keys from memory snapshots of OpenSSH processes. Furthering this line of inquiry, another pivotal work titled „SSHkex: Leveraging virtual machine introspection for extracting SSH keys and decrypting SSH network traffic“ [2] introduced the concept of leveraging Virtual Machine Introspection (VMI) for extracting SSH's session keys directly from a server's memory.

2 Research Questions

Write down and explain your research questions (2-5)

3 Structure of the Thesis

Explain the structure of the thesis.

4 Example citation & symbol reference

For symbols look at.

5 Example reference

Example reference: Look at chapter 1, for sections, look at section 4.

Figure 1: Meaningful caption for this image

First column	Number column
Accuracy	0.532
F1 score	0.87

Table 1: Meaningful caption for this table

6 Example image

Example figure reference: Look at Figure 1 to see an image. It can be `jpg`, `png`, or best: `pdf` (if vector graphic).

7 Example table

Table 1 shows a simple table[1]

[1] Check `https://en.wikibooks.org/wiki/LaTeX/Tables` on syntax

8 Background

Introduce the related state-of-the-art and background information in order to understand the method developed in the thesis.

9 Methods

Describe the method/software/tool/algorithm you have developed here

10 Results

Describe the experimental setup, the used datasets/parameters and the experimental results achieved

11 Discussion

Discuss the results. What is the outcome of your experimetns?

12 Conclusion

Summarize the thesis and provide a outlook on future work.

A Code

B Math

C Dataset

Acronymes

SSH Secure Shell. 1

VMI Virtual Machine Introspection. 1

References

[1] Christofer Fellicious et al. „SmartKex: Machine Learning Assisted SSH Keys Extraction From The Heap Dump“. In: arXiv:2209.05243 (Sept. 13, 2022). arXiv: `2209.05243[cs]`. URL: `http://arxiv.org/abs/2209.05243` (visited on 08/17/2023).

[2] Stewart Sentanoe and Hans P. Reiser. „SSHkex: Leveraging virtual machine introspection for extracting SSH keys and decrypting SSH network traffic“. In: *Forensic Science International: Digital Investigation* 40 (Apr. 2022), p. 301337. ISSN: 26662817. DOI: `10.1016/j.fsidi.2022.301337`. URL: `https://linkinghub.elsevier.com/retrieve/pii/S2666281722000063` (visited on 08/17/2023).

Additional bibliography

[3] Vivek Gite. *How To Reuse SSH Connection To Speed Up Remote Login Process Using Multiplexing.* nixCraft. Aug. 20, 2008. URL: `https://www.cyberciti.biz/faq/linux-unix-reuse-openssh-connection/` (visited on 10/21/2022).

[4] Weijie Huang and Jun Wang. „Character-level Convolutional Network for Text Classification Applied to Chinese Corpus“. In: arXiv:1611.04358 (Nov. 15, 2016). arXiv: `1611.04358[cs]`. URL: `http://arxiv.org/abs/1611.04358` (visited on 08/17/2023).

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich diese Masterarbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe und alle Ausführungen, die wörtlich oder sinngemäß übernommen wurden, als solche gekennzeichnet sind, sowie, dass ich die Masterarbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt habe.

Passau, August 17, 2023

Lahoche, Clément Claude Martial