IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 6, Ser. I (Nov. –Dec. 2021), PP 27-28
www.iosrjournals.org

Your Linux Passwords Are in Danger: MimiDove Meets the Challenge

Igor Korkin[1], Svetlana Golub[2]
Independent Researcher, igor.korkin@gmail.com
Bachelor of Cyber Security, glb.svtln@gmail.com

GNOME desktop environment stores user's credentials in process memory, which poses an obvious danger and needs to be fixed. The competitive advantage of the proposed security tool (MimiDove) includes its ability to quickly detect and remove passwords containing both ASCII characters and Unicode characters.

Key words: *Linux passwords; application security; MimiPenguin; Mimipy;*

Date of Submission: 04-11-2021 Date of Acceptance: 18-11-2021

I. Introduction

Linux GNOME desktop uses gnome-keyring-daemon for storing security credentials such as usernames and passwords. After a user is logged in, the password is stored in daemon memory, and to prevent its leakage the password has to be zero-overwritten.

Security researcher Seong-Joong Kim [1] from South Korea discovered that gnome-keyring 3.18.3 does not overwrite users' credentials. These credentials are not cleared automatically and reside in plaintext in process memory. This happens because there are no routine calls to overwrite sensitive data due to unnecessary compiler optimization. As a result, any user with an appropriate privilege can extract them by memory acquisition.

Security researcher Hunter J. Gregal from the USA developed a tool called MimiPenguin [2] to extract user's passwords from the memory of gnome-keyring-daemon. MimiPenguin has several drawbacks: it is slow; it can gain passwords containing only ASCII characters; it does not support removing the extracted passwords.

Another researcher Nicolas Verdier from the USA has improved MimiPenguin tool and implemented a new tool called Mimipy [3]. This tool can do both: location and removing passwords from memory. However, Mimipy has the same drawbacks as MimiPenguin: it works slowly and can protect ASCII-character passwords only.

MimiDove

We have analyzed the gnome-keyring-daemon memory for CentOS by using different accounts in one machine. We have proved that gnome-keyring-daemon stores the users' passwords in memory and all passwords are located in the same memory area. This fact makes it possible to significantly speed up the process of searching for the passwords in memory.

Research of 'gnome-keyring-daemon' revealed that users' passwords are located in stack, which is mapped via anonymous regions (i.e. not file backed) with enabled RW access.

MimiDove algorithm includes the following steps:

1. Extract user hashes from /etc/shadow.
2. Dump "gnome-keyring-daemon" using /proc/PID/maps.
3. Locate possible passwords: for each memory chunk extract the strings of 4-256 symbols.
4. Calculate hash(string) and check if match with users' hashes.
5. Zeroing extracted passwords.

UNIX-based operating systems are ubiquitous all over the world and in general cases users' passwords can include both ASCII and Unicode characters. It is crucial for OS security to prevent password leakage including UNICODE-based passwords.

To meet this challenge a new open-source tool called MimiDove [4] has been developed. It expands the MimiPenguin and Mimipy features and includes the following competitive advantages: it can locate and remove passwords containing both ASCII characters and Unicode characters; it is also much faster.
The comparison table is given below.

Tool Name	Average Work Time, sec	Locate ASCII passwords	Locate UNICODE passwords	Remove ASCII passwords	Remove UNICODE passwords
MimiPenguin	150	YES	NO	NO	NO
Mimipy	90	YES	NO	YES	NO
MimiDove	**20**	**YES**	**YES**	**YES**	**YES**

MimiDove has been successfully tested using the following OSes:

- CentOS 7.8.2003, GNOME Keyring 3.28.2
- Ubuntu 18.04.4 LTS, GNOME Keyring 3.28.0.2
- Ubuntu 20.04.2 LTS, GNOME Keyring 3.36.0
- Kali GNU/Linux Rolling, GNOME Keyring 3.36.0

The Gnome Keyring developers have been informed about this issue since 2017, but this issue still exists for several versions of the GNOME keyring. The plaintext passwords are still located in memory. MimiDove meets this challenge.

II. Conclusion

- First, it has been proved that the GNOME desktop environment stores users' passwords in plain text, which is crucial for many users and systems. MimiPenguin can extract them from memory, while MiniPy can also overwrite them. Both these tools support only ASCII characters passwords, without UNICODE symbols support. It is crucial for OS security to prevent password leakage including UNICODE-based passwords.
- Second, a new open-source tool called MimiDove has been released, which extends the features of MimiPenguin and MiniPy. The tool can quickly detect and remove passwords containing both ASCII characters and Unicode characters. MimiDove has been successfully checked on various systems: CentOS, Ubuntu, Kali GNU/Linux Rolling.

References:

[1]. F. Besson, A. Dang, T. Jensen (2018). Securing Compilation Against Memory Probing. PLAS '18 – 13th Workshop on Programming Languages and Analysis for Security

[2]. H. Gregal. (2017). Mimipenguin. https://github.com/huntergregal/mimipenguin

[3]. N. Verdier, (2017). Mimipy. https://github.com/n1nj4sec/mimipy

[4]. S. Golub. (2021). MimiDove. https://github.com/SvetlanaGolub/MimiDove

Igor Korkin. "Your Linux Passwords Are in Danger: MimiDove Meets the Challenge." *IOSR Journal of Computer Engineering (IOSR-JCE),* 23(6), 2021, pp. 27-28.