Your Linux Passwords Are in Danger: MimiDove Meets the Challenge

Svetlana Golub
Igor Korkin

Who we are

Svetlana Golub

- Bachelor of Cyber Security
- alumni of NRNU MEPhI (Moscow Engineering Physics Institute)
- Cryptology and Cybersecurity Department

Igor Korkin, PhD

- Supervisor
- Speaker at BlackHat, HITB, CDFSL
- Independent Researcher

Clear text passwords in process memory:

memset ( )

- gnome-keyring-daemon
- apache2
- vsftpd
- sshd
- gdm-password

Seong-Joong Kim – "Credentials located in gnome-keyring can be compromised easily"

MimiPenguin

by Hunter Gregal

"A tool to dump the login password from the current Linux desktop user"

```
[svetlana@localhost mimipenguin]$ sudo ./mimipenguin
[+] Searching: [SYSTEM - GNOME] (gnome-keyring-daemon)
  [-] user1:Cul1rZ4rgEJdampeW85l
  [-] user2:MVG+tJ,$^Jk='-lR_wfH
It takes 0 minutes 31 seconds
```

MimiPy

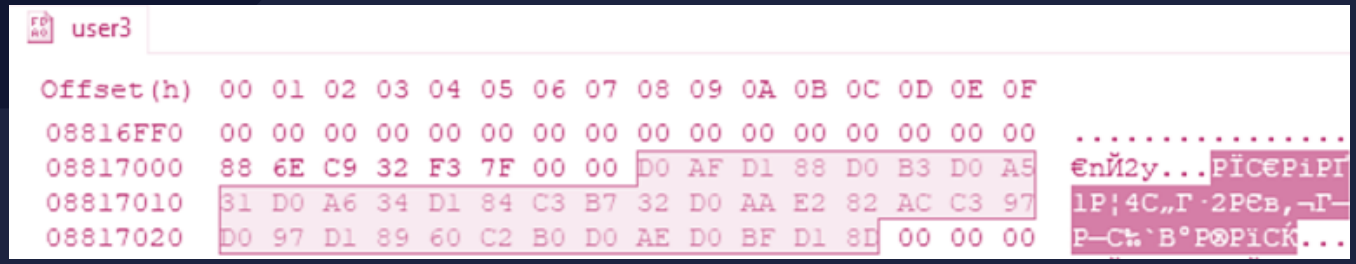
by Nicolas Verdier

- It can locate passwords in memory and overwrite them to prevent their leakage

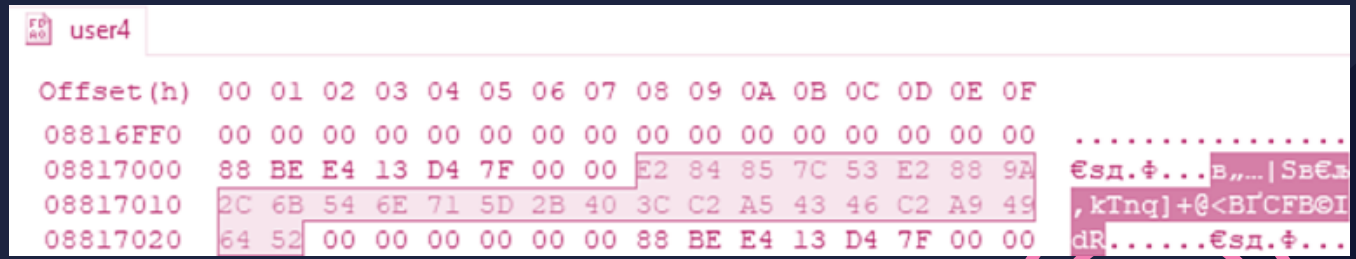
```
[svetlana@localhost mimipy]$ sudo python mimipy.py
[SYSTEM - GNOME] :
        - Process       : /usr/bin/gnome-keyring-daemon
        - Username      : user1
        - Password      : Cul1rZ4rgEJdampeW85l
[SYSTEM - GNOME] :
        - Process       : /usr/bin/gnome-keyring-daemon
        - Username      : user2
        - Password      : MVG+tJ,$^Jk='-lR_wfH
Script executed in 20.4207558632 seconds
```

Let's try some Unicode in passwords:

- ЯшгХ1Ц4ф÷2Ъ€×3щ`°Юпэ 0xd0afd188d0b3d0a531…



- %|S√,kTnq]+@<¥CF©IdR 0xe284857c53e2889a2c…



The downsides of MimiPenguin and MimiPy

— They cannot dump passwords with Unicode, only the ASCII characters are supported:

```
[svetlana@localhost mimipenguin]$ sudo ./mimipenguin
[+] Searching: [SYSTEM - GNOME] (gnome-keyring-daemon)
It takes 0 minutes 46 seconds
```

```
[svetlana@localhost mimipy]$ sudo python mimipy.py
Script executed in 35.502106905 seconds
```

— They are so slow …

MimiDove Can Tackle both challenges!

— Now Unicode symbols will be located:

```
[svetlana@localhost MimiDove]$ sudo ./mimidove
[+] Searching: [SYSTEM - GNOME] (gnome-keyring-daemon)
  [-] user3:ЯшгX1Ц4ф÷2ъ€×3щ`°Юпэ
  [-] user4:%|S√,kTnq]+@<¥CF©IdR
It takes 8 minutes 18 seconds
[svetlana@localhost MimiDove]$
```

— Work time is 8 min. How to reduce it?

8

Why search everywhere?

— First, we determine the memory area

```
[svetlana@localhost MimiDove]$ sudo ./mimidove --region
Finding region of memory
[+] Searching: [SYSTEM - GNOME] (gnome-keyring-daemon)
  [-] user1:Cul1rZ4rgEJdampeW85l
Password was found in 23 region
```

— Second, we search only through this area

```
[svetlana@localhost MimiDove]$ sudo ./mimidove --region 23
Searching in 23 region of memory
[+] Searching: [SYSTEM - GNOME] (gnome-keyring-daemon)
  [-] user1:Cul1rZ4rgEJdampeW85l
  [-] user2:MVG+tJ,$^Jk='-lR_wfH
  [-] user3:ЯшгX1Ц4ф÷2Ъ€×3щ`°Ю∩э
  [-] user4:%|S√,kTnq]+@<¥CF©IdR
It takes 1,700 seconds
```

MimiDove Algorithm

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 fast algorithm:

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.

Keep your passwords safe. Overwrite them!

before

after

user4

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
08816FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
08817000	88	BE	E4	13	D4	7F	00	00	E2	84	85	7C	53	E2	88	9A	€зд.ф...в„…|Sв€љ
08817010	2C	6B	54	6E	71	5D	2B	40	3C	C2	A5	43	46	C2	A9	49	,kTnq]+@<BЃCFB©I
08817020	64	52	00	00	00	00	00	00	88	BE	E4	13	D4	7F	00	00	dR.....€зд.ф...
08817030	58	BE	E4	13	D4	7F	00	00	00	00	00	00	00	00	00	00	Xзд.ф.....
08817040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
08816FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
08817000	88	BE	E4	13	D4	7F	00	00	00	00	00	00	00	00	00	00	€зд.ф.....
08817010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
08817020	00	00	00	00	00	00	00	00	88	BE	E4	13	D4	7F	00	00	..€зд.ф...
08817030	58	BE	E4	13	D4	7F	00	00	00	00	00	00	00	00	00	00	Xзд.ф.....
08817040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Time to compare: technical features

Tool Name	Can it locate passwords?		Can it remove passwords?	
	ASCII	Unicode	ASCII	Unicode
MimiPenguin	+	–	–	–
Mimipy	+	–	+	–
MimiDove	✚	✚	✚	✚

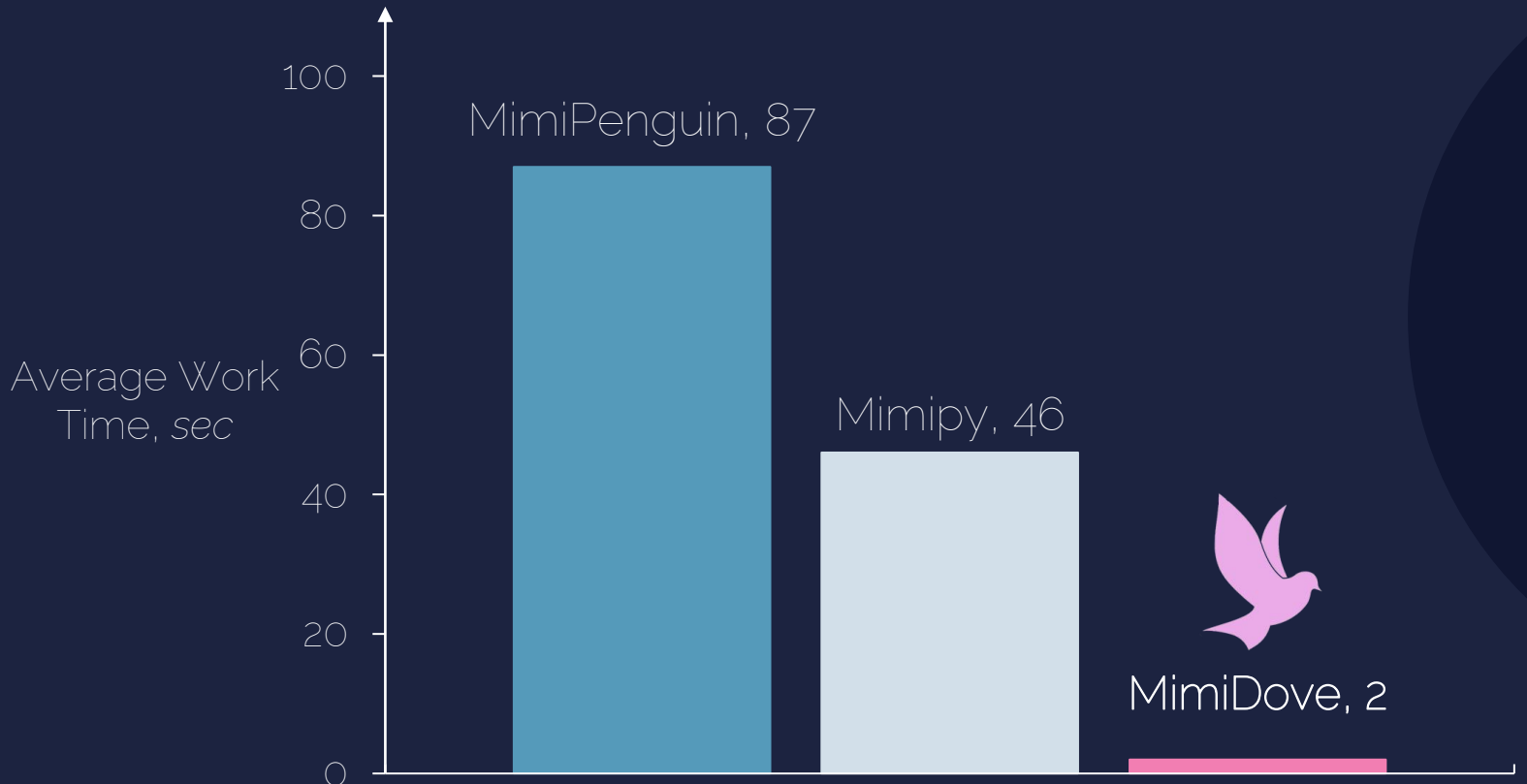
Example of tested passwords:

- Cul1rZ4rgEJdampeW85l
- MVG+tJ,$^Jk='-lR_wfH
- ЯшгX1Ц4ф÷2Ъ€×3щ`°Юпэ
- %|S√,kTnq]+@<¥CF©IdR

Example of tested 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

Time to compare: work time



github.com/SvetlanaGolub/MimiDove

Thank you

Svetlana Golub glb.svtln@gmail.com
github.com/SvetlanaGolub/MimiDove

Igor Korkin igor.korkin@gmail.com
igorkorkin.blogspot.com