Tranalyzer2

t2PSkel

t2PSkel
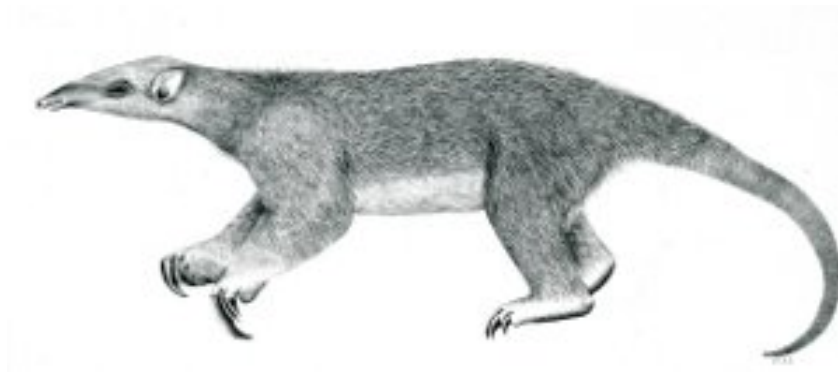
Tranalyzer Development Team

Contents

b

1   t2PSkel

1.1   Description

The t2PSkel plugin analyzes ...

1.2   Dependencies

1.2.1   External Libraries

This plugin depends on the **XXX** library.

Arch: `sudo pacman -S XXX`

Ubuntu/Kali: `sudo apt-get install XXX`

OpenSUSE: `sudo zypper install XXX`

Red Hat/Fedora: `sudo yum install XXX`

MAC OSX: `brew install XXX`

1.2.2   Other Plugins

This plugin requires the `tcpFlags` plugin.

1.2.3   Required Files

The file `file.txt` is required.

1.3   Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
T2PSKEL_VAR	0	Whether (1) or not (0) to output `t2PSkelVar`	
T2PSKEL_IP	0	General description of `T2PSKEL_IP` 0: description of value 0 1: description of value 1 2: description of value 2	
T2PSKEL_VEC	0	Description of `T2PSKEL_VEC`	`T2PSKEL_IP=1`

1.4   Flow File Output

The t2PSkel plugin outputs the following columns:

Column	Type	Description	Flags
t2PSkelStat	H8	Status	
t2PSkelText	S	describe t2PSkelText (string)	
t2PSkelVar	U64	describe t2PSkelVar (uint64)	T2PSKEL_VAR=1
t2PSkelIP	IP4	describe t2PSkelIP (IPv4)	T2PSKEL_IP=1
t2PSkelVar1_Var2	H32_H16	describe t2PSkelVar1_Var2	

If T2PSKEL_VEC=1, the following columns are displayed:

t2PSkelVar3_Var4	R(U8_U8)	describe t2PSkelVar1_Var2	
t2PSkelVector	R(R(D))	describe t2PSkelVector	

1.4.1   t2PSkelStat

The t2PSkelStat column is to be interpreted as follows:

t2PSkelStat	Description
0x01	Flow is t2PSkel
0x02	—
0x04	—
0x08	—

1.4.2   t2PSkelVar1

The t2PSkelVar1 column is to be interpreted as follows:

t2PSkelVar1	Description		t2PSkelVar1	Description
0x01	—		0x10	—
0x02	—		0x20	—
0x04	—		0x40	—
0x08	—		0x80	—

1.5   Packet File Output

In packet mode (-s option), the t2PSkel plugin outputs the following columns:

Column	Type	Description	Flags
t2PSkelCol1	I8	describe col1	

1.6   Plugin Report Output

The following information is reported:

- Number of XXX packets

- Aggregated status flags (`t2PSkelStat`)

1.7 Additional Output

Non-standard output:

- `PREFIX_suffix.txt`: description

1.8 Post-Processing

1.9 Example Output

1.10 Known Bugs and Limitations

1.11 TODO

- TODO1

- TODO2

1.12 References

- RFCXXXX: Title

- https://www.iana.org/assignments/