機器學習與資訊安全之應用

期中報告

Here is where your presentation begins

index

資料集描述

- 八個 malware family：Android、Bashlite、Mirai、Unknown、Tsunami、Dofloo、Xorddos 與 Hajime
- 不是 API call sequence，而是 system call sequence
- 主要使用 TIMESTAMP 跟 SYSCALL 兩個欄位

```
PID,TIMESTAMP,SYSCALL,CATEGORY,SPLIT,ARGC,ARG1,ARG2,ARG3,ARG4,ARG5,ARG6,RESULT,ELAPSED
1807,"1565514492.511934","execve",,0,3,"""/aafb16e1""","[""/aafb16e1""]","0x7fff1c6a23d8 /* 9 vars */",,,,0,"0.002625"
1807,"1565514492.523300","ioctl",,0,3,"0","TCGETS","0x7ffddcb70340",,,,"-1","0.000290"
1807,"1565514492.526832","ioctl",,0,3,"1","TCGETS","0x7ffddcb70340",,,,"-1","0.000225"
1807,"1565514492.528700","rt_sigprocmask",,0,4,"SIG_BLOCK","[INT]","NULL","8",,,0,"0.000389"
1807,"1565514492.531051","rt_sigaction",,0,4,"SIGCHLD","{sa_handler=SIG_IGN, sa_mask=[CHLD], sa_flags=SA_RESTORER|SA_RESTART,
sa_restorer=0x54349c}","{sa_handler=SIG_DFL, sa_mask=[], sa_flags=0}","8",,,0,"0.000269"
1807,"1565514492.533222","rt_sigaction",,0,4,"SIGTRAP","{sa_handler=0x424b90, sa_mask=[TRAP],
sa_flags=SA_RESTORER|SA_RESTART, sa_restorer=0x54349c}","{sa_handler=SIG_DFL, sa_mask=[], sa_flags=0}","8",,,0,"0.000225"
1807,"1565514492.534593","open","IO",0,2,"""/dev/watchdog""","O_RDWR",,,,,"-1","0.000694"
1807,"1565514492.538108","open","IO",0,2,"""/dev/misc/watchdog""","O_RDWR",,,,,"-1","0.000378"
1807,"1565514492.539324","shmget",,0,3,"IPC PRIVATE","209","IPC CREAT|0666",,,,0,"0.002137"
```

Siamese network for few -shot learning

方法一

10種類型

1.File system

2.Network

3.Time

4.Process management

5.Signals

6.Inter Process Communication

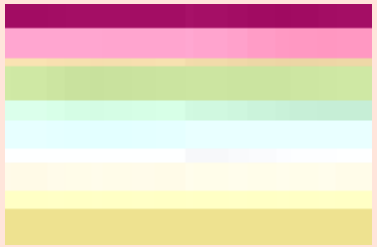
7.Non-uniform memory access

8.Linux key management

9.System-wide

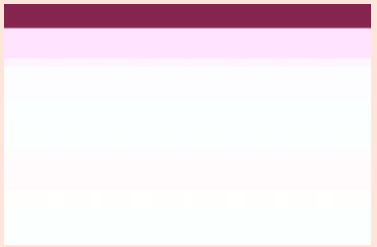
10.Other

Siamese network for few -shot learning
方法一



Bashlite

Miral



Unknown

- 2-shot-3-way
- 訓練張數:6張　　測試張數:1128張
- train accuracy:0.75　test accuracy:0.5

Siamese network for few -shot learning
方法二

- category 分類改用該 system call 需要引入哪個 header

SYNOPSIS top

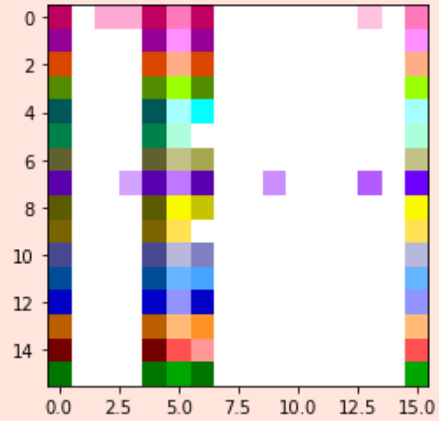
```
#include <unistd.h>

int execve(const char *pathname, char *const argv[],
           char *const envp[]);
```

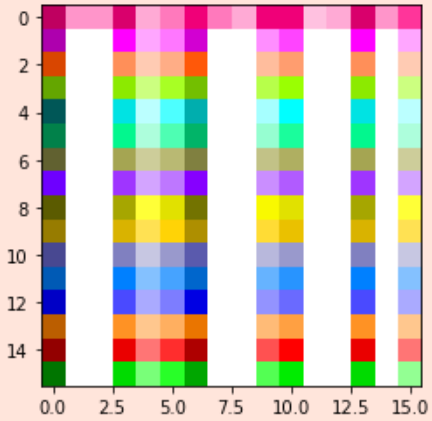
- 轉成 16 * 16 的 image
- 3 way 5 shot
- Train acc: 0.71 Test acc: 0.66

Siamese network for few -shot learning

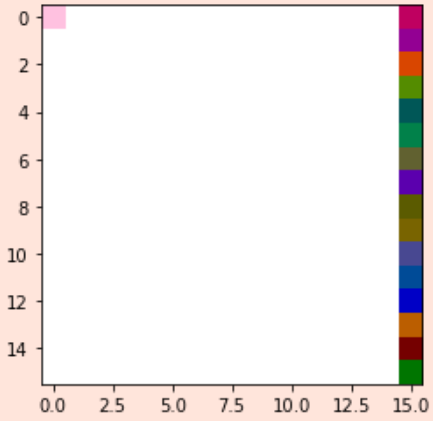
方法二



Mirai



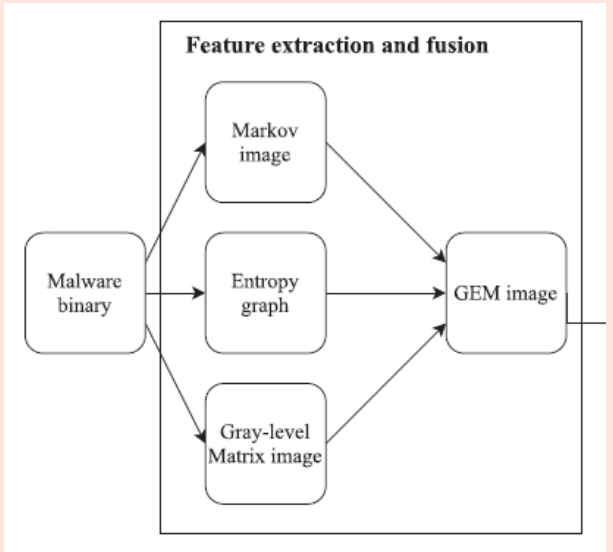
Dofloo



Bashlite

Siamese network for few -shot learning
方法三

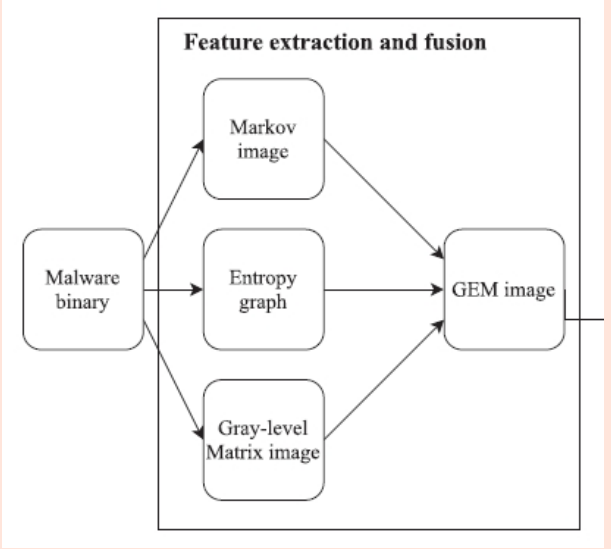
- input 使用 binary file
- 三種方法分別生成 RGB



- Markov image：取 binary 的 2-gram byte 的 frequency matrix 和 probability matrix
- Entropy graph：每 128 bit 切分成一個區塊，計算每個區塊的 Shannon entropy 後繪成圖表，再 resize 成 256 * 256

Siamese network for few -shot learning
方法三

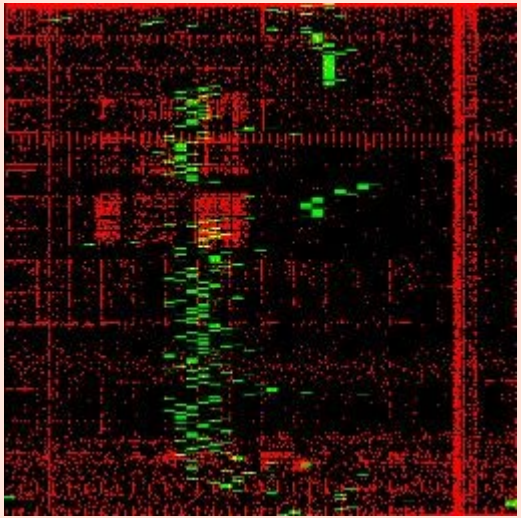
- Gray-level matrix image：將 2-gram byte matrix 的 frequency matrix 的數值降為 0~128，接著分別用 4 個角度 0度, 45度, 90度, 135度 的 Gray-Level Co-occurrence Matrix，Gray-Level Co-occurrence Matrix 是計算圖片 中不同角度下相鄰的 pixel 出現的機率，得出 4 個 128 * 128 的 matrix 後，將他們拼在一起，得到第三個 matrix。



Siamese network for few -shot learning
方法三

- Result
- 10 training data and 90 test data

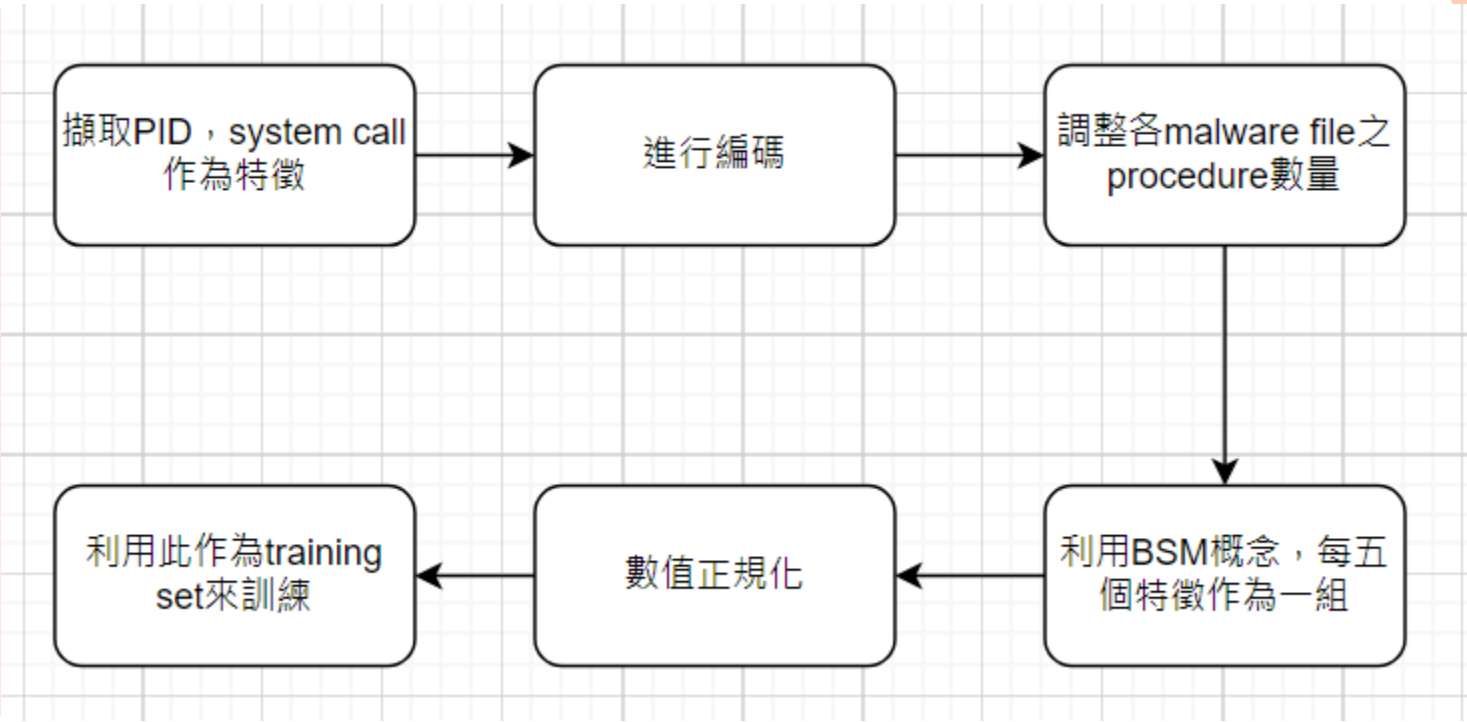
- Train loss: 0.3495
- Train accuracy: 0.7500
- Test loss: 0.69
- Test accuracy: 0.53



非few-shot 方法實作比較(BSM方法實作)

PID	TIMEST	SYSCALL	CATEGO	SPLIT	ARGC
2794	.57E+0	execve		0	
2794	.57E+0	rt_sigprocmask		0	
2794	.57E+0	rt_sigaction		0	
2794	.57E+0	rt_sigaction		0	
2794	.57E+0	socket		0	
2794	.57E+0	connect		0	
2794	.57E+0	getsockname		0	
2794	.57E+0	close	IO	0	
2794	.57E+0	brk		0	

非few-shot 方法實作比較(BSM方法實作)



非few-shot 方法實作比較(BSM方法實作)

```
Average scores for ten folds:
> Accuracy: 93.15210223197937 (+- 0.6515772298552106)
> Loss: 0.2691150188446045
----------------------------------------------------------------
DecisionTree:  0.9230577153306758
RandomForestClassifier:  0.95229585191617
KNeighborsClassifier:  0.9215201747115549
```

比較

Dynamic API call sequence visualization for malware classification	**Malicious Code Detection: Run Trace Output Analysis by LSTM**
image classification	text classification
經特徵提取後，需再轉換為 image	不須進行額外的轉換
惡意程式會將程式碼進行混淆，產生的 image 即有所不同，可能造成模型無法有效判斷	較能不受程式碼混淆技巧的影響
需要惡意程式完整的執行活動行為	擷取特徵時，不一定要有完整的執行行為
使用較少的training data便可得一定的準確率	需要較大量的training data才能有一定的準確率