加密勒索軟體行為偵測 (以Mac OS X為例)

Henry

HITCON 2016

About Me

- 黃禹程 (Henry)
- Developer at Verint
- 專長: Web Development
- 資安是興趣
- Chroot成員

大綱

- 偵測模型
- Mac OS X上用FUSE實作成果演示
- 實作說明
- 問題與討論
- 新專案：RansomCare
- 結論

與平台無關

偵測模型

對勒索軟體的假設

- 世上只有兩種勒索軟體
  - 覆寫型 (OVERWRITE): 加密並覆寫原檔
  - 開檔型 (NEW_FILE): 產生新加密檔並刪除原檔
- 一定會保留檔案全部內容
- 只具一般使用者權限
- [optional] 只關注某些檔案類型
  - Ex. docx, pptx, xlsx, pdf, png, jpg, ...

對勒索軟體的假設 (continued)

- 覆寫型: 必覆寫全檔，且檔案內容變質
  - MIME Type改變 (目前只採用此項)
  - 相似度變低
  - Entropy變高
- 開檔型: 必讀取全檔，且讀完會刪檔
- 進入點是readdir (列出某目錄下的檔案)

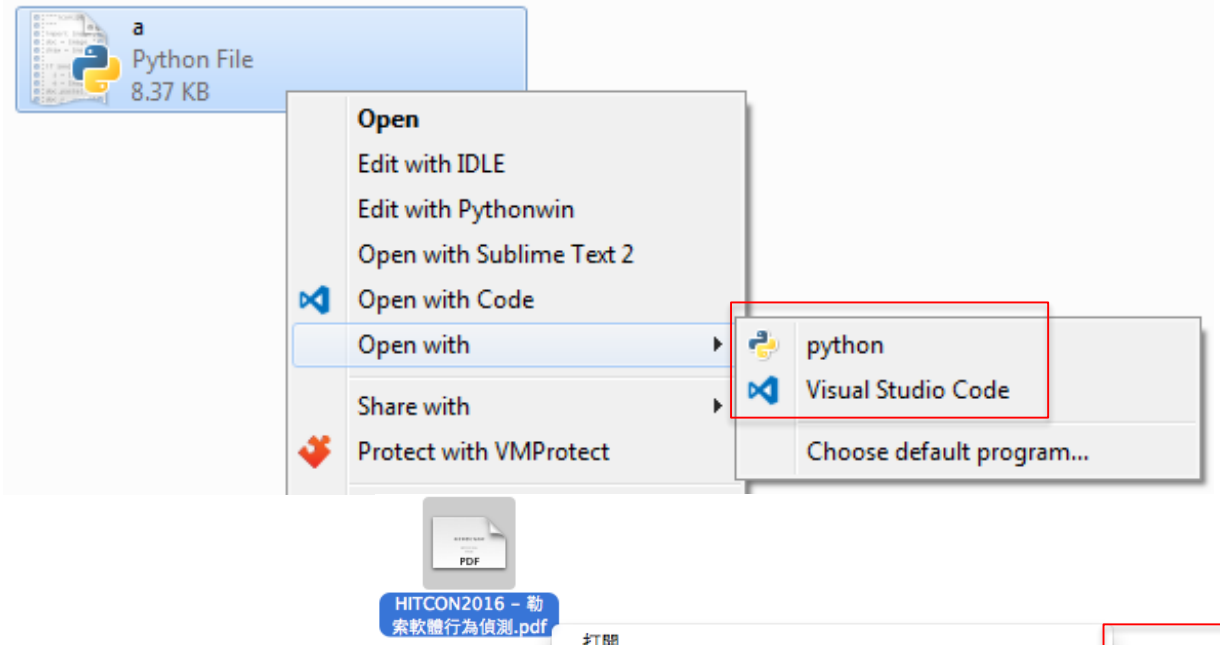
歸納：執行路徑

- 覆寫型：***readdir → open → read all → write all → release (檔案變質)***
- 開檔型：***readdir → open → read all → (write to somewhere) → unlink***
- 對所有行程都追蹤這麼長的路徑很耗資源
  - 利用白名單

合理的白名單？

- 系統程式
- 在開啟選單中的程式
- 所開檔案副檔名不被關注
  - 不是.docx, .pdf, .png, ...

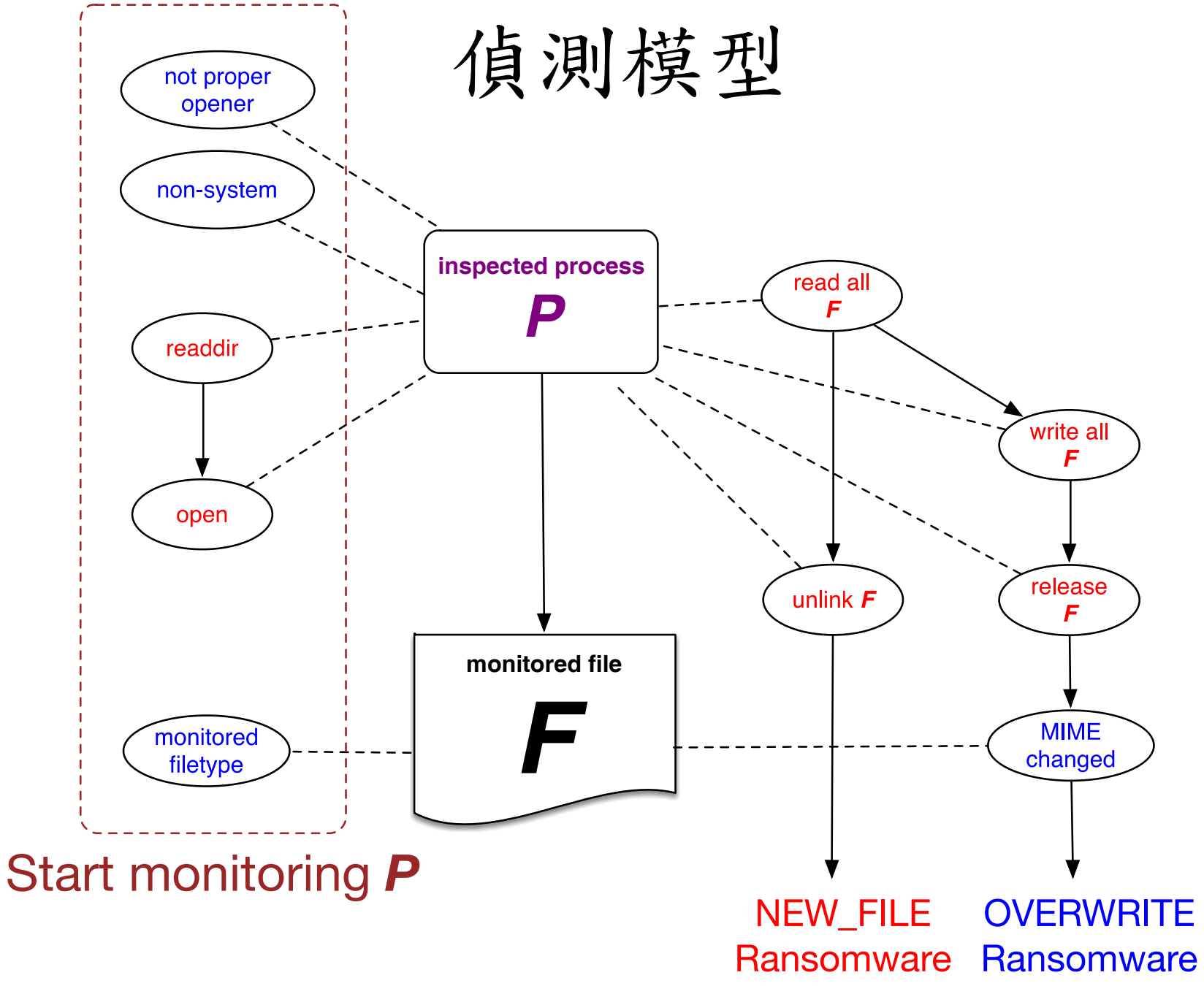
開啟選單


a
Python File
8.37 KB
Open
Edit with IDLE
Edit with Pythonwin
Open with Sublime Text 2
Open with Code
Open with
Share with
Protect with VMProtect
python
Visual Studio Code
Choose default program...

PDF
HITCON2016 – 勒索軟體行為偵測.pdf

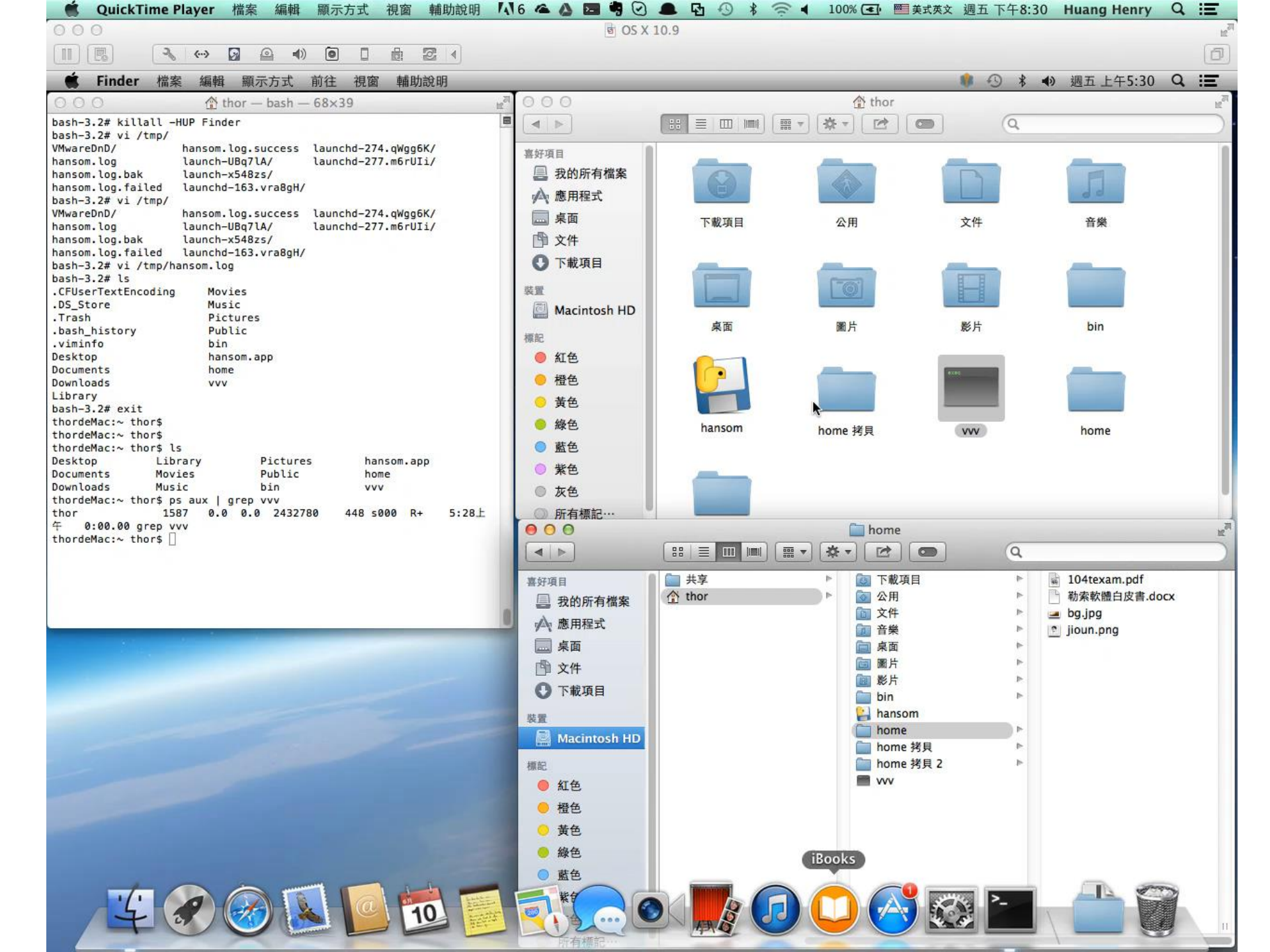

打開
打開檔案的應用程式
丟到垃圾桶
簡介
壓縮「HITCON2016 – 勒索軟體行為偵測.pdf」
將「HITCON2016 – 勒索軟體行為偵測.pdf」燒錄到光碟…
複製
製作替身
快速查看「HITCON2016 – 勒索軟體行為偵測.pdf」
共享
拷貝「HITCON2016 – 勒索軟體行為偵測.pdf」
剪下 "HITCON2016 – 勒索軟體行為偵測.pdf"
整理所選範圍
打開顯示方式選項
標記…
預覽程式（預設值）
010 Editor
Adobe Acrobat
Adobe Illustrator CS6
Adobe Photoshop CS6
Adobe Reader 9.3 — Malware_Forensics_Course（VMware Fusion 8.1.0）
ColorSync 工具程式
Evernote
GIMP
Google Chrome
iBooks（1.0.1）
LaTeXiT
Mendeley Desktop（1.11）
OmniGraffle（6.0.5）
OmniGraffle 5 Professional（5.4.4）
PDF Toolkit（1.8）
PDFpenPro
Safari

偵測模型

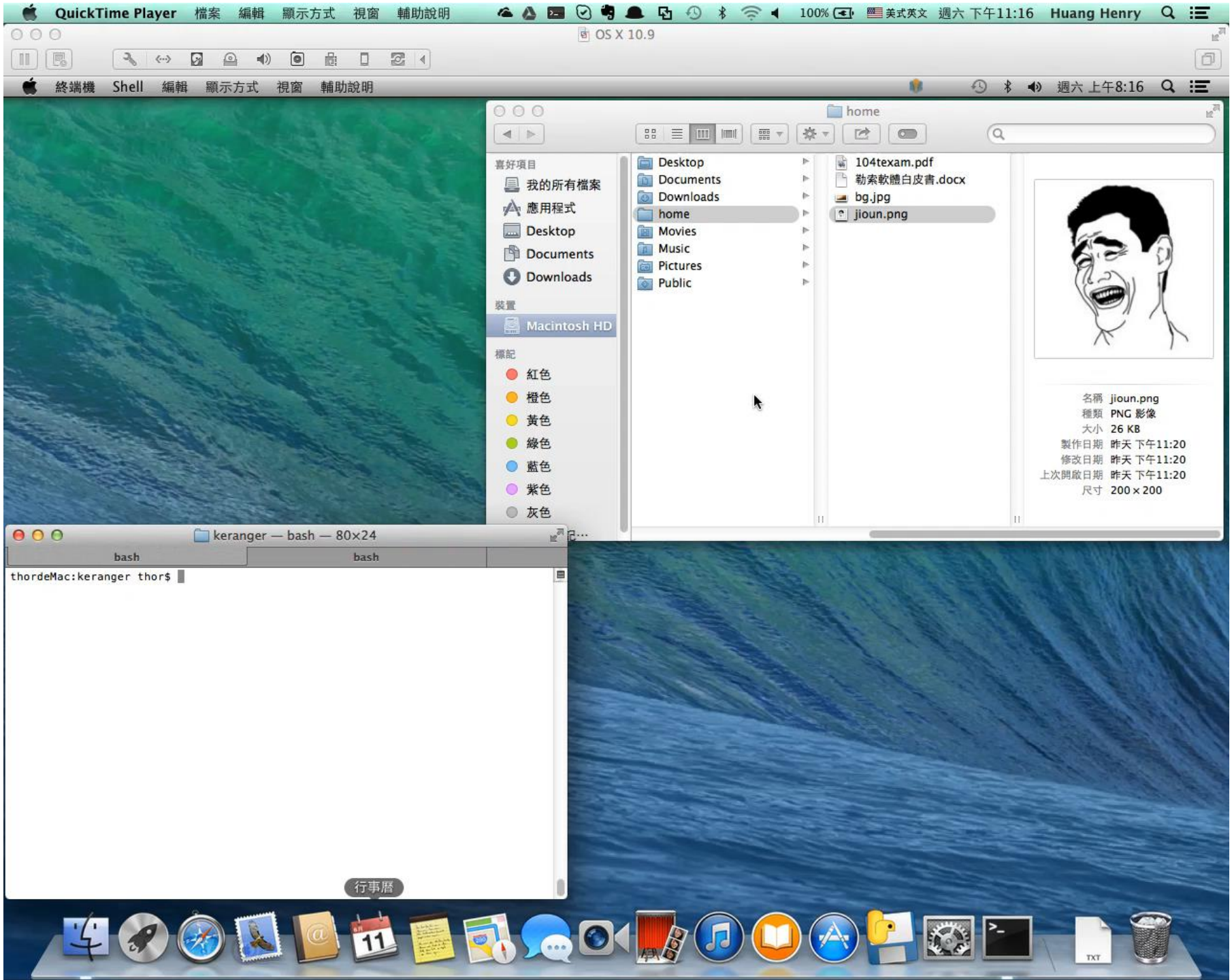

not proper opener
non-system
readdir
open
inspected process
P
read all
F
write all
F
unlink F
release
F
monitored file
F
monitored filetype
MIME changed
Start monitoring P
NEW_FILE
Ransomware
OVERWRITE
Ransomware

Hansom - 用FUSE實作的Proof of Concept

DEMO - HANSOM


QuickTime Player 檔案 編輯 顯示方式 視窗 輔助說明
100% 美式英文 週五 下午8:30 Huang Henry
OS X 10.9
Finder 檔案 編輯 顯示方式 前往 視窗 輔助說明
週五 上午5:30
thor — bash — 68×39
bash-3.2# killall -HUP Finder
bash-3.2# vi /tmp/
VMwareDnD/ hansom.log.success launchd-274.qWgg6K/
hansom.log launch-UBq7lA/ launchd-277.m6rUIi/
hansom.log.bak launch-x548zs/
hansom.log.failed launchd-163.vra8gH/
bash-3.2# vi /tmp/
VMwareDnD/ hansom.log.success launchd-274.qWgg6K/
hansom.log launch-UBq7lA/ launchd-277.m6rUIi/
hansom.log.bak launch-x548zs/
hansom.log.failed launchd-163.vra8gH/
bash-3.2# vi /tmp/hansom.log
bash-3.2# ls
.CFUserTextEncoding Movies
.DS_Store Music
.Trash Pictures
.bash_history Public
.viminfo bin
Desktop hansom.app
Documents home
Downloads vvv
Library
bash-3.2# exit
thordeMac:~ thor$
thordeMac:~ thor$
thordeMac:~ thor$ ls
Desktop Library Pictures hansom.app
Documents Movies Public home
Downloads Music bin vvv
thordeMac:~ thor$ ps aux | grep vvv
thor 1587 0.0 0.0 2432780 448 s000 R+ 5:28上午 0:00.00 grep vvv
thordeMac:~ thor$
thor
喜好項目
我的所有檔案
應用程式
桌面
文件
下載項目
裝置
Macintosh HD
標記
紅色
橙色
黃色
綠色
藍色
紫色
灰色
所有標記…
下載項目
公用
文件
音樂
桌面
圖片
影片
bin
hansom
home 拷貝
vvv
home
home
共享
thor
下載項目
公用
文件
音樂
桌面
圖片
影片
bin
hansom
home
home 拷貝
home 拷貝 2
vvv
104texam.pdf
勒索軟體白皮書.docx
bg.jpg
jioun.png
iBooks


QuickTime Player 檔案 編輯 顯示方式 視窗 輔助說明
100% 美式英文 週六 下午2:21 Huang Henry
OS X 10.9
Finder 檔案 編輯 顯示方式 前往 視窗 輔助說明
週五 下午11:21
thor
喜好項目
我的所有檔案
應用程式
桌面
文件
下載項目
裝置
Macintosh HD
標記
紅色
橙色
黃色
綠色
藍色
紫色
灰色
所有標記…
下載項目
公用
文件
音樂
桌面
圖片
影片
hansom
ransom_overwrite
home
home 拷貝
home 拷貝 2
home
104texam.pdf
勒索軟體白皮書.docx
bg.jpg
jioun.png
備忘錄


QuickTime Player 檔案 編輯 顯示方式 視窗 輔助說明
100% 美式英文 週六 下午11:16 Huang Henry
OS X 10.9
終端機 Shell 編輯 顯示方式 視窗 輔助說明
週六 上午8:16
home
喜好項目
我的所有檔案
應用程式
Desktop
Documents
Downloads
裝置
Macintosh HD
標記
紅色
橙色
黃色
綠色
藍色
紫色
灰色
Desktop
Documents
Downloads
home
Movies
Music
Pictures
Public
104texam.pdf
勒索軟體白皮書.docx
bg.jpg
jioun.png
名稱 jioun.png
種類 PNG 影像
大小 26 KB
製作日期 昨天 下午11:20
修改日期 昨天 下午11:20
上次開啟日期 昨天 下午11:20
尺寸 200 × 200
keranger — bash — 80×24
bash
bash
thordeMac:keranger thor$
行事曆

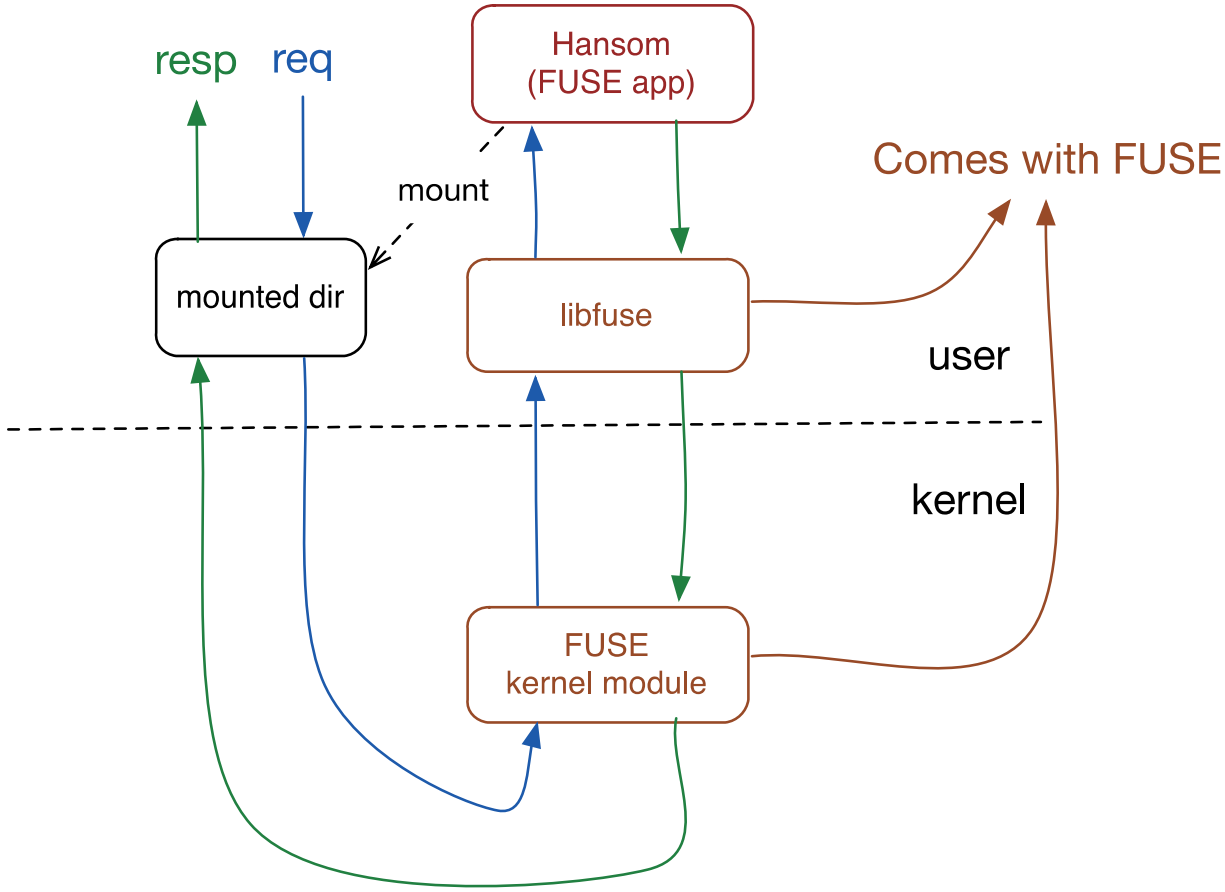
Hansom如何利用FUSE來偵測ransomware？

實作說明

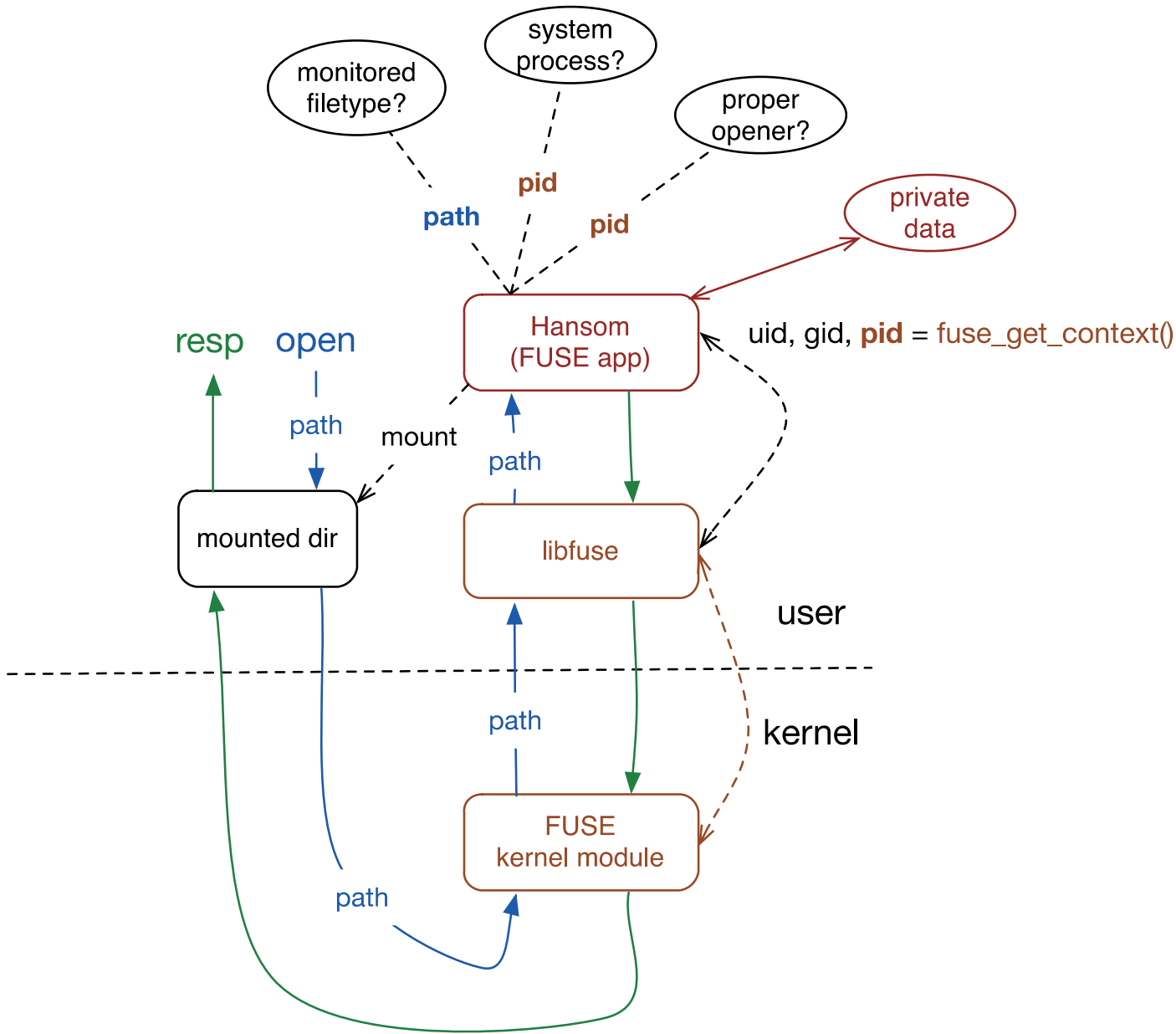
FUSE[1]

- Filesystem in USErspace (OSX: osxfuse[2])
  - FUSE kernel module
  - libfuse[3] (library in userspace)
- FUSE的kernel module把filesystem的操作請求交由userspace的程式來作回應

圖解Hansom實作


resp
req
Hansom
(FUSE app)
mount
Comes with FUSE
mounted dir
libfuse
user
kernel
FUSE
kernel module

例：open

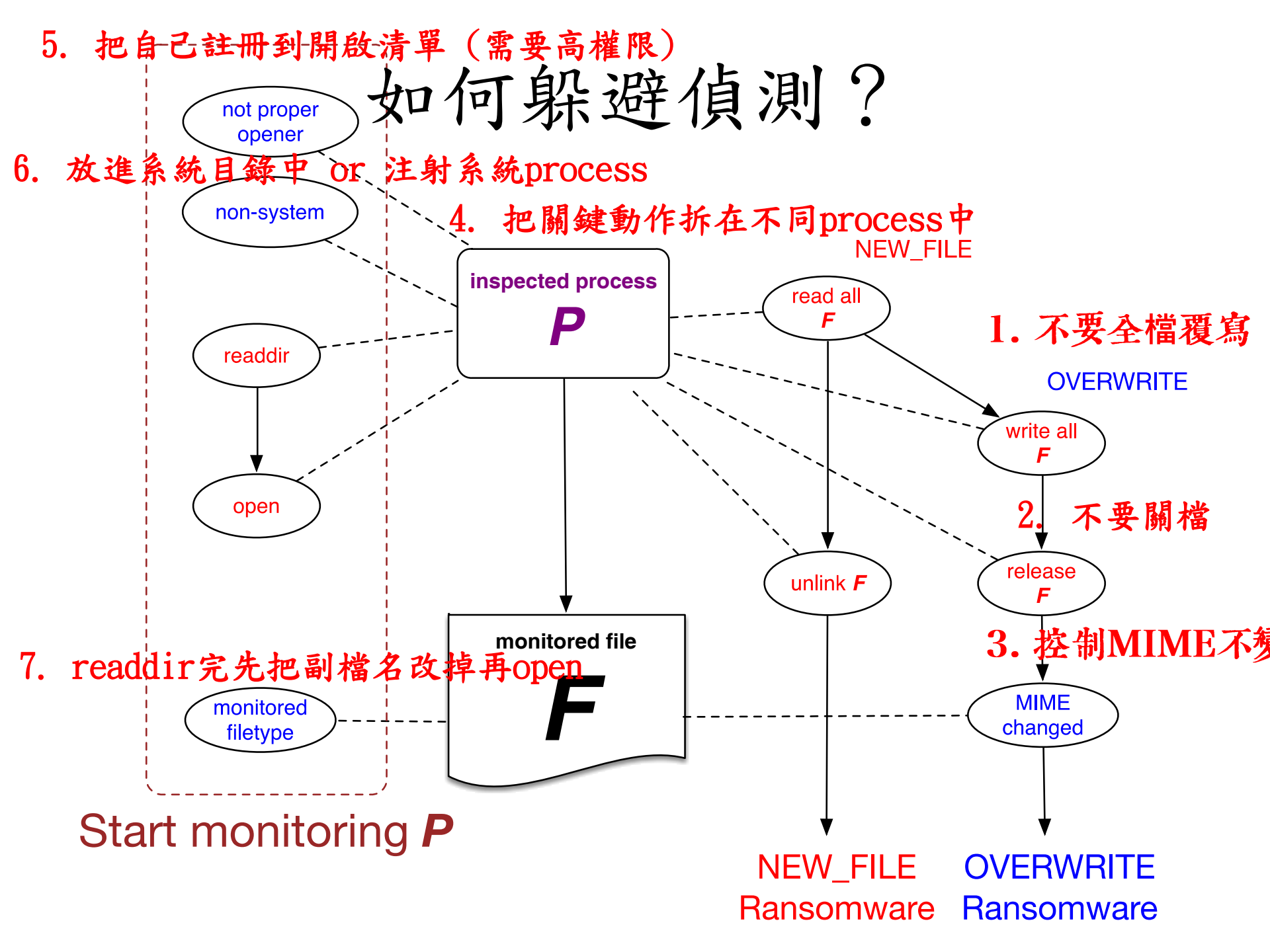

system process?
monitored filetype?
proper opener?
pid
path
pid
private data
Hansom (FUSE app)
uid, gid, pid = fuse_get_context()
resp
open
path
mount
path
mounted dir
libfuse
user
path
kernel
FUSE kernel module
path

如何躲避偵測？改進空間？

問題與討論

5. 把自己註冊到開啟清單（需要高權限）

如何躲避偵測？

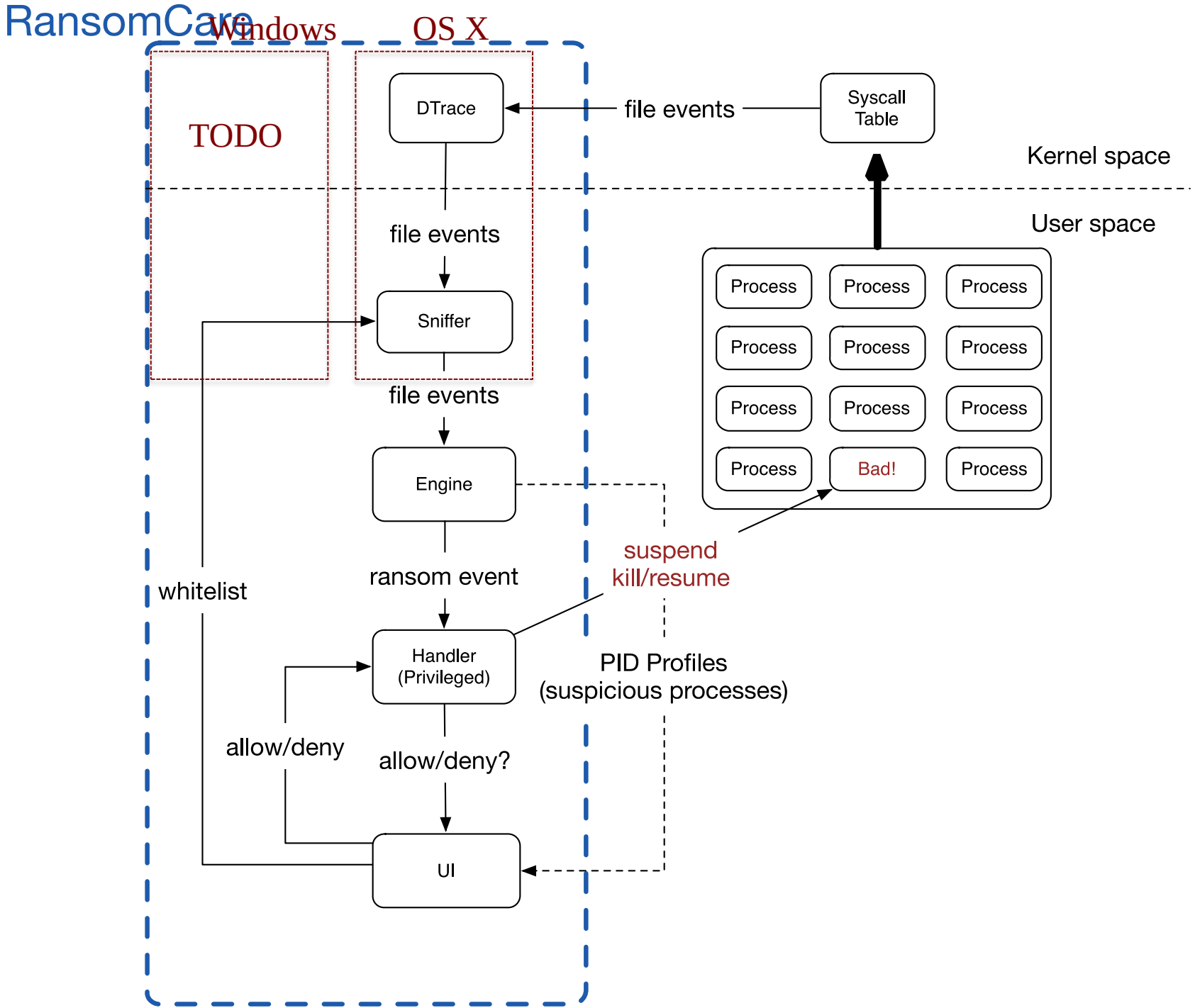


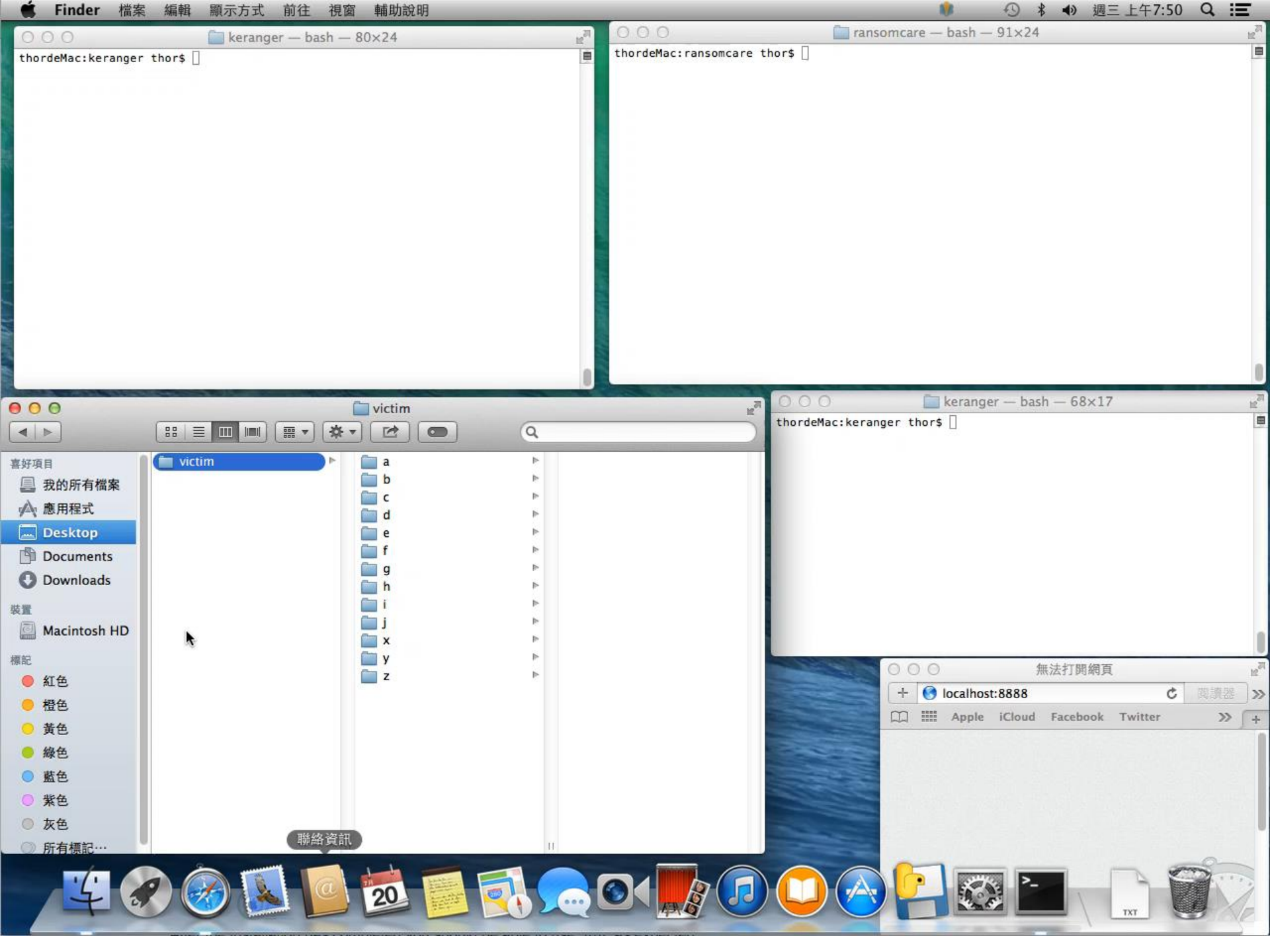
改進空間及方向？

- 偵測方式：inline mode v.s. sniffer mode
- FUSE的作法
  - Inline mode
  - Ransomware演化前可有效偵測
  - 會影響系統效能 (syscall從kernel → user → kernel)
- 較理想的作法
  - 從Kernel mode將關鍵行為事件傳回user mode判斷
    - 判斷跟系統操作非同步 → 不影響系統穩定性
  - User mode: 監控honey file

https://github.com/Happyholic1203/ransomcare

RANSOMCARE


RansomCare
Windows
OS X
TODO
DTrace
file events
Syscall Table
Kernel space
User space
file events
Sniffer
Process
Process
Process
Process
Process
Process
Process
Process
Process
Process
Bad!
Process
file events
Engine
suspend
kill/resume
whitelist
ransom event
Handler (Privileged)
PID Profiles
(suspicious processes)
allow/deny
allow/deny?
UI


Finder 檔案 編輯 顯示方式 前往 視窗 輔助說明
週三 上午7:50
keranger — bash — 80×24
thordeMac:keranger thor$
ransomcare — bash — 91×24
thordeMac:ransomcare thor$
victim
喜好項目
我的所有檔案
應用程式
Desktop
Documents
Downloads
裝置
Macintosh HD
標記
紅色
橙色
黃色
綠色
藍色
紫色
灰色
所有標記…
a
b
c
d
e
f
g
h
i
j
x
y
z
keranger — bash — 68×17
thordeMac:keranger thor$
無法打開網頁
localhost:8888
Apple
iCloud
Facebook
Twitter
聯絡資訊

結論

結論

- 本模型只看行為 → 與平台無關
- 該模型能偵測KeRanger及自製ransomwares
  - 尚未在OSX外實驗
- Ransomware會演化 勢必會有一番攻防
  - 最頭痛的演化方向：高權限、DLL side loading等
- 知道盾的作法 也探討了矛的新切入角度
- Inline mode penalty: 系統效能/穩定性
- Sniffer mode penalty: 有些檔案會犧牲 誤判率較高

Reference

- [1] FUSE https://en.wikipedia.org/wiki/Filesystem_in_Userspace
- [2] osxfuse https://osxfuse.github.io/
- [3] libfuse https://github.com/libfuse/libfuse

Related Works

- Emsisoft Behavior Blocker (2015)
  - 成功偵測20支ransomware (連結裡有demo)
- CryptoDrop (IEEE ICDCS 2016)
  - 成功偵測492個ransomware sample
  - Windows Kernel Driver
  - Indicators
    - File Type Changes: magic number
    - File Similarity: sdhash outputs similarity bettween two files
    - Shannon Entropy: entropy of an array of bytes

各位的指教都是進步的動力！

Q & A?

謝謝！