科技部資訊安全實務研發計畫
『系統測試報告書』

System Testing Plan Document

巨量規模資安日誌之潛伏惡意行為偵測技術

MOST 105-2221-E-011 -085 -MY3

研究團隊

主 持 人：　李漢銘 教授(台灣科技大學資工系)

協同研究人員：　王俊欽
賴家民
李漢超
洪斌峰
陳俊賢
謝奇元
黃佳郁
羅煜賢
謝義桐
劉珈妤
宋狄勳

Dept. of Computer Science and Information Engineering
National Taiwan University of Science and Technology

Ministry of Science and Technology

2018/05/15

版次變更記錄

Version	Author	Description	Completed Date
0.1	賴家民	First Release	2018/05/15

目錄

1. 簡介 (Introduction)

本系統為巨量規模資安日誌之潛伏惡意行為偵測系統，開發期程共三年，第一年度開發之系統對於企業內架設之 Proxy 所收集到的企業內使用者對外連線紀錄進行潛伏惡意行為偵測。第二年為偵測不同種類之惡意網域，有利於企業偵測所遭遇之社交工程攻擊手法。本文件為第三年計畫工作發表於 The 2nd International Conference on Machine Learning and Soft Computing(ICMLSC2018)之論文：Implementation of Adversarial Scenario to Malware Analytic，其系統各子系統之功能測試報告。

1.1 測試目的 (Scope of Testing)

本次軟體測試的目的在於確認本計畫所提之惡意程式分類器之分析系統之各子系統能依預期正確地提供功能。

1.2 接受準則 (Acceptance Criteria)

- 本系統需要對所有列為必要(Critical)之需求作必要性測試。
- 測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需要能符合預期測試結果方能接受。
- 以測試案例為單位，當測試未通過時，需要進行該單元的測試，其接受的準則與前一項規定相同。

2. 測試環境 (Testing Environment)

2.1 硬體規格 (Hardware Specification)

- 64 位元 4 核心處理器以上
- 16 GB 系統記憶體以上
- 500 GB 硬碟空間以上
- Gb 網卡乙張

2.2 軟體規格 (Software Specification)

- MAC OS

2.3 測試資料來源 (Test Data Sources)

測試資料來源為 Microsoft Malware Classification Challenge (BIG 2015)所提供之資料集，可於下列網址獲得更多資訊：https://www.kaggle.com/c/malware-classification。

3. 測試時程、程序與責任 (Testing Schedule, Procedure, and Responsibility)

本節敘述測試時程(Testing Schedule)、程序(Testing Procedure)以及負責人員(Testing Responsibility)之細節。

3.1 測試時程 (Testing Schedule)

本系統的測試時程及查核點如 表 3-1 與 表 3-2 所示：

表 3-1 測試時程

時程	實驗平台架設	2017/08/~2017/11/
	測試資料收集	2017/08
	系統接受度測試	2017/12

表 3-2 查核點

查核點	實驗平台架設	2017/11/30
	測試資料收集	2017/08/31
	系統接受度測試	2017/12/31

3.2 測試程序 (Testing Procedure)

3.2.1 接受測試 (Acceptance Testing)

根據系統功能之切分，設計出以下接受測試步驟。

1. 測試 OP code 特徵萃取功能相關之 FT1 Test case。
2. 測試建立惡意程式分類器之功能相關之 FT2 Test case。
3. 測試 JSMA((Jacobian-based saliency map approach)算法功能相關之 FT3 Test case。
4. 測試成功率計算功能相關之 FT4 Test case。

3.3 人員職責分配 (Personnel Responsibilities Assignment)

人員職責分配請參考 表 3-3。

表 3-3 人員職責分配

Testing Cases	Personnel
FT1	賴家民、謝奇元(紀錄)
FT2	賴家民、黃佳郁(紀錄)

FT3	賴家民、洪斌峰(紀錄)
FT4	賴家民、陳俊賢(紀錄)

4. 測試案例 (Test Cases)

本節敘述驗收測試案例(Acceptance Test Cases) 執行細節。

4.1 接受測試案例 (Acceptance Testing Cases)

各子系統的需通過下列測試案例：

4.1.1 AT1 Test Case

Identification	FT1
Name	輸入惡意程式資料集，輸出為僅剩 OP code 之 140 維之向量以及分類之結果
Requirement number	OP-001
Severity	Critical
Test data	微軟 BIG 2015 惡意程式資料集
Preconditions	無
Steps	1. 輸入惡意程式資料集 2. 輸出 140 維之向量與分類結果，總數約 1 萬筆
Expected result	得到 1 萬筆向量
Post Conditions	無

4.1.2 AT2 Test Case

Identification	FT2
Name	輸入 1 萬筆 140 維之向量與其分類結果，輸出可得到 1 個惡意程式分類器
Requirement number	MA-001
Severity	Critical
Test data	抽取 4/5 資料集為訓練資料，其餘 1/5 資料集為測試資料
Preconditions	無
Steps	1. 輸入 1 萬筆 140 維之向量與分類結果 2. 輸出 1 個已訓練之惡意程式分類器模型
Expected result	得到 1 個已訓練之惡意程式分類器模型
Post Conditions	無

4.1.3 AT3 Test Case

Identification	FT3
Name	輸入 1 萬筆 140 維之向量與分類結果，輸出可得八萬

	筆可引導惡意程式分類器錯誤分類之 140 維向量
Requirement number	AD-001
Severity	Critical
Test data	1 萬筆 140 維之向量與分類結果
Preconditions	無
Steps	1. 輸入 1 萬筆 140 維之向量與分類結果 2. 輸出 8 萬筆 140 維之向量與預期誤導，即預期攻擊分類器之分類結果
Expected result	8 萬筆 140 維之向量與預期誤導惡意程式分類器之分類結果
Post Conditions	

4.1.4 AT4 Test Case

Identification	FT4
Name	輸入 8 萬筆 140 維之向量與預期誤導惡意程式分類器之分類結果，輸出計算對惡意程式分類器之攻擊成功率
Requirement number	SR-001
Severity	Critical
Test data	8 萬筆 140 維之向量與預期攻擊分類器之分類結果
Preconditions	無
Steps	1. 輸入 8 萬筆 140 維之向量與預期誤導惡意程式分類器之分類結果 2. 輸出得到對惡意程式分類器之攻擊成功率
Expected result	得一對惡意程式分類器之攻擊成功率
Post Conditions	

5. 測試結果與分析 (Test Results and Analysis)

5.1 接受測試案例 (Acceptance Testing Cases)

本子系統之模組驗證測試結果如表 5-1 所示。

表 5-2 Module Validation Test Results

Test Case	Result(Pass/Fall)	Comment
FT1	Pass	
FT2	Pass	
FT3	Pass	
FT4	Pass	
Rate	100%	

Appendix A： 追朔表 Traceability

A.1 需求 vs. 測試案例 (Requirements vs. Test Cases)

調查後所得之需求如下所述：

- OP-001 輸入惡意程式資料集，輸出可以得到 1 萬筆向量與其分類之結果。
- MA-001 輸入 1 萬筆向量與其分類之結果，輸出可得到一個訓練後之惡意程式分類器。
- AD-001 輸入 1 萬筆向量與其分類之結果，輸出 8 萬筆向量與其預期誤導分類之結果。
- SR-001 輸入 8 萬筆向量與其預期誤導分類之結果給惡意程式分類器，輸出攻擊成功率。

Test Cases / Requirement	FP1	FP2	FP3	FP4
OP-001	V			
MA-001		V		
AD-001			V	
SR-001				V