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
魏得恩
陳勁維
魏俐嘉
蘇珮涵
游文傑
洪斌峰
陳俊賢
謝奇元
黃佳郁
羅煜賢

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

Ministry of Science and Technology

2017/06/13

版次變更記錄

Version	Author	Description	Completed Date
0.1	陳勁維	First Release	2017/06/13
	魏俐嘉		
	蘇珮涵		
	游文傑		

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。本文件為本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潛伏惡意行為偵測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
- 24 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)

- Ubuntu 14.04
- Windows 10

2.3 測試資料來源 (Test Data Sources)

測試資料來源為自行在網路上收集之黑名單，如 DNS-BH、Ransomware tracker 及 Malware Domain List，共計約 800 Domain，2 萬多 URL。

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	2017/02/01~2017/02/2
	測試資料收集	2017/03/01~2017/04/3
	系統接受度測試	2017/05/01~2017/05/3

表 3-2 查核點

查核點	實驗平台架設	2017/02/28
	測試資料收集	2017/04/30
	系統接受度測試	2017/05/31

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 Page Tracking 功能相關之 FT1 Test case。
2. 測試 Domain and URI Content Data Extractor 功能相關之 FT2 Test case。
3. 測試 Score Table Constructor 功能相關之 FT3 Test case。
4. 測試 Graph Constructor 功能相關之 FT4 Test case。
5. 測試[資料隱藏]功能相關之 FT5 Test case。
6. 測試 Binary threshold 功能相關之 FT6 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	游文傑、陳勁維(紀錄)

FT2	游文傑、蘇珮涵(紀錄)
FT3	游文傑、魏俐嘉(紀錄)
FT4	游文傑、陳勁維(紀錄)
FT5	游文傑、陳勁維(紀錄)
FT6	游文傑、陳勁維(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	輸入網域名稱，輸出可以得到網域追蹤之 Domain 與 URI List
Requirement number	PT-001
Severity	Critical
Test data	自行收集之黑名單
Preconditions	無
Steps	1. 輸入網域名稱 2. 輸出可以得到網域追蹤之 Domain 與 URI List
Expected result	得到網域追蹤之 Domain 與 URI List
Post Conditions	無

4.1.2 AT2 Test Case

Identification	FT2
Name	輸入 Domain 與 URI List，輸出可分別得到關於 Domain 的多個維度向量值與關於 URI 的多個維度的向量值
Requirement number	DE-001
Severity	Critical
Test data	所收集到的 Domain 與其追蹤後的 URI List
Preconditions	無
Steps	1. 輸入 Domain 與 URI List 2. 輸出各 Domain 與各 URI 之向量值
Expected result	得到各 Domain 與各 URI 之向量值
Post Conditions	無

4.1.3 AT3 Test Case

Identification	FT3
Name	分別輸入 Domain 與 URI List 與人工決定的分數，輸

	出可得 Domain 與 URI 之分數對照表
Requirement number	ST-001
Severity	Critical
Test data	1. 所有已經向量化之 Domain 與 URI List 2. 依據 Domain 屬性，人工標記分數
Preconditions	無
Steps	1. 輸入 Domain 與 URI List 與人工標記的分數 2. 輸出 Domain 與 URI 之分數對照表
Expected result	得到 Domain 與 URI 之分數對照表
Post Conditions	儲存該分數對照表

4.1.4 AT4 Test Case

Identification	FT4
Name	輸入 Domain 與 URI，輸出可得一 Domain 與 URI 結合之無向圖
Requirement number	GC-001
Severity	Critical
Test data	所收集到的 Domain 與其追蹤後的 URI List
Preconditions	無
Steps	1. 輸入 Domain 與 URI List 2. 輸出得一 Domain 與 URI 結合之無向圖
Expected result	得一 Domain 與 URI 結合之無向圖
Post Conditions	儲存該無向圖

4.1.5 AT5 Test Case

Identification	FT5
Name	**[資料隱藏]**
Requirement number	BP-001
Severity	Critical
Test data	**[資料隱藏]**
Preconditions	無
Steps	1. **[資料隱藏]** 2. **[資料隱藏]**
Expected result	**[資料隱藏]**

Post Conditions	[資料隱藏]

4.1.6 AT6 Test Case

Identification	FT6
Name	輸入節點數值，輸出二元類型字串
Requirement number	TI-001
Severity	Critical
Test data	所建構之無向圖，其所有節點數值
Preconditions	無
Steps	1. 輸入所建構之無向圖，其所有 Domain 與 URI 節點節點數值 2. 輸出 Domain 與 URI 節點之二元類型字串
Expected result	輸出 URI 節點之二元類型字串
Post Conditions	輸出偵測結果

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	
FT5	Pass	
FT6	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：

- PT-001　輸入網域名稱，輸出可以得到網域追蹤之 Domain 與 URI List。
- DE-001　輸入 Domain 與 URI List，輸出可分別得到關於 Domain 的 9 個維度向量值與關於 URI 的 6 個維度的向量值。
- ST-001　分別輸入 Domain 與 URI 的向量值與人工預先決定的分數，輸出可得 Domain 與 URI 之分數對照表。
- GC-001　輸入 Domain 與 URI，輸出可得一 Domain 與 URI 結合之無向圖。
- BP-001　**[資料隱藏]**。
- TI-001　輸入節點數值，輸出類型字串。

Test Cases / Requirement	FP1	FP2	FP3	FP4	FP5	FP6
PT-001	V					
DE-001		V				
ST-001			V			
GC-001				V		
BP-001					V	
TI-001						V