財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

射頻器材及通傳終端資安檢測技術指引
(無線網路攝影機)

107/06/11

無線網路攝影機資安檢測技術指引

通傳會 5/25 已預告「無線網路攝影機資通安全檢測技術指引」

- 內容有任何意見或修正建議者，請於7/24內陳述意見或洽詢

Wi-Fi Client 無線介面資安檢測要求

7.2 模糊測試

7.3 使用者識別及鑑別功能測試

5.3.3 Wi-Fi通訊安全測試

5.3.3.1 安全的Wi-Fi組態設置測試

5.3.3.2 無線網路傳輸安全機制設置測試

檢測細項 –模糊測試 範例

檢測項目	7.2.1 初階模糊測試	
檢測細項	驗證無線網路攝影機之Wi-Fi通訊協定是否具備模糊攻擊相關能力。	
	檢測方法	**判定標準**
	1.在測試平臺使用模糊測試工具，對待測物進行5,000筆隨機樣本之測試， 2.並將結果儲存在測試平臺。前述隨機樣本至少應包含以下通訊協定： A. IEEE 802.11x。 B. WPA2（含）以上版本。 C. WMM Specification Version1.2（含）以上版本。	測試過程中待測物應正常運作。

7.2 模糊測試

Test runs

20180326-1747-16 : 802.11 WPA Client Test Suite

Diagnoses

Valid case instrumentation	DISABLED
External instrumentation	DISABLED
Protocol semantics	ENABLED
Connection based instrumentation	ENABLED
SNMP instrumentation	DISABLED
SNMP Trap instrumentation	DISABLED
ISASecure CCM	DISABLED
SafeGuard	DISABLED
Syslog instrumentation	DISABLED
Instrumentation fail limit	2
Instrumentation frequency	1

Total of 10001 cases were executed.

Combined overall verdict **PASS**

Verdict from tcp / protocol instrumentation	pass	The test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases.
0	fail	There is a reason to believe that the SUT crashed or malfunctioned in some other detectable way while executing these test cases.
9999	pass	The test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases.
1	user-stop	The test was stopped by the user.
1	n/a	These test cases are not expecting the system under test to send any kind of reponse, and there was no basic instrumentation which would have probed the system under test status during the test run. Therefore a diagnosis cannot be established.

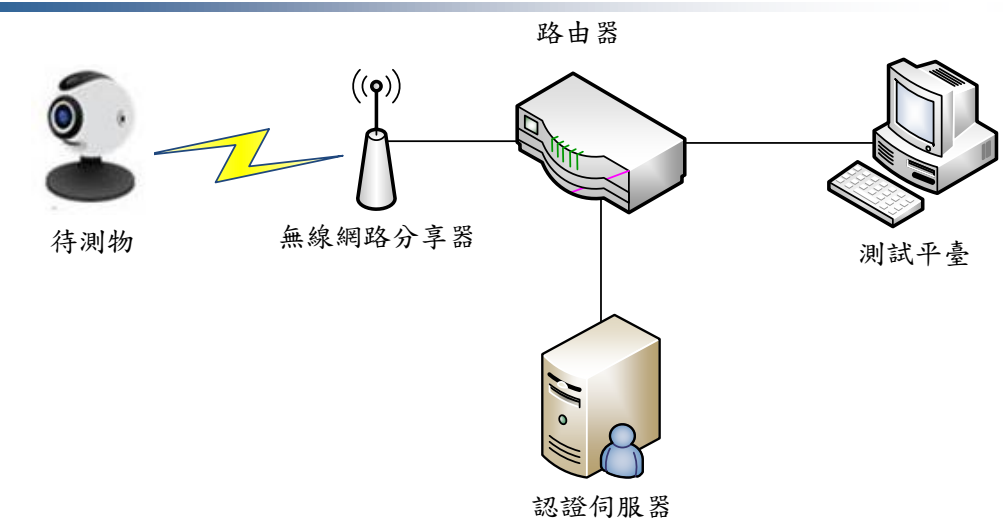
7.2.1模糊測試 (初階、中階、高階)

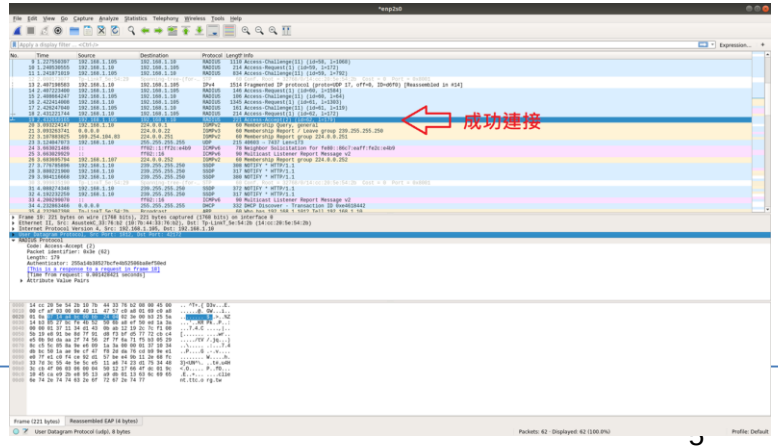
- 對待測物進行5,000(初級)、7000(中級) 、10000(高級)筆隨機樣本之測試
- 測試過程中待測物應正常運作

檢測細項 –使用者識別及鑑別功能測試 範例

檢測項目	7.3.1 高階802.1x使用者識別及鑑別功能測試	
檢測細項	驗證產品是否具備使用者識別及鑑別相關能力。	
	檢測方法	**判定標準**
	1. 開啟待測物之802.1x 存取鑑別功能。 2. 透過測試平臺觀察是否可瀏覽待測物所攝影之視訊或捕捉之靜態圖像。	通過認證伺服器鑑別後正確連接。

7.3 使用者識別及鑑別功能測試

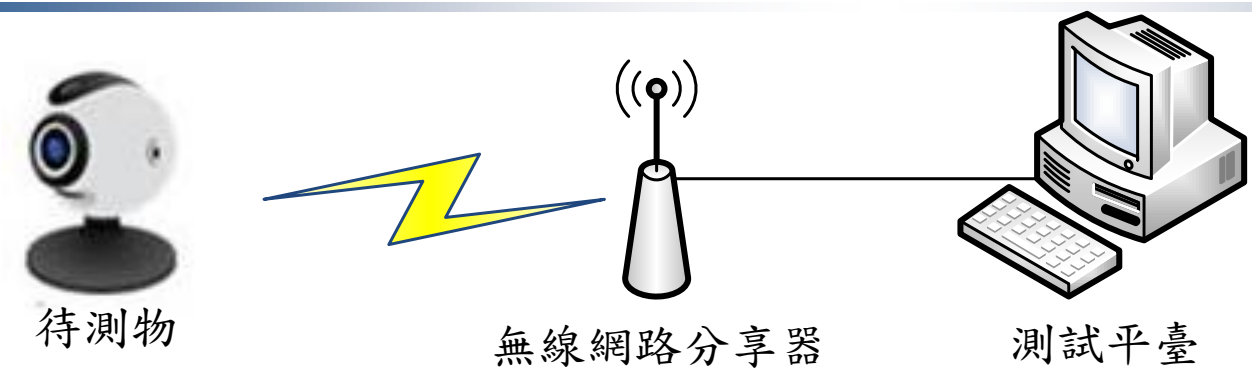




7.3.1 802.1x使用者識別及鑑別功能測試 (高階)

- 開啟待測物之802.1x 存取鑑別功能
- 確認802.1X 正確連接

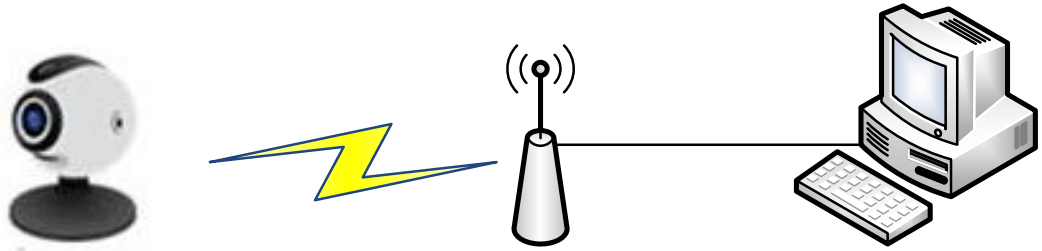
5.3.3 Wi-Fi通訊安全測試(1/2)



5.3.3.1 安全的Wi-Fi組態設置

- 產品提供WPS PIN開/關之功能
- WPS PIN功能預設為關閉

5.3.3 Wi-Fi通訊安全測試(2/2)



5.3.3.2 無線網路傳輸安全機制設置測試

- Wi-Fi預設加密模式為「WPA2」
- 確認傳輸是否採用「Wi-Fi保護存取2」加密方式

Wireless

Status of Wireless Networks

SSID	Mode	Security	Channel	Signal strength	Bit rate
TTC	Master	unsecured	11	57 %	
TTC	Master	unsecured	11	65 %	
TTC	Master	unsecured	11	52 %	
AndroidAP	Master	WPA2-PSK	11	78 %	
Wireshark	Master	WPA2-PSK	11	92 %	
ess_test	Master	WPA2-PSK	9	100 %	
WPA2	Master	WPA-802.1X/WPA2-802.1X	6	96 %	
TTC	Master	unsecured	6	77 %	
ess_mobile_testing	Master	WPA2-PSK	1	100 %	
TTC	Master	unsecured	1	88 %	
TTC	Master	unsecured	1	82 %	

Refresh

Wireless Settings

SSID: Wireshark

Network type: Master / Ad-Hoc

Security: WPA-/WPA2-PSK

WPA settings:

Pre-shared Key: Manual hex (64 HEX chars)

Passphrase (8 to 63 ASCII chars)

Passphrase: **********

Warning! Passphrases and keys saved here will be sent to the AXIS M1031-W in plain text.

Save Reset

檢測要求-書面檢視資料

初階(B)	中階(M)	高階(H)
1.檢測申請書 2.設備概述說明 3. IP CAM廠商填寫文件(初階)	1.檢測申請書 2.設備概述說明 3. IP CAM廠商填寫文件(初階、中階)	1.檢測申請書 2.設備概述說明 3. IP CAM廠商填寫文件(初階、中階、高階)

書面檢視處理原則

符合下列情況之一者即由檢測實驗室通知送測單位於期限內補齊，未補齊則將文件與送測設備退還至送測單位：

1.檢測申請書未填寫完整
2.設備概述說明未填寫完整
3.送測設備之名稱、型號、版本或數量等不符
4.送測設備非送測等級所需之設備
5.送測設備功能不符合要求

書面檢視資料(1/5)

- 申請單位應依送測文件描述，提供相關符合性說明文件，以協助檢測實驗室與測試人員瞭解待測物運作方式與相關功能，藉以提升檢測效率，並確保宣稱的內容與實際產品相同

檢附文件項目(必要文件)	說明
設備概述說明	描述產品相關資訊，廠牌、型號、外觀等
IP CAM廠商填寫文件	內容包括設備功能說明及權限說明
中文或英文之使用手冊或說明書乙份	提供無線網路攝影機之使用手冊，提供測試人員檢測參考
電子檔乙份	包含送測設備之設備概述說明與檢附文件之電子檔，供檢測實驗室備查

書面檢視資料(2/5)設備概述說明

- 申請單位應於送測前詳細填寫設備概述說明，以利後續檢測人員檢測

申請者（公司、商號名稱）	□ 製造商 □ 進口商 □ 經銷商
製造商	
設備名稱	
廠牌	
型號	
軟、韌體版本	
通訊介面	
安全功能	
外觀	

書面檢視資料(3/5) IP CAM廠商填寫文件(初階)

申請單位應於送測前詳細填寫IP CAM廠商填寫文件以利後續檢測人員檢測

1.產品是否有除錯模式:
□是(請繼續回答2)　□否(請繼續回答3)

2.請說明產品進入除錯模式之方法:

3.產品支援更新方式:
□離線更新(請繼續回答4)　□線上更新(請繼續回答5)

4.離線更新韌體所使用之加密演算法與韌體所使用之數位簽章:

5.產品更新相連伺服器宣告與韌體所使用之數位簽章:
注意:若韌體檔案經過加密處理，則廠商須提供解密工具。

6.產品敏感性資料保存方式與敏感性資料儲存保護之演算法:

7.應用程式介面各角色存取權限說明:

8.日誌檔存取權限與保存期限說明:

9.各角色存取權限說明:

10.隱私存取權限說明:

書面檢視資料(4/5) IP CAM廠商填寫文件(中階)

1.日誌檔儲存空間不足時，系統異常警示運作方法:

2.憑證上傳的操作說明:

書面檢視資料(5/5) IP CAM廠商填寫文件(高階)

1.安全啟動功能之設計說明:

2.安全區域功能說明:

3.多因子鑑別操作之產品說明:

產業意見徵詢

4/10召開「無線網路攝影機測試資安檢測指引」產業意見徵詢會議

Q1:通傳會在網路攝影機的角色分工？

通傳會主要針對無線介面資安要求，未來也將依此擴及其它IoT產品。

Q2:廠商產品要送測，需適用有線還無線網路攝影機檢測？

應視產品類型、應用需求而定，若僅有線應用需求進行驗證，後續無線仍須進行驗證。

Q3:無線網路攝影機僅限定在Wi-Fi，是否考量其它無線協定（藍芽、Zig Bee）？

以IP CAM目前僅使用Wi-Fi協定，並無使用Bluetooth或ZigBee協定。

Q4:測試項目僅模糊測試與802.1X，是否足夠抵擋無線攻擊威脅？

在無線攻擊類型中，模糊測試主要針對可能的injection攻擊、802.1x認證主要針對偽冒AP或WPA2 KRACKs攻擊，在無線阻斷攻擊，原「影像監控系統資安標準之測試規範-共通要求」5.1.2.2實體異常狀態警示機制測試方法內已描述"將網路線拔除或天線遮罩，使操控主機因訊號中斷而無法存取產品。故不在無線測試規範再做描述。

後續工作

「射頻器材及通傳終端資安檢測技術指引」後續工作

- 無線網路接取設備（ Wi-Fi AP）
- 無線路由器
- 有線電視機上盒（STB）
- 電腦無線輸入裝置（無線鍵盤、滑鼠、簡報筆）

報告結束