【行動應用資安聯盟】

111 年度物聯網資安檢測(第二場)一致性會議

一、 時間：111 年 7 月 7 日 14:00~15:30

二、 地點：Cisco Webex 線上會議

三、 主辦單位：經濟部工業局

四、 受委託單位：財團法人工業技術研究院

五、 執行單位：台北市電腦公會

六、 主席：行動應用資安聯盟 陳振楠 會長

七、 出席人員(依單位筆劃排序)：

(一)技術委員：

1. 國立政治大學資訊科學系	左瑞麟 教授
2. 行動應用資安聯盟	林金城 資深顧問
3. 臺灣電腦網路危機處理暨協調中心	林志鴻 組長
4. 國立臺灣科技大學資訊管理系	查士朝 教授
5. 國立臺灣師範大學資訊工程學系	紀博文 助理教授
6. 財團法人資訊工業策進會資安所	高傳凱 副主任
7. 淡江大學資訊工程學系	黃仁俊 教授
8. 國立臺灣科技大學資訊管理系	黃政嘉 助理教授
9. 行動應用資安聯盟	蔡志明 技術顧問
10. 國防大學資訊工程學系	羅嘉寧 副教授

(二)認可實驗室：

1. 安華聯網科技股份有限公司 資安檢測實驗室
   潘勤強 副處長
2. 行動檢測服務股份有限公司 智能物聯網檢測實驗室
   譚仲良實驗室主管、張嘉宏、葉偉雄 工程師
3. 財團法人台灣商品檢測驗證中心 資通訊檢測實驗室
   王煜詔組長
4. 資誠企業管理顧問股份有限公司 資訊安全暨鑑識科技實驗室
   唐雍為副總、林柏偉經理、李國樞資深顧問

5. 數聯資安股份有限公司 資通安全檢測實驗室
沈智揚副理、林彧卉、陳囿精資深工程師

(三)秘書組：
台北市電腦公會 劉瑞梅 總監
蔣瑋玲 專案經理
尹大湘 高專
杜秉蓁 高專
雷力學 專員

八、 議程：

時間	議程	主講人
14:00~14:10	一、主席致詞	陳振楠會長
14:10~15:10	二、聯盟報告事項： ➢物聯網資安認驗證制度 1.【調整】產品認驗證申請類型/流程/重點 2.【調整】物聯網資安認驗證制度規章 v1.1 3.【說明】資安標準/測試規範 4.【公告】申訴處理程序及流程 5.【更新】物聯網資安驗證產品費用 ➢資安標準/規範安全測項 1. 影像監控系統_一般要求 2. 聯盟信箱問題	秘書組
15:10~15:40	三、實驗室提案內容 ➢110/12/3 一致性會議提問 ➢111/3/17 一致性會議提問 ➢111/5/11~111/5/13 提案內容	秘書組
15:40~15:50	臨時動議	陳振楠會長
15:50~16:00	結論	陳振楠會長

九、 報告事項：

略(請見附件)

十、 實驗室提案內容討論：

提案一：資安標準/版本：IoT-2001-1 v2.0
設備名稱：網路攝影機
測試編號：5.2.4.2
說　明：前置條件內說明「應提供能進入產品作業系統的方法，及敏感性資料之存放位置」。對於國外品牌設備，若原廠不願意提供相關資料，將使得實驗室在檢測上有困難，針對此情況，聯盟是否能接受「廠商提供截圖的方式，讓實驗室審閱是否符合標準」？
決　議：
1. 5.2.4.2 測項僅接受實測，不接受廠商用截圖方式

提案二：資安標準/版本：IoT-2001-1 v2.0
設備名稱：網路攝影機
測試編號：5.4.1.1
問題主旨：實驗室間測試手法與判定標準不一致之情況
說　明：此測項要求產品使用者在登出後，應再次登入才能取得資訊，目前公告的標準/規範，未對測項限制 LOG OUT 時間，以致於可能造成不同實驗室之判定不同。
建　議：
(一)應明訂測試方法為「因該測項要求產品使用者在登出後，應再次登入才能取得資訊」,建議在測試中註明,「在 LOG OUT 後應立刻 Revoke 該 session」。
(二)建議聯盟官網應有公告區，提供一致性會議對現行標準之各測項調整之結論；並提供一個正式管道，讓實驗室及廠商能即時反應實際檢測上之問題。
決　議：
1. 同實驗室建議方案「在登出後應立即註銷該連線識別碼」。
2. 官網專區：因對現行標準/規範內容調整而更新的文件，統一置於【最新消息】及【下載專區】

提案三：資安標準/版本：IoT-2001-1 v2.0
設備名稱：網路攝影機
問題主旨：系列產品的判斷準則
說　明：
(一) 在「系列產品申請物聯網資安標章實驗室查檢表」中，A.2.3 的查檢項目：主機板上通訊、微控制、影像晶片有差異，即不符合系列產品。但影像晶片是否會影響資安?比如產品韌體、SOC、微控制均完全相同，但主產品沒有影像晶片，系列產品增加熱成像功能而增加影像晶片。按此查檢表將不能被認定為系列。

(二)廠商系統組態檔為二進位檔案，應如何驗證主、系列相同未變。關於系統組態檔驗證的相關要求。以下為實際案例說明：
廠商提供主、系列產品之組態檔，內容為二進位資料，只有韌體於執行過程中可讀取。系統外無讀取程式可讀取內容。因而實驗室無法驗證該組態檔是否相同。若依 hash 來驗證，會因型號等無關組態設定的差異而使 hash 不同。

(三)SOC 晶片版本因不同年份而產生不同編號，舉例說明，三張電路板與 SOC 的晶片主型號均相同，但第二排、第三排不相同，經與晶片原廠詢問，所得到之回函(如 email 往來信件)，其資料是否足夠證明是同一個晶片？

建　議：

(一)明確列舉影像晶片差異影響資安之部分，使廠商理解要求之目的。或可接受影像晶片差異不影響資安，可被接受為系列產品。

(二)對於系列產品的驗證，是否可以廠商宣告為證明依據。若實驗室需查證宣告的正確性，則需要有明確的查證方向，再由廠商截圖佐證…等等。

(三)廠商宣告，原廠信件往來應可作為佐證依據。

決　議：

1. 此案目前資料尚不夠詳盡，建議實驗室再補充相關事證資料，以利聯盟專家檢視與討論，決議後會另信回覆實驗室。
2. 晶片是否認定為系列產品，聯盟專家會再進行研議，並於下次一致性會議說明。

十一、 散會