財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

2018

亞洲·矽谷計畫-強化物聯網資安防護

推廣說明

財團法人電信技術中心

亞洲·矽谷計畫-強化物聯網資安防護 (第1期)

建立物聯網系統層級資安防護評估機制

- 完成智慧家庭及智慧交通物聯網系統層級資安防護評估機制
- 物聯網資安試驗平臺
- 提供物聯網系統層級資安評估及檢測服務
- 與國際驗證單位合作

強化物聯網資訊分享與分析

- 規劃成立物聯網資訊分享及分析中心 (IoT-ISAC)
- 建立IoT-ISAC運作與技術服務模式

人才培育及知識擴散

- 物聯網資安防護評估機制與IoT-ISAC服務推廣
- 辦理說明會、培訓活動及成果發表會

物聯網資安試驗平臺

物聯網系統層級資安防護評估試驗平臺

物聯網系統層級資安防護評估試驗平臺規劃必須能夠完整實現MVS評估程序，進行智慧家庭及智慧交通的最佳實務應用(Best Practice)

試驗平臺包含
1、威脅建模平臺
2、漏洞檢測平臺
3、滲透測試平臺

威脅建模平臺

第3步 根據資產表及網路與資料流架構進行資安威脅列表

第2步 解析並記錄智慧家庭或智慧交通系統架構及資料流向

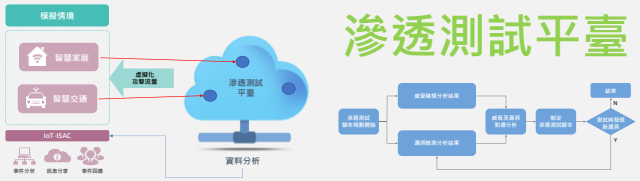
第1步 確認設備資產

- 威脅建模平臺將整合Microsoft Threat Modeling Tool(TMT)及以架構為基礎(Architecture-based)的威脅建模。
- 透過威脅建模平臺，可以得知受測智慧家庭或智慧交通系統的潛在威脅、各項設備軟硬體資訊及功能運作流程等資料

漏洞檢測平臺

- 漏洞檢測平臺對於可能產生重大資安威脅的設備及相關通訊協定進行漏洞檢測
- 以靜態源碼、韌體檔及惡意程式掃描檢測，並基於找出之CVE漏洞所對應CVSS權重值結果為主進行漏洞風險高低評估，並針對開源代碼的合規性進行檢測，確保授權(License)和智慧財產權的合法使用

滲透測試平臺



- 滲透測試主要的目的在於透過檢測手段評估威脅建模的各種威脅在各種檢出的漏洞下，確認實現該項威脅的可能性
- 滲透測試執行將參考OWASP物聯網定義的攻擊面向(Attack Surface)，針對不同攻擊面向進行評估與規劃

建立物聯網系統層級資安防護評估機制

1.1 完成智慧家庭及智慧交通物聯網系統層級資安防評估機制

DREAD威脅模型評估及風險值給分參考

評估風險係數的演算法模型，對這5個維度針對每個威脅進行等級評估。5個維度的平均值即為該威脅風險值，風險值越大，表示威脅風險越高

	低	中	高
給分	1	2	3

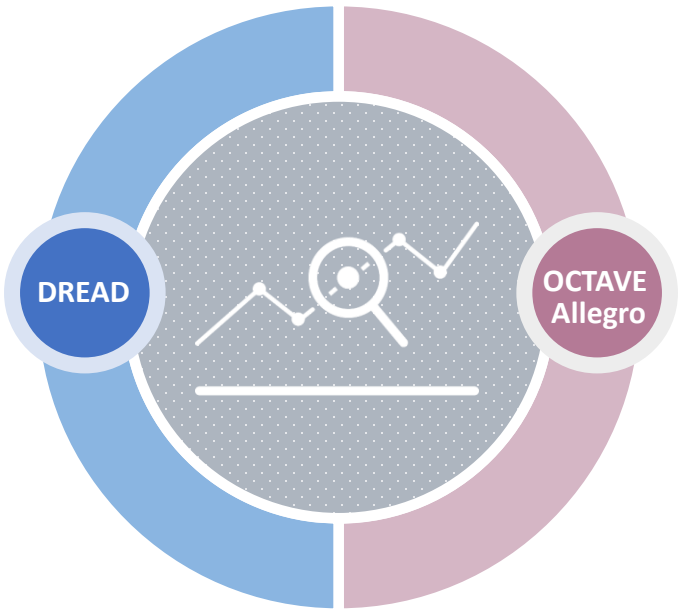
D — Damage Potential 潛在破壞性
如果這個"漏洞風險被攻擊者利用"進行攻擊，會對企業和組織造成多少破壞

R — Reproducibility 重現難度
要重現這個漏洞攻擊的難度有多大

E — Exploitability 可利用性
要發動這個攻擊需要哪些條件

A — Affected Users 受影響用戶
有多少用戶會遭受到這個風險漏洞的影響

D — Discoverability 發現難度
對於攻擊者來說，要發現這個漏洞的難度有多大



OCTAVE Allegro影響程度評估準則

偏重於威脅發生造成使用者各種層面的影響評估。各維度的影響程度區分低(Low)、中(Moderate)、高(High)三級。

Reputation and Customer Confidence 聲譽及客戶信心
非商業用戶商譽受影響，商譽回復費用為0或低於或高於1萬美金；商業用戶回復費用為0或低於或高於10萬美金，且流失率低於 5 %或5-10%或10%上者

Financial Loss 財物損失
非商業用戶增加的年維運費用及一次性財務損失；商業用戶的年營收損失

Productivity 生產力
商業用戶增加人力成本低於5萬美金、介於5~10萬美金或高於10萬美金

Life Safety and Health 生命安全與健康
對於使用者生命、健康及安全性等影響程度

Fine and Legal Penalty 罰金與法律懲罰
罰金、無法律訴訟或訴訟損失及是否須接受政府部分或其他調查單位查詢等影響

物聯網資安試驗平臺

提供物聯網系統層級資安評估及檢測服務

Start 受測廠商可上網登錄及填寫必要資訊，本團隊會有專人聯繫並確認評估及受測範圍。之後進行MVS評估程序，產出測試報告並提出改善建議。若受測廠商有其他國際資安驗證要求，本團隊也可協助評估報告轉換。

01 物聯網資安評估登錄

必要資訊確認
- 受測環境
- 系統架構

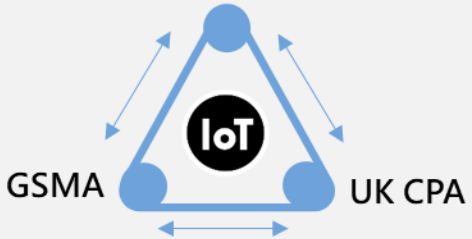
02 MVS評估程序

威脅建模、漏洞測試
滲透測試、影響評估

國際物聯網資安認證體系

主導單位或組織	引用標準
UL	CAP Program, UL 2900 series
ICSA, an independent Lab of Verizon	Internet of Things (IoT) Security Testing Framework
IEC/ISA	IEC 62443 series
ENISA	Under development, could base some parts of CC
UK, NCSC	Commercial Product Assurance (CPA) Scheme
資安處、通傳會工業局	Testing Specifications of Selected IoT Devices

國際驗證要求報告轉換
UL2900



03 物聯網資安評估結果分析

透過評估及檢測結果分析，收集有用情資並產生STIX 格式

04 分享資安情資給IoT-ISAC會員

IoT-ISAC
WEB UI或XML

事件分析　訊息分享　事件回應

物聯網資訊分享及分析中心 (IoT-ISAC)

IoT-ISAC會員服務項目

資安事件通報

即時對資安事件進行蒐集及分析，並可分享至其他領域ISAC，以達成政府與民間資安聯防效益。

資安情資分享

針對IoT-ISAC服務對象之資安風險進行情資蒐集、交換以及分析，與IoT-ISAC會員分享，以利管理與資安人員及早因應，考量資安訊息龐大且雜，未來針對付費會員可進行客製化服務。

資安監控與偵測

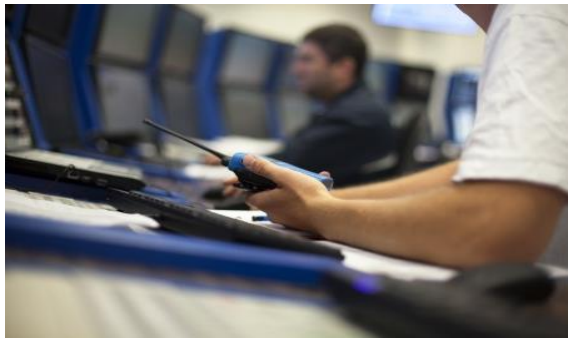
針對IoT-ISAC進行監控，透過網頁查詢事件分類、事件通報、事件處理、事件管理、知識庫、日誌紀錄（包括事件日誌與監控設備維運日誌）及相關資安統計圖表

緊急情況合作

研判與通知緊急資安事件，協助掌握整體資安現況及趨勢

威脅與弱點分析

結合本計畫物聯網資安試驗平臺及IoT-ISAC蒐集的資安威脅情資進行分析，並將分析結果納入資安通報系統，以防範未發生的資安威脅



國際交流

IoT-ISAC初期將提供國外情資分享與交流(擬與日本NICT、ICT-ISAC等合作)，並與國際驗證單位合作追蹤全球網路事件，加強跨國事件應變能力。

資安教育訓練

提供資安教育訓練，定期針對資安相關人員進行初階及中高階之培訓，同時結合其他領域ISAC共同舉辦資安人才培育活動。

資安事件協助處理

協助IoT-ISAC會員進行資安控管、漏洞評估及系統層級資安評估服務以及資安事件提供緊急應變的處理方式

說明會、教育訓練及相關培訓活動

免費參加培訓、推廣等各項資安相關活動

推廣說明會

資安防護評估與檢測機制及IoT-ISAC推廣說明會，分別於北、中、南辦理，分享國內外最新資安技術及產業趨勢議題，與產、官、學、研代表共同交流，現場提供物聯網資安防護評估機制與IoT-ISAC說明，及加入會員與相關Q&A服務。

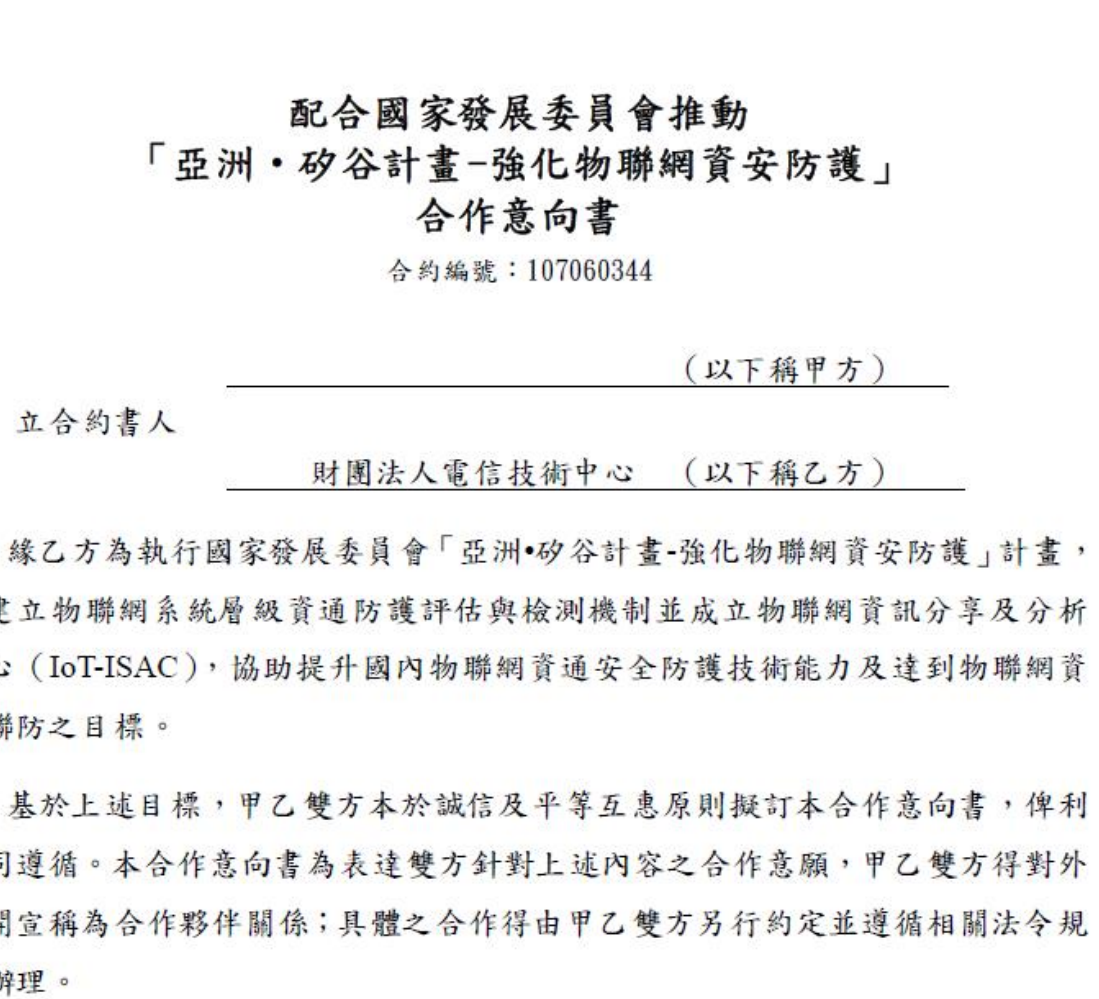
資安研討與人才培訓

辦理資安技術研討交流，建立人員培訓機制，針對一般人員、資訊人員及主管等不同對象，規劃資安認知、作業實施、專業技術或管理課程，以提升人員的資訊安全意識，落實資安通報流程、事件處理等作業流程，並強化資安人員技術的研發創新能力，培育物聯網資安關鍵人才能量。

防禦測試與攻防演練暨成果發表會

- 協助物聯網廠商及縣市政府等相關人員瞭解IoT-ISAC運作模式，共同參與系統層級資安防護審核平台測試。
- 舉辦實際攻防演練並展示資安防禦測試平臺，同步與產業串連，將整體資安分享及防禦機制能移轉給產業。

加入我們!



配合國家發展委員會推動
「亞洲・矽谷計畫-強化物聯網資安防護」
合作意向書

合約編號：107060344

（以下稱甲方）

立合約書人

財團法人電信技術中心　（以下稱乙方）

緣乙方為執行國家發展委員會「亞洲•矽谷計畫-強化物聯網資安防護」計畫，擬建立物聯網系統層級資通防護評估與檢測機制並成立物聯網資訊分享及分析中心（IoT-ISAC），協助提升國內物聯網資通安全防護技術能力及達到物聯網資安聯防之目標。

基於上述目標，甲乙雙方本於誠信及平等互惠原則擬訂本合作意向書，俾利共同遵循。本合作意向書為表達雙方針對上述內容之合作意願，甲乙雙方得對外公開宣稱為合作夥伴關係；具體之合作得由甲乙雙方另行約定並遵循相關法令規定辦理。

服務內容

- 物聯網系統層級資安防護評估服務主要針對物聯網系統進行整體性資安防護能力進行評估。
- IoT-ISAC會員相關資安服務，包含客製化國內外物聯網資安情資分享，主動提供給會員提供關注的情資來源、資安事件應處建議等
- 免費參加各種本計畫舉辦之相關資安訓練及攻防演練等活動。

聯絡方式

高軟辦公室

80661高雄軟體園區復興四路2號7樓之3(B棟)

連絡電話:07-9700910#36

聯絡窗口:陳振財 副理

gechion@mail.nsysu.edu.tw

會員報名

https://goo.gl/forms/FjHtq54ZixTYv0iA2