TAICS TC5
網路與資訊安全技術委員會

[TC5 第六次工作會議通知 暨 提案徵求]				
Date: 2016-09-14 **Designator:** doc.: TAICS TC05-16-0010-00-00				
Author(s):				
Name	**Affiliation**	**Address**	**Phone**	**email**
高傳凱	資訊工業策進會	台北市民生東路四段 133 號 2F	02-66072038	marskao@iii.org.tw

Abstract

台灣資通產業標準協會 TC5 第六次工作會議通知暨提案徵求，會中將針對本年度工作產出-「物聯網(IoT)資安白皮書」及「家用基站(Home eNB)資安檢測規範」之相關提案、工作進度及編撰內容進行討論。

台灣資通產業標準協會(TAICS)

TC5 網路與資訊安全技術委員會

TAICS TC5 #6 工作會議

1. 會議通知

- **會議日期**：2016.09.14
- **會議時間**：14:00~16:00
- **會議地點**：永豐餘大樓 TAICS 台北辦公室第一會議室（台北市重慶南路二段 51 號 8 樓之 1）
- **會議主席**：TC5 主席 洪光鈞總經理
- **會議議程**：

時　間	議 程	主持人
13:30~14:00	報到	
14:00~14:05	主持人開場	TC5 主席 **洪光鈞總經理**
14:05~14:10	議程確認與第五次工作會議紀錄認可	TC5 秘書處 **高傳凱博士**
14:10~15:00	專題演講 IoT 資安檢測案例分享(暫定)	
15:00~15:50	提案討論: IoT 或 HeNB 方面之提案	
15:50~16:00	臨時動議	TC5 主席 **洪光鈞總經理**
16:00	散會	

- **報名方式：請於 105 年 09 月 13 日(二)以前至下列網址線上填寫，謝謝。**

http://www.taics.org.tw/index.php/meeting/show/id/2e11933aaf351034a9b5343980d8bc23

若您尚未註冊會員員工帳號請先到下列網址註冊:
http://www.taics.org.tw/index.php/member/register

- 會議聯絡人：高傳凱先生 **marskao@iii.org.tw** | 電話 02-66072038

2. 提案徵求

針對上述議程及待議事項，TC5 技術工作委員會特此進行提案徵求，並提供物聯網(IoT)資安白皮書及家用基站(Home eNB)資安檢測規範大綱供參(見附件)，以下為提案方式說明：

- 2016.08.09 ~ 2016.09.13，請 email 至 marskao@iii.org.tw（請提供提案文件標題、作者、公司、與議程相關章節）
- 逾期之提案將被視為較低優先權，有可能不會在本次會議中討論。

附件 1(供參考)

物聯網(IoT)資安白皮書

1. 前言

1.1. 全球 IoT 發展進程

描述 IoT 的背景、環境、網路架構、商業趨勢等情境。

1.2. 全球 IoT 的資安發展

描述 IoT 資安的國內外發展現況

2. IoT 的資安威脅現況

2.1. 應用層的安全威脅

此層主要是指物聯網服務的應用層威脅，此層的應用為雲端運算、巨量資料分析等。

2.2. 網路層的安全威脅

此層主要是指物聯網服務的網路層威脅，主責將收集的資料傳遞至網際網路，是集合各種有線及無線等多種通訊協定(ethernet、3G、4G 及 Wi-Fi 等)的環境。

2.3. 感測器層的安全威脅

此層主要是指物聯網服務的感測器層威脅，用來監控並搜集環境變化或物體移動的能力，由感測元件所構建的環境，包括實體、感測器、感測區網及通往網路層的閘道器，然而實體的部份又會根據不同的網路服務(ethernet、3G、4G 及 Wi-Fi 等)有不同硬體條件的感測器(如：穿載裝置、醫療儀器、環境監控等)。

3. 未來 IoT 的資安需求建議

3.1. 應用層的安全需求

提供應用層的資安需求建議。

3.2. 網路層的安全需求

提供網路層的資安需求建議。

3.3. 感測器層的安全需求

提供感測器層的資安需求建議。

結論

附件 2(供參考)

家用基站資安檢測規範

1. 前言
2. 適用範圍
   說明本規範適用範圍。
3. 檢測安全等級
   說明檢測安全等級劃分原則
4. 資安檢測基準

4.1. HeNB 身分認證的安全

4.1.1. 演算法強度

4.1.2. 軟/硬體憑證的保存

4.1.3. 軟/硬體憑證的唯一性

4.1.4. 軟體憑證的設計(應設計出廠即內建憑證)

4.1.5. 硬體憑證的設計(e.g., removable token, 應設計出廠即內建憑證)

4.1.6. 身分認證程序的落實

4.2. HeNB 的實體層安全

4.2.1. 無線電資源管理

4.2.2. 硬體部件的設計(e.g., 天線被替換)

4.2.3. 環境資訊的保護(e.g., 消耗功率、溫度等)

4.3. HeNB 的系統安全

4.3.1. 系統設定的管控

4.3.2. 存取控制(ACL)清單的管控(e.g., 存取權限, 異動通知, handover)

4.3.3. CSG ID 設定的管控

4.3.4. 內建電信商管理政策的保護(e.g. IPsec 的使用, 封包的過濾政策)

4.3.5. 網路管理介面的管控

4.3.6. 內建防火牆設定的管控

4.3.7. 時間伺服器(Time Server)的配置