影像監控系統資安標準-第二部: 網路攝影機
Video Surveillance System Security Standard - Part 2: IP Camera

資策會 資安所 技術經理

台灣資通產業標準協會 網路與資訊安全技術工作委員會 組長

高傳凱 博士

主辦單位 經濟部工業局

執行單位 財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

台灣資通產業標準協會 Taiwan Association of Information and Communication Standards

影像監控系統系列資安標準框架

TAICS TS 14-1
第一部:一般要求

- 5.1 實體安全要求
  - 5.1.1. 產品外接實體介面安全
  - 5.1.2. 實體異常行為警示
  - 5.1.3. 安全啟動
- 5.2 系統安全要求
- 5.3 通訊安全要求
- 5.4 身分鑑別與授權安全要求
- 5.5 隱私保護要求

TAICS TS 14-2
第二部:網路攝影機

- 5.1.1 產品應符合TAICS TS 14-1 5.1節安全要求
- 5.2.1 產品應符合TAICS TS 14-1 5.2節安全要求
- 5.3.1 產品應符合TAICS TS 14-1 5.3節安全要求
- 5.4.1 產品應符合TAICS TS 14-1 5.4節安全要求
- 5.5.1 產品應符合TAICS TS 14-1 5.5節安全要求

實體安全
系統安全
通訊安全
身分鑑別與授權安全
隱私保護
特有安全要求

TAICS TS 14-3
第三部:影像錄影機

- 5.1.2. 實體防護

實體安全
系統安全
通訊安全
身分鑑別與授權安全
隱私保護
應用程式安全
特有安全要求

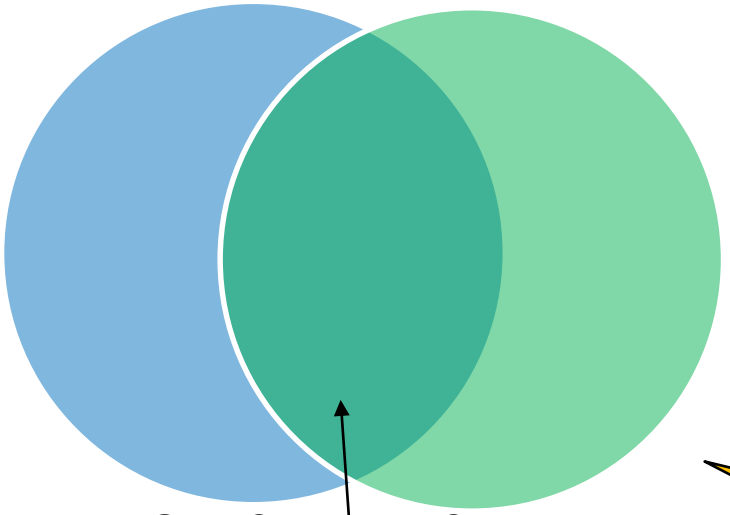
TAICS TS 14-4
第四部:網路儲存裝置

實體安全
系統安全
通訊安全
身分鑑別與授權安全
隱私保護
應用程式安全
特有安全要求

影像監控系統資安標準
第一部:網路攝影機

安全面向	安全要求分項	認證	加密	完整性	資安漏洞	警示與記錄
實體安全	5.1.1.實體埠之安全管控			●		
	5.1.2.實體異常行為警示					●
	5.1.3.實體防護			●		
	5.1.4.安全啟動	●		●		
系統安全	5.2.1.作業系統與網路服務安全				●	
	5.2.2.網路服務連接埠安全				●	
	5.2.3.更新安全	●	●	●		
	5.2.4.敏感性資料儲存安全		●			
	5.2.5.網頁管理介面安全				●	
	5.2.6.操控程式之應用程式介面安全	●				
	5.2.7.系統日誌檔與警示					●
通訊安全	5.3.1.敏感性資料傳輸安全	●	●	●		
	5.3.2.通訊協定與設置安全		●		●	
	5.3.3.Wi-Fi通訊安全				●	
身分鑑別與授權	5.4.1.鑑別機制安全	●				
	5.4.2.通行碼鑑別機制	●				
	5.4.3.權限控管	●				
隱私保護	5.5.1.隱私資料的存取保護	●				●
	5.5.2.隱私資料的傳輸保護	●	●	●		

OWASP IoT Top 10涵蓋率



有6成的涵蓋率

For Example: (未包含的OWASP資安要求)

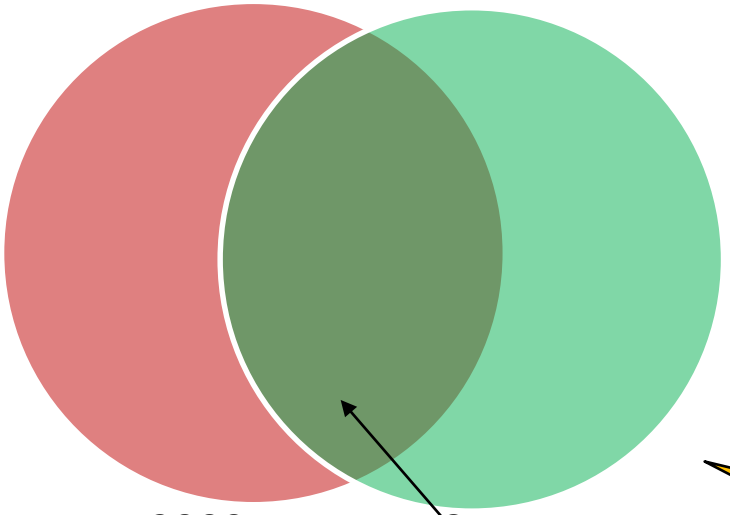
1. Ensuring the update server is secure.
2. the use of external ports such as USB to determine if data can be maliciously accessed on the device without disassembling the device.

8成9涵蓋率

去除掉IP CAM標準適用範圍外的要求

- I5: Privacy Concern (Privacy Notification)
- I6: Insecure Cloud Interface
- I7: Insecure Mobile Interface

ANSI/CAN/UL 2900-1 涵蓋率



For Example: (未包含的ANSI/CAN/UL 2900-1資安要求)

1. Binary code and Byte code analysis.

7成2涵蓋率

去除掉IP CAM標準適用範圍外的要求

- 12. Vendor Product Risk Management Process

網路攝影機v1.0與v2.0的差異 (1)

- 5.1.1 實體埠之安全管控
- 5.1.1.1 產品僅提供使用者有限權限之設計，即預設不應透過實體埠存取產品作業系統之除錯模式。(1級)
- ~~5.1.1.2 電路板上除錯測試用之連接器須移除。(2級)~~
- 5.1.1.2 卸除式儲存媒體使用的插槽須移除；抑或卸除式儲存媒體支援儲存媒體保護機制，即產品之儲存媒體不應在本機以外的機器被存取。(2級)
- 5.1.3 實體防護
- ~~5.1.3.2 晶片上不應存在晶片編號，且電路板上不應存在除錯測試用之功能編號。(3級)~~
- 5.2.4 敏感性資料儲存安全
- 5.2.4.3 產品須提出金鑰管理程序，以確保金鑰管理的品質。
- 5.2.7 日誌檔與警示
- ~~5.2.7.3 須要求產品之日誌檔留存時間，且符合NIST SP 800-92 [16]中high impact systems的日誌資料維護長度。~~
- 5.2.7.3 產品之安全事件日誌檔須具備日誌滾動(log rotate)機制。(1級)

網路攝影機v1.0與v2.0的差異 (2)

- 5.3.2 通訊協定與設置安全
- 5.3.2.2 產品所提供之自行開/關「網路裝置資訊探詢」功能，預設須為關閉，包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。(第3級)
- 5.4.1 鑑別機制安全
- 5.4.1.3 產品應具備上傳憑證之功能，以增加憑證鑑別機制之可信度。(第2級)
- 5.4.1.4 產品每一次還原出廠設定時，憑證之金鑰(包括SSH及TLS)都須改變，確保每台產品金鑰之唯一性，及降低金鑰外洩可能引發之資安風險。(第2級)
- 5.4.2 通行碼鑑別安全
- 5.4.2.2 廠商所生產之裝置，其預設通行碼都須相異；抑或首次成功取得產品存取之授權，須強制更改預設通行碼。 (1級)
- 5.5.1 隱私資料的存取保護
- 5.5.1.2 產品應支援隱私遮罩，避免正常作業引發之隱私外洩風險。

網路攝影機v1.0與v2.0的差異 (3)

- 附錄A 安全通道應使用之密碼套件:
  - **TLSv1.2**
    - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_SHA256
  - **TLSv1.3**
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256
    - TLS_AES_128_CCM_SHA256
    - TLS_AES_128_CCM_8_SHA256