影像監控系統網路攝影機資安標準暨測試規範

TAICS TC5 網路與資訊安全技術委員會/資策會 資安所

高傳凱 博士

2017/07/27

大綱

- 推動ICT產品資安檢測
- IoT系列資安標準
- 標準適用範圍
- 標準框架
- 資安技術要求
  - 預設密碼與強密碼
  - 認證與授權
  - 已揭露之資安漏洞
  - 韌體的保護
  - 機敏資訊的機密性
  - 通訊組態設定
  - 隱私權
- 專家建議

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

推動ICT產品資安檢測

標準推動

政府、民間使用單位

需求

提升國內資安環境

聯網設備商

需求

排除設備商外銷障礙

參照國際資安標準

NIST National Institute of Standards and Technology

OWASP Open Web Application Security Project

UL

GSMA

Spec

研擬連網設備資安標準與檢測規範及試檢測涵蓋3項設備

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

制度建立

推動資安檢測制度與檢測報告國際認可

檢測實驗室國際認證

ACCREDITED

TAF

智慧聯網產品資安認證

產業提升

輔導廠商提升產品資安品質

輔導取證

資安培訓

資安諮詢

目的

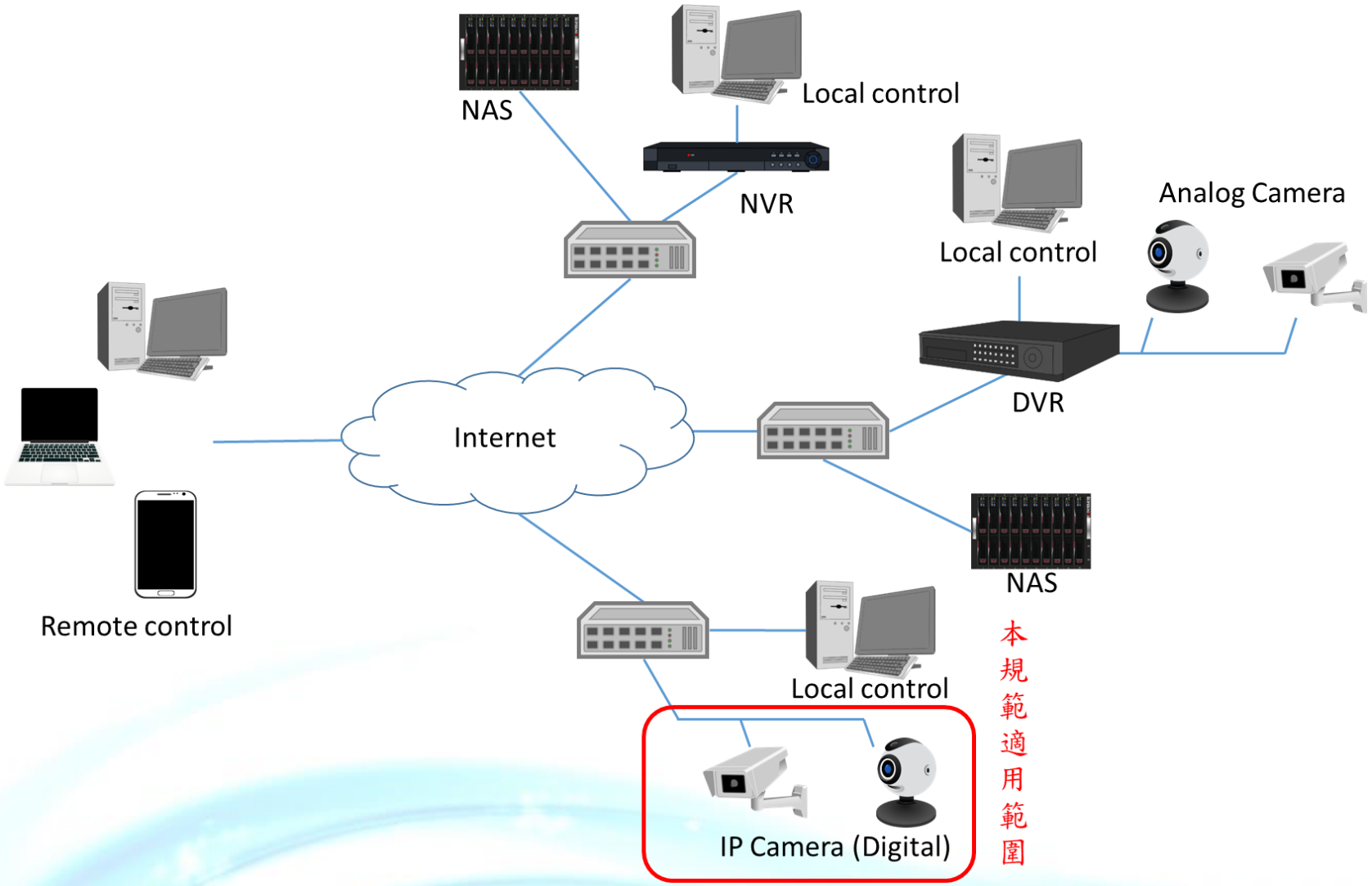
1. 完備資安法制環境
2. 推升資安產業自主能量
3. 優質化企業競爭力

IOT系列資安標準

The Series of IoT Security Standards

Common Security Requirement	Video Surveillance System	Accessory Application	Industrial control system	Connected car system	Medical devices	POS system
TAICS 0111-1 Cybersecurity	TAICS 0111-2-1 IP Camera	TAICS 0111-3-1 Web App	In Planning	In Planning	In Planning	In Planning
	TAICS 0111-2-2 DVR/NVR	TAICS 0111-3-2 Mobile App				
	TAICS 0111-2-3 NAS	TAICS 0111-3-3 Cloud Service				

標準適用範圍


NAS
Local control
NVR
Local control
Analog Camera
DVR
Internet
Remote control
NAS
Local control
IP Camera (Digital)
本規範適用範圍

標準框架

系統安全確保
保證網路攝影機於動態、靜態情況下，其軟體、韌體之安全性

→ 系統安全

- 作業系統安全
- 韌體程式安全
- 機敏性資料儲存安全
- 遠端管理介面安全

傳輸機密性
機敏資料的傳輸加密，及降低傳輸功能本身所引發的資安威脅

→ 通訊安全

- 資料傳輸安全
- 安全設置
- 通訊協定安全

存取控制
認證機制的落實、密碼認證的強度要求及用戶授權之管控

→ 身分認證與授權

- 認證機制安全
- 密碼認證安全
- 權限管控

隱私權
限制隱私資料的蒐集、使用、存取權限，並確保影音資料能安全傳輸

→ 隱私保護

- 隱私資料的蒐集保護
- 隱私資料的存取保護
- 隱私資料的傳輸保護

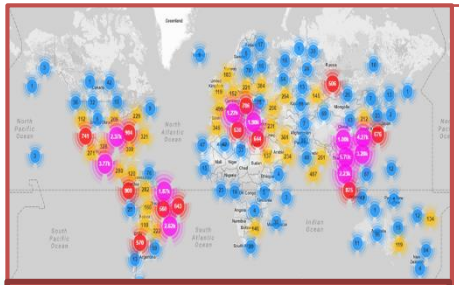
資安技術要求1 -
強制更換預設密碼與禁用弱密碼

章節	編號	安全要求	狀態
3.3.2	3.3.2.1	網路攝影機之密碼認證機制，密碼強度必須遵守政府組態基準(GCB) CCE-33789-9 最小密碼長度之規定	M
3.3.2	3.3.2.2	廠商所出產之網路攝影機其預設密碼都需相異	O
3.3.2	3.3.2.3	首次登入網路攝影機必須強制更改預設密碼	M
3.3.2	3.3.2.4	網路攝影機在登入密碼的設計上必須有輸入頻率及次數的限制	M

Insecam Project

攻擊簡介

Insecam計畫，公布包括會議、賣場、旅遊景點通通入境，直播的網站分類除美、韓、中有數千鏡頭外，台灣也在其中。這些畫面並非「駭」來的，皆是因未設定或未更改預設密碼，才會在網上流出



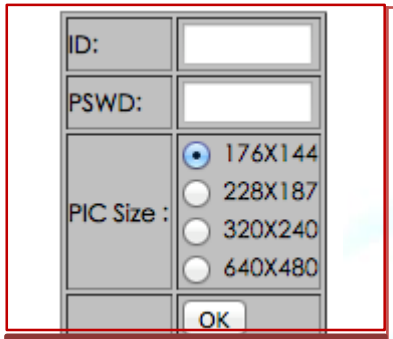
2016年中國雄邁

攻擊簡介

2016年10月，Mirai殭屍網路大軍，發現許多遭到控制的物聯網裝置來自採用中國製造商「雄邁」機板癱瘓資安部落格KrebsOnSecurity與法國網站代管服務供應商OVH網路

資安技術要求2 - 落實認證與授權

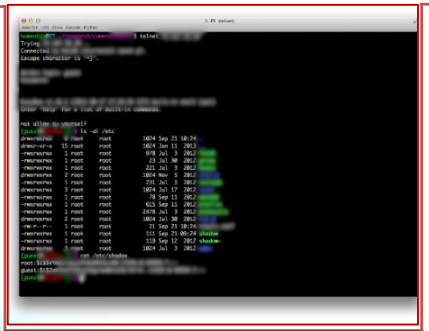
章節	編號	安全要求	狀態
3.3.1	3.3.1.1	遠端存取網路攝影機資源需經過身分認證機制，且必須為強認證機制	M
3.3.1	3.3.1.2	認證資訊的傳輸必須經過加密保護，且加密演算法強度需符合「附錄A」的要求	M
3.3.3	3.3.3.1	網路攝影機資源的存取，必須具備權限管控機制	M
3.3.3	3.3.3.2	網路攝影機之授權行為，需存在閒置時限	M



國外V牌無預設密碼

攻擊簡介

國外v牌廠商的產品似乎沒有預設帳號密碼，若使用者未設定帳號密碼，攻擊者只要直接點「OK」按鈕就可以登入系統，而這樣子的裝置 在台灣有三百多台。



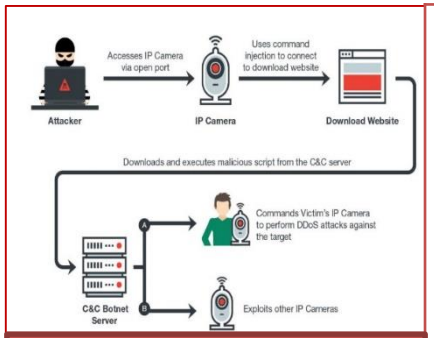
國外H牌權限管控不當

攻擊簡介

除了 root 帳號之外還有一組 guest 帳號，並且 guest 的密碼非常簡單，加上當初建置系統時並未檢查機敏檔案的權限是否設定錯誤，導致攻擊者可先用 guest 帳號登入，再去 /etc/shadow 讀取 root 密碼。

資安技術要求3 - 已知資安漏洞的防範

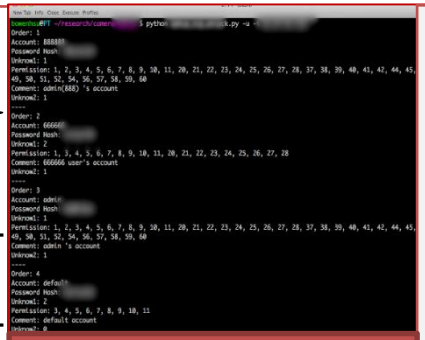
章節	編號	安全要求	狀態
3.1.1	3.1.1.1	網路攝影機之作業系統，不得存在已揭露之重大CVE漏洞	M
3.1.1	3.1.1.2	網路攝影機僅開啟必要之網路服務	M
3.1.1	3.1.1.3	網路攝影機所開啟之網路服務，不得存在已揭露之重大CVE漏洞	M
3.1.4	3.1.4.1	網頁管理介面不應該存在OWASP top 10中所揭露之常見網站安全風險	M



CVE漏洞

攻擊簡介

駭客鎖定的網路攝影機都是由不同代工廠商製造，但同時都具有相同的5個漏洞，包含CVE-2017-8224、CVE-2017-8222、CVE-2017-8225 CVE-2017-8223 和 CVE-2017-8221。



開啟非必要port

攻擊簡介

國外D牌設備，建立多組預設帳密，使用者不見得每一組都會更改，還開了特殊的 port，直接送出含有特定內容的封包到這個 port 就可以執行相對應的指令，而在這個過程中完全沒有任何認證機制。

資安技術要求4 - 防止機敏資訊從韌體走漏

章節	編號	安全要求	狀態
3.1.2	3.1.2.1	網路攝影機必須具備韌體更新機制	M
3.1.2	3.1.2.2	網路攝影機之韌體更新機制，必須經過加密保護，且加密演算法強度需符合「附錄A」的要求	M
3.1.3	3.1.3.1	網路攝影機之機敏資料應避免出現於裝置韌體程式碼中(i.e., hardcode)	M

韌體檔的竄改

攻擊簡介

由於韌體檔案隨處可得且均未加密，經下載拆解後可竄改內部檔案，達到開啟遠端後門程式，並取得系統管理者權限。

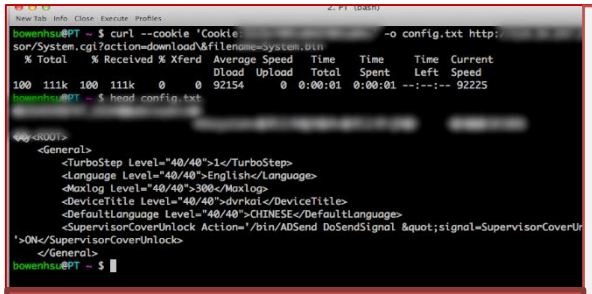
韌體中發掘金鑰

攻擊簡介

由於韌體檔案隨處可得且均未加密，經下載拆解後，於其中找到其加解密金鑰，可解讀自傳送途中攔劫的加密資料，甚至可套用在廠商其它同款的IP camera中。

資安技術要求5 - 機敏資料之隱密性確保

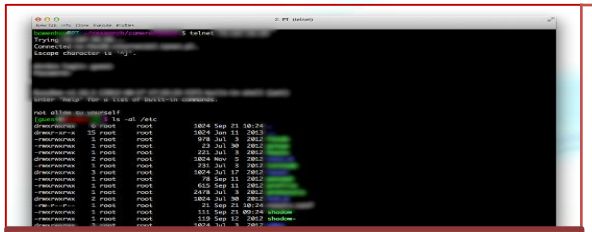
章節	編號	安全要求	狀態
3.1.3	3.1.3.2	網路攝影機之機敏資料必須加密儲存，且加密演算法強度需符合「附錄A」的要求	M
3.2.1	3.2.1.1	機敏資料之網路傳輸必須經過加密保護，且加密演算法強度需符合「附錄A」的要求	M



弱加密演算法

攻擊簡介

該系統將帳號密碼轉為 Base64 編碼後直接當作 cookie 內容，因此若預設帳號密碼分別是 abc 與 123，將 abc:123 用 Base64 編碼過後可得到 YWJjOjEyMw==，接著將 Cookie: SSID=YWJjOjEyMw== 這串內容加到 request 的 HTTP header 中，就可以到處測試該設備是否使用預設帳號密碼。



國外H牌權限管控不當

攻擊簡介

除了 root 帳號之外還有一組 guest 帳號，並且 guest 的密碼非常簡單，加上當初建置系統時並未檢查機敏檔案的權限是否設定錯誤，導致攻擊者可先用 guest 帳號登入，再去 /etc/shadow 讀取 root 密碼。

資安技術要求6 - 正確的通訊功能設定

章節	編號	安全要求	狀態
3.2.2	3.2.2.1	網路攝影機需提供使用者，可自行開/關網路裝置資訊探詢功能	M
3.2.2	3.2.2.2	網路攝影機上不可存在不安全的無線網路設定	M

UPnP資安風險

攻擊簡介

漏洞管理與滲透測試公司Rapid7，發佈長達29頁的《UPnP安全漏洞》報告，超過8,000萬個單一IP被確認，會回應來自網際網路上的UPnP裝置探勘請求，這些漏洞會讓攻擊者瀏覽到機密商業文件及擷取密碼，或允許他們遠程控制具有UPnP的印表機和網絡攝影機。

WPS資安風險

攻擊簡介

資安專家Stefan Viehbock 的研究中，發現此加密技術其實存在著十分重大的安全漏洞。平均只需要兩小時左右，便能以不斷嘗試密碼組合的暴力（Brute Force）攻擊，破解WPS 密碼保護的路由器。

資安技術要求7 - 未知攻擊的預防

章節	編號	安全要求	狀態
3.2.3	3.2.3.1	網路攝影機所使用之通訊協定(見附錄B)，必須經過異常輸入檢測，且不能發生崩潰(crash)導致服務中止的情形。	O

2015年台灣台中

攻擊簡介

吳女準備洗澡只穿內衣褲，攝影機出現怪聲還會自動轉動，手機登入後竟發現機器登入人數是2人，當時螢幕的畫面停留在被害者的下半身，閃躲鏡頭時機器竟然跟著轉，研判產品可能留有後門。

資安技術要求8 - 隱私保護

章節	編號	安全要求	狀態
3.4.1	3.4.1.1	網路攝影機在蒐集影音資料時，應給與適當的提示	O
3.4.1	3.4.1.2	網路攝影機所儲存的隱私資料，只有已被授權的個體才可以存取	M
3.4.2	3.4.2.1	網路攝影機所儲存的隱私資料必須受到加密保護，且加密演算法強度需符合「附錄A」的要求	M
3.4.2	3.4.2.2	網路攝影機應具備使用者刪除隱私之功能，提供對所儲存隱私資料的刪除權限	M
3.4.3	3.4.3.1	網路攝影機隱私資料的傳送不得為明文	M

住家外架設監視器

案例簡介

一名王姓女老師在大樓住處外裝設2支監視器，拍攝角度讓對門鄰居感覺出入被監控，因此提告；法院判決出爐，王姓女老師需要拆監視器、賠償2萬，理由是該樓層戶數只有3戶進出少，拍攝到的電梯口已經類似私領域，侵犯到鄰居隱私權。


柯P的監視器政策

案例簡介

105年北市長柯文哲提議要用路口監視器舉發違規停車，監視器難道只會拍攝違停？牽著小孩子走馬路的媽媽、熱戀中的情侶、坐著輪椅的老人還是在路邊聊天的外勞，執法人員要盯著監視器觀看多少市民的私生活？有多少畫面要歸檔，等著國家隨時取用？

專家建議-國際標準/規範對應

對應表

項次	IP CAM資安標準	UL 2900-1	OWASP Top 10
1	4.3.1.1.遠端存取網路攝影機資源應經過身分認證機制，且必須為強認證機制。	8.3 Service that are accessible over a remote interface shall require user authentication prior to access.	I2: Insufficient Authentication/Authorization Ensure that any access requiring authentication requires strong passwords

差異表

項次	IP CAM資安標準	UL 2900-1
1	網路攝影機在蒐集影音資料時，應給與適當的提示	無
2	網路攝影機所儲存的隱私資料，只有已被授權的個體才可以存取	無

專家建議-資安需求分級

新版本

編號	技術要求	狀態	安全分級 LV 1	LV 2	LV 3
3.2.1.1	機敏資料之網路傳輸必須經過加密保護，且加密演算法強度需符合「附錄A」的要求	M		✓	✓
3.2.2.1	網路攝影機需提供使用者，可自行開/關網路裝置資訊探詢功能	M	✓	✓	✓
3.2.2.2	網路攝影機上不可存在不安全的無線網路設定	M	✓	✓	✓
3.2.3.1	網路攝影機所使用之通訊協定(附錄B)，必須經過異常輸入檢測，且不得發生崩潰(crash)導致服務中止的情形	O			✓

專家建議-檢測一致性

1. 測試方法說明
   - 測試方法：

     由測試 PC 連線至網路攝影機，啟動模糊器(fuzzer)測試工具，輪流對受測之網路攝影機之通訊協定(見附錄D)，其所有欄位至少 10 萬筆唯一且獨立之測試項，或者最少 8 小時的異常輸入測試(fuzz testing)。檢查通訊傳輸技術介面或受測系統是否仍正常運作。
2. 實驗室檢測工具的建議清單
3. 廠商自我檢測工具的提供
4. 偕同廠商、測試實驗室及驗證單位啟動一致性會議


THANK YOU