



影像監控系統網路攝影機資安標準暨 測試規範

TC5 網路與資訊安全工作組

高傳凱 博士

2017/07/27



- 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

推動ICT產品資安檢測



標準推動

制度建立

產業提升



需求

參照國際資安標準



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

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



智慧聯網產
品資安認證

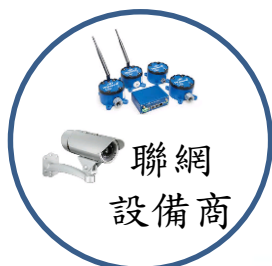
輔導廠商提升
產品資安品質

輔導
取證

資安
培訓

資安
諮詢

提升國內資安環境



需求

排除設備商外銷障礙

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

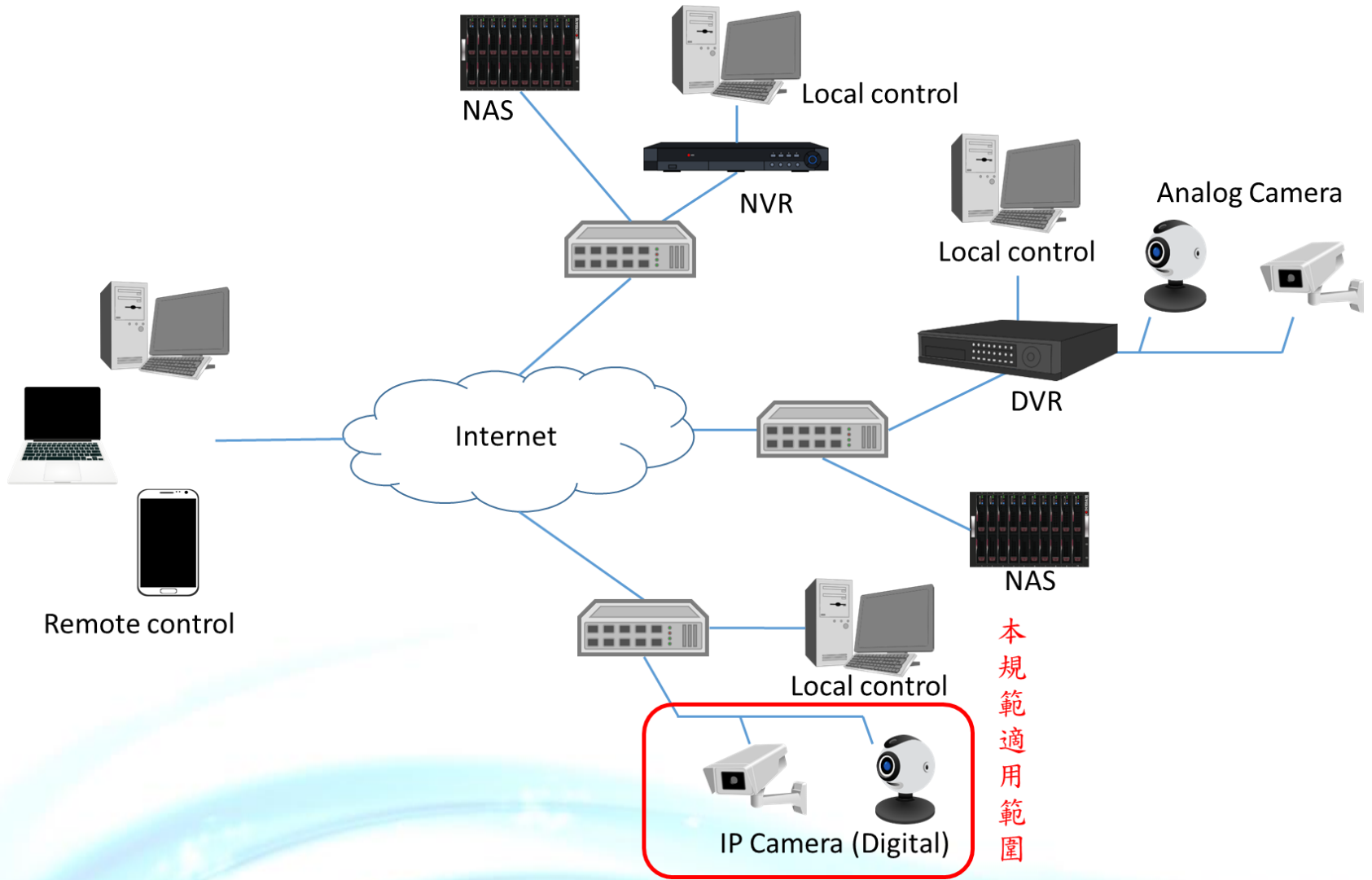


The Series of IoT Security Standards

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





標準框架





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

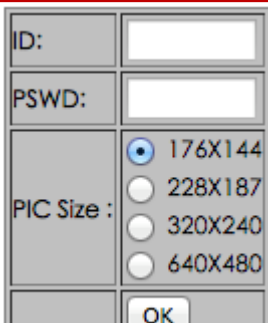
2016年10月，Mirai殭屍網路大軍，發現許多遭到控制的物聯網裝置來自採用中國製造商「雄邁」機板癱瘓資安部落格 KrebsOnSecurity與法國網站代管服務供應商OVH網路



落實認證與授權



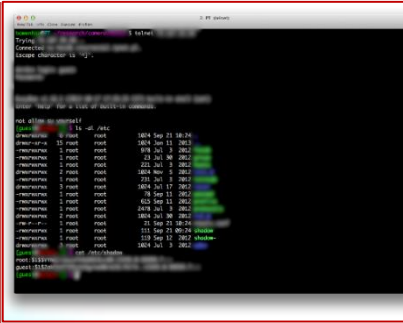
章節	編號	安全要求	狀態
3.3.1	3.3.1.1	遠端存取網路攝影機資源需經過身分認證機制，且必須為強認證機制	M
3.3.1	3.3.1.2	認證資訊的傳輸必須經過加密保護，且加密演算法強度需符合「附錄A」的要求	M
3.3.3	3.3.3.1	網路攝影機資源的存取，必須具備權限管控機制	M
3.3.3	3.3.3.2	網路攝影機之授權行為，需存在閒置時限	M



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，而這樣子的裝置在臺灣有三百多台。

國外V牌無預設密碼



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。

國外H牌權限管控不當



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(hardcode)	M

```

check_factory_mode()
{
    factory_mode_file="/mnt/sd/jsw_factory_mode.txt" 在 SD 卡內置入特定檔案
    if [ -f "$factory_mode_file" ] || [ "$CHECK_DID" == "AHUA-000099-00CEX" ]; then
        echo "***** J58 FACTORY MODE *****"
        (factory_mode) 開啟特定 Flag
        factory_mode_ip=$(cat "$factory_mode_file"|grep -E "(0-9)\.\.(0-9)\.\.(0-9)\.\.(0-9)" |
            if [ 1 -z "$factory_mode_ip" ]; then
                factory_static_eth0_ip=${factory_mode_ip}
            fi
            echo "factory_static_eth0_ip: ${factory_static_eth0_ip}"
        else
            echo "***** NORMAL MODE *****"
            factory_mode=0
        fi
    }
    if [ "$factory_mode" == "1" ];then
        echo "factory default active Telnet ... Ok"
        telnetd & 靜發 telnet 服務 (目前設定密碼可直接登入)
    fi
}

```

韌體檔的竊改

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。



加密是由演算法與密鑰共同運行將明文變成密文

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。



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

```

bownhsu@PT ~ $ curl --cookie 'Cookie
sor/System.cgi?action=download&filename=system.011
% Total % Received % Xferd Average Speed Time Time Time Current
100 111k 100 111k 0 92154 0 0:00:01 0:00:01 --:--:-- 92225
bownhsu@PT ~ $ head config.txt

<General>
<TurboStep Level="40/40">1</TurboStep>
<Language Level="40/40">English</Language>
<Maxlog Level="40/40">300</Maxlog>
<DeviceTitle Level="40/40">dvrkai</DeviceTitle>
<DefaultLanguage Level="40/40">CHINESE</DefaultLanguage>
<SupervisorCoverInLock Action="/bin/ADSend DoSendSignal &quot;signal=SupervisorCoverIn
">0</SupervisorCoverInLock>
</General>
bownhsu@PT ~ $
  
```

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。

```

root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/lib/mandrake:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
cu:x:11:11:cu:/var/spool/cu:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
root:x:1000:1000:root:/root:/bin/bash
bownhsu:x:1001:1001:bownhsu:/home/bownhsu:/bin/bash
  
```

國外H牌權限管控不當

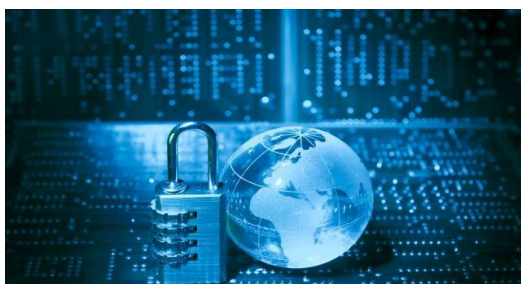
攻擊簡介

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**。



正確的通訊功能設定

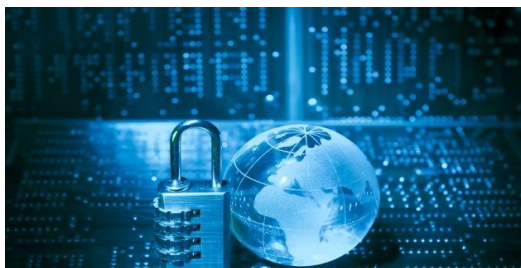
章節	編號	安全要求	狀態
3.2.2	3.2.2.1	網路攝影機需提供使用者，可自行開/關網路裝置資訊探詢功能	M
3.2.2	3.2.2.2	網路攝影機上不可存在不安全的無線網路設定	M



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的印表機和網路攝影機。



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。



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



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，廠商事後發現機器都處在**原廠設定**

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私生活？有多少畫面要歸檔，等著國家隨時取用？



■ 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	II	✓	✓	✓
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



台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

