網路攝影不設防，直播主角換你當

■ 國防部中校參謀　葉清源

國外網站《Insecam》全天候播放來自世界各地的網路直播畫面，前陣子也有臺灣女生的寢室曝光，致其個人隱私全被看光光，這猶如電影《楚門的世界》般的情節正在現實中上演，你是否已經成為最佳男（女）主角了？

「出門在外，想關心一下家中的長輩，於是登入居家安全系統來查看家中的情況」；「炎炎夏日，在外勤奮地跑了一天的業務，為了回家時能有一個舒服的環境，於是遠端啟動家中的冷氣機」；「出門旅遊，看見難得的美景，為了讓親朋好友也能立刻欣賞到相同的景色，所以拍照留念並立刻打卡上傳雲端」；這些在現代看似理所當然的服務，皆拜現今網路發達及科技進步所賜，讓我們平淡無奇的生活處處

充滿了便利，但是，在這便利科技的黑暗面中，隱藏了什麼樣的危機呢？

許多人都知道，現在居家防護系統非常多樣化，除了租用保全公司所提供的服務外，熟悉電腦及網路架構的用戶也可以購買相關設備，自行架設一套自己的防護系統，但這些保護居家安全的雲端設備，該由誰來保護它的安全？近年來，網路攝影機遭駭事件層出不窮，國外號稱擁有最多線上攝影機的網站《Insecam》，光是監看臺灣的攝影機就有四百多部（其中二百多部是落於臺北市區），而這個網站甚至依據攝影機的廠牌、架設地區、城市，以及時區等項目進行分類，讓有特殊興趣的人士可以隨時選擇他們想觀看的鏡頭。那麼，當我們使用這些設備時，為避免隱私外露，該採取哪些保護措施？建議各位最基本一定要做到的，就是將登入系統的密碼更換為高強度密碼，另外亦需不定時地更新系統軟體，以及檢查連線紀錄，以避免遭人監看而不自知的情況發生。

《Insecam》網站全天播放來自全球各地的攝影直播畫面，根據攝影機廠牌、架設地區、城市等項目進行分類，其中監看臺灣的攝影機多達四百多部。（Photo Credit: Insecam, https://www.insecam.org/en/）

其次聊聊雲端家電的便利與風險，可連接雲端的家電，除了最常見的冷氣之外，現在亦有廠商開發電動門、智慧電表、空氣清淨機、電鍋等智慧型連網裝置。這類家電的確可以為我們的生活帶來相當程度的便利，達到節電、省時並提供舒適的生活環境，但若此類系統設計有缺陷，難保駭客不會運用這些設備來進行惡意攻擊。例如，在寒冷的冬天啟動冷氣並將其溫度

網路攝影機是透過製造商的伺服器或雲端登入，只要被植入木馬或資料外流，都有可能被偷盜帳號；圖為民眾購買網路攝影機監控寵物，沐浴時竟遭駭客入侵偷窺的真實案例。（圖片來源：截自 TVBS 新聞）

調降至 19 度，進行無意義的惡搞；或是竊賊趁家中無人時透過遠端搖控開啟電動門，趁機入侵住宅搜括財物，相信無人願意上述情況發生。

那麼，我們該如何善用這些設備，而又不用擔心它可能隱藏的危害呢？商品生產者當然需要背負最大的防護責任，定時檢測並更新相關系統軟體，而使用者務必保護控制裝置的安全。舉例來說，若透過手機使用雲端 APP 來控制家中的冷氣，那麼，這部手機就不要安裝太多應用程式；再者，家中的智慧型裝置若是透過 Wi-Fi 進行連線，則 Wi-Fi 密碼也不應該設定的太過簡單，以上兩點防護作為無需高超的電腦功力，一般人應該都可以做到。

至於即時分享旅遊美景這類的行為，究竟隱藏了什麼樣的危機呢？首先我們該考慮到，有哪些人可以看到我們上傳的照片，如果隨意一個路人都可以存取我們的照片，那我們就不該上傳較隱私或者是背景為機敏地區的照片。此外，亦應留心提供服務的供應商背景，還有使用前應詳讀使用合約，因為某些公司在合約條款中提到，客戶上傳照片後，版權就屬於該公司所有，他們可以任意使用，這類型的合約

物聯網的發展讓雲端家電在我們生活中越來越普遍，各式家電用品都可透過 APP 遠端遙控，提供人們更加舒適的生活環境，卻不能不提防有心人士的惡意攻擊。

非常不合理，但多數使用者均未查覺，致損害了自身的權益。另外，若決定使用這類型服務時，仍應注意登入服務的密碼設定是否安全，照片中是否夾帶 GPS 資訊等等，才能達到較佳的保護效果。

整體而言，智慧型裝置已為現代生活帶來了相當程度的便利，只是身為使用者的我們，除了懂得如何「用」以外，更該瞭解安全防護做法；好好保護自身隱私，就不會成為最佳男（女）主角而不自知！

即時分享旅遊美景，除了應考量照片內容的隱私權和背景的機敏性外，更應注意服務供應商的合約條款，以免在不知不覺中損害了自身權益。

當門禁系統成為駭客的挖礦機

■ 臺北市立中正高中資訊組長　李詩婷

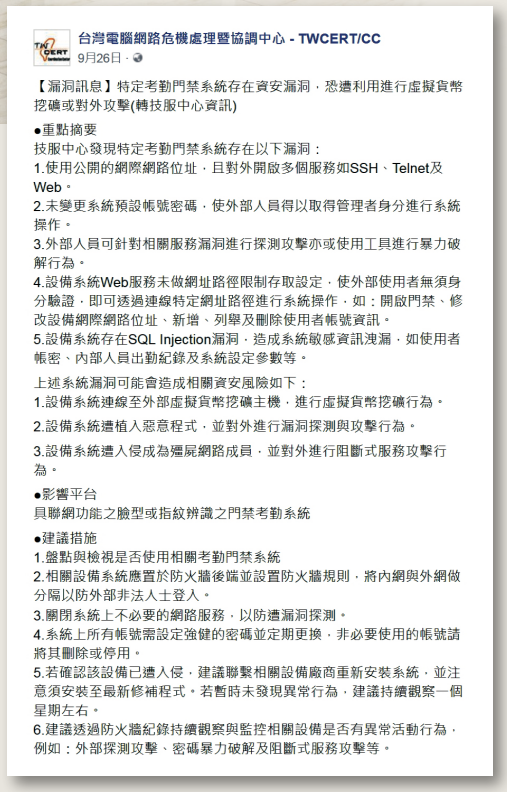
物聯網的時代來臨，新興科技帶來便利的同時，背後也隱藏了重大的資安風險，機關在採購相關設備時也要小心謹慎，減少資安事件發生的機會。

門禁系統潛藏安全漏洞

好萊塢特務電影的駭客，只要手邊有一台電腦就能控制任何資訊系統，從屏蔽大樓監視器的畫面，或是遠端控制門禁鎖，讓人輕易地進出機關重地等都只是小菜一碟。以上場景觀眾已經司空見慣，但若以為這些只會出現在電影裡那就是大錯特錯了，隨著駭客手法日新月異，電影中的許多情節都已成真。

電影裡駭客攻破門禁裝置系統的情節，恐怕在真實生活中上演。

《台灣電腦網路危機處理暨協調中心（TWCERT／CC）》於去（2017）年9月時就發出警告，數個特定考勤門禁系統中已被發現存在資安漏洞，可能被駭客利用而植入木馬或後門等惡意程式，不僅具有機敏資訊（例如內部人員出勤紀錄、員工編號或帳號密碼等）外洩的風險，而且可能被駭客進一步取得系統完整的控制權。



台灣電腦網路危機處理暨協調中心 - TWCERT/CC
9月26日 ·

【漏洞訊息】特定考勤門禁系統存在資安漏洞，恐遭利用進行虛擬貨幣挖礦或對外攻擊(轉技服中心資訊)

●重點摘要
技服中心發現特定考勤門禁系統存在以下漏洞：
1.使用公開的網際網路位址，且對外開啟多個服務如SSH、Telnet及Web。
2.未變更系統預設帳號密碼，使外部人員得以取得管理者身分進行系統操作。
3.外部人員可針對相關服務漏洞進行探測攻擊亦或使用工具進行暴力破解行為。
4.設備系統Web服務未做網址路徑限制存取設定，使外部使用者無須身分驗證，即可透過連線特定網址路徑進行系統操作，如：開啟門禁、修改設備網際網路位址、新增、列舉及刪除使用者帳號資訊。
5.設備系統存在SQL Injection漏洞，造成系統敏感資訊洩漏，如使用者帳密、內部人員出勤紀錄及系統設定參數等。

上述系統漏洞可能會造成相關資安風險如下：
1.設備系統連線至外部虛擬貨幣挖礦主機，進行虛擬貨幣挖礦行為。
2.設備系統遭植入惡意程式，並對外進行漏洞探測與攻擊行為。
3.設備系統遭入侵成為殭屍網路成員，並對外進行阻斷式服務攻擊行為。

●影響平台
具聯網功能之臉型或指紋辨識之門禁考勤系統

●建議措施
1.盤點與檢視是否使用相關考勤門禁系統
2.相關設備系統應置於防火牆後端並設置防火牆規則，將內網與外網做分隔以防外部非法人士登入。
3.關閉系統上不必要的網路服務，以防遭漏洞探測。
4.系統上所有帳號需設定強健的密碼並定期更換，非必要使用的帳號請將其刪除或停用。
5.若確認該設備已遭入侵，建議聯繫相關設備廠商重新安裝系統，並注意須安裝至最新修補程式。若暫時未發現異常行為，建議持續觀察一個星期左右。
6.建議透過防火牆紀錄持續觀察與監控相關設備是否有異常活動行為，例如：外部探測攻擊、密碼暴力破解及阻斷式服務攻擊等。

《台灣電腦網路危機處理暨協調中心（TWCERT／CC）》於去年時發出警告，數個特定考勤門禁系統中已被發現存在資安漏洞。（資料來源：台灣電腦網路危機處理暨協調中心FB，https://www.facebook.com/twcertcc/posts/2015215518708183）

「運算資源」成為駭客覬覦目標

不要以為駭客只會針對資料有興趣，就心存僥倖。許多資安事件案例顯示，駭客想竊取的已不只是有價值的「資料」，而是轉為鎖定裝置的「運算資源」。典型的攻擊手法是植入殭屍（bot）病毒，成為受駭客控制的殭屍電腦，潛伏並隨時等候駭客下一步命令，一旦殭屍網路大軍成形，就能用來發動分散式阻斷服務攻擊（Distributed Denial-of-Service attack, DDoS），讓雲端服務或網站連線負載量過大而造成服務停擺。

除此之外，新型態的攻擊手法則是植入比特幣挖礦的惡意程式，讓裝置搖身一變成為駭客專屬的虛擬貨幣挖礦機，不僅難以追查，還能立即替駭客帶來金錢上的利益，比過去還要設法販賣機敏資料或向被害企業組織勒索贖金更方便省事。

物聯網裝置成為駭客眼中的肥羊

門禁卡感應、指紋辨識、車牌辨識等門禁系統皆屬於物聯網（Internet of Things, IoT）技術的應用，物聯網是近年來最火紅的技術之一，其應用例如智慧家電、居家安全偵測及監控系統或穿戴式裝置等，並可與監控系統、網路、中央控制等系統整合，以進行數據收集與遠端控制。

然而，在一窩蜂擁抱物聯網技術的熱潮中，不得不重視的是其背後所隱藏的隱私問題和資安風險。據資安業者卡巴斯基實驗室（Kaspersky

駭客於物聯網植入比特幣挖礦的惡意程式，使裝置在民眾不知情下成為其專屬的虛擬貨幣挖礦機。

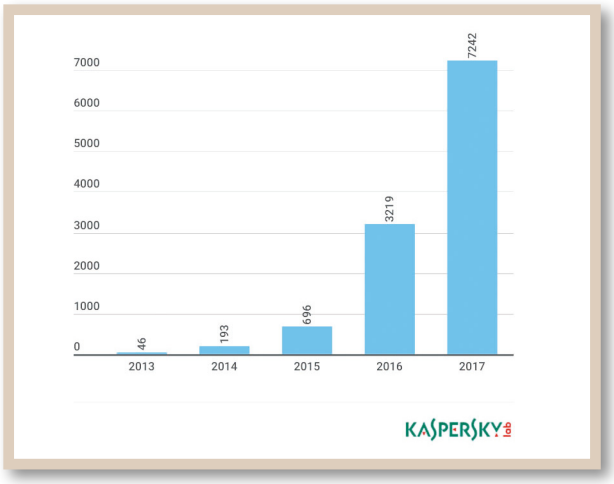
物聯網熱潮掀起產業新革命，應用範圍包含居家安全監控、智慧家電、穿戴式裝置等領域，卻容易變成駭客攻擊的新目標。

Lab）調查，光是去年就出現逾四千種新 IoT 惡意程式，遠高於前年的 3,219 種。

分析 IoT 惡意程式如此蓬勃發展的原因，是因為物聯網裝置具有以下特性，故容易成為駭客攻擊的目標：

一、資通安全易被忽略

人們通常會專注於保護個人電腦和智慧型手機的隱私，但卻容易忽略物聯網裝置的資安風險。在僥倖心理下，即使知道所使用的裝置系統已有安全漏洞，也可能因為成本預算及人力等考量而無法進行產品升級或汰換。



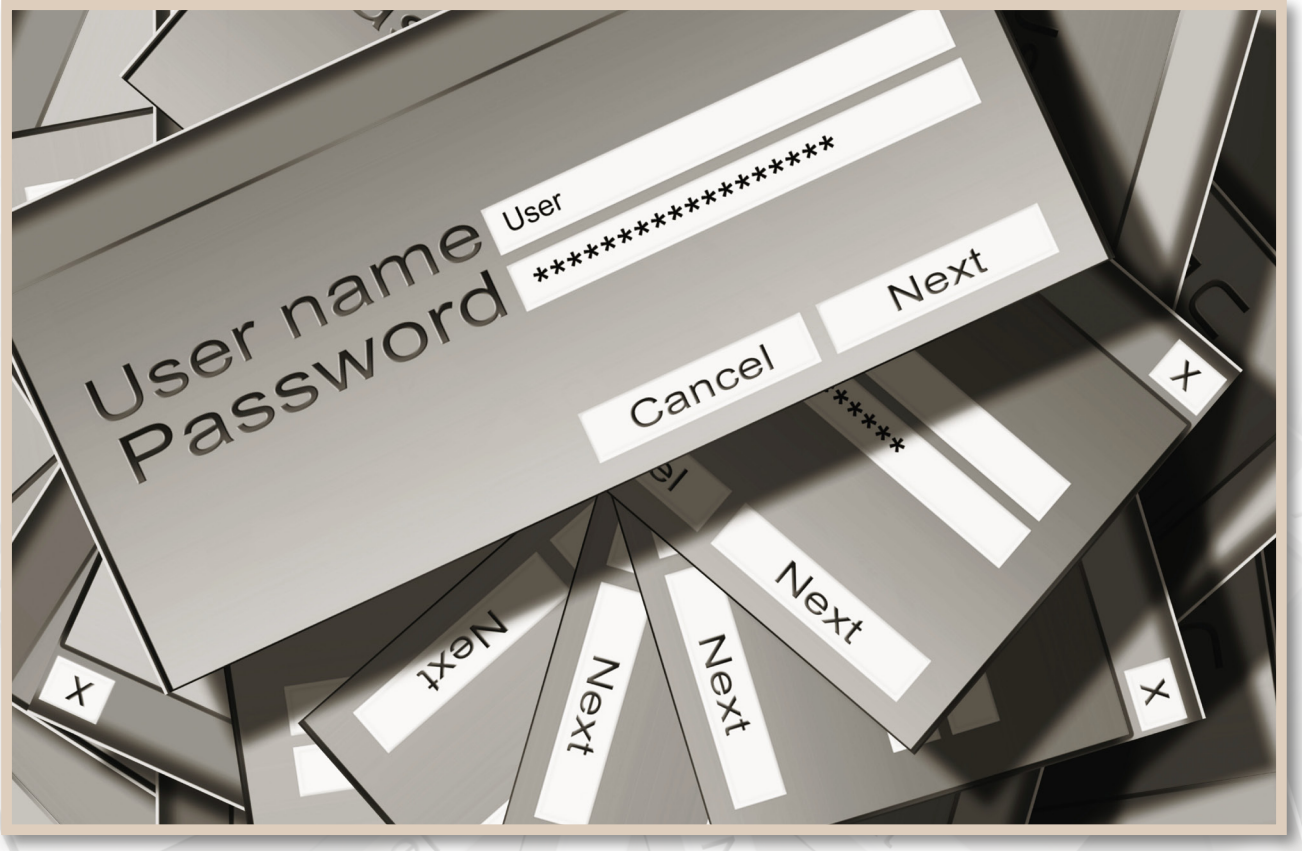
根據資安業者卡巴斯基實驗室調查，每年發現的物聯網惡意程式樣本數量逐年攀升，2017 年更比前年多出 4 千多種新 IoT 惡意程式。（資料來源：卡巴斯基實驗室，https://securelist.com/honeypots-and-the-internet-of-things/78751/）

二、與一般電腦存在同樣的安全問題

隨著物聯網裝置功能需求提高，裝置內部所使用的作業系統也向一般使用者電腦貼近，以應付高階的運作需求。以物聯網裝置可能搭載的 Linux 嵌入式作業系統為例，其內部的核心（Kernel）與上層應用軟體和函式庫也可能存在與一般電腦相同的安全漏洞。例如 2014 年 9 月曾爆發的 Shell Shock 重大漏洞（CVE-2014-6271），可能造成目標主機的機敏資料洩露或甚至被駭客所控制，影響的範圍主要為使用 bash shell 的作業系統，包含 CentOS、Ubuntu 及 Mac OS X 等，而亦有不少 Linux 嵌入式作業系統內建了 bash shell，故同樣存在資安風險。

三、安全性漏洞修補頻率低

在電腦或是手機上還有多種防毒軟體可以安裝使用，例如微軟、Apple 或 Google 等亦常會釋出安全性修補程式，但卻少有針對物聯網裝置開發專門的防護軟體，只能仰賴裝置製造商釋出的韌體（即燒錄於硬體內的軟體）更新。在成本的考量下可



物聯網裝置應避免使用預設的帳號密碼，降低駭客入侵的風險。

能無法於一年內更新一次，且即使製造商釋出了更新，使用者端也不具備自動修補的能力，故常見的狀況是裝置的韌體未更新，最後只能以汰換硬體收場。

四、常使用預設的帳號密碼

物聯網裝置為了方便進行大量生產，往往會使用預設的帳號密碼，這種現象可能出現於同一個型號的產品或甚至同一個產品線的所有裝置，且工廠出貨後部署至使用者端時，裝機人員也不會特定去修改裝置的預設帳號密碼，甚至可能無法修改，故大開駭客方便之門。駭客只要鎖定共同供應契約清單上所列的裝置，一旦成功破解，則採購同一型號的機關組織皆有被入侵的風險。

五、不易發覺異常

功能需求及成本考量下，物聯網裝置本身往往不需具備大型的使用者螢幕，僅需顯示必要訊息（例如通行碼或異常燈號），故入侵行為也不易被直接發覺。

六、長期不關機

駭客入侵成功後，除了要避免被資安設備察覺，還需要確保惡意連線的暢通，否則好不容易攻下的據點若隨時會失效，那就不符合攻擊的時間成本。而物聯網裝置的需求就是要能隨時提供服務，例如門禁系統必須24小時開啟，且隨時連結網路，一旦被成功入侵就可讓駭客長時間使用，可能被當作駭客的跳板機或是殭屍網路成員，長期潛伏並靜待駭客下達攻擊命令。

結論

現今的物聯網資安防護仍相當脆弱，特別是在連網裝置端點上的安全防護更是被人所忽略，全球的物聯網裝置於2020年預估會成長到二百至五百億台，更顯出潛藏資安問題的急迫性。資安專家建議使用者在架設物聯網裝置時，**應變更裝置的預設帳號密碼**，且**不要讓裝置暴露在公開網路上讓人隨意存取**，並且**關閉系統尚不必要的網路服務**，以防有心人士惡意探測系統上的漏洞；若設備有疑似遭到入侵的跡象或異常行為，應**立即聯繫相關設備廠商重新安裝系統或更新韌體版本**。只要遵行這幾項建議，即可大幅降低資安風險，減少被惡意程式狙擊成功的機會。