# 物聯網：正視安全問題（上篇）

**撰文**：David Mudd

BSI 全球數位與聯網產品驗證總監

David Mudd 是 BSI 物聯網首席專家，為 BSI 營運的 193 個國家/地區客戶提供卓越且專業的技術與產業知識。David 也是物聯網安全基金會（IoT Security Foundation）的測試與驗證工作團隊成員，曾編纂法規和技術準則，並為許多出版品撰寫文章，在全球各地介紹並發表相關演說。


A 資料來源：McKinsey，2015

B 資料來源：PwC，2015

C 資料來源：Gartner，2017

D 資料來源：Gartner，2017

E 來源：英國文化媒體暨體育部（DCMS）–安全設計報告，2018 年 3 月

F Gartner IoT report announcement，2016 年 4 月 25 日

據估計，英國每個家庭至少擁有 10 台連網裝置，到 2020 年，這個數字預計將增加到 15 台[E]。同時，估計有超過四分之一已被識別的攻擊將會與聯網裝置有關[F]，最近備受關注的漏洞事件已證明了這個現象。

## 目錄



## 執行摘要 Executive summary


- 物聯網（IoT）帶來了好處，也伴隨著風險，特別是安全風險。
- 物聯網的安全威脅非常真實、危險且持續上升。
- 身為連網產品或系統的供應商，您需負起商業上的義務，對客戶負責，以確保安全。
- 安全性不只限於密碼保護與加密。
- 專家研究和歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）所發布的新國際技術規範都強調──必須解決一系列基本問題。
- 挑戰之一包括歐盟《一般資料保護規範》（GDPR）的合規性，而英國的消費類物聯網設備安全行為準則（Code of Practice for Consumer IoT Security）能夠協助解決主要的 GDPR 問題。
- 若製造商無法解決安全挑戰，則會增加消費者的不信任感，並降低對製造商及其產品的商業信心。
- 安全性事件將產生嚴重的負面影響，包括採取法律行動並對其處以罰款、銷售額與利潤下降，及聲譽受損與商業投資減少。
- 另一種作法，是採用物聯網最佳實務來因應安全上的挑戰，有助於建立穩健的商業主張和組織的韌性。透過獨立驗證，您可以從競爭中脫穎而出，贏得消費者與企業的信任和信心，使銷售業績和利潤最大化。
- ETSI 技術規範是 BSI 物聯網驗證計劃的核心，其中包括新的 IoT BSI Kitemark。
- 是時候採取行動了，讓 BSI 來協助您。

## 簡介：安全性的警鐘

物聯網帶來了許多益處，並繼續呈倍數成長。若不是大眾對於物聯網產品和系統的安全有疑慮，物聯網實質上能帶來不同凡響的改變。

無論是提供消費者電子產品，或是企業對企業 ( B2B ) 的產品，都存在安全風險。所有物聯網裝置和系統都容易遭受外部威脅的攻擊，包括那些沒有直接配備安全或保全功能的裝置和系統；甚至是您可能從來都沒想過會成網路罪犯目標的裝置，例如連上網路的洗衣機。

英國政府的 2018 年報告《設計安全》對於大規模的裝置中斷和嚴重破壞的可能性提出了警告：「網路犯罪分子可能利用物聯網裝置和相關服務中的漏洞來針對資料和硬體進行存取、損壞和摧毀，或造成實體性或其他類型的傷害。其中，可以大規模利用這些漏洞，讓衝擊力道跨越領土疆界，波及國內外的受害者。」

消費者信任的缺乏，可能降低製造商對於物聯網產品和系統獲利的信心。

由於成本和風險過高，導致無法證明在物聯網技術和新產品開發等領域進行投資的合理性。

身為物聯網產品的製造商，若您的產品中嵌入了安全的第三方物聯網系統，您可能會認為您的產品能已達成「安全」的目標。抑或安全密碼和加密的功能，又或者是密碼和區塊鏈安全機制也許能給予您某種程度的安全感。但是，在一個充斥著複雜網路犯罪的世界中，你可能已經犯下極嚴重的錯誤判斷。

隨著一般家庭連網裝置的普及且同時使用多部裝置，服務供應商的需求只會有增無減。當前，許多智慧產品製造商並未對其產品的安全性給予足夠的重視；至關重要的是著手變革──從設計階段就納入相關安全措施，而非事後才考慮。

網路產品或系統的供應商永遠有「負責」該系統安全性的義務。除商業驅動程式外，他們還有責任關心客戶，確保其安全性，而非依賴第三方供應商或不健全的技術。

## 解決關鍵的安全問題

開放網路應用程式安全專案（OWASP - OWASP 成員包括來自世界各地的安全專家） 的研究顯示，當今資訊安全不能僅仰賴密碼保和加密保護。

針對物聯網系統的建立、部署或管理，OWSAP 歸納出需避免的十大 IoT 安全漏洞，清單內包含製造商、企業和消費者應優先處理的風險議題，幫助他們解決安全疑慮。

英國政府和產業界透過制定一套合作方式來保護消費者，同時繼續支援並鼓勵物聯網創新。2018 年 10 月，由負責英國網路安全政策的英國文化媒體暨體育部（Department for Digital, Culture, Media and Sport, DCMS）發布了一份實務指南作為 IoT 產業的行為準則，確保消費性 IoT 產品在設計階段考慮到安全性，以強化使用者裝置的安全。

該行為準則是英國文化媒體暨體育部（DCMS）與英國國家網路安全中心（National Cyber Security Centre, NCSC）共同制定，並得到了物聯網安全基金會（IoT Security Foundation, IoTSF）的背書，BSI 是該基金會成員之一。

2019 年初，歐洲電信標準協會（ETSI）發布了首份適用於全球的消費者物聯網安全技術規範《ETSI TS 103 645》。該規範係以英國的《物聯網安全實踐準則》為基礎，目的不單只是滿足歐洲而是因應全球需求。

**OWASP 近期更新物聯網應用程式的十大安全漏洞：**

1. **密碼強度低、容易猜測或硬編碼密碼（Hard-coded passwords）**
2. **不安全的網路服務**
3. **不安全的生態介面**
4. **缺乏安全的更新機制**
5. **使用不安全或過時的組件**
6. **隱私防護不足**
7. **不安全的資料傳輸和儲存**
8. **缺乏裝置管理**
9. **不安全的預設值**
10. **缺少實體強化機制**

## 業界技術規範

ETSI 技術規範係由 13 項保護物聯網裝置的準則所組成，各別加以解釋並整理總結如下：（第 5~13 項刊載於**〈物聯網：正視安全問題（下篇）〉**）

### 1. 無預設密碼

**所有物聯網裝置應設置不同密碼，並且不可被重置為任何通用預設值。**

此項主要適用於裝置製造商。規範中指出：「許多市面上販售的物聯網裝置都使用同樣的預設使用者名稱和密碼（例如：admin），並期待消費者會自行變更。這種做法便是物聯網中許多安全問題的根源，應盡早汰除，並遵循密碼和其他身份驗證方式的最佳作法。」

此項建議受 IT 安全公司卡巴斯基實驗室（Kaspersky Lab）研究的支持。該公司發現，傳播 IoT 惡意軟體中最盛行的方法仍然是「暴力破解」密碼。駭客將反覆嘗試各種密碼組合，以獲得裝置存取權限。在檢測到的攻擊中，有 93%使用了暴力破解的手段。

### 2. 實施漏洞披露政策

**所有提供互聯網連接裝置與服務的公司都應採取漏洞披露政策，並提供對外的聯絡窗口，以便安全研究人員或其他人員能夠報告他們所發現的問題。這些被披露的漏洞，應及時採取措施處理。**

此項主要適用於裝置製造商、物聯網服務供應商，以及行動應用程式開發商。該規範詳述：「掌握安全性漏洞可以讓公司做相對的應變。公司還應持續監控、識別和改正其產品和服務中的安全漏洞，以此作為產品安全生命週期的一部分。應該在第一時間向受影響的利害相關者進行漏洞的報告。如果無法做到這一點，可將漏洞通報給相關主管機關；此外，也鼓勵企業廠商與主管機關共享情資。」

### 3. 保持軟體更新

**連網裝置中的軟體元件應能夠安全地更新。更新作業應適時進行，且不應影響裝置功能。應針對終端裝置發佈報廢政策，明確規定裝置軟體的維護更新期限，以及訂定該支援期限的原因。此外，應清楚告知消費者各項更新的內容，且更新作業應該要容易實施。當裝置老舊且無法透過硬體升級方式更新時，則應進行隔離且汰換。**

此項主要適用於裝置製造商、物聯網服務供應商和行動應用程式開發商。規範中提到：「還應確保安全修補程式（patches）的出處，並透過安全管道進行傳送。在更新期間，裝置的基本功能應儘可能持續運作，例如：手錶應能繼續顯示時間、家庭

恆溫裝置應仍能運作、鎖具應繼續維持解鎖或上鎖狀態。這看似出於設計考量，但如果考量不當或管理不當，可能會成為某些裝置和系統類型的嚴重安全問題。

在裝置售出後應提供軟體更新，並於合理期間內，持續為裝置進行更新。在購買產品時，應向消費者說明軟體的更新支援期限。零售商和/或製造商應將更新的必要性告知消費者。對於受到限制無法進行軟體更新的裝置，應明定裝置更換的支援條件和期限。」

### 4. 安全地儲存憑證與機敏資料

**任何憑證都應安全地儲存在服務系統和裝置中。裝置軟體中的硬編碼(Hard-coded)憑證是不可被接受的。**

此項主要適用於裝置製造商、物聯網服務供應商和行動應用程式開發商。規範中解釋：「對裝置和應用程式實施逆向工程，便可以輕鬆找到憑證，例如：軟體中的硬編碼使用者名稱和密碼，而用來遮蔽或加密這些硬編碼資訊的簡單隱匿技術，其實非常容易被破壞。此外，像是加密金鑰、裝置識別碼和初始化向量（Initialization vectors）等機敏資料應該安全的儲存，並且應使用安全的、受信任的儲存機制，例如：可信執行環境（Trusted Execution Environment）架構以及相關受信任且安全的儲存方式。」

**〈物聯網：正視安全問題（下篇）〉待續...**

更多 **IoT 物聯網** 白皮書、網路研討會（webinar）等資訊，請造訪 BSI 官網：bsigroup.tw