

物聯網：正視安全問題（下篇）

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。



The Internet of Things:
get serious about security
A whitepaper

目錄

1. 執行摘要
2. 簡介：安全性的警鐘
3. 解決關鍵的安全問題
4. 業界技術規範
5. 技術規範與歐盟《一般資料保護規範》（GDPR）
6. 透過 BSI 建立韌性

物聯網：正視安全問題（上篇）

物聯網：正視安全問題（下篇）

業界技術規範

歐洲電信標準協會 (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 1~4 項刊載於 [〈物聯網：正視安全問題 \(上篇 \)〉](#))

5. 安全通訊

敏感性資料(包括任何遠端管理與控制)在傳輸過程中，應根據適合的技術和用途屬性進行加密，並該對所有加密金鑰進行安全管理。

此規範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。ETSI 規範中補充說：「強烈建議採用開放式且經產業審查認可過的網際網路標準。」

6. 減少暴露的攻擊面 (Attack surfaces)

所有裝置與服務應以「最小權限原則」進行運作。未使用的連接埠應予關閉、不應讓硬體暴露不必要的存取途徑、不需使用的服務則不應提供，且程式碼應儘量簡化，僅提供服務運作必需之功能。使用適當權限執行軟體時，同時兼顧安全與功能性。

此規範主要適用於裝置製造商和物聯網服務供應商。規範中指出「最小權限原則是良好安全工程的基石，除了適用於物聯網外，亦適用其他領域的應用」。

7. 確保軟體完整性

應使用安全啟動 (Secure Boot) 機制驗證物聯網裝置上的軟體。如果檢測到未經授權的變更，則該裝置應向消費者/管理員發出警示，且該裝置不應連線到執行警告功能所需範圍之外的網路。

此規範主要適用於裝置製造商。此規範補充：「在前述情況下進行遠端設備還原，應是在已知的良好狀態下，例如本機端已儲存正確的軟體版本，以實現裝置的安全還原與更新。這將可避免服務被阻斷、昂貴的召回作業或到府維護，同時管理網路裝置受到攻擊者利用軟體更新的漏洞，或者破壞其他網路通訊機制而被接管的潛在風險。」

8. 確保個人資料受到保護

裝置和/或服務應根據適用的資料保護法進行資料處理，例如歐盟的《歐盟一般資料保護規範》(GDPR) 和英國《資料保護法 2018》。裝置製造商和物聯網服務供應商應針對每個裝置與服務，向消費者提供清楚透明的資訊，讓消費者知道他們的資料是被如何使用、由誰使用、以及用於何種目的。這也適用於任何可能涉及的第三方 (包括廣告商)。如果在徵得消費者同意的情況下對其個人資料進行處理，則必須有效且合法地獲取這些資料，並提供管道讓消費者有機會隨時撤回這些資料。

此規範主要適用於裝置製造商、物聯網服務供應商、行動應用程式開發商和零售商。規範中詳細提到：「本規範可確保：

- 物聯網製造商、服務供應商和應用程式開發人員在開發和提供產品和服務時，應遵守資料保護義務
- 根據資料保護法處理個人資料
- 協助使用者確保其產品的資料處理作業是一致的，且依照指定的方式運作
- 透過適當的裝置設定與服務功能，為使用者提供保護隱私的方法」

9. 使系統具備持續運作的韌性 (resilience)

應考慮到資料網路和電源中斷的可能性，並根據物聯網裝置與服務的使用情況或其他中繼系統的需要，確保物聯網裝置與服務具有韌性。只要合理可行範圍內，當網路中斷時，物聯網服務與本機皆應保持運作。當恢復電力時，物聯網服務應可進行俐落的復原動作。裝置應該能夠在合理的方式連回網路，而非進行大規模的重新連線。

此規範主要適用於裝置製造商和物聯網服務供應商。規範指出：「消費者依賴物聯網系統和裝置來進行日益重要的用途，這些用途可能與安全相關，甚至影響生命安危。一旦網路中斷，本機依舊可操作並保持服務運作，是提高系統韌性的措施之一。其他措施則可包括在服務中建立備援，以及抵禦 DDoS 攻擊。所需的韌性應依使用情況而定。但同時應考慮可能中繼系統、服務或裝置等其他因素，因為這些因素所產生的影響可能遠比預期的要廣泛。」

10. 監控系統遙測 (Telemetry) 數據

如果遙測數據是透過物聯網裝置與服務所收集，例如使用狀況和測量數據，則應監控其是否有安全異常的現象。此規範主要適用於物聯網服務供應商。

11. 使消費者易於刪除個人資料

裝置與服務應採相關組態設定，以便在所有權轉移、消費者欲刪除個人資料和/或丟棄裝置時，可以輕鬆地從中刪除個人資料。對於消費者個人資料該如何刪除，應予明確說明。

此規範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。

12. 簡化裝置的安裝與維護

對於物聯網裝置的安裝和維護，應採用最少的設定步驟，並且應遵循可用性 (Usability) 相關的安全性最佳實務方式。還應向消費者提供有關如何對裝置進行安全設定的指引。

此規範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。規範指出：「適當解決使用者介面中的複雜性與不良設計，可以減少甚至消除因消費者困惑或組態設定錯誤所引起的安全性問題。向使用者提供有關如何對裝置安全進行組態設定的明確指引，也可以減少他們所面臨的威脅。」

13. 驗證輸入資料

使用者介面輸入的資料、應用程式介面 (**API**) 所傳輸的資料，或在服務和裝置間所傳輸的資料，皆應進行驗證。

此規範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。在程式碼規範中註明：「錯誤的格式化資料，或在不同類型的介面間傳輸的程式碼，皆可能破壞系統。攻擊者經常運用自動化工具，來攻擊因資料參數未經驗證而出現的潛在弱點和漏洞。舉例包括但不限於以下資料：

- 非預期的類型，例如可執行的程式碼，而非使用者所輸入的文字
- 超出範圍，例如超過感測器極限的溫度值」

ETSI 技術規範與 GDPR

歐盟最近所實施的《一般資料保護規範》(**GDPR**) 延伸了個人資料的定義，涵蓋到許多連線到網路的應用程式，增加了物聯網供應商的安全挑戰。該規範對於在歐盟提供產品或服務的所有製造商和服務供應商皆具有約束力。

ETSI 技術規範直接連結到 **GDPR**，探討組織應如何處理其資料以及應採取的因應措施，以確保資料的安全性。

產品本身不能證明 **GDPR** 的合規性 (需對整個組織的流程進行評估方能確認)，但該作業規範解決了部分 **GDPR** 問題。具體來說，實施原則 8 和原則 11 將可滿足 **GDPR** 的關鍵要素，而搭配總體安全性以及對組織的整體考量，將使企業能夠滿足合規要求。

透過 BSI 建立韌性

BSI 擁有世界級的網路安全技術能力，獲得了國際公認的網路安全技術認證機構 CREST 認可，並在產品測試與驗證上，累積了數十年的經驗。

BSI 透過高階技術團隊及最先進的物聯網實驗室，為各項物聯網產品提供快速且有效的測試。在產品設計流程的早期階段便就安全性議題提供寶貴的回饋意見，BSI 可以在競爭激烈且分秒必爭的產業中加速產品上市時間，並降低上市會遭遇到的風險。

BSI 與客戶合作，驗證產品或服務是否符合良好的物聯網安全設計規範。透過 BSI 的驗證方案，裝置製造商、物聯網服務供應商和行動應用程式開發商可以向其客戶證明其產品對於預期用途而言是安全的。

如今，BSI 透過與利害關係者密切溝通及合作，並以 OWASP 研究和 ETSI 技術規範為基礎，開發出物聯網驗證解決方案—IoT 風箏標誌（Kitemark）。

BSI IoT 風箏標誌可幫助消費者判斷哪些網路產品是安全、可靠，且適得其用。這些裝置必經嚴格的測試，以確保效能符合預期、能進行正確的通訊，並在其預期用途上是安全可靠的。BSI 風箏標誌的主要優勢在於：

- 適切性—以風險為基礎，並依據用途/環境進行測試
- 靈活性—從測試方案中「挑選清單」量身定做最適切的測試項目
- 適應性—隨著網路安全技術、威脅和標準的發展持續進化
- 全面性—能夠涵蓋供應鏈、既有系統和雲端層/應用程式

組織需要一個可靠的資訊安全標準，以提供持續、持久的韌性。BSI 是全球目前唯一提供 ETSI 技術規範獨立性驗證或合規性的組織。BSI 可以幫助您建立信任與信心，協助您確保產品的安全、可靠並持續符合期待的運作著。

立即採取行動

放眼蓬勃發展的物聯網商機，應採安全的方法建立消費者信任、商業信心和組織韌性。然而，欲建立一個安全的物聯網系統，不能僅仰賴安全密碼和加密措施的保護。BSI 可以幫助您克服這項挑戰。現在正是聯絡我們的時候。



為什麼該選擇 BSI？

BSI 是一個值得信賴、獨立的網路安全領導者，透過塑造、共享、深植及支援來協助物聯網產業創新，並且安全可靠地使用「智慧」應用程式、資料與裝置。透過我們的物聯網專家和社群組織，在物聯網領域中塑造新契機與創造領先業界的最佳實務上，BSI 一直站在最前線。這就是為什麼我們可以提供最佳解決方案，幫助建立您產品的信任和信心。

BSI 已成為國際性的知名組織，與 193 個國家/地區中 86000 多家客戶進行合作。在涵蓋汽車、航太、建築環境、食品和醫療等多項產業領域中擁有豐富的技術和經驗。BSI 透過制定標準與知識解決方案、驗證和專業服務的專業知識，協助客戶提升業務績效，幫助客戶永續成長、管理風險，令組織更具韌性。



我們的產品與服務

知 識

我們發展並傳授予客戶的知識是我們業務的核心。作為聲譽卓著的標準專業機構，我們持續召集產業界的專家，來制定地方性、區域性標準及國際標準。事實上，全球 10 大管理系統標準中有 8 個由 BSI 率先制定。

保 證

由獨立的第三方稽核來確認組織的流程或產品是否符合標準的要求，可確保我們的客戶達成高標準的卓越績效。我們運用世界級的實施方案與稽核技巧，確保標準為客戶帶來的效益能發揮到最大。

合 規

想要長期、確實地獲利，我們的客戶必須確保能夠持續符合相關法規、市場需求或標準的要求，並內化為一種習慣。我們提供一系列的服務與差異化管理工具，讓組織的合規流程能更順利地進行。

- [洽詢 BSI](#) | [稽核驗證](#)、[產品測試](#)、[BSI 訓練學苑](#)、[VerifEye 認證平台](#)、[BSOL 標準資料庫](#)