物聯網需要更好的安全性

IoT Needs Better Security

作者：Hemant Patel, CISM, ITIL, PMP, TOGAF
Is a principal advisor at Computer Sciences Corporation, SC, as a part of the US Chief Technology Officer team. His expertise includes IT enterprise architecture, information security, portfolio planning, big data, web and e-commerce, analytics, enterprise resource planning and customer relationship management systems. His global experience includes working in the defense, manufacturing, health care, utilities, banking and insurance industries. Patel can be contacted at hpatel63@csc.com or mr.hemant.patel@hotmail.com.

譯者: 謝家蘭，國立政治大學會計學系特聘教授,電腦稽核協會專業發展委員會委員/編譯出版委員會委員

物聯網（IoT）是一個連接事物（固定或移動設備）的生態系統。2016年商業內幕報告(Business Insider report)稱，到2020年將有340億台設備連接到互聯網，而2015年將達到100億台。此外，物聯網設備將佔其中的240億，而傳統的計算設備（如智能手機，平板電腦，智能手錶）將包括100億台。而且，未來五年，將近6萬億美元將用於物聯網解決方案。[1]

為什麼我們需要物聯網安全？

產業正在快速變化，新的物聯網用例正在成熟。越來越多的功能被添加到物聯網系統中，以實現率先面市的優勢和功能的優勢，而物聯網系統設備的安全性在設計過程中往往被忽略。從最近的駭客事件中可以明顯看出：

- 美國食品和藥物管理局發布針對心臟設備的安全建議，以解決駭客威脅問題，聖猶達兒童研究醫院修補了易受攻擊的醫療物聯網設備。[2]
- 駭客對特斯拉Model S汽車展開無線攻擊。[3]
- 研究人員駭客Vizio智能電視訪問家庭網絡。[4]

在物聯網安裝和安裝後配置過程中也容易遺漏安全的考量，ForeScout物聯網安全調查指出：「最初認為他們的網絡上沒有物聯網設備的受訪者實際上有8種物聯網設備類型（當被要求從設備列表中選擇時），只有44%的受訪者的物聯網擁有已知的安全策略。」[5]此外，只有30%的人確信他們確實知道他們網絡上的物聯網設備。[6]

這些駭客攻擊和ForeScout調查結果的影響表明，物聯網安全需要全面實施。這需要了解物聯網架構。

物聯網架構

Zachman Framework[7]解答了關於物聯網why, how, what, who, where和 when的問題。Why的物聯網安全問題已經在這裡得到解決。在四個“建築層次”中解釋了how以及what問題。圖1描述了透過Zachman框架回答的IoT安全體系結構問題。

圖 1—Zachman Framework 物聯網安全體系結構

問題	物聯網安全
Why?	安全漏洞、威脅建模的例子
How?	設備配置、整合、準則及流程
What?	其組成及關係列表
Who?	用戶、管理員、供應商、產業體系
Where?	架構中的每一層和組成
When?	設計，配置/實施和操作

Source: H. Patel. Reprinted with permission.

為了理解物聯網安全需求，需要對物聯網有較高階的概念。如圖 2 所示，資訊從邊緣層（即物聯網設備、組件/機器）流向數據層，接著再流向商業智慧（BI）層，最後再流向操作和策略（OpS）層。本地網絡或寬帶區域網絡連接設備層。通常，許多設備會被分組來作組件或機器的組裝。設備之間的通信不一定會出現在組件或機器中。設備和組件連接到集線器或網路，以封裝獨特的設備功能並實現更好的標準化和管理。

整體安全方法包括各層的安全性和各層之間的通信安全性。除邊緣層以外的層可以駐留在場所或雲端中。理解每個層次的安全需求非常重要。

邊緣層安全性

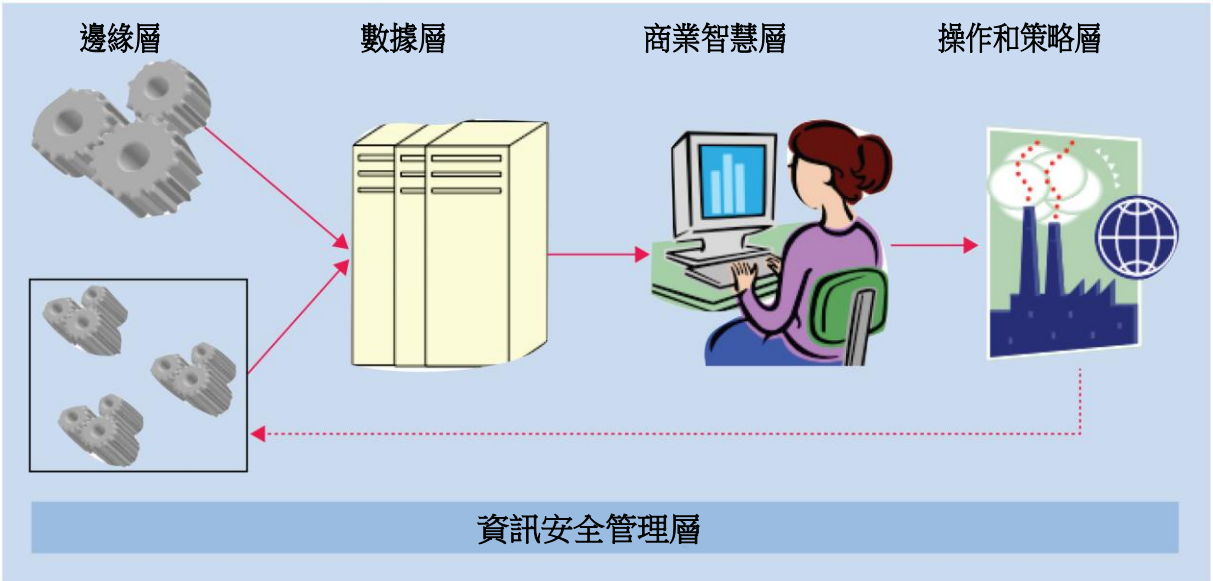
物聯網安全應該成為資訊安全這個廣泛主題的一部分。邊緣層設備/感應器產生由物聯網體系結構的上游組件處理的數據。數據量遠遠超過互聯網用戶活動產生的數據量。

在基於設備的安全和物聯網集線器/網路管理軟件領域存在著巨大的競爭，並且存在大量的準則。 Microsoft，IBM和Allegro等組織在高級應用程序編程接口（API）和工具中封裝基於設備的安全性方面做得很好。圖3描述了邊緣層安全架構的基本構建模塊。集線器或網路支持與物聯網安全相關的安全管理、存儲管理和通信組件。

> 全面性安全(holistic Security)包含對每個層級的安全與對層級間的通訊保全。

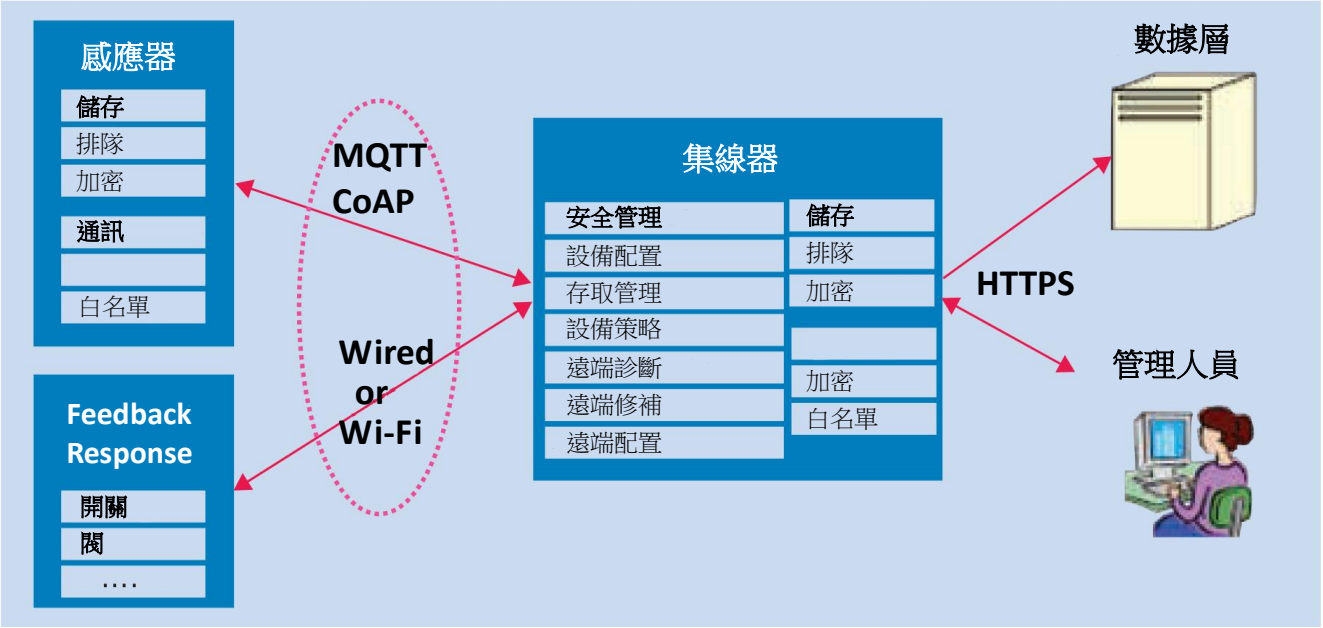
設備可以與集線器互相連接或通信，並且這種通信軟體需要更小的排隊能力。有更好的協議接著早先的傳輸控制協議（TCP）被採用，包括：

圖 2—物聯網架構



Source: H. Patel. Reprinted with permission.

圖三—物聯網邊緣層安全架構



Source: H. Patel. Reprinted with permission.

- 消息隊列遙測傳輸（MQTT）-基於TCP的協議支持設備認證，安全套接字層（SSL）/傳輸層安全性（TLS）加密、排隊和訂閱功能。
- 約束應用協議（CoAP）-基於用戶數據報協議（UDP）的傳輸，支援微型設備，且佔用空間小於HTTP。它支援高級加密標準（AES）加密。[8]

無線區域網路(WLAN)被廣泛應用於許多使用 WPA2 安全系統的領域中。Wi-Fi系統缺乏安全性結構及時常使用安全性較弱之密碼成為最常被駭客入侵之系統。一個通訊閘可以連接到多個集線器並提供較高層級的資料傳輸協議如：超文字傳輸安全協定(HTTPS)，支援傳輸層安全性加密及表現層狀態轉換(REST)-簡單物件存取協定(SOAP)訊息。

裝置及集線器的賣家需要支援安全協定及管理，正如文中所描述，賣家的支援可能因為多個不同的協議及不同的身份驗證方式而變得非常複雜。

另外一個需要被監督的事件是物聯網是否發生故障。故障發生的源頭可能是安全漏洞也有可能是其他原因。故障可能會引起裝置不停嘗試接觸資訊，結構並未限制重試的次數，可能有無數次的重試。每次的重試都會把一個錯誤訊息傳回集線器中，集線器可能會取得無數錯誤的訊息(類似阻斷服務攻擊[DDoS])物聯網的集線器有可能會因為過大的負荷而無法正常運作，影響集線器的可用性。

故障有可能會使物聯網暫停生產資訊。使集線器無法接收任何資訊，並影響集線器之誠信。因此，裝置故障有可能會影響到物聯網安全性系統的可用性及誠信(訊息的基本安全品質)。

資料層安全

資料層的活動包括數據接入，數據工程及使用結構化查詢語言(SQL)或傳統資料庫 NoSQL 科技數據轉換或大數據科技。SQL 資料庫提供資料列層級及單元性安全保護。較早之前的大數據科技提供資料夾及操作系統層級安全性保護，但是現時提供較低層級的安全性保護，例如，Apache Sentry[9] 以角色為基礎的存取控制。

安全子層包括網路安全、授權與鑑定、資料倉儲與資料管理的產業標準加密。數據管理指示資料分開討論，包括企業數據建構、數據沿襲、審計與監管。低品質的數據建構及數據管理沿襲會犧牲掉資料的一致性與可用性。

為維持數據之保密性，系統監管、權限及轉置需要符合幾個產業的標準如：美國健康保險便利和責任法案(HIPAA)及支付卡產業資料安全標準(PCI DSS)。一篇ISACA®過去的文獻，「裝置安全之回到未來：平衡 FIPPs 與積極管理物聯網保密和安全性風險」[10]，解釋物聯網各個部分處理數據過程中的保密性考量。

BI 層級安全

資料遮罩、身份別授權與單一登入(SSO)提供此層級的安全性保護除了網路安全及防火牆。BI(預測的，規範的)模型管理是資料監管的議題。此模型需要足夠的測試與認可。使用有缺陷的智慧有可能會因資料不足而影響企業的決定，並毀壞企業的名譽與信用。

資料外洩防護(DLP)與備用科技可提供額外的安全性保護。

OpS 層級安全

反饋迴路可能會出現在裝置的運作系統中。傳統網路安全及防火牆、身份別授權，及SSO都在本層中提供安全性保護。

DevOps工具可降低建構錯誤與疏失的風險，建構錯誤與疏失可能會影響到系統的可用性。

策略會根據BI的結果決定一系列的動作。一個策略可能只是為了監察物聯網裝置中所接收的資訊，或包括處理物聯網裝置中所接收的資訊及根據有限度的資訊改變物聯網裝置。兩種策略(需求與設計)及反饋迴路(執行)均需被驗證/測試。

> 裝置故障會影響 IoT(物聯網)安全的可用性與完整性(資訊安全的基本品質)。

威脅管理與風險管理

圖2顯示反饋迴路的OpS層級至邊緣層級的架構。當缺少反饋迴路及裝置中的資料為非機密性時，在合理風險管理的情況下可降低接觸資料及資料加密的安全性保護。

風險緩和與反應策略可能會根據以下問題設計：

- 折衷性的裝置可使其他裝置與集線器折衷嗎？
- 折衷性的裝置可以多快速的察覺與孤立呢？
- 折衷性的裝置可帶來什麼影響？

> 物聯網安全並不只是裝置層級的安全性保護；它應該被應用到所有電子元件或物聯網的每個層級中。

這些問題並不是很全面但應在設立風險管理指引時被考慮進去。

結論

物聯網安全性保護系統設計及執行時常缺乏優先性考量。物聯網安全並不只是裝置層級的安全性保護；它應該被應用到所有電子元件或物聯網的每個層級中。安全性保護需要被應用在物聯網系統生命週期的每一個階段中，包含設計、安裝、結構及運作階段。

此外，較強的密碼及金鑰認證，難以猜測的裝置或名稱/身份標識，程式碼監管與分析，主動性的用戶及裝置管理，及附著於產業指引及企業安全性推薦如美國國家標準暨技術研究院會使用物聯網。

END NOTES

1 BI Intelligence, "Here's How the Internet of Things Will Explode by 2020," *Business Insider*, 31 August 2016, *www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2*

2 Bacon, M.; "St. Jude Medical Finally Patches Vulnerable Medical IoT Devices," *TechTarget*, 13 January 2017, *http://searchsecurity.techtarget.com/news/450410935/St-Jude-Medical-finally-patches-vulnerable-medical-IoT-devices*

3 Golson, J.; "Car Hackers Demonstrate Wireless Attack on Tesla Model S," *The Verge*, 19 September 2016, *www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs*

4 Zorz, Z.; "Researchers Hack Vizio Smart TVs to Access Home Network," *Help Net Security*, 12 November 2015, *https://www.helpnetsecurity.com/2015/11/12/researcher-shack-vizio-smart-tvs-to-access-home-network/*

5 ForeScout, IoT Security Survey Results, *https://www.forescout.com/iot-security-survey-results/*

6 *Ibid.*

7 Zachman, J.; "The Concise Definition of the Zachman Framework," Zachman International Enterprise Architecture, 2008, *https://www.zachman.com/about-the-zachman-framework*

8 Eclipse, MQTT and CoAP, IoT Protocols, *www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php*

9 Sentry, Apache Sentry, *http://sentry.apache.org/*

10 Rotman, D.; C. Kypreos; S. Pipes; "Back to the Future in Device Security: Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk," *ISACA® Journal*, vol. 6, 2015, *https://www.isaca.org/Journal/archives*

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 3 2017 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2017,Volume 3中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每

年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。