# Securing the Internet of Things

IEEE, Computer, September 2011, Vol. 44, Iss. 9,
pp. 51 – 58, doi: 10.1109/MC.2011.291

Authors：Rodrigo Roman, Pablo Najera, and Javier Lopez,
University of Malaga, Spain

Present：李郁孟

Student num：ma190208

# Outline

- 1. Introduction
- 2. Infrastructure seeds
- 3. Coping with old and new threats
- 4. Work in progress
- 5. Conclusion

# 1. Introduction

- 物聯網(The Internet of Things, IOT) ，將日常生活中的物品，經由傳感器，透過無線射頻辨識系統(RFID)與網際網路連接起來，實現物品的自動識別與資訊的互聯與共享。
- 在物聯網中，每一個現實物件會有一個虛擬的對象。
- 物聯網帶來了前所未有的方便和經濟，但它也將需要新的方法，以確保其安全和道德。

# 2. Infrastructure seeds

- 物聯網物件具有五個主要特點：

1. 存在性(Existence)
2. 自我意識性(Sense of self)
3. 連結性(Connectivity)
4. 互動性(Interactivity)
5. 動態性(Dynamicity)
6. 環境意識(Environmental awareness)(可選的)

# 2. Infrastructure seeds(Cont)

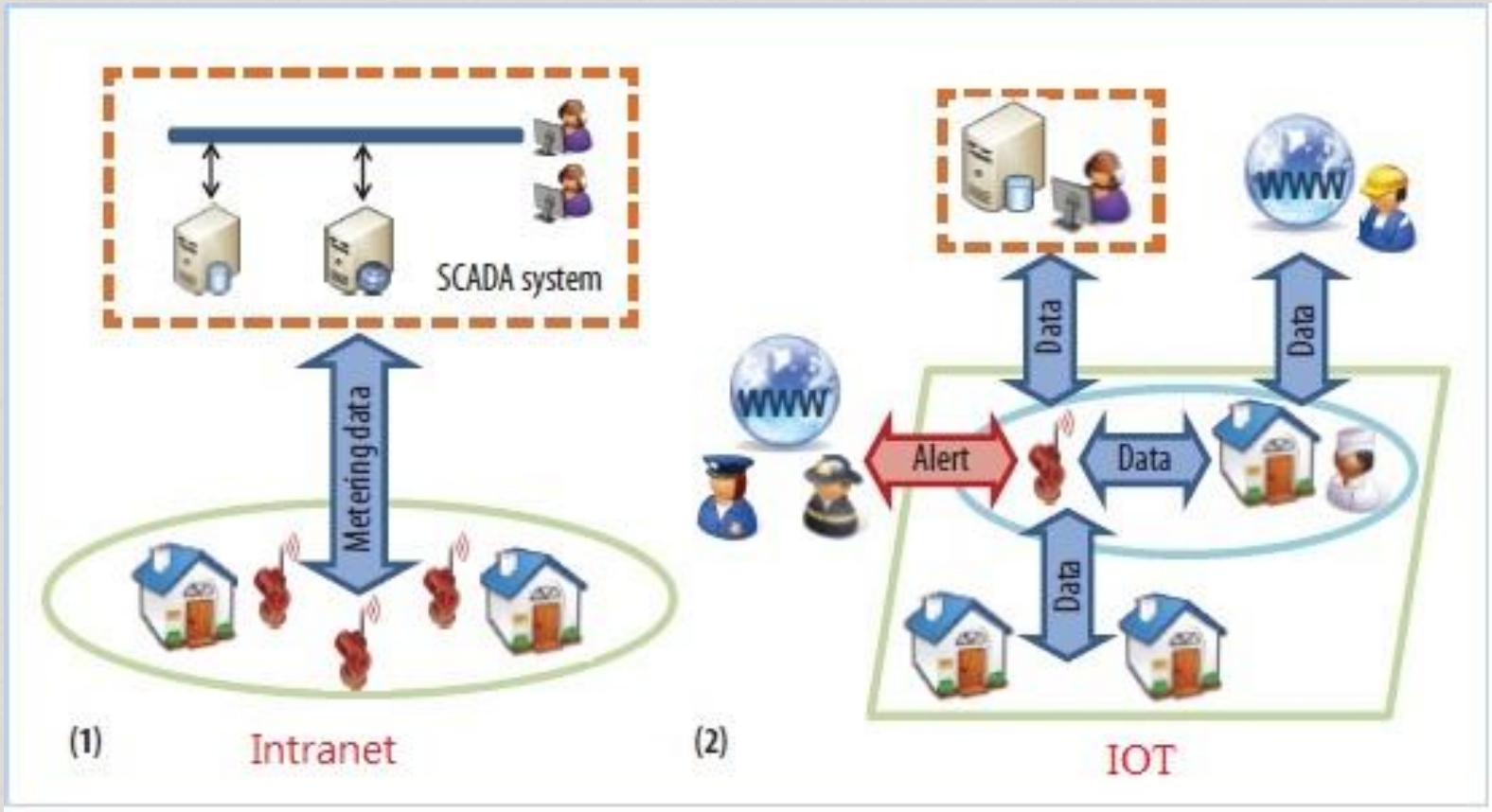


圖1、在兩種情況下的智能電錶應用。

# 3. Coping with old and new threats

- 數十億的智能的物件於隨機和不可預知的方式與其他真實和虛擬實體進行互動，什麼保護措施是可行的？
- 無線通訊，訊號在空氣中傳播，容易遭受外部攻擊與干擾。
- 容易可存取的物件在未受保護的區域，很容易受到物理傷害。

# 3. Coping with old and new threats(Cont)

- 協定與網路安全：

●AES加密保護程度有限。

●加密機制必須更強大，機制可能包括對稱演算法、雜湊函數和亂數產生器。

# 3. Coping with old and new threats(Cont)

- 資料和隱私：

1. 隱私保護設計 (Privacy by design)

2. 透明度( Transparency)

3. 資料管理( Data management)

# 3. Coping with old and new threats(Cont)

- 資料和隱私(續)：

4. 身份管理 (Identity management)

- 物件的身份可以是不同的標識及其同機制。
- 物件可以有一個核心身份和一些臨時身份 。
- 物件可以識別其身份或具體特點。
- 物件知道其擁有者的身份。

# 3. Coping with old and new threats(Cont)

- 信任及管治：

- 信任是降低物件的不確定性，提供在整個互動的信任。

- 管治將有助於加強在物聯網的信任。但是，管治是一個雙刃劍。

# 3. Coping with old and new threats(Cont)

- 容錯性(Fault tolerance)：

●實現物聯網的容錯性，將需要三個合作努力：

1. 所有物件預設情況下為安全
2. 物聯網的物件能夠知道網路和其服務的狀態
3. 物件要能夠保衛自己的網路故障和攻擊

# 4. Work in progress

**Table 1. Standards for IoT technologies.**

| Standard | Purpose | Security |
|---|---|---|
| 1. ISO/IEC 14443 | Architecture for contactless proximity cards 非接觸式感應卡的體系結構 | Information flow protection (AES) 資訊流量保護 |
| 2. IEC 62591 (WirelessHART) | Protocol for industrial wireless sensor networks工業無線感應器網路通訊協定 | Encryption, authentication, key management 加密、身份驗證、金鑰管理 |
| 3. GS1 keys | Identification system 識別系統 | Unique identifier definition |
| 4. ucode | 與硬件無關的識別碼 Hardware-agnostic identifier | 唯一識別碼定義 Unique identifier definition |

表1、物聯網技術標準

# 4. Work in progress(Cont)

| Table 2. IETF standards that might be implemented in the IoT. | | |
|---|---|---|
| Standard | Purpose | URL |
| 1. 6LowPAN | IP connectivity IP連接性 | http://datatracker.ietf.org/wg/6lowpan |
| 2. ROLL | IP connectivity IP連接性 | http://datatracker.ietf.org/wg/roll |
| 3. CoRE | Lightweight REST Web service architecture 輕量級REST Web服務體系結構 | http://datatracker.ietf.org/wg/core |
| 4. CoAP | Generic Web protocol definition 通用Web協議定義 | http://datatracker.ietf.org/wg/core |

表2、可能在物聯網實施的 IETF 標準

# 4. Work in progress(Cont)

- 可能在物聯網實施的 IETF 標準：

1. 6LowPAN(IPv6 over Low power WPAN)

- 為物聯網網路層採用 IPv6 之技術，描述 IPv6 封包如何承載在 IEEE 802.15.4通訊協定上。

- 目的為建立良好的網域，如新興起的傳感器網路，越來越多地被用於無線技術。

# 4. Work in progress(Cont)

- 可能在物聯網實施的 IETF 標準(續)：

2. ROLL(Routing Over Low power and Lossy networks)

- 為了制定出適合低功率網路的路由協議，然後研究了路由協議中路徑選擇的定量指標。

- 目的為能夠讓傳感器選擇最佳的路徑。

# 4. Work in progress(Cont)

- 可能在物聯網實施的 IETF 標準(續)：

3. CoRE(Constrained RESTful Environments)

- 討論資源受限網路環境下的訊息讀取操控問題。

- 目的為制定輕量級的應用層協議 (CoAP, Constrained Application Protocol)。

# 4. Work in progress(Cont)

- 可能在物聯網實施的 IETF 標準(續)：

4. CoAP(Constrained Application Protocol)

- CoAP設計為使用兩個設備在相同受限的網路，甚至跨互聯網的服務器和設備之間。

- 目的為在互聯網上的服務就能夠直接透過CoAP協議或者透過HTTP與CoAP協議之間的閘道來進行資源讀取、修改、刪除等操作。

# 4. Work in progress(Cont)

- 可能在物聯網實施的 IETF 標準(續)：

4. CoAP(Constrained Application Protocol)(續)

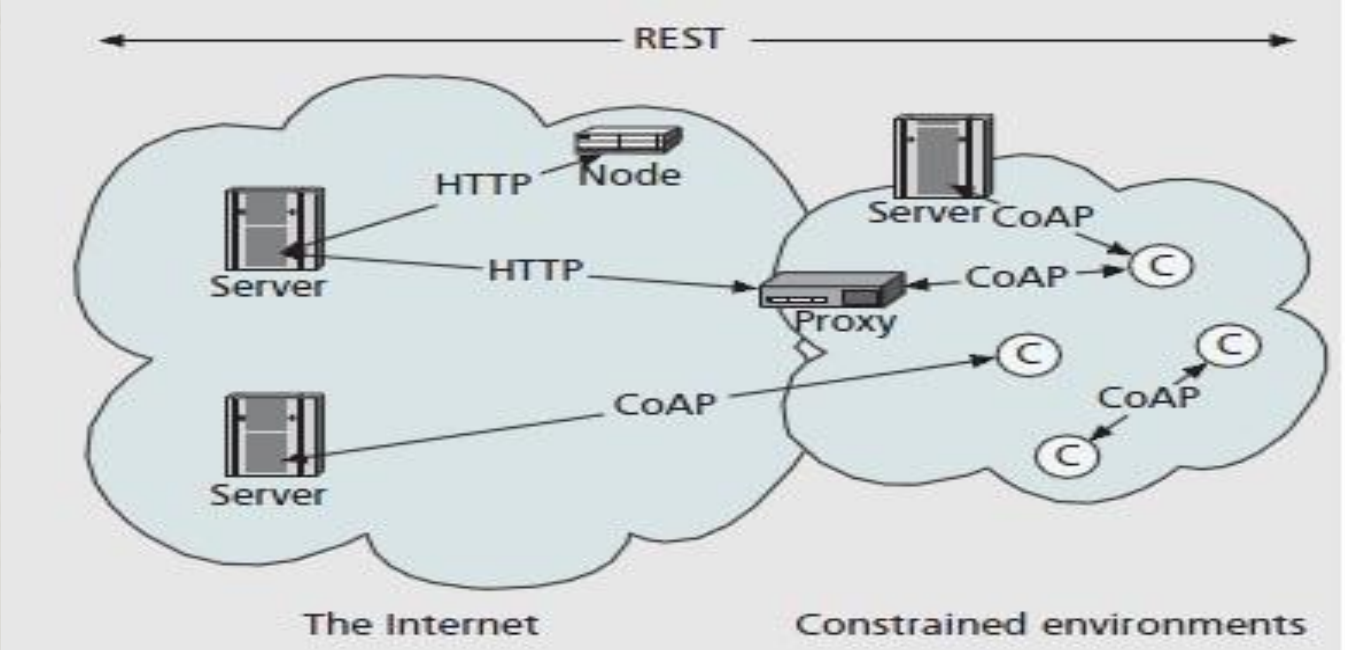


圖2、受限RESTful的環境架構

# 5. Conclusion

- 物聯網已經不是一個概念。
- 透過遵守安全要求，它可以完全發展成一個模式，將改善日常生活的許多方面。
- 在一些方面未解決的問題仍然存在，如加密機制、網路協定、資料和身份管理、用戶的隱私、自我管理和值得信任的架構。

Thank you for listening.

# References


- 1. B. Daskala, ed., Flying 2.0—Enabling Automated Air Travel by Identifying and Addressing the Challenges of IoT & RFID Technology, European Network and Information Security Agency, 2010; www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel.
- 2. O. Garcia-Morchon et al., “Security Considerations in the IP-Based Internet of Things,” IETF, Mar. 2011; http://tools.ietf.org/html/draft-garcia-core-security.
- 3. R. Roman, J. Lopez, and P. Najera, “A Cross-layer Approach for Integrating Security Mechanisms in Sensor Networks Architectures,” Wireless Comm. and Mobile Computing, vol. 11, no. 2, 2011, pp. 267-276.
- 4. S. Raza, T. Voigt, and U. Roedig, “6LoWPAN Extension for IPsec,” Proc. Workshop Interconnecting Smart Objects with the Internet, Internet Architecture Board, Mar. 2011; www.iab.org/about/workshops/smartobjects.
- 5. R. Roman et al., “Key Management Systems for Sensor Networks in the Context of the Internet of Things,” Computers & Electrical Eng., Mar. 2011, pp. 147-159.
- 6. H. Akram and M. Hoffmann, “Support for Identity Management in Ambient Environments—The Hydra Approach,” Proc. IEEE Int’l Conf. Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services
- (I-CENTRIC 08), IEEE CS Press, 2008, pp. 371-377.
- 7. A. Sarma and J. Girão, “Identities in the Future Internet of Things,” Wireless Personal Comm., Mar. 2009, pp. 353-363.

# References(Cont)


- 8. E. Rekleitis, P. Rizomiliotis, and S. Gritzalis, “A Holistic Approach to RFID Security and Privacy,” Proc. 1st Int’l Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010; www.nics.uma.es/seciot10/files/pdf/rekleitis_seciot10_paper.pdf.
- 9. J. Sen, “Privacy Preservation Technologies in Internet of Things,” Proc. Int’l Conf. Emerging Trends in Mathematics, Technology, and Management, 2011; http://arxiv.org/ftp/arxiv/papers/1012/1012.2177.pdf.
- 10. G. Broenink et al., “The Privacy Coach: Supporting Customer Privacy in the Internet of Things,” Proc. Workshop What Can the Internet of Things Do for the Citizen?(CIOT 2010); Radboud Univ., May 2010; http://dare.ubn.ru.nl/bitstream/2066/83839/1/83839.pdf.
- 11. S. Radomirovic, “Towards a Model for Security and Privacy in the Internet of Things,” Proc. 1st Int’l Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010; ww.nics.uma.es/seciot10/files/pdf/radomirovic_seciot10_paper.pdf.
- 12. http://baike.baidu.com/view/1915042.htm
- 13. http://6lowpan.tzi.org/
- 14. http://datatracker.ietf.org/wg/6lowpan/charter/
- 15. http://baike.baidu.com/view/223508.htm
- 16. http://www.autooo.net/utf8-classid123-id55412.html
- 17. http://www.chttl.com.tw/web/ch/service/data/10102c.pdf
- 18. http://www.c114.net/m2m/2493/a564691-2.html
- 19. http://wbb.forum.impressrd.jp/feature/20100730/806