Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Views & Comments

设计不安全：当今物联网设备的安全问题

Maire O'Neill

Research Director, Secure Digital Systems at the Center for Secure Information Technologies (CSIT), Queen's University Belfast

在当今科技时代，有人用一个灯泡就可以非法访问你的网上银行账户，而这一切都归因于物联网(IoT)。随着越来越多的设备被连接到互联网，IoT俨然已经成为现实。事实上，自动取款机(ATM)已经投入使用很多年了，最近我们又安装了一种可以远程连接到电网上的智能电表。现在我们又有了智能手表和智能婴儿监视器，还有更多诸如此类的新的IoT设备的例子。

加特纳公司(Gartner)表示，IoT对我们日常活动产生的影响将进一步扩大，预计到2020年，将会有250亿台设备连接到网络[1]。然而，思科公司(Cisco)认为，到2020年，将会有500亿台设备连接到网络[2]。加特纳公司还预测，随着车对车(car-to-car)通信技术和无人驾驶汽车技术开始变得司空见惯，汽车行业将会在连接设备方面展示出最快的增长速度。智能设备和传感器将会出现在我们的家里、汽车里、工作场所中、远程健康感应器中和无人驾驶汽车中。IoT具有真正地彻底改革当今我们与世界互动方式的潜力。

1. 挑战

连接设备的预期量迫切需要实现机器对机器(machine-to-machine)的通信，这意味着我们将不再直接控制设备交流的对象。此外，设备数量的不断增长促使犯罪分子和黑客开发新的攻击方法和新的攻击界面，这将造成严重的安全和隐私问题。对IoT设备的实际攻击已被证实是一个真正的威胁。我们再以灯泡为例，2014年安全专家已经展示过他们如何入侵一个与互联网相连接的领先品牌的灯泡，并且获取了与电灯路线相连的家庭用户的WiFi用户名和密码[3]。调查显示，智能电表、家庭自动化设备也可能遭受攻击。2015年，在一场通过汽车互联娱乐系统远程切断发动机并控制汽车转向和刹车的现场展示出现后，克莱斯勒汽车公司(Chrysler)对其所有客户的汽车进行了安全升级[4]。很显然，这些网络连接设备会遭受严重威胁的事实及可能会导致的严重的现实后果是IoT设备安全保障面临的众多挑战之一。

问题的复杂之处在于IoT无处不在。嵌入式设备本身往往是低成本、低功耗的设备，它们被限制在内存卡和计算机中，这样不法分子就能够实际接触设备。因此，包括边信道攻击(SCA)在内的物理攻击是可能的，它可通过使用电力、电磁辐射、时序分析或声学的方式从电子设备中提取密钥。在通行证[5]、汽车防盗系统[6]和现场可编程门阵列(FPGA)装置的数字流[7]中已经出现了这类攻击。

量子计算机也可能会对当今的安全产生重大影响。公共密钥加密是当今安全应用方面的一个基本元素，它被用于保障电子邮件和网上交易的安全。然而，由于它是计算密集型的，要真正实施会很昂贵。同样也有人认为，由于量子计算的计算能力很强，它的安全性将不复存在。例如，RSA公钥加密算法基于整数因子分解问题，量子计算机与传统计算机相比，前者能极迅速地进行多位数的因式分解。量子安全或后量子密码是指传统的非量子密码算法，它们不仅在当今是安全的，而且在实用

英文原文: Engineering 2016, 2(1): 48–49
引用本文: Maire O'Neill. Insecurity by Design: Today's IoT Device Security Problem. *Engineering*, http://dx.doi.org/10.1016/J.ENG.2016.01.014

量子计算成为现实后依旧具有安全性。它们基于目前公共密钥技术的不同的隐蔽难题。2015年8月，鉴于量子计算机的潜在威胁，美国国家安全局宣布把由美国国家标准与技术研究所(NIST)指定的Suite B加密算法过渡为量子抵抗算法[8]。

2. 我们如何应对这些挑战?

我们如何应对这些挑战？目前研究人员正在开发许多新的安全技术和解决方案，用以帮助解决IoT设备的安全问题。包括笔者前面已经提到过的量子安全算法；然而，在许多情况下这些算法是不实际的，并且其中许多算法甚至比当前的公共密钥技术更为复杂。此外，它们的密钥长度往往要大得多，这使得它们对低成本设备来说不切实际。目前，实用且最优的量子安全解决方案的发展是一个非常开放的研究课题。

现在有一系列关于解决措施的倡议，包括由美国NIST、欧洲标准化机构和欧洲电信标准化协会(ETSI)所主持的专题研究, 还包括由欧洲H2020项目资助的“ 未来新兴密码安全架构(SAFEcrypto) ” 项目[9]。后者的工作已经开展，结果显示轻量化的量子安全解决方案是可行的[9]。

提供设备认证的另一种方法是利用物理不可克隆功能(PUF)。PUF利用硅芯片制造工艺的变化来产生一个独特的数字指纹。由于每个芯片都不同，在接受同样的挑战时，没有任何两个芯片可以做出相同的反应，从而允许使用PUF技术进行设备识别和认证。同时，它们具有防篡改的优势，可以被用于检测克隆设备。本质上它们是轻量级的，根据最近提出的PUF方案(图1)，其质量只占一个低成本FPGA设备的不到1 % [10]。因此，它们可以作为有效的信任锚，使轻便的设备认证装置嵌入到IoT系统中。

3. 结论

总之，各家公司在竞相向市场推出IoT设备时，许多公司都经常忽略安全问题，或时常事后才想起安全问题。事实表明, IoT设备已遭受众多攻击，这些攻击可能产生严重的后果。因此，这些公司有必要花时间考虑设备的安全性，包括在产品最初设计时提供适当的安全方案，如PUF和量子安全技术。

最后，IoT设备的安全性仅是IoT生态系统的一个层面(图2)。第二层面是设备间的通信，因为其安全性也非常关键；最后，必须要安全地存储和分析从如此庞大的设备群体中得到的数据。因此，需要对IoT生态系统的所有层面的安全和隐私做出改变，从而确保其未来的可用性和可接受性，从根源上保障IoT设备的安全。

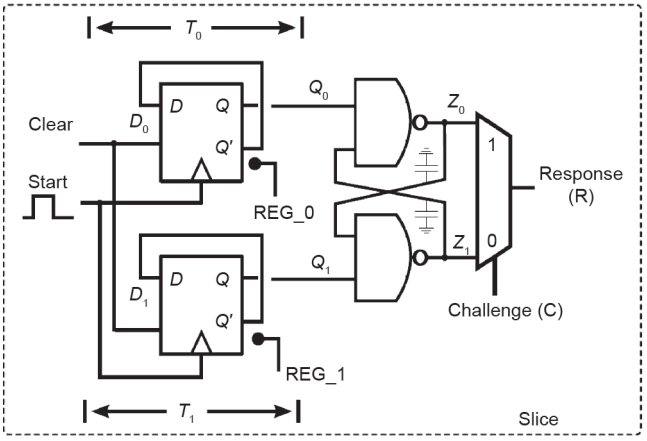

图1. 一位PUF识别信号发生器元件设计。

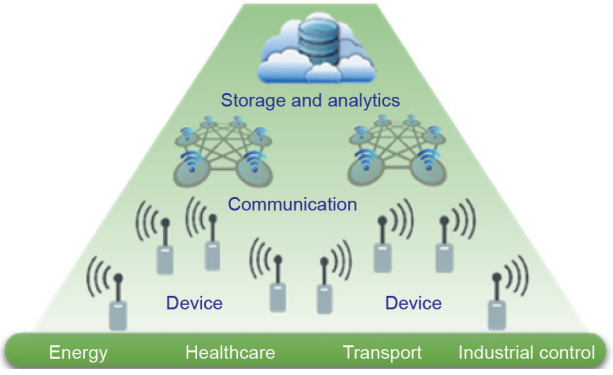

图2. IoT生态系统。

References

[1] Rivera J, Van der Meulen R. Gartner says 4.9 billion connected “things” will be in use in 2015 [Internet]. 2014 Nov 11 [cited 2016 Feb 20]. Available from: http://www.gartner.com/newsroom/id/2905717.
[2] Cisco. Internet of things (IoT) [Internet]. [cited 2015 Jul 23]. Available from: http://www.cisco.com/web/solutions/trends/iot/portfolio.html.
[3] Chapman A. Hacking into internet connected light bulbs [Internet]. 2014 Jul 4[cited 2015 Sep 15]. Available from: http://contextis.com/resources/blog/hacking-internet-connected-light-bulbs.
[4] Greenberg A. Hackers remotely kill a jeep on the highway—with me in it [Internet]. Wired 2015 Jul 21 [cited 2015 Sep 15]. Available from: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[5] Oswald D, Paar C. Breaking Mifare DESFire MF3ICD40: power analysis and templates in the real world. In: Preneel B, Takagi T, editors Cryptographic Hardware and Embedded Dystems—CHES 2011: 13th International Workshop; 2011 Sep 28-Oct 1; Nara, Japan. Berlin: Springer; 2011. p. 207–22.
[6] Eisenbarth T, Kasper T, Moradi A, Paar C, Salmasizadeh M, Shalmani MTM. On the power of power analysis in the real world: a complete break of the KeeLoq code hopping scheme. In: Wagner D, editor Advances in Cryptology—CRYPTO 2008: 28th Annual International Cryptology Conference; 2008 Aug 17-21; Santa Barbara, CA, USA. Berlin: Springer; 2008. p. 203–20.
[7] Moradi A, Kasper M, Paar C. Black-box side-channel attacks highlight the im-

portance of countermeasures—an analysis of the Xilinx Virtex-4 and Virtex-5 bitstream encryption mechanism. In: Dunkelman O, editor Topics in Cryptology—CT-RSA 2012: The Cryptographers' Track at the RSA Conference 2012; 2012 Feb 27-Mar 2; San Francisco, CA, USA. Berlin: Springer; 2012. p. 1–18.

[8] National Security Agency. Suite B Cryptography today [Internet]. 2015 Aug 19 [cited 2015 Sep 15]. Available from: https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml.

[9] SAFEcrypto. About SAFEcrypto [Internet]. [cited 2015 Sep 15]. Available from: www.safecrypto.eu.

[10] Gu C, O'Neill M. Ultra-compact and robust FPGA-based PUF identification generator. In: Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS'15); 2015 May 24–27; Lisbon, Portugal; 2015. p. 934–7.