Engineering 2 (2016) 48–49

Contents lists available at ScienceDirect

Engineering

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

Views & Comments

Insecurity by Design: Today's IoT Device Security Problem

Maire O'Neill

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

In today's technological age someone could gain access to your online bank account through a light bulb. This is due to the Internet of Things (IoT). The IoT has become a reality as more and more of our devices are being connected to the Internet. In fact, automated teller machines (ATMs) have been online for many years, and more recently we have had the installation of smart meters remotely connecting to the electricity grid. We now have smart watches and smart baby monitors, and there are many more examples of new IoT devices.

The influence of IoT in our day to day activities is set to further increase with a projected 25 billion connected devices by 2020, according to Gartner [1], while Cisco believes that by 2020, 50 billion devices will be network-connected [2]. Gartner also predicts that the automotive industry will show the highest growth rate in connected things as car-to-car communication and self-driving car technology begin to become commonplace. Smart devices and sensors will be found in our homes, our cars, our workplaces, in remote health sensing, and in self-driving cars. IoT has the potential to truly revolutionize how we interact with the world today.

1. Challenges

The expected volume of connected devices necessitates the use of machine-to-machine communication meaning that we will no longer have direct control over with whom or what our devices are communicating. In addition, the growing presence of devices enables new attack methods and new attack surfaces for criminals and hackers to exploit, posing serious security and privacy issues. Practical attacks of IoT devices have already been shown to be a real threat. Returning to the light-bulb example, in 2014, security experts demonstrated how they could hack a leading brand of network-connected light bulb and obtain the Wi-Fi username and password of the household to which the lights were connected [3]. Attacks have also been shown against smart meters, home automation devices, and in 2015 Chrysler had to send out a security update to all its customers after a live demo showed how to remotely cut the engine and take control of the steering and brakes of their cars via its network-connected entertainment system [4]. It is very evident that the fact these devices are network-connected poses serious threats, which could have significant real-world consequences. This is one of the many challenges in providing IoT device security.

Compounding this problem is the fact that to enable the ubiquitous nature of the IoT, the embedded devices themselves are often low-cost, low power devices that are restricted in both memory and computing power, and adversaries will have physical access to the devices. As such, physical attacks are possible including side-channel attacks (SCAs), which can be used to extract the secret key from electronic devices using power, electromagnetic (EM) emanations, timing analysis or acoustics. Such attacks have been shown against transit cards [5], car immobilisers [6], and Field Programmable Gate Array (FPGA) device bitstreams [7].

Quantum computers may also have a significant impact on today's security. Public-key cryptography, which is an essential element in security applications today, is used to secure everything from email to online transactions. However, it is computationally intensive and expensive to implement. It is also believed that it will no longer be secure due to the computational capabilities of quantum computing. For example, the RSA algorithm is based on the integer factorization problem and quantum computers are expected to be able to factorize large numbers at an exponential speedup over today's classical computers. Quantum-safe or post-quantum cryptography refers to conventional non-quantum cryptographic algorithms that are secure today but will remain secure even after practical quantum computing is a reality. They are based on different underlying hard problems to current public-key techniques. In August 2015, the National Security Agency announced that the Suite B cryptographic algorithms as specified by the National Institute of Standards and Technology (NIST) will be transitioning to quantum-resistant algorithms in light of the potential threat of quantum computers [8].

2. How can we address these challenges?

So how can we address these challenges? There are many new security technologies and solutions currently being developed that can help to address IoT device security problems. These include quantum-safe algorithms which I have already mentioned; however, in many cases they are not practical and many are even more complex than current public-key techniques. Also, their key sizes tend to be much larger, making them impractical for low-cost devices. The development of practical and optimal quantum-safe solutions is very much an open research problem at the moment.

http://dx.doi.org/10.1016/J.ENG.2016.01.014

There are a number of initiatives currently addressing this, including workshops being hosted by NIST in the US, and by the European standardisation body, European Telecommunications Standards Institute (ETSI). There are also European H2020 funded projects including the SAFEcrypto project [9]. Work has already been carried out in this project to show that it is possible to achieve light weight quantum-safe solutions [9].

An alternative approach for providing device authentication, in particular, is the utilization of a physical unclonable function (PUF). PUFs use the manufacturing process variations of silicon chips to generate a unique digital fingerprint. Since every chip is different, no two chips give the same response when supplied with the same challenge. This allows the use of PUF technology for both device identification and authentication. They also have the advantage of being tamper resistant and as such can be utilized to detect cloned devices. They are inherently lightweight, with a recently proposed PUF solution (Fig. 1) occupying less than 1% on a low-cost FPGA device [10]. As such, they can be used as an effective trust anchor to enable lightweight device authentication in embedded IoT systems.

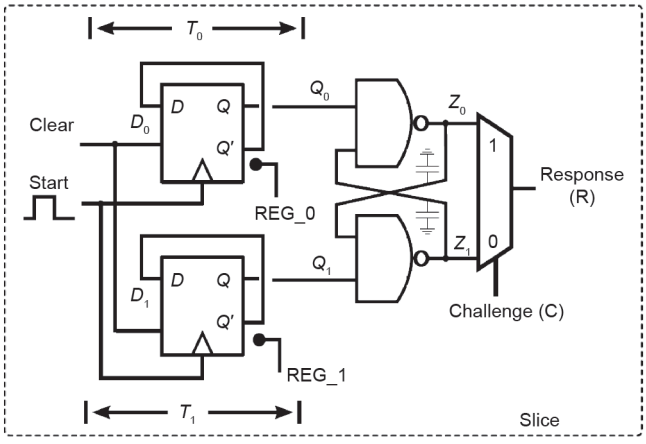

Fig. 1. One-bit physical unclonable function (PUF) identification generator cell design.

3. Conclusions

In conclusion, as companies race to get IoT devices to market, many are forgetting about security or all too often, security is an afterthought. Numerous attacks of IoT devices have already been demonstrated, and these attacks could have significant consequences. Therefore, it is vital that companies take the time to consider the security of their devices and include appropriate security solutions, such as PUF and quantum-safe techniques, from the outset of their design.

Finally, the security of IoT devices can be regarded as just one layer of the IoT ecosystem (Fig. 2). A second layer is the communications between the devices, the security of which is also vital; and thirdly, the amount of data being generated from such a volume of devices must also be stored and analyzed securely. Therefore, a step change in the security and privacy of all layers of the IoT ecosystem is needed to ensure its usability and acceptance in the future, with secure IoT devices at the root.

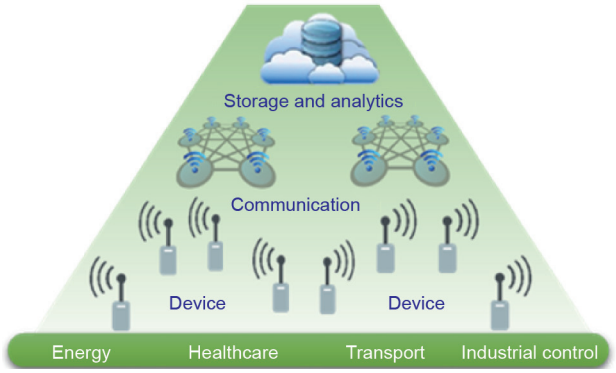

Fig. 2. IoT ecosystem.

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 importance 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.