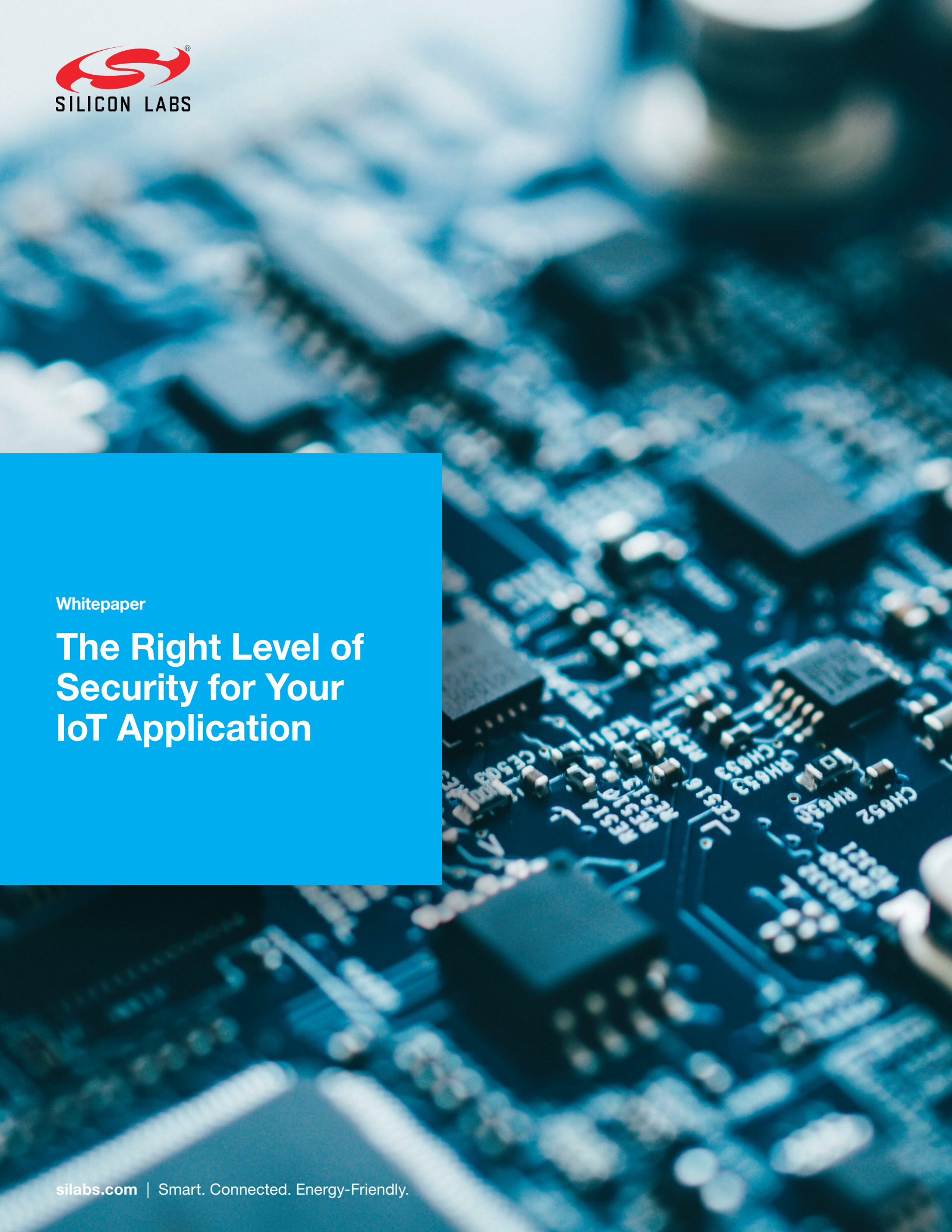


SILICON LABS

Whitepaper

The Right Level of Security for Your IoT Application

The Right Level of Security for Your IoT Application

Many of the things we use on a daily basis are becoming smart and connected. The Internet of Things, or IoT, is designed to help improve our lives by driving and tracking our personal goals that could include fitness, waste reduction, or productivity. The IoT has also facilitated new subscription business models for corporations such as those that provide streaming television, or music dialed in to our personal tastes, or those that provide replacement consumables such as water and air filters. Many embedded developers realize the potential benefits of the IoT and are actively developing various applications to simplify our lives and grow corporate revenues.

However, along with these benefits come risks. No one wants to design an application that's vulnerable to hacking or data theft – the loss of customer and/or company data often results in huge financial consequences. Undesirable events like high-profile hacks can lead to serious brand damage and loss of customer trust, and worst-case events can slow down or permanently reduce the adoption of IoT.

The Internet of Things (IoT) allows us to optimize and improve most aspects of modern life on an unprecedented scale as billions of IoT devices unleash billions of dollars in economic value [1].

In the race for time-to-market, proper security is inconvenient because it adds costs related to development, components, and complexity. At the same time, in many industries, it is not crucial to have adequate security. The issue is that bad press and major security and privacy issues might temporarily or permanently slow down the adoption of IoT for improving our lives. Many are already skeptical about connecting the simple devices we rely on in our everyday lives, and security researchers are calling the IoT a catastrophe waiting to happen [2].

In fact, quite recently, there have been a number of highly publicized hacks that have gained wide attention [3,4], so one could argue that the catastrophe is already underway.

The Hacking of Quantum Cryptopgraphy

The situation resembles that of Quantum Cryptography. Quantum Cryptography [5] (often referred to as Quantum Key Distribution) is a beautiful technology that unlike other key distribution schemes promises unconditional security based on the laws of physics. In comparison, most key distribution schemes rely on assumptions of the computational complexity of factoring large numbers or the discrete logarithm problem.

Discovered in 1984, it took until about the year 2000 before commercial cryptography systems were launched. Relying on single photons, building a quantum cryptographic system is complicated, and, again, time-to-market was of the essence. In 2010, the first security loophole that completely broke the security of the systems was published [6]. Quantum Cryptography is theoretically unbreakable, but, in reality, there were side-channels not considered during the design of these systems. Also, interestingly, no loopholes were discovered until a dedicated team was established to break into them. Until this team was established, the entire industry was focused on making quantum cryptography systems robust and getting them to market.

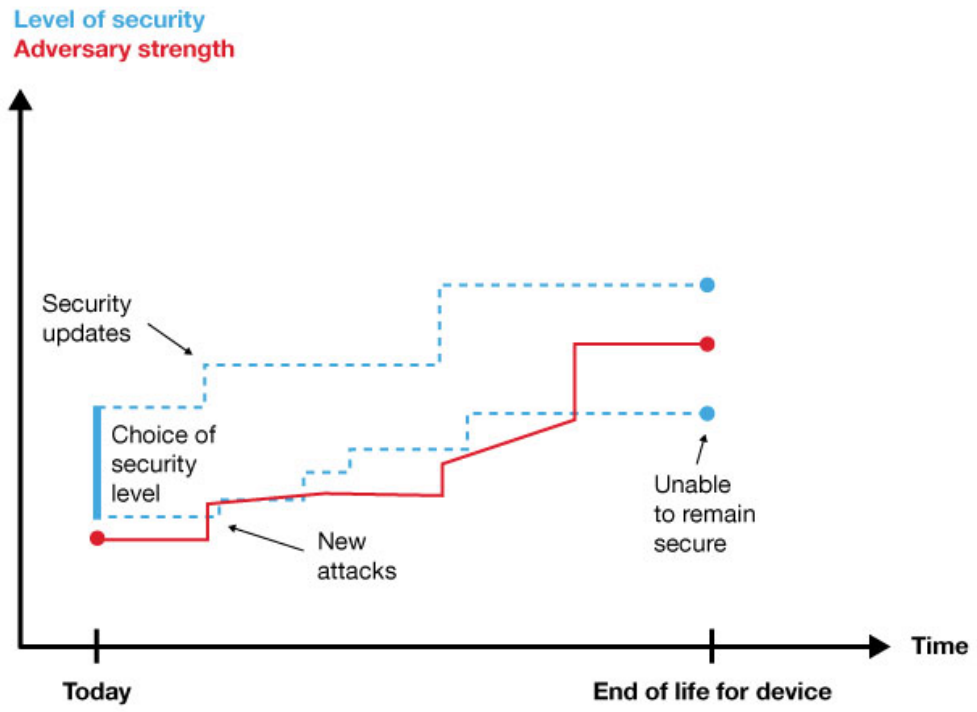
Several things can be learned from the Quantum Cryptography analogy. Notably, it was widely believed that Quantum Cryptography systems were unconditionally secure until a novel attack strategy rendered that premise untrue. In other words, the systems were secure against any attacker that was not aware of, or was not going to utilize, the blinding attack. This shows how there are always assumptions about a potential adversary – who you are secure against, even in cases where one tries to reduce the number of assumptions to a bare minimum.

One other interesting lesson from the hacking of quantum cryptography is that it showed the importance of upgradable security. When the blinding attacks were discovered, the manufacturers of these systems were given a grace period to patch the vulnerabilities. It turned out that it was possible to close the vulnerabilities via software updates. This article will not discuss the distribution of the software updates (this would require a quantum secure bootloader!), but the important point is that the security needed to be upgraded over the lifetimes of the systems.

Threat Modelling: What Attacker are You Protecting Against?

Security is not binary: secure, or insecure. The question one should ask is “secure against what and do you even know?” The reality is that there are different levels of security, and a device can only be considered secure in the context of a particular attacker where the level of security is higher than the capabilities of the attacker.

Class	Hobbyist/Script-Kiddie	Advanced Hackers	Security Researchers	Nation-State Attacks
Motivation	Fun, curiosity, fame, challenge	Fame, financial	Curiosity, improve security, novel ideas and attacks, financial	Espionage, sabotage
Resources	Limited, commodity hacking equipment	Semi-specialized equipment, experts in a single domain	Ultra-specialized equipment, experts in multiple domains	Unlimited



The graph above shows how security upgrades are necessary to evolve with the security level of the attacker. A high level of security and hardware primitives (such as extra memory) maximizes the likelihood that security issues can be patched in the future for both the security of the cloud vendor or the consumer. Image owned by Silicon Labs.

Typically, the relevant class(es) of attacker(s) will be determined by which assets and threats are relevant for a given application. It should, however, be mentioned that the cost of securing against more sophisticated attackers grows tremendously and should not be underestimated. It is also worth mentioning that against more sophisticated attackers, it is necessary to consider more domains than the product itself: typical business processes, physical security, and people.

The capabilities of the attacker are typically non-static, and, therefore, the security level will change over time. The improved capabilities of the attacker can evolve in several different ways, from the discovery and/or publication of issues and vulnerabilities to broader availability of equipment and tools. We have already discussed how this happened in the example of Quantum Cryptography, but let's also review a few examples of how this has happened in classical security.

In 1977, the data encryption standard (DES) algorithm was established as a standard symmetric cipher. DES used a 56-bit key size; so, due to increases in available computational power, the standard became vulnerable to brute-force attacks within 20 years. In 1997, it was shown that it took 56 hours to break the algorithm via brute-force. With DES clearly being broken, triple DES, basically running DES three times with different keys, was established as a standard secure symmetric cipher. Regarding the security level of DES, there has been speculation that if governments could already break the cipher in 1977, DES could never resist nation-state attacks. However, since the early 2000s, DES could not even protect against hobbyists with personal computers due to the widespread availability of suitable computational power.

Since 2001, the advanced encryption standard (AES) has replaced DES. But even AES does not guarantee security. Even when the algorithm could not be easily broken, the implementation could be hacked, just like what happened with Quantum Cryptography. Differential power analysis (DPA) attacks are made by measuring the power consumption or the electromagnetic radiation of the circuit performing the cryptography. The side-channel data is then

used to obtain the cryptographic keys. Specifically, DPA involves capturing a large number of power consumption traces followed by analysis to reveal the key. DPA was introduced in 1998, and, since then, companies like Cryptographic Research Inc. (now Rambus) sold tools for performing DPA attacks, although at prices that made them inaccessible to most hobbyists and researchers. Today, hardware tools for performing advanced DPA attacks can be purchased for less than $300, and advanced post-processing algorithms are available free-of-charge online. Thus, the ability to conduct DPA attacks has migrated from nation-states and wealthy adversaries to nearly any hacker.

Now, let's discuss these historic lessons in the context of IoT-device longevity. The typical lifetime of an IoT-device depends on the application, but, in industrial applications, 20 years is common and will be the timespan used for this discussion. A device that launched in 1998, for example, was once only vulnerable to nation-state attacks; today it must be able to withstand DPA attacks by hobbyists with $300 tools, some spare time and lots of coffee. Predicting the future capabilities of a class of adversaries is very difficult if not impossible, especially over a 20-year timespan. What will a potential adversary look like in 2040? One might speculate whether it will even be human.

Security Levels for Example Applications

Three example applications will be discussed here: smart-home door locks, smart-home environmental sensors, and life-supporting medical devices.

The primary function of the smart-home door lock is to control the perimeter of the home. It is typically connected, and the homeowner can often remotely unlock the door.

Let's first discuss the class of adversary. It does not make sense to consider nation-state adversaries in the context of a door lock. If nation states really want to enter a home, they will typically have other easier options than a door lock. Security researchers and advanced hackers are adversaries who should be considered for this application. Security researchers will gladly publish IoT security horror stories that make end-users uncomfortable with having a connected door lock[7]. This has an interesting consequence, where the security solution must withstand public and media scrutiny even if there are deliberate and reasonable tradeoffs. In other words, this calls for a higher security level than what is strictly necessary.

Advanced hackers could use door access to rob houses without leaving a trace. An interesting aspect of this scenario is that it can be very hard to realize that there has been a robbery in the first place, as has already occurred in some cases [8].

For the smart home environmental sensor, there are other interesting considerations. In the broadest sense, environmental data could be used to control actuators. If this is the case, manipulating seemingly non-sensitive sensor data can have a big impact. One example could be if the fire alarm trigger automatically opens a door lock. Therefore, best practice should be to minimize assumptions on the sensor data usage and assume that the data is as sensitive as anything it can be used for. At the core of IoT is scalability, both for value and against adversaries; so, it can be hard to imagine up-front how large-scale sensor attacks can be valuable.

In these smart-home devices, two particularly interesting challenges come up: commissioning and longevity. For commissioning, the install process has a direct impact on ease-of-use. Therefore, there have historically been many tradeoffs of security versus usability, some having been identified later. This would again call for higher security rather than longevity, as smart home-devices can be installed for decades. This raises the question of backwards compatibility. Consumers want assurances of future support, or, at least, they become upset if support is suddenly removed [9]. The best strategy for handling backwards compatibility is to upgrade to the latest security protocols in the field [10]. This is not always possible due to hardware constraints and because it calls for an increase in the hardware capabilities of deployed devices beyond what was identified as strictly necessary at the time of their release.

The last case of a medical device is particularly interesting. From a safety perspective, it involves strict testing and processes. But, from a security perspective, there have hardly been any requirements. Not only that, but historically, there have been a number of hacks of this class of devices [11].

For these devices, nation-state security may be the right adversary class. Hacking and controlling these devices can be used as a discrete and untraceable way of assassinating important individuals. What is certain is that the security of these devices will be subject to standards and certifications that will hopefully take these risks into account.

Regulatory and Standards Initiatives

The regulatory and standards initiatives around IoT Security are too extensive to cover here, but a few key elements and initiatives must be mentioned.

Regulatory and standards initiatives must address two key aspects: incentive and scalability.

For incentive, we have already discussed how vendors have conflicting interests and may be incentivized to lower the security of a device below what is a reasonable level for society because of increased development complexity and costs. Therefore, regulatory initiatives must find ways to incentivize without thwarting innovation. This is where General Data Protection Regulation (GDPR) has an interesting approach. The fining of companies that lose valuable data serves as an incentive without limiting how the companies secure their data and can serve as an inspiration for IoT security regulation.

For the foreseeable future, there are not enough security engineers in the world to secure IoT device demand and therefore, any scheme must be re-usable to aid in its adoption and address scalablility. ARM [12], one of the leading vendors of intellectual property used by the embedded microcontroller industry, introduced its Platform Security Architecture (PSA) to address this requirement.

The PSA solves the problem of scalability through a balanced certification scheme and off-the-shelf secure components. This should make it possible for someone without an extensive security background to evaluate different vendors based on the certification and implement secure solutions using the components. The biggest challenge for PSA is that it is tied to an IP-vendor, and, as such, it is likely not acceptable for broad standardization, even if it implements a good strategy for scalability.

Different devices require different levels of security. In this paper, we have discussed how considerations of adversaries and longevity can impact the appropriate security level in an application. Furthermore, we have discussed how certification and standardization can help in the longer term.

References

[1] McKinsey & Company, The Internet of Things: Mapping the value beyond the Hype, June 2015.

[2] B. Schneier, http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/, visited 16/01-2019.

[3] B. Krebs, Hacked Cameras, DVRs Powered To-days Massive Internet Outage, https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/ October 2016, visited 16/01-2019.

[4] E. Ronen, C. O'Flynn, A. Shamir and A. Weingarten, IoT Goes Nuclear: Creating a ZigBee Chain Reaction, https://eprint.iacr.org/2016/1047.pdf, visited 16/01-2019.

[5] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145-195 (2002)

[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination", Nat. Photonics 4, 686-689 (2010)

[7] Updated: Your Z-Wave Smart Locks are Safe and Secure, https://www.silabs.com/community/blog.entry.html/2018/05/23/tl_dr_your_door_is-g1zC, visited 16/01-2019.

[8] The hotel room hacker, https://www.wired.com/2017/08/the-hotel-hacker/, visited 16/01-2019.

[9] Nest is permanently disabling the Revolv smart home hub, https://www.theverge.com/2016/4/4/11362928/google-nest-revolv-shutdown-smart-home-products, visited 16/01-2019.

[10] The IoT requires upgradable security, http://www.newelectronics.co.uk/electronics-technology/the-iot-requires-upgradable-security/156211/, visited 16/01-2019.

[11] Go ahead, hackers. Break my heart, https://www.wired.com/2016/03/go-ahead-hackers-break-heart/, visited 16/01-2019.

[12] PSA: Next steps toward a common industry framework for secure IoT, https://www.arm.com/company/news/2018/02/psa-next-steps-toward-a-common-industry-framework-for-secure-iot, visited 16/01-2019