Summary of an Open Discussion on IoT and Lightweight Cryptography[*]

Chair: Adi Shamir
Summary: Alex Biryukov, Léo Perrin

Abstract

This is a summary of the open discussion on IoT security and regulation which took place at the Early Symmetric Crypto (ESC) seminar. Participants have identified that IoT poses critical threat to security and privacy. It was agreed that government regulation and dialogue of security researchers with engineers and manufacturers is necessary in order to find proper control mechanisms.

1 Introduction

On the last day of Early Symmetric Crypto (ESC) seminar (January, 2017) an open discussion about Internet of Things (IoT) and lightweight cryptography took place. It involved all the workshop participants, about 40 researchers from academia and industry, from senior researchers to postdocs and Ph.D. students. These notes are a summary of the main points that were raised during this discussion.[1]

The discussion started with a short introduction by Prof. Adi Shamir. He observed that the spread of the IoT is unstoppable, that such devices are already being sold and used. For example, "smart" lightbulbs such as the Philips Hue use the Zigbee protocol to communicate with their owners' smartphones. Other home appliances are already being connected to the internet: fridges, TVs, washing machines... And applications to other areas are expected, from the supply chain to public transport.

This trend cannot be stopped and will only accelerate in the foreseeable future. Meanwhile, there have been major attacks against network-enabled "things". For example, *shodan* is a search engine indexing various devices connected to Internet (web cams, control systems, servers, etc.), which can then be used to find vulnerable ones. There have also been ransomware attacks targeting the owners of "smart" TVs. Such threats are likely to occur more frequently in the future. In the light of these observations, this discussion tried to address the following question:

What should be done about the IoT security?

[*] Published in the proceedings of ESC'17 – Early Symmetric Crypto workshop, 2017.

[1] The points raised by the participants are not sorted chronologically but by theme.

Adi Shamir has asked the participants to vote on whether they thought involving governments was necessary. A majority has agreed. What form should this intervention take? The following ideas were suggested by the participants. They can be sorted into four broad categories: the first deals with devices' update mechanisms, the second with liability issues, the third with the influence of specific properties of the devices (i.e. with a partition of the IoT space), and the last considers separating real world from cyber functionalities.

2 Update Mechanisms

Current status-quo in the industry seems to be that firmware needs to be updatable so that vulnerabilities found after the launch of a product can be patched. However, firmware updates also open the doors to attacks exploiting the update mechanism itself. This very dangerous attack vector would be disabled in the absence of updates. If functionality of a device is well-defined, and if the firmware has been thoroughly tested, it may well be acceptable to make firmware not updatable. To give a real-world example: the firmware of smart cards in the payment industry was for a long period not updatable. In cases where update mechanism is inevitable there also should be a way to force manufacturers to update their firmware in the cases of disasters. There may also be issues related to companies disappearing from the market, while their potentially vulnerable products are still in wide use – how should these be updated? In fact, Germany considers forcing the storage of the source code in some trusted institution so that if the company disappears, it is possible to fix the problem anyway.

On the technical side, should we force the use of public key crypto to secure firmware update? After all, the attack against the Philipps HUE smart lightbulb was made possible by a misplaced use of symmetric cryptography. Using public key crypto would simplify key management: instead of using a hard to protect symmetric key, a public key would be used instead. While public key cryptography is far more demanding in terms of resources, updates are not expected to be common enough for this to be a significant issue.

When it comes to implementing sophisticated update mechanisms, another problem is that less secure devices will probably be cheaper than secure ones.

3 Liability

In case of a problem with an IoT device, who is responsible for fixing it? There are different ways to approach this question.

It could be possible to fine customers if they use/keep using insecure devices. There is no precedent we are aware of for such measures[2]. For example, no such thing exists for PC owners. It would also be hard to enforce .

Some form of insurance against malfunctions could be made mandatory. In this case, the cost of refunding customers could be solved by factoring this cost into the product prices.

If a product is insecure because of a gross negligence from its manufacturer, said manufacturer should be liable. However, this would imply differentiating

[2] Note that in some countries (ex. Italy) it is illegal to use police radio scanners, as another example Doppler receivers (to detect speed cameras) tend to be outlawed in Europe

gross negligence from "honest" mistakes. For example, having a default password in a multitude of devices could be considered gross negligence.

Some devices can obviously be regulated (e.g. medical devices, see American FDA) but they only represent a tiny fraction of all devices. What about self-driven cars? There is currently a substantial debate about liability in this case. After an accident, who is liable? The driver? The car manufacturer? The programmer? It seems like those involved are converging towards having the car manufacturer to be liable.

Connection of millions of identical devices to public resources like Internet should probably be tightly regulated in a way similar to radio spectrum regulation, since the consequences of abuse of such devices by attackers are comparable to jamming the public resource.

For short life-cycle disposable items it could be that part of the price paid by the consumer for the device is retained in a common disaster recovery fund and released to the manufacturer only at the end of the lifetime of the device, if no disaster has happened. In the case of a security disaster, cost of recovery is reduced from the fund. This model is reminiscent of how copyright is factored into the cost of media via government levy (tax). This model might not be feasible without government regulation.

Finally, computer security could be considered like a common property. The legislative framework handling e.g. pollution could be adapted, so that a company releasing an insecure device is responsible for handling the consequences. Similarly, a user connecting a device known to be insecure to a network would be liable for the problems caused.

4 Influence of Devices' Specifics

It may be beneficial – or even necessary – to consider different classes of devices. Instead of fitting all IoT devices into a single legislative framework, it may be better to treat them differently depending on their specifics.

For example, we could sort devices according to the danger posed by a security breach. Getting access to a pacemaker is far more dangerous than accessing a smart curtain. On the other hand, estimating how dangerous a breach is can be difficult. Hacking into a smart light-bulb may seem harmless but it can allow the remote infection of other similar products and then using those to effectively jam wifi signal across a large area. We could separate devices according to the networking abilities: if it is not connected to the Internet, it cannot do too much harm. Similarly, if it is connected but has a very low bandwidth, a security breach may not be very dangerous.

5 Clear Separation Between Cyber and Physical Worlds

Security measures could be implemented physically into some devices, like the floppy disks in the past which could be taped to make them read-only guaranteeing that no malware could infect them. For example, there could be a physical switch separating between smart/dumb functionality or, in general, between physical and cyber capabilities of the device. Similarly, in a smart-car, there should be a physical separation between the car entertainment system (which is connected to the Internet) and the main car functionality. Since we live in the physical world, there is no need for the cyber to be in complete control of our lives. However, this most likely needs to be enforced by regulation.

Devices could also be given a limited shelf life after which they must be discarded. This last option would unfortunately have an environmental cost. In fact, stimulative regulation might be sufficient. Devices could be simply labelled to specify e.g. whether they require a permanent Internet connection, whether they use it only for updates, whether they send data to a central server, etc.

6 Concluding Remarks

The approaches outlined above share common limitations. First of all, laws would need to be approved in a lot of independent countries in order for them to be efficient. We also need to keep the danger of surveillance in mind. For example, smart-meters for electricity pose a significant privacy threat which is not addressed by the points raised above. Besides, government involvement may backfire if the laws adopted are not carefully thought through.

How could cryptographers help? We could create/participate in forums and public discussions, communicating with engineers and manufacturers. We could write white papers with security recommendations and systematization of knowledge (SoK) papers.

Having forums gathering manufacturers, governments and academics to discuss these matters would be welcome. Those that currently exist are usually organised by manufacturers, whose incentive is to sell more products, while privacy and security are just added costs and overheads. While ISO/IEC is exploring IoT standardization, security and privacy are low on their priority list.

At the end of the debates, participants agreed that:

- the IoT is unstoppable,
- some regulation is needed,
- a major security risk (but not the only one) is the firmware update chain.

7 Acknowledgement

We thank Joan Daemen for his valuable comments on a first draft of this summary.