GHOST on top of the EU Cybersecurity Act

Internet of Things and in short IoT, these electronic devices that one way or another are exchanging bits and bytes on the Internet and are seemingly everywhere nowadays. They can be found at homes, at work places, in the city infrastructure, embedded in cars, power grids and on people themselves as wearables and other electronic 'gadgets', all of which aimed at performing specific tasks. These networked objects are equipped with sensors, actuators, processing and connectivity protocols, enable object interaction, often times without any human intervention, and steadily grow in numbers. In early 2017, Gartner forecasted 8.4 billion active IoT devices to be used in 2017 and up to 20.4 billion by 2020[1] .These numbers seem to conflict with the statistics summarised by Financeonline.com in a recent (January 2020) web report[2] ,where it reported for 2017 20.4 billion devices. It is unclear why these numbers differ to this extend (perhaps, different categorisation on what is an Internet of Things (IoT) device), but we leave this discrepancy for another day to be explored. The bottom line is that there are billions of these devices active to date and it is predicted to increase their number tremendously over the next few years.

This rises the concerns to what it means to live in a world surrounded by devices, which provide their (continuous) observations as a multi dimensional data language, speaking to known and unknown entities on the World Wide Web. The main concern stems from its inheritance, namely the prevalent privacy and security issues surrounding the more traditional Internet-enabled devices (personal computers). Due to IoT's deployment environment, capabilities (often limited) and their tasks, it often is exposed as an easy target and therefore even amplifies the issues at hand.

How do we protect the devices that are installed in our environment and guarantee that their operation is conform its description and will remain to do so over time? This problem however can already originate all the way back to the manufacturer of even the tiniest component used in a device. On 27th of June 2019, the European Union (EU) Cybersecurity Act entered into force, which allows the European Union Agency for Cybersecurity (ENISA) to apply more resources on the establishment and regulation of EU wide cybersecurity certification for products. In what manner this will take shape has yet to be seen, as through the H2020 program, Universities, companies and non-profit organisations are being called to cooperate on providing solutions to this complex problem, as well as to become an advisor to them in the Stakeholder Cybersecurity Certification Group (SCCG).

The certification of products, specifically for cybersecurity, is a step in the good direction, as for example it might be very similar as the Conformité Européene (CE) marking which we already have in the EU. But how can it guarantee a safe operation over time, other than legislative measures? It needs dedication, thus time and money, from the manufacturer and/or provider to provide security updates and patches, which may simply not be possible or feasible in the long run. It may however have beneficial side effects, as manufacturers are forced to take greater care of their products. For example, Android devices, which to date remains problematic concerning their support and upgrade ability to the latest system[3] . Many manufacturers seem to favour people which throw out their one year old phone to simply 'buy' a new one, which then comes installed with a more recent version of Android. So, not only the durability of the device but also the environment may benefit from applying cyber security/supportive legislative measures and certification that will chance the mindset of the manufacturers, but it may come at the cost of having less profit.

More on the problematic side, the whole process for certification may, aside from a lot of extra paperwork, raise the bar for the cost of entry to the market. Whereas a manufacturer may self certify a product for a CE marking, it raises the question if this would also be possible for cybersecurity? For the big companies the certification through a third party certainly would not be a problem, as often they already have ISAE, ISO or SOC certifications to provide their products world wide. How would it affect start-ups, and possibly any small to medium business, that plans to bring a product on the market with a cloud digital infrastructure? Furthermore, over time older devices become more susceptible for attacks as newer security measures cannot be provided, due to lack of support, processing power or other (hardware) dependencies. To illustrate this a bit further, in May 2019 Zscaler published a white paper stating that 91.5% of IoT communications used within corporate

[1] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[2] https://financesonline.com/iot-statistics/

[3] https://www.computerworld.com/article/3175067/android-upgrade-problem.html

networks are unencrypted[4] .

It is here that the idea of GHOST came to be, with utilising a personalised monitoring approach, learning the device 'normal' behaviour and taking automatic decisions and/or informing the owner of a device of any unusual activity. GHOST can monitor any device solely by its communication and be confined to a gateway or router in order to minimise exposure of the monitoring system itself. This is a strength as well as a weakness of the GHOST system, for its strength is being device agnostic, as it learns the device and can be personally configured by the user. Its weakness, however, as long as a device's communication pattern is not disturbed, GHOST will not detect any tampering with a device directly. This could still lead to unwanted data access of the device by direct access. In the paper by Abdulghani [5] this particular problem is addressed by proposing a framework of IoT classification and provide the linkage between guidelines, mitigation techniques and the attacks. The work was further expanded into a reference model for securing IoT[6] , that specifically takes into account legacy or generally low performance devices, where IoT devices are embedded with security structures according to their classification. A set of IoT devices form a connected awareness in which the more capable IoT devices will monitor the lesser IoT, and the lesser IoT are only allowed to communicate if the higher capable IoT approve it. To enable this vision, however, it needs to be implemented by the IoT manufacturers, and it only works best if all adhere to the same standard. This brings us back to the importance of the EU Cybersecurity Act ... "We will watch your career with great interest".

Abbreviations

CE Conformité Européene

ENISA European Union Agency for Cybersecurity

EU European Union

IoT Internet of Things

SCCG Stakeholder Cybersecurity Certification Group

Document History

#	Date	Description
0.1	30/01/2020	Original version for GHOST project
0.2	30/01/2021	Republish for I-Sec website

The Information Security Group

UNIVERSITÉ DE GENÈVE

Geneva School of Economics and Management
Information Science Institute

[4] https://www.zscaler.com/blogs/research/iot-traffic-enterprise-rising-so-are-threats
[5] https://isec.unige.ch/#publicationModal5
[6] https://archive-ouverte.unige.ch/unige:123701