CHARIOT – 3rd Workshop

Wednesday 22 October 2020 (online)

IoT Data Security and Privacy Solutions – Challenges and Opportunities for Airports

IoT System and NIS Directive

Possible Impact and Solutions

Francesco Capparelli
Senior Fellow Researcher
Istituto Italiano per la Privacy - NGIoT

Introduction

- The NISD is focused on establishing a common level of security for network and information systems.

- These systems are a vital component to address the risks of lack of business continuity or incident that can compromise the ordinary operativity that may be affect citizens in important sectors of a society.

- The NISD focuses on two types of service providers, the operators of essential services (OES) and the relevant digital service providers (DSP).

- The NISD it is connected to the European Union's initiatives to develop IoT platforms and IoT large scale pilots that are heavily involved in essential services of society, such as energy, transportation and health.

Security in ICT is ICT itself

IoT is just one layer

- The NISD establishes several requirements for OES, which focus around risk management and incident prevention and reporting – topics which, at first encounter, seem closely related to components of the GDPR.

- Articles 14 and 16 represent the core of the NISD. The legislator's approach in establishing these obligations is consistent with the principle of accountability and risk analysis which also pervades the regulatory framework of the General Data Protection Regulations.

- Privacy by design is Security by design

- Security in IoT = Trust in IoT

- While the GDPR is placed in a perspective of necessary contextualization regarding all organizations that process personal data, the NISD operates upstream of this categorization by distinguishing in the two macro-categories mentioned above, OES and DSP, and in sub-sets divided by their belonging to different sectors.

- Although differences can be appreciated in the listing of obligations for organisations belonging to the two macro-categories, the risk-based approach remains partially unchanged.

- OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of network and information systems which they use in their operations, pursuant to article 14 NISD. In the same article, it is emphasized, that the level of security must be appropriate to the risk posed, therefore, following a risk-based approach.

- It is expected that the identification and assessment of risk must necessarily be based on recognised international standards. The main and most appropriate standard for defining risk within the scope of NISD is ISO/IEC 27001 as it integrates within it the definitions of security event and incident i.e. some of the key words of the NIS Directive. It should also be noted that both the Information Commissioner's Office, which is the independent UK regulator for data protection and freedom of information, and ENISA, the European Network and Information Security Agency, make explicit reference to ISO/IEC 27001 as a valid standard for this purpose

- ENISA has focused on the role of the risk assessment, through the description of sophistication levels – basic, industry standard and state of the art - that can be used to select the relevant security measures of objectives

- It should be noted that ENISA has issued guidelines on minimum security measures to be implemented within organizations, mapping the most relevant international security standards, in "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers" which can be considered valid not only for DSPs but for organizations in general, and detailing and contextualizing from a sectoral point of view with regard to OES.

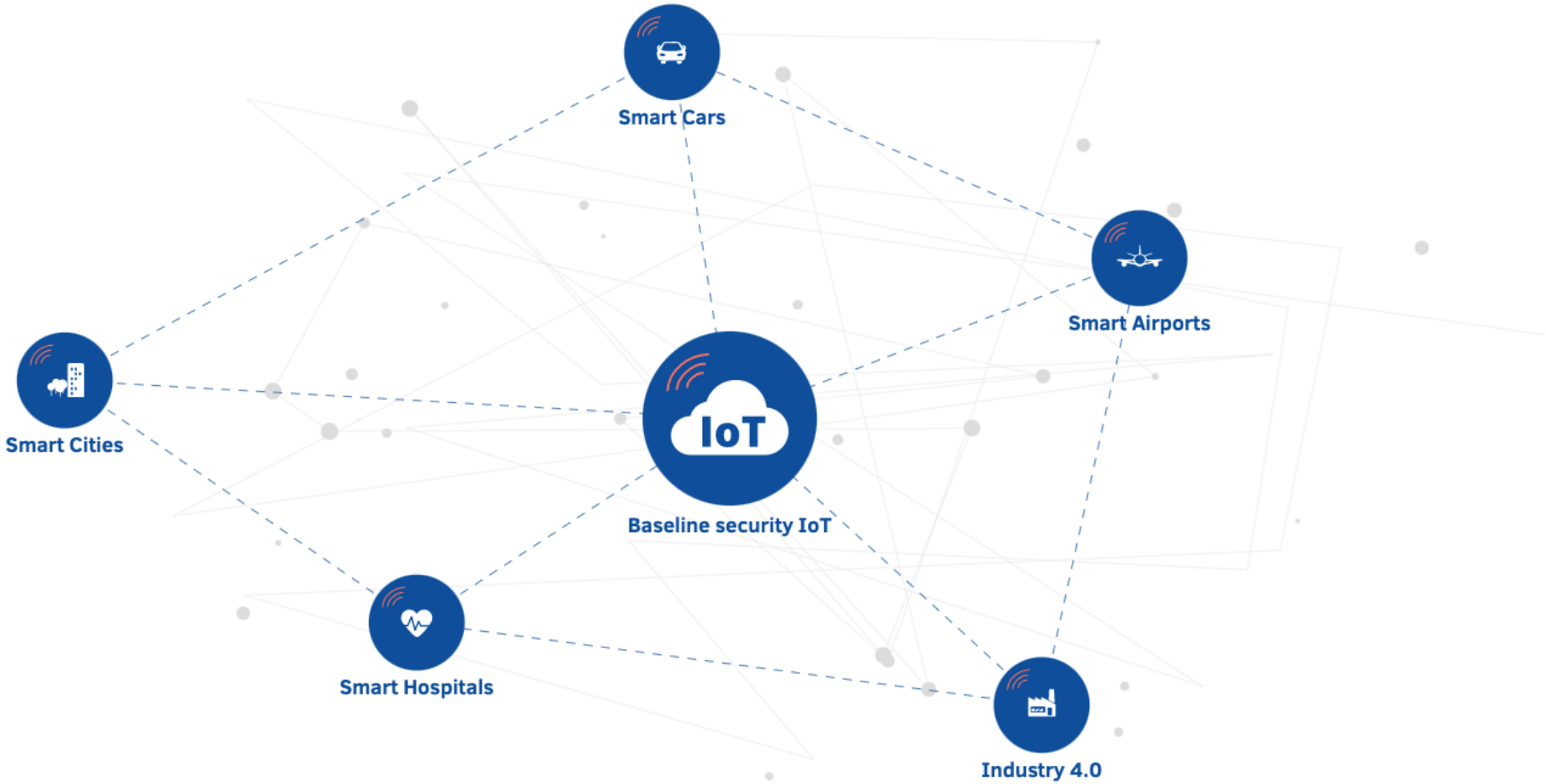
- In fact, ENISA has also produced Guidelines on assessing the compliance of OES with the NISD, whereby it has enlisted a set of questions which correspond to security measures and appropriate evidence that can be used to support the implementation of such security measures.

- and what about IoT?

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

More ≡ | English (en)

COVID19 | TOPICS | NEWS | PUBLICATIONS | EVENTS 4



- It is necessary to specify that the Guidelines issued by ENISA are an interpretative basis of what is meant by adequate security measures under Art. 14 and 16 NISD. It is therefore essential to distinguish the need to formalise procedures relating to processes within organisations, in order to comply with the requirements of the Guidelines, from the need to formalise procedures relating to processes as organisational mitigation measures deriving from risk analyses.

- The management of the risk related to information security, requires an adequate method of risk assessment and treatment that will be contextualized from the point of view of the sector to which the organization belongs and the economic framework in which the organization operates.

- The risk assessment aims to identify the risks in such a way that the results of the analysis constitute the guidelines on which to base the actions and priorities relating to the implementation of mitigation measures for the risks identified. This assessment should be carried out on a periodic basis, with predetermined cyclicality, in order to mitigate possible changes in the organization with respect to all the variables considered.

- ISO/IEC 27005 is a useful guide for risk management, setting out criteria to be followed to carry out risk assessment and risk treatment, to guide when to accept the risk and how to monitor it.

- Within the function of the IoT deployments, there are also concerns for the implementation of the NISD. First and foremost, is the fact that regular monitoring, auditing and testing can only occur when the IoT devices are of a limited amount. Therefore, auditing becomes impractical and unrealistic when smart infrastructure may consist of the deployment of hundreds or even thousands of devices within a certain region. A lack of monitoring is a challenge that has high stakes, since an attack of one device may mean an attack to the entire network or information system.

- Therefore, guidelines and procedures are necessary to assist controllers in carrying out regular monitoring and testing activities. This way, a continuous exercise of investigating security measures can be guaranteed, and the IoT device can ensure the ongoing protection personal data and IoT functionality.

- In such a scenario, the heterogeneous connections determine what in information security is technically defined as an "increase of the exposed surface", with an exponential extension of the hardware and software vulnerabilities, connected to potential risks of exploitation by cyber criminals.

- One of the most significant and unfortunately continuously expanding attacks of the IoT ecosystem is DDoS (Distributed Denial of Service), which exploits the vulnerabilities of the protocol related to IoT to perpetrate, more often, systemic attacks.

- Are Guidelines enough in this scenario?

- ISO 22301:2019 may be the answer!

- This, through an increasing proliferation of malware-infected botnets and vulnerable servers that automatically generate further attacks against vulnerable targets.

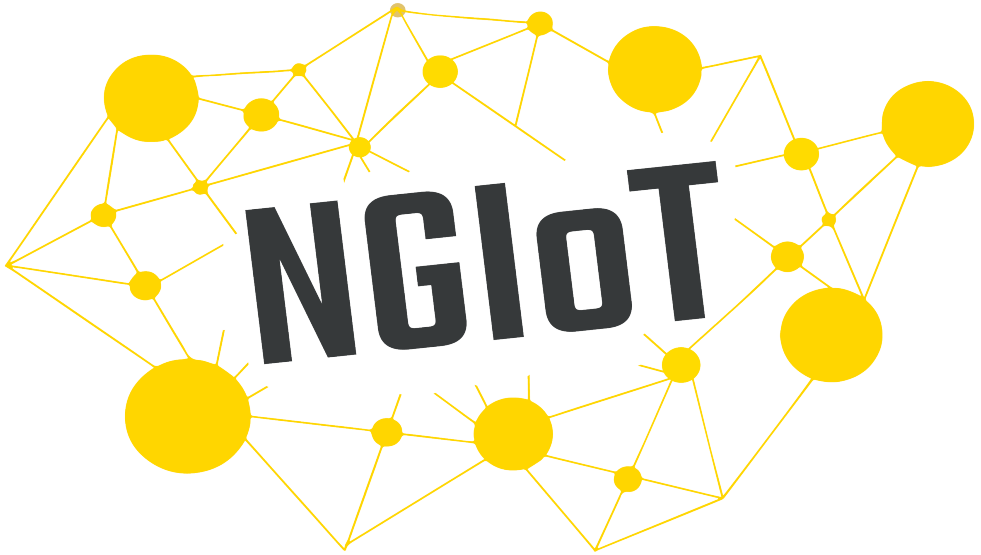
- DDoS attacks are aimed precisely at disrupting services, which is exactly what the legislator wants to prevent through NISD, i.e. the disruption of services that are essential for the citizenry that could compromise user security and national security.

- In many cases of DDoS attacks, cybercriminals tend to falsify the IP address of a target connected to the IoT in order to send a series of information requests to a vulnerable server that generate an amplified amount of responses (packet amplification) to the IP address of the victim, effectively frustrating the defense capabilities of the affected server.

- Many devices heterogeneously connected to the IoT, in fact, while having good connectivity, access unmonitored network segments, thus making them vectors of a significant volume of DDoS attack traffic, also due to their reduced processing capacity.

- In such cases, it is not uncommon for IoT devices to be used as proxies and, therefore, the compromise of a device connected to a network inevitably makes all other internal and external resources vulnerable. In general, DDoS attacks exploit the most widespread and consolidated Internet protocols such as Network Time Protocol (NTP), DNS (Domain Name System) and SSDP (Simple Services Discovery Protocol) and are characterized by IP address falsification and packet amplification

Contact Details



Istituto Italiano per la Privacy - NGIoT

Francesco Capparelli

f.capparelli@istitutoprivacy.eu

The project CHARIOT has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780075