The Hague, 24 April 2016

EDOC # 830746 v2

Cybersecurity and the Internet of Things – a Law Enforcement Perspective[1,2]

Europol, European Cybercrime Centre

1. Introduction

The Internet of Things (IoT) is characterized by a constantly growing network of connected devices, actuators and sensors that can interact with or collect data on their internal states or the external environment, using a variety of different protocols and standards. The IoT creates the ability for physical objects, which were previously often unconnected and without computing power, and people to remotely interact through the internet. It is one of the characteristics that make devices 'smart' as they become (more) context-aware.

The Internet of Things is also characterized by the convergence of people, processes, data, and objects by combining communications between machines, between people and machines and between people to deliver new or enhanced services and to provide improved contextual awareness and decision support.

Cloud Computing and Services provide the dynamic, scalable and ubiquitous infrastructure and services needed to support the storage and distributed processing of the data collected via the IoT. The ever-increasing amount of data that is being collected via the IoT – from different sources and on a variety of aspects, including data that was previously not or difficult to capture – links it to the concept of Big Data, which in essence is about new ways of analyzing, visualizing and leveraging large amounts of data in real-time or near real-time.

These concepts are a driving factor behind new types of 'critical infrastructure' such as smart cars, smart ships, smart homes, smart grids or smart cities.

However, the IoT plays a crucial role in more conventional types of critical infrastructure too as more and more smart sensors are being used in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) control systems as well as Automatic Identification System (AIS) tracking systems.

2. Risks and Challenges

The Internet of Things uses a variety of different software and hardware products as well as communication standards and connectivity protocols. Combined with the large and constantly increasing number of connected devices, this creates a broadened attack

[1] 2015 Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015

[2] 2014 Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

surface and increased number of attack vectors. In fact, the Open Web Application Security Project (OWASP) highlights several different attack surfaces such as a device's physical memory and interface (e.g. USB port), firmware, local data storage, update mechanism, network services, Cloud interface, mobile application and third-party APIs (application program interfaces). Basically, this means that any internet-facing device can become the target of an attack using a variety of different entry points.

The heterogeneity and complexity of the software and hardware ecosystem powering the IoT along with a lack of security and privacy by design creates substantial cybersecurity risks for industry, consumers and operators alike. Such environments are difficult to manage, control and safe-guard, considering also that many IoT devices have no built-in security features. In fact, due to the small size of some of these connected devices, resource limitations in terms of memory, battery and computing power are such that they are unable to perform cryptographic operations or scan for malware. In this regard, many of the so-called smart devices could actually be considered to be rather dumb when it comes to their lack of awareness to their risk posture.

As the IoT is more widely adopted and becomes increasingly part of production ecosystems one can also expect to see a higher degree of homogeneity and standardization when it comes to some of the hardware and software that is being used. As a consequence, the IoT runs the risk of failures that result from a single fault in software or hardware components used in smart devices, which present a mayor risk to cybersecurity. If such an exploitable failure is detected it can affect a potentially very large number of devices thereby creating a large number of potential victims. If there is even an option to fix such a vulnerability, this usually takes time, often years. Examples are smart TVs that may run operating systems used also in smartphones, which are often vulnerable to many of the same attacks, or home routers and IoT hubs.

A clear indicator of the growing adoption of the IoT is the rising number of smart 'things' such as smart homes, smart cars, smart medical devices and even smart weapons. This contributes to an increasing digitisation and online presence of personal and social lives, an increasing level of interconnectivity and automation, and an increasing amount of data that is being collected and analysed. This includes for instance facial and speech recognition features in smart devices or wearable technology that can process data. Apart from the aforementioned cybersecurity risks, this also creates a number of challenges in terms of identity, privacy and trust:

The data that is being collected and processed via the IoT creates new privacy issues as the combination of different categories of data can offer new insights. Since Big Data aids de-anonymisation – either through patterns and correlations that become visible in bigger data sets and/or the combination with other data sources – it becomes harder to protect privacy and personal data.

Because of the scale of the IoT, trust between different devices can be hard to engineer and expensive to guarantee. Yet, there is a need for strong and robust cross-platform authentication and identification services in order to restrict access to data and devices to authorized entities.

Moreover, the fact that smart devices are used to create contextual awareness and offer decision support makes them a target for data manipulation too.

Finally, large scale attacks against these new types of 'critical infrastructure' as well as existing infrastructures could have a significant impact in terms of safety, security, public health or the economy. Examples could include new forms of blackmailing and extortion schemes, hacked smart cars, medical devices or weaponized drones, data theft, attacks resulting in physical and mental harm, and new types of botnets. As with

any cyber threat, such attack scenarios are not limited to a particular category of attackers or a particular set of motives.

3. Law Enforcement Considerations

For law enforcement, the Internet of Things presents specific investigative challenges due to the diversity of hardware, software and communication standards and connectivity protocols being used. Some of the relevant data may be located in the Cloud, which will frequently require cross-border co-operation and legal assistance. In some instances, however, the amount of relevant data that can be extracted for investigative purposes may be minimal. Also, it can be expected that the IoT will further complicate the attribution of crimes, given the increased attack surface(s) and large number of attack vectors.

Extracting, identifying and combining the relevant evidence will routinely become a Big Data problem, requiring law enforcement to have the necessary skills, tools and expertise available.

An important application of Big Data in the area of law enforcement is predictive policing - the application of mainly quantitative analytical techniques to identify likely targets for intervention and to prevent crime, or solve past crimes by making statistical predictions. It is seen as a method that allows law enforcement to work more effectively and proactively with limited resources. The IoT can support predictive policing by providing the necessary data sets for the identification of patterns and correlations. The underlying models have a number of limitations such as the general inability to answer the question of causality. It is therefore important to use this concept carefully, proportionally and in line with relevant legislation and regulations.

As mentioned before, any smart device storing valuable data or providing crucial services can be the target of a cyber-attack. This can range from very small devices, to smart cars, to smart container ships, to smart cities.

Considering also the relevant findings and recommendations in Europol's EC3's 2014 and 2015 Internet Organised Crime Threat Assessment reports, this necessitates further attention and consideration by law enforcement as the IoT is increasingly becoming a reality and connected devices are regularly comprised. Specifically, this calls for a broader focus on potential targets, criminal modi operandi, and mitigating, preventive and investigative measures.

4. Opportunities and Recommendations

While the Internet of Things makes the protection of data, establishing trust and ensuring privacy and security more challenging, it can also help address the new challenges and threats in cyberspace, for instance in the form of data-driven security or behaviour-based security.

The IoT in combination with Big Data analytics, machine learning and Artificial Intelligence approaches can help improve cybersecurity through better threat detection and prediction, intelligence collection and analysis, and faster response. A combination of human-driven techniques, which typically rely on rules and may therefore miss any attacks that do not match the rules, and machine-learning approaches using anomaly detection, which tends to trigger false positives, may leverage the advantages of both domains.

Another potentially interesting approach to increasing cybersecurity for the IoT and to establishing trust and ensuring privacy in the decentralised network it creates is the use of the blockchain or Distributed Ledger Technology (DLT). DLT can potentially provide a framework to facilitate transaction processing and coordination among interacting IoT

devices, allowing each to manage its roles and behavior and thereby making them (more) autonomous. It may also be applied to ensure that the operating system and firmware used in a smart component of critical infrastructure has not been tampered with.

For law enforcement in particular, the potential benefits include improved and more targeted analytical capabilities, an increased chance to find relevant evidence, improved triaging, the ability to create a denser timeline of events, and better support for the automated analysis of crime-relevant data, including speech, image and video recognition. In addition to the need to adhere to the principles of lawfulness and proportionality, it is of course of utmost importance to balance the potential benefits against the negatives that may result from reduced privacy and other unintended consequences.

The complexity and resulting cybersecurity challenges in relation to the IoT ecosystem call for a holistic, smart and agile approach; the multi-faceted nature of the challenges and risks demands an equally faceted response by all relevant stakeholders with a view to ensuring cybersecurity. Consequently, cooperation and public private partnerships will play an increasingly important role – ideally, all IoT actors and relevant stakeholders should engage in discussions on IoT design choices and their implications.

Security-by-design and privacy-by-design should be the guiding principles when developing IoT devices and enabling services. This includes the need to only collect the minimum amount of data necessary, automatically protect personal data by using proactive security measures (e.g. end-to-end encryption) and means to make individuals less identifiable, implement data retention policies, ensure transparency, and provide opportunities to assess any analytical processing, to mention some.

The Internet of Things is no longer a futuristic concept but a well-established and constantly expanding model. It is therefore timely to hold a multi-stakeholder discussion on cybersecurity, putting it at the heart of the IoT.

* * *