CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Bulletin - Volume 2, Number 3, September/2017

IoT and the Industry 4.0

Rodrigo Filev

The terms internet of things and advanced manufacture are undoubtedly among the most discussed topics of this decade, and they bring the paradox between good fortune and the scrapping of man. The academic and technical literature have been systematically presenting technologies, systems integration, platforms, security and privacy. The synergy between the internet of things and digital manufacturing has created industry 4.0 or advanced manufacturing (broader term), a recurring subject of several forums, among them the World Economic Forum. The consequences of these two new paradigms (IoT and advanced manufacturing) are, among others, profound changes in labor relations and privacy and security issues.

> In the evolution of the internet of things and advanced manufacturing, there are several global challenges to be discussed and solved.

Cybersecurity is already an old topic in technology forums and has been around for a long time in everyday activities. After all, who never bothered to update an antivirus from your computer? But the contours of today's security threats far outweigh purely cybernetic issues for one reason: if the Internet of Things integrates the virtual world with the physical world in an unprecedented way, and has as one of its consequences advanced manufacturing, a threat of Security with origin in the virtual world can affect how the physical perspective? In addition, is the reciprocal one true? In the second half of 2016 news that could go unnoticed long ago confirmed fears discussed in academic and business environments: a medical equipment company has announced a safety flaw in a blood glucose meter. Through this security breach, an individual could alter the measures of said apparatus, which could cause a patient to administer inappropriate amounts of insulin to his body. Of course, the consequences can cause severe damage to health.

In an IoT society, it is already necessary to protect an individual from a virtual fault that can cause physical harm. Maybe you could think that the solution is to install a firewall on your blood glucose meters or use encrypted communication channels would solve the problem. Fortunately, the challenge is more complex and exciting because the data from these new IoT systems describe both particularities of the environments and details about the people in these environments, such as private health or private data. In addition, failures or attacks on IoT systems can cause material damage not only to an individual, but also to an entire community. In another example, there have been very well documented attacks on vehicles that could be driven at a distance by an attacker, rendering the driver impotent.

There are no security mechanisms that prevent threats to your privacy. Paradoxically, changes in the boundaries of privacy bring new, surprising, and beneficial services in many ways. For the consumer, the use of a certain free service that requests in return access to the data of the individual seems a good deal, and even harmless. However, the consumer does not pay attention to the fact that each of the applications he uses (the services of an intelligent city and the captured data) generate profiles of use of the service. Certainly, these profiles seek to represent the citizen in a kind of avatar, or seek to classify an individual into a stereotype (persona). In both cases, the idea is to better offer customer service. In this scenario, there is a risk that a particular service may produce a profile or classify a particular individual incorrectly and even harmful, which can also be considered a security breach. Suppose that a researcher or security professional works on a sensitive topic, such as fighting a crime.

Suppose such a professional fights off sexual crimes committed against children and adolescents. Suppose also that this same professional has children still in infancy or pre-adolescents. Imagine the situation this professional goes to work and leave your smartphone by your side constantly, connected to the wireless network of your workplace. Absolutely feasible and existing scenario today. Something that happens is that the manufacturer of the smartphone operating system of this professional informs the data network and the location in which it is, and given the time of registration and day of the week is not difficult to conclude that the individual is working. Likewise, if the professional is to be a sexual predator in an investigation and use the Internet to infiltrate a particular virtual community, it is possible that the browser registers the accesses of the individual. Collected data may infer that the user accesses data on child pornography and as both, the computers and the smartphones, of various professionals are on the same network, so there is at least one candidate to be a sexual predator at that location. If the system knows that security professionals work there, that is fine. However, if this professional is anywhere else, using a laptop and with the smartphone in his pocket, then an IoT system can presume that the user of that smartphone is a sexual predator. After all, the use of the laptop plus proximity to the smartphone indicate a dangerous subject. If this information is shared with other systems, something commonplace today, what can happen if this individual goes to a children's clothing store to buy something for one of their children? What would the store system recommend? Could the store be warned about a potentially dangerous customer?

This fictitious scenario can occur if there are no data management mechanisms that are able to discern sensitive issues. Imagine similar situation in advanced manufacturing, where one would want to produce customized products for any individual. Suppose the drug industry can produce a particular remedy at the appropriate dosage for the consumer's body. This industry will probably need genetic data from an individual, and without adequate privacy control, the potential security risk of that such data is unclear, but the estimated impacts are tremendous.

In the evolution of the internet of things and advanced manufacturing, there are several global challenges to be discussed and solved, and we cannot afford not to have an active voice on such issues. Although privacy and security are being discussed from a technological point of view, it seems to fit human beings as integrated with the security and privacy solution, not just a user, since personal questions and values will be fundamental for the new services to be secure.

Rodrigo Filev *is PhD in Computer Engineering from Escola Politécnica da Universidade de São Paulo, and researcher at the CEST-USP.*

Coordinator: Edison Spina

This article is a result from the author's ascertainment and analysis, without compulsorily reflecting CEST's opinion.