Internet of Things: A Security Challenge

Jean-Pierre Kuilboer
University of Massachusetts
Boston, MS USA
Jeanpierre.kuilboer@umb.edu

Noushin Ashrafi
University of Massachusetts
Boston, MS USA
noushin.ashrafi@umb.edu

Abstract

The Internet of Things (IoT), Internet of Everything, or Industrial Internet can be briefly defined as the network of physical or virtual smart objects that contains embedded technology to communicate and sense or interact with their internal states or the external environment. The "*Smart*" qualifier implies objects should learn from their environment and adapt in subsequent use-cases. Whereas IoT presents pervasive opportunity to create new economic value by making things smart, it also entails unprecedented complexity and increased 'attack surface' in the security and privacy dimensions. Manufacturers have demonstrated a serious weakness in their deployment of Security & Privacy by design. As IoT Research is rapidly progressing from observational to solutions aimed at multiple domains (e.g. Auto, Wearables, Health & well-being, home, retail, city, robotics & HMI), security threats and prevention methods must be understood and addressed.

The predicted economic impact of the Internet of Things (IoT) will be measured in US$ trillions, and the number of connected devices could reach 20-50 billion by 2020, yet addressing the security aspects of this hyper-connected world is far from resolved. Several bodies including IETF, IEEE, ITU-T SG20, the European IERC, OWASP IoT project, and OMG have recognized the threat and started defining mechanisms and best practices to secure the overall IoT ecosystem. However, even for the experts this multitude of sources can at time be confusing.

This study explores and compares some of the initiatives launched to solve the threat to security in the IoT sphere. For example, the IEEE has recently initiated a new project "P2413 - Standard for an Architectural Framework for the Internet of Things" to avert the fact that most current standardization activities were confined to very specific verticals and represent disjointed and often redundant developments. It should provide a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety." ITU-T has a program under development led by Study Group 20 aimed at IoT. Given that IoT is a complex system of interconnected smart "objects", the Object-Management group has also launched an initiative aimed at the Industrial Internet of Things (IIoT).

Furthermore, worldwide industry and public funds such as Horizon 2020 Framework in the EU and through NSF in the US have initiatives to exploit the potential impact of IoT on overall economy. However, during the timeline gap expected before standards are settled, large industry groups such the Open Connectivity Foundation and the AllSeen Alliance have formed, pushing for de-facto directions often with overlapping memberships but divergent recommendations. Moving forward without addressing the privacy/security hurdle could derail the safe adoption of the technology. This research provides an in-depth study/review of ongoing efforts by public and private organizations to address the security aspect of IoT linked to Hardware, Software, Interfaces, Systems Interconnectivity, and frameworks.