Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-21 (2016) 423–430

Privacy Matters – Issues within Mechatronics

Steve Watt*, Chris Milne*, David Bradley, David Russell***, Peter Hehenberger******
Jorge Azorin-Lopez*****

** University of St Andrews, St Andrews, Fife, FY16 9AJ, UK (email: cio@st-andrews.ac.uk & c.milne@st-andrews.ac.uk)*
*** Abertay University, Dundee DD1 1HG, UK (email: dabonipad@gmail.com)*
**** Penn State Great Valley, Malvern, PA 19355, USA (email: drussell@psu.edu)*
***** Institute of Mechatronic Design and Production, Johannes Kepler University, Linz, Austria (email: peter.hehenberger@jku.at)*
****** Computer Technology Department, University of Alicante, Alicante, Spain (email: jazorin@dtic.ua.es)*

Abstract: As mechatronic devices and components become increasingly integrated with and within wider systems concepts such as Cyber-Physical Systems and the Internet of Things, designer engineers are faced with new sets of challenges in areas such as privacy. The paper looks at the current, and potential future, of privacy legislation, regulations and standards and considers how these are likely to impact on the way in which mechatronics is perceived and viewed. The emphasis is not therefore on technical issues, though these are brought into consideration where relevant, but on the soft, or human centred, issues associated with achieving user privacy.

Keywords: Privacy, Users, Big Data, Security, Mechatronics, Cyber-Physical Systems, Internet of Things.

1. INTRODUCTION

While at its fundamental level mechatronics remains structured around the integration of the core technologies of mechanical engineering, electronics and information technology, the nature of the systems within which mechatronic components and devices are being used has been and is undergoing a significant shift. In particular, referring to Fig.1, mechatronic devices and components are increasingly associated with both Cyber-Physical Systems and the Internet of Things [Bradley DA 2015; Bradley DA 2016]. While the design processes and methods associated with mechatronics remain reasonably robust, the relationships of Fig. 1 must inevitable be associated with increasing levels of abstraction as the domain of the design moves from mechatronics to Cyber-Physical Systems and into the Internet of Things with components, unknown to the user, or indeed the designer, in other than a functional sense, being autonomously selected by the system on the basis of context, need and functionality.

Additionally, many of the resulting participatory systems, structured along the lines of Fig. 2, are associated with aspects of data collection, often involving personal or user data, and with the creation of larger data sets resulting from the aggregation of data from and across multiple users. This aggregation of data then has implications for the privacy and security of both individual users and aggregated users across all data collected [Patton 2014; Borgohain 2015; van der Sloot 2014].

To date, emphasis in relation to the safeguarding of personal data has largely been on the '***hard***' aspects of system security and less on the '***soft***' issues associated with the privacy of individual users. However, recent studies, as for instance by the US Government [Executive Office 2015], have suggested a need to reinforce privacy issues through a combination of legislation, regulation and standards, including in the US the potential for a "*Privacy Bill of Rights*". The introduction of such legislation will impact upon the design processes for mechatronic components and devices and their use in association with Cyber-Physical Systems and the Internet of Things, and hence on the relationships with system users.

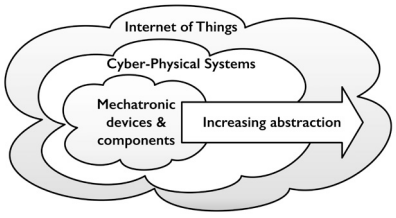

Fig. 1. Increasing abstraction from Mechatronics to Cyber-Physical Systems and the Internet of Things.

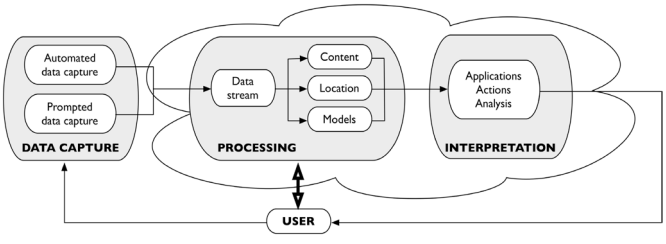

Fig. 2. A participatory system.

The paper thus provides an overview of current, and potential future, issues associated with privacy legislation, regulation and standards before consider how these are likely to impact upon the design process itself.

10.1016/j.ifacol.2016.10.641

Drawing on research by the authors in areas such as engineering design, smart systems; including smart homes, domotics and smart grids, eHealth and manufacturing as well as experience in managing the day-to-day operation of large information systems and in engineering education, the paper also considers how privacy issues can be translated into future, user-oriented, systems.

2. MECHATRONICS, CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS

Referring again to Fig. 1, within the context of the paper the relationship between mechatronics components and devices, Cyber-Physical systems and the Internet of Things may be summarised as follows:

Mechatronics Smart components and devices characterised by an integration of technologies and a transfer of functionality from the mechanical to the electronics and software domains.

In illustration, many vehicle systems from drive train management to environmental control can be considered as essentially mechatronic in nature.

Cyber-Physical Systems (CPS) These are formed by an aggregation mechatronic (or other) components through the medium of a smart network supported by and associated with intelligent software to manage the contribution of the individual components to the CPS, and to the CPS in its entirety.

Thus, a vehicle could be considered as a CPS structured around an aggregation and assembly of mechatronic components and devices [Shi 2011].

Internet of Things (IoT) The IoT provides access to information, context dependant and otherwise, as well as sourcing a range of software, platforms and infrastructure services and functions. In many cases, these will be sourced on demand without necessarily any a priori knowledge as to their origins or structure.

Thus, individual vehicles may communicate with each other to establish traffic flows and determine optimum routing as well as with other systems and agencies, for instance to adjust home based environmental control systems based on estimated arrival times.

3. SECURITY v PRIVACY

Though issues of security and privacy are closely linked, and indeed sometimes seem to be considered as the same, in the context of the paper, security is considered as being conventionally associated with those '***hard***' elements such as encryption and firewalls which are intended to protect against intrusion while privacy deals with the '***soft***', or people oriented issues such as the ownership of data and its use. That implies that there is a synergistic relation between security and privacy in which the relationship may well be determined by function.

Consider the instance of the integrated vehicle systems outlined in Section 2. Here, the autonomous flow of data between individual vehicles and, say, a home system can support enhanced traffic management resulting in reduced energy consumption (and of associated CO_2 levels), but also has the potential to provide information at the level of the individual which could, for instance, be used to indicate whether a house is currently occupied.

A shift in emphasis at the level of the individual towards privacy as opposed to security implies that the emphasis of the associated protocols also moves away from providing a hard, or impenetrable, security boundary, to more function based strategies to ensure privacy. In that context, the interest in using techniques such as the blockchain database structures [BBC News 2016; Sweeney 2002; Harrison 2015] is potentially of significance.

Perhaps therefore it is no coincidence that the annual World Economic Forum Risk Report [WEF 2016] has consistently over a period of over 10 years identified cyber security and associated factors such as privacy of the individual as a major, and high impact, risk area.

3.1 The Role of Big Data

The term big data is generally applied to large and complex data sets for which conventional data processing methods and techniques are inadequate. Such sets are often structured around personal data, as for instance health related data, and can be added to, often at the moment without the knowledge of the individual using the device, by devices such as those used to measure exercise levels. The following provides some indication of the types of data sets, and the numbers, involved.

- A study suggests by McKinsey suggests that retailers who fully leverage big data could see an increase in operating margins of as much as 60% [Court 2015].
- IDC[1] estimate that in 2015 Financial Services worldwide spent $114 billion on mobility, cloud, Big Data & analytics [IDC 2015].
- Forbes suggest that the Advanced and Predictive Analytics (APA) software market is likely to grow from $2.2 billion in 2013 to $3.4 billion in 2018 [Columbus 2014].

The analysis of such data sets has resulted in the evolution of methods such as predictive analytics, knowledge discovery and data mining as a means of extracting information, and hence knowledge, from such data. However, the ability to extract such knowledge also carries with it privacy implications for those individuals whose data is incorporated into the overall data set [Ekbia 2015; Kambatla 2014].

In recognition of this potential conflict between the individual and the potential use of Big Data, in the US, the President's Council of Advisors on Science and Technology (PCAST)

[1] International Data Corporation