1- Cyber-Physical-Social System (CPSS) engineering: foundations, concepts, and model-based techniques through a systematic literature review

The notion of Cyber-Physical-Social System (CPSS) has been developed as a result of integrating social actors (humans) into Cyber-Physical Systems (CPS), where a CPSS can be described as a system consisting of cyber components, physical components as well as social components [1]. Although the notion of CPSS has been around for over a decade, it is still an emerging research area.

This thesis aims at identifying the foundations, key concepts, and model-based techniques for designing CPSS through a Systematic Literature Review (SLR) concerning the related literature. The SLR process is expected to follow well-established procedures for performing (e.g., [2]), i.e., 1- planning the review, 2- conducting the review, and 3- reporting the results of the review. Finally, the student is expected to identify related challenges and future research based on the results of the review.

References


2- Citizens as Data Donors (CaDD) – a method for maximizing participation through privacy assurance and behavioral change.

Mohamad Gharib, Lecturer of Software Engineering (mohamad [dot] gharib [ä] ut [dot] ee)

Citizens Science (CS) is a research technique that enlists the public in gathering data. Although citizens themselves can be the source of such data, most of their participation in CS so far focused on furnishing data concerning almost everything except themselves. In particular, citizens can participate as data donors (CaDD), where they allow professionals to collect and/or have access to their Personal Data (PD) for the purposes of the public good. However, PD cannot be used without citizens' consent, therefore, citizens need to be well motivated to participate as PD donors.

This thesis aims at proposing and validating a method for maximizing citizens' participation as data donors by understanding and addressing their privacy requirements taking into consideration the perceived benefits and ease of the donation behavior. The method will be based on the Theory of Planned Behavior (TPB) [1], which has been proven to be a useful tool in explaining, predicting and changing many humans’ behaviors. Moreover, the TPB was a foundation for the Technology Acceptance Model (TAM) [2] that models how individuals come to accept and use a certain new technology.

If you want to have a look at a preliminary version of this work including the types of techniques to be used for developing the method, please check this paper [3]. A successfully completed thesis may result in the publication of a scientific paper.

References
3- Towards a model for valid informed privacy consent

Mohamad Gharib, Lecturer of Software Engineering (mohamad [dot] gharib [ät] ut [dot] ee)

``I have read and agree to the Privacy Policy``. This can be described as one of the biggest lies in the current times, and that is all what a service provider needs to acquire what can be called ``informed consent``, which allows it to do as it pleases with your Personal Information (PI). Although many developed countries have enacted privacy laws and regulations to govern the collection and use of PI as a response to the increased misuse of PI, these laws and regulations rely heavily on the concept of informational self-determination through the ``notice`` and ``consent/choice`` model. This model is inefficient for acquiring informed consent simply because current mechanisms for presenting the notice and obtaining the consent are deeply flawed as indicated by many researchers because they are neither useful nor usable. More specifically, most notices are long and complex [1]; hard to be understood by ordinary people [2], and do not help much in predicting potential future use of PI nor assessing the consequences and risks related to such potential use [3]. Therefore, most data subjects, usually, blindly accept such notices [4]. However, if a data subject did not read the notice, or she read it but did not understand, or she read and understand it, but lack the cognitive competence to make an informed decision, such consent cannot be informed [5], accordingly, it is not valid [6]. This leads us to the research question “What constitutes valid informed privacy consent?” The main aim of this thesis is answering the aforementioned research question proposing a model for acquiring valid informed privacy consent.

References

4- An integrated approach for analyzing cyber-security attacks for safety-critical Cyber-Physical Systems (CPSs)

Mohamad Gharib, Lecturer of Software Engineering (mohamad [dot] gharib [ät] ut [dot] ee)

The increased digitization of traditional Physical Systems (PSs) gave birth to the so called Cyber-Physical Systems (CPSs), which integrate sensing, computational, and control capabilities into traditional PSs combined with network connectivity. Consequently, traditional security solutions, although well established and consolidated, might not be effective to protect CPSs against human planned, malicious, complex attacks, which are the typical modern cyber-security attacks. This is quite clear with the increasing number of cyber-security attacks that now can target some of the safety-critical functionalities of CPSs. For instance, modern automotive vehicles have been proven vulnerable to hacking attacks aiming at getting control over the safety-critical functions of the vehicle [1]. An example is the hijacking of the steering and braking units in a Ford Escape [2]. Similarly, hackers were able to remotely hijack a Tesla Model S from a distance of around 12 miles [3]. Chrysler announced a recall for 1.4 million vehicles after a pair of hackers demonstrated that they could remotely hijack a Jeep’s digital systems over the Internet [4]. These are just a few examples of how attackers can exploit weaknesses in the design of safety-critical CPSs and use these weaknesses to conduct their attacks.

This thesis aims at proposing an approach that can identify potential cyber-security attack(s) that the safety-critical functionality of concern might be subject to, analyze how each identified attack may succeed (e.g., attack method/means, attacker’s capabilities), the potential consequences in case such attack success. Then, identify countermeasures to prevent or at least mitigate/minimize the consequences of the attack.

Application domain can be the automotive domain, or any other safety-critical CPS domain such as Industrial Internet of Things (IIoT), Smart Cities, etc.

References