IPACSO White Paper

Introducing the IPACSO Framework

September 2015

I. What is IPACSO?

IPACSO which is an acronym for Innovation Framework for Privacy And Cyber Security Market Opportunities is funded under the 7th Framework Program of the European Union. The IPACSO Project has developed a structured knowledge and decision support framework which can be used for identifying, assessing and exploiting market opportunities in the privacy and cyber security industry domain. Privacy and Cyber Security (PACS) are areas which are presently experiencing and will continue to experience rapid and sustained growth; yet there are a unique set of characteristics relating to the field which make it difficult for new organizations to enter the market. IPACSO has developed a framework which operates as a knowledge resource which offers guidance and support tools to those who are looking to innovate and create new products or services in the field of privacy and cyber security. The consortium is comprised of five participating partners two of whom (Waterford Institute of Technology and Deutsches Institut für Wirtschaftsforschung) are academic with the remaining three (Espion, LSEC and Vasco Data Security) being industrial.

This white paper will begin by describing privacy and cyber security and explaining their importance in the contemporary hyper connected world; by doing this it will demonstrate the business potential of the PACS domain. It will then proceed to examine some the market aspects including the size of the PACS market along with some of its unique characteristics related to aspects such as trust, regulation and the changeability of requirements. Following this will be an introduction of the IPACSO framework and a discussion outlining some of the aspects of the IPACSO 'solution'.

II. Privacy

Privacy is a complex concept which can vary in meaning according to time, place and social context. According to sociologist Gary Marx 'privacy is like the weather, much discussed little understood and difficult to control' (Ritzer 2007). Conceptualizing privacy is fraught with difficulties due to the fact that traditional definitions and commonly held assumptions about it have been rendered problematic in the face of technological advances and changing socio-cultural norms about what constitutes the public and the private. Privacy is often conceptualized in terms of a spatial metaphor with compromises of privacy being described using terms such as invasion or breach. Privacy is also commonly conceived of as an individualist value where it is a means of shielding the individual from unwanted intrusions from the social world at

large. Psychologist Alan Westin defined privacy as 'the claim of individuals groups or institutions to determine for themselves when, how and to what extent information about them is viewed by others' (Westin 1967, p. 7). This definition is most prescient for the purposes of the IPACSO project where privacy is primarily concerned with the ability of individuals to control the flows of personal data relating to them. The data in question is that which is related to the 'digital footprint' of the individual such as data generated in consumer interactions, financial data, health data, data generated using social media platforms and any other types of digitally generated meta data which can be linked to an individual. In using most online digital technologies there is a trail of data generated about the user which can be a revealing indication of the lifestyle, interests and activities of the person. Such data is a valuable resource and as such is a core component in the financial models of some of the largest internet companies such as Google and Facebook.

The normalization of the widespread collection of such data has potentially severe consequences on privacy and the rights of individuals. As a relatively new phenomenon the practice of pervasive data collection is yet to be fully realized and interrogated by much of the general public. Despite this there is a noticeable trend towards privacy as a desirable trait in new technologies as is evident in the popularity of the search engine duckduckgo, or the Mozilla Firefox web browser. As part of the IPACSO project there has been an analysis of the Marketplace for Privacy-related Products and Services. Privacy enhancing technologies (PET's) have a large market potential as companies can position privacy as a unique selling point of their products. The market segment for privacy enhancing technologies which is the least exploited is that which facilitates privacy for individuals, thus products which aim to grant control over personal data are more likely to be profitable in future.

III. Cyber Security

The last thirty years has seen a noticeable trend towards the ever increasing digitisation of networks. These newly digitised networks include many of those which are crucial for the smooth running of much of the key architectures of the developed world. These networks include essential infrastructures which are used to facilitate communication, finance and banking, utilities such as electricity, as well as the networks which power social networking and the consumer society. The fact of this exponential increase in the use of digital systems means that there are a new set of associated risks relating to keeping systems secure and keeping out virtual intruders with malicious intent. The fact that digital networks are globally connected and dispersed means that the potential pool of attackers is far larger and can be drawn from locations all over the world. In many ways the facets of digital networks which make them usable and powerful

resources are concurrently sources of weakness and risk. An increase in the use of digital networks means an increase in risk, and when these networks control the key utilities of the contemporary world it is imperative that adequate and proper protection is maintained so as to avoid their breakdown and the attendant threats to social political and economic order.

The combination of these factors means that there is an ever increasing need for cyber security. These risks are posed not just to individuals but to all organisations including businesses, nation states, corporations and so on. New technologies mean new weaknesses, and the incorporation of digital networked technologies into new areas increases their vulnerability to outside attacks. An example of this can be seen in July 2015 when IOActive Vehicle Security Research demonstrated vulnerabilities in on board computer systems of Chrysler motor vehicles. The vulnerabilities enabled these cars to be hacked by outsiders allowing for the remote control of a number of core controls including steering and brakes. This example demonstrates how the digitisation of existing technologies can open them up to new and unforeseen threats which can be a formidable danger to public safety. Developments in the fields of Cloud Computing and the Internet of Things (IoT) will increase the digitisation of everyday objects making them subject to such threats meaning that there is an ever increasing need to ensure security.

With the potential for disruption and danger inherent in the increasing use of networked digital technologies has come the linked increase in the use of cyber techniques as an offensive weapon. At the level of the nation state Cyber Warfare can be described as the 5th domain of war after sea, air, land and space and state sponsored hacking groups are increasingly engaged in offensive actions. There are a number of reasons why such groups are beneficial to states, they are cheap to set up and can be capable of inflicting a lot of damage on an adversary. Most importantly however they can operate with the principle of plausible deniability meaning that the sponsors of such actions can carry out attacks while denying having any involvement. An example of this can be seen with Cyber Berkut who are a pro-Russian hacking group who are waging cyber war alongside the real world military actions of their counterparts in Ukraine. As well as carrying out DDOS attacks on opponents and those who sympathise with them Cyber Berkut have been actively engaged in propaganda activities throughout the conflict in Ukraine.

The fields of privacy and cyber security are set to increase in both size and importance as instances of privacy breaches, cyber espionage, data dumps and malicious hacking activities become more prevalent and more public. As well as this, the

increase in the use of networked digital technologies and the extension of their use in realms which have previously been analogue and offline means that more realms of social life will be subjected to the dispersed risks described above. The next section will examine the size of the market in privacy and cyber security.

IV. A Market Perspective

As outlined above Privacy and Cyber security are both areas of development which are expected to see large scale growth. The size of the markets will grow in tandem with the increasing digitization of other infrastructures and the need to keep them secure from outside malicious interference. There are a number of other aspects however which may influence the perceived need for cyber security including other high profile attacks or incidents which engender a feeling of vulnerability in the general populace. Such incidents are likely to lead to calls for legislation and state intervention to ameliorate the problem which if acted upon could have many ramifications for those working in the area. One of the key characteristics of the PACS market is that products and services developed must be robust and capable of withstanding attack while at the same time being fluid with the capability to adapt quickly to changes in the threat environment. These changes could include changes in legislation or advances in the capabilities of the attackers just as much as it could include changes in geo-political relations.

V. Quantifying PACS

The market in privacy and cyber security is one which is difficult to accurately quantify for a number of reasons, the first of which is that it is difficult to demarcate the boundaries of which products and services are part of the market. Many PACS products and services are embedded within larger systems and bundled within other services and so it can be difficult to accurately gauge their size or value. As well as this some players in the PACS field are subsumed within larger companies or organizations and do not produce individualized accounts which would make it possible to measure their size. A further difficulty in quantifying the PACS market is that many organizations do not publicize the details of their PACS systems for security reasons. If the details regarding size or spend on security systems are publicized then it can act as a means of flagging weaknesses of the system to potential attackers. If there is the perception of low levels of security then this sets them as a target for obvious reasons but conversely if there is the perception given of high levels of security then there is the

possibility that hackers who are motivated by demonstrating technical proficiency to gain esteem within counter-cultural social groups will see this as a desirable target.

One measure by which it is possible to attempt to quantify the market size is by looking at the amount of money which is invested in it. The MIT Technology Review recently claimed that in 2014 venture capitalists invested 2.3 billion US Dollars into the market. This figure marked a steady increase of 156% since 2011 and this trend was reported as being likely to continue as 75% of CIO's surveyed in research conducted by Piper Jaffray stated that their spend on PACS would increase in 2015. IPACSO has compiled many of the publically available statistics which would assist in attempting to ascertain the overall size of the market including reports by Frost and Sullivan, Pierre Audoin Consultants, and Gartner among others. These sources have identified the PACS market as being worth in US Dollars between 62.4 billion and 95.6 billion for the year 2014, with projected growth rates ranging from 8% to 13.4% between 2014 and 2020. This means that the market is predicted to be worth somewhere between 145 to 155 billion US Dollars per annum by 2020.

There are different types of markets in PACS which are generally defined by the type of user. For example the market for personal users who wish to protect their personal information and avoid identity theft is very different to the market for a large scale organisation which has to protect its networks and business assets from malicious attack. The IPACSO project has conducted analysis which deems the market in small scale PACS solutions for the individual consumer to be the least exploited and to have considerable potential for new entrants. PACS markets are highly segmented as each type of buyer will have a different set of requirements, will be attempting to protect different types of networks and information and will be subject to different sets of regulation. Due to these factors there is also much variation within each market segment; if large organisations are considered there is much variance as to the PACS requirements according to the type of organisation. For example a hospital will have a different range of requirements and legally binding regulations to adhere to than a credit card company and so each will have significantly different PACS requirements.

The nature of PACS products make it so they are similar in many ways to insurance, they serve to mitigate against potential and unknowable problems and so it can be difficult to quantify their value. PACS products are intangible and immaterial and so cannot be seen or held, they protect against threats that may never happen and it can be difficult to quantify when they have successfully thwarted an attack. For these reasons it can be difficult to quantitatively justify spending on; faced with investment

choices between equipment which could boost productivity and PACS it is easier to make a business case for the former.

A further reason why the PACS domain differs from many others in the technology sector is that there are a range of significant barriers to entry into the market. PACS markets are primarily based on trust and so it is crucial that any organization hoping to sell PACS products is demonstrably trustworthy. As mentioned above it is unlikely that organizations will openly advertise the operations of their systems or their security needs because making such information available in the public domain would conceivably put the system at risk by publically demonstrating systemic weaknesses. For this reason tenders which are sought for security products are not necessarily public and instead often operate within relatively closed circles meaning that new entrants to the market can find it difficult to gain a foothold in such processes and participate successfully in tendering processes. In PACS markets trust is a central commodity which is crucial for a number of reasons. There must be trust in the technical competence of the developers as any exploitable weaknesses in a security system can undermine it entirely. There must also be trust in the motives and reputation of a PACS company; with security being mission critical to most organisations it is imperative that any PACS companies have the reputational requirements and can be seen as a trusted broker in the market.

VI. Introducing the IPACSO Framework

Due to the set of characteristics which make PACS different from other business areas of technological development there is an identified need for guidance and assistance which is specifically tailored to this domain. The main output of the IPACSO project is the IPACSO framework which is a knowledge resource for those who are engaged in the field of PACS development. The framework is set up in a manner which offers resources to assist in all stages of development from coming up with and developing an idea to bringing it to market and generating revenue. The framework thus acts as a means of guiding the user through these processes via the use of downloadable templates. These templates offer methodologies which assist in the various stages of the innovation process which include generating and assessing ideas, building a prototype and testing it for usability, market feasibility and a range of other tests relevant to innovation. The IPACSO framework offers resources which are as relevant to small start- ups as they are to large scale organizations. The structure of the framework allows users to drop in at any development stage and find relevant information irrespective of whether it is help coming up with ideas or help bringing a product to market.

Figure 1 the IPACSO Framework

The framework is designed so as to be intuitive and usable with clear divisions in content which guide the target user to the relevant content. The Framework consists of five themes: ideas, product, process, market and people with each button on the framework leading to a raft of resources relevant to the theme. For example under the ideas theme there are resources which can be used to assist in any of the steps in the innovation process. The ideas theme is subdivided into two subthemes of ideation and conceptualization. Ideation is the actual starting point for innovation and broadly speaking involves the creative process of searching for, generating, developing and communicating new ideas. This process involves a number of stages which include scanning the market, defining the problem, generating and capturing ideas and then assessing them to determine whether or not they are worth progressing. For each of the stages of progression there is a host of resources which can guide the user through the process and assist them in each stage of idea generation.

This level of detail is apparent for each of the IPACSO themes as is evident from figure 2 which displays the depth of content for each of the six themes.

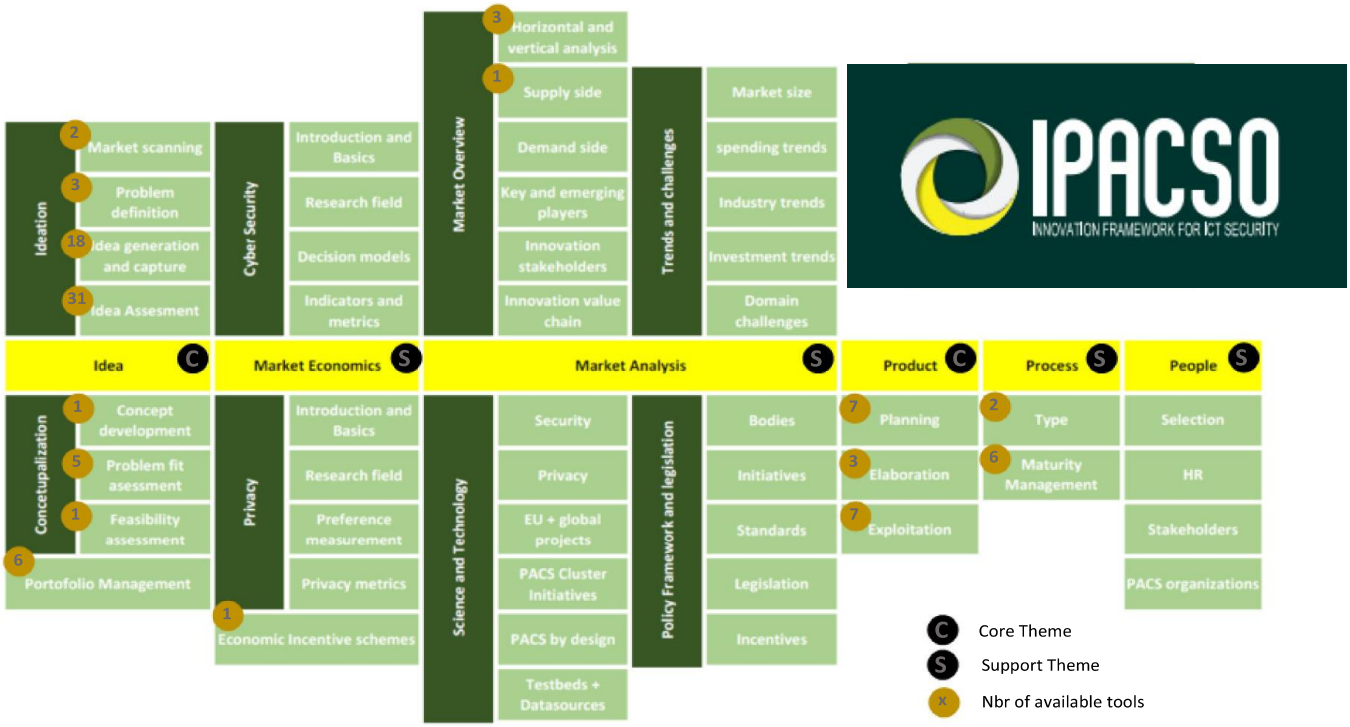

Figure 2

VII. Conclusion

The completed IPACSO framework is a useful resource for those who are involved in innovation in the Privacy and Cyber Security space. As a knowledge resource the framework offers a detailed set of methodologies which can be instrumental in carrying out innovative actions. While the framework is designed for use in the PACS domain many of the resources and methodologies are transferable for use in other fields of activity. There are also however themes which are solely focused on PACS, in particular the market theme which offers deep level analysis of the different aspects of the PACS market as well as PACS economics. This theme offers detailed fine grained analysis of an emerging field which while being important is yet to be the subject of such deep analysis.

The framework has been designed for the benefit of a range of user types, it is not a static or linear 'how to' guide and instead is a resource which users can drop in and out of as their needs see fit.