BUILDING International Cooperation for Trustworthy ICT

User oriented approaches to Trust, Privacy and Security

BIC Discussion Paper **30 August 2012**

Aljosa Pasic[1]

Jim Clarke[2]

[1] AtoS, Spain

[2] Waterford Institute of Technology, Ireland

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

The authors have reflected on the topics related to the BIC Working Group on "user oriented approaches to Trust, Privacy and Security" that have been raised during the BIC project workshop events and summarise in this discussion paper.

The terms "user", "user empowerment" or "user-centricity" have often been used (and misused) in ICT and especially in trust, privacy and security research. There is an obvious difference between corporate user and "domestic" user, their requirements, perception, attitudes and awareness. All over the world, however, this difference is slowly fading as the most of users mix their private and professional life which results in the "transposition" of habits from one milieu to another. Bring your own device (BYOD) is just the latest example of this trend.

The human user perceives everything about an application or service through its human-computer interface (HCI), whether it is the quality of service, its responsiveness, performance, or the security and trustworthiness of the service/system. The identified threats to user interface security include substitution of the real interface by a different service by an attacker or fooling the user into visiting a hoax site with the looks like the real site. Some of the old security challenges, which are still open today, include linking visual trust to computational trust mechanisms and how to make HCIs which are designed for ordinary users and not security professionals, as well as the ability to correctly model systems based on user behaviour. By formalizing unexpected (unusable) behaviour of users, security mechanisms and actions can be included in the design phase to further tighten security.

During the previous events related to international cooperation, either in BIC or in INCO-Trust project, user oriented approaches did not limit only to HCI. In the continuation we revisit some of the topics in trust, privacy and security (TPS) research that include user-centricity with special focus on international dimension.

User orientation and international TPS research

At the BIC workshop held in Amsterdam during July 2011 [1], Dr. Barend Taute from South Africa explained that cyber security awareness is needed for users at all levels. This level of awareness is quite difficult in the developing world due to the lower levels of ICT literacy, and moving in a short time from very low levels of communications to full broadband connectivity. This makes them both more vulnerable and potentially becoming the hosts for cyber attacks. We need to look at creative ways to raise awareness so that the message is retained, e.g. using games and videos. As a matter of fact, "gamification" and serious games are recent trends that could be also applied in TPS research. There are already relevant projects on visualization of e.g. cyber threats, such as those presented at the INCO-Trust workshop in New York, May 2010 [2]. Visualization also solves, at least partially, issues of cognitive bias or language barriers.

In the area of user-centric identity management, Glenn Gran from Sweden presented at the BIC Amsterdam workshop (July 2011) about the GINI-SA project [3]. GINI-SA is based on the assumption that individuals, i.e. citizens, consumers, users of any related services, should be able to manage their own identity data and provide it in an open and flexible manner. On this basis, the user can create and manage its own Individual Digital Identity (INDI) throughout its lifecycle (creation, change, management, revocation etc.). The speaker highlighted the fact that the INDI is verifiable against authoritative registers or data sources that the user selects. In principle, the INDI can be verified in two different ways:

1. the user submits data to the Operator and these are verified against data sources of the users choice; or
2. the user does not submit data to the Operator but points to the data source where the data is located, and registers verified (and verifiable) links to those data.

Obviously, the latter is preferable from a privacy point of view since it removes the need to disclose the identity and send new data to the operator. This also has implications arising from identity and privacy related issues on a global scale, as Alberto Crespo (technical coordinator of the STORK project [4]) from Spain mentioned during BIC Working Groups (WGs) workshop held in Brussels during June 2012 [5]. There are complex relationships spanning across borders and world regional areas. User's trust in e-Relations depends on their effective participation with choices to decide which personal data is to be released under specific conditions which gives the feeling of being in control (digital sovereignty and informational self-determination). The new draft of EU Data Protection Regulation constitutes a good basis in this direction and constitutes a good framework for discussion with other important countries seeking complementarily at policy level: Australia, Canada, United States, Brazil, APEC countries, etc. The STORK project has already proven the feasibility of a de-centralized approach to enable around 30 electronic services portals from 15 different European countries to authenticate securely foreign users presenting their national eIDs (more than 110 different eIDs are supported). The STORK 2.0 project allows also cross-border representation and management of roles, mandates and powers of representation to act on behalf of legal persons. It is also necessary to understand the different meanings of identity in other countries: Japan, China, India, etc… A similar argument has to be made for dealing with cyber attacks / hackers with different behaviours depending upon geography, legislation and

culture. It must be taken into account that some security topics cannot be shared easily and ways of incentivizing this must be discussed. Emerging threats and actors are acting globally, said Sotiris Ioannidis from Greece at the BIC WGs workshop in Brussels (June 2012), and the recent attack clearly showed how our current international cyber security data sharing tools, policies, and infrastructures failed in front of a threat that was designed to focus against a specific user target instead of blindly targeting the entire community.

A very good example of international cooperation is in the area of Mobile Security, suggested by BIC International Advisory Group (IAG) member, Abhishek Sharma from New Delhi, India at the first BIC Annual Forum in November 2011 [6]. Malicious applications are usually free and get on a phone because users voluntarily install them. Once on a handset, the programs steal personal information such as account passwords and logins and send it back to the hacker. Social Networking has seen growth in enormous proportion with the similar growth in the use of smart phone. As fallout, mobile malicious links on social networks are effectively spreading malware. Participants tend to trust such networks and are, thus, willing to click on links that are on "friends'" social networking sites. This brings us back again to topics of user awareness, but also interconnection of (global) issues. The slogan "it is someone's else´s problem" is simply not holding for cyber security. In this sense, the research on user context is also essential since the use and operation of mobile devices, as well as so called Internet of Things, is very context-sensitive.

In the session on trust management in secure software, it was also mentioned that it is not enough for users and entities to be distinguished not only based on their static (certified) identities but also based on their (un)expected, dynamically varying qualities that are relevant to the specific interaction context. Decisions are often based on directly verifiable evidence, but in a highly open system could be also based on indirect evidence reported by other entities. In these cases, the notion of trust becomes central.

Indeed, trust is a very general concept, with different meanings in different communities and cultures. Usually, trust is decided in several dimensions: We can trust a system for correctly functioning (system trust), we can trust a person to act in our behalf (delegation trust), etc. In general, we trust something/someone for a purpose in a given context, and such interpretation is often used in computer science where several trust management models have been developed (initially for modelling access control issues, and more recently to model relationships in social computing). Indeed, in modern pervasive ICT systems, trust is a first-class object that need to be evaluated, analyzed, used, negotiated. Research on models for trust formation, evolution, delegation, dissolution and more specifically social (community based) models of trust should be investigated e.g. how security level prediction of software works based on recommendations from different users in different cultures/communities. Social Computing, for example, enables user-centric, collaborative knowledge sharing to build communities of people using the Internet. Although social computing has been, so far, treated mainly from a negative perspective in TPS research community (e.g. lack of privacy), there are also some positive aspects that should be investigated (e.g. understanding shifts in trust management). Social Computing in emerging countries was a topic animated by Professor Marijke Coetzee, Academy for Computer Science and Software Engineering at the University of Johannesburg, South Africa during the session at BIC workshop in Brussels [5] (June 2012). In Africa, Internet access is not affordable. In addition, low availability of international bandwidth, poorly structured markets, lack of existing infrastructure and low population densities all ensure that mobile is a strong entry point for networks in Africa. In many developing nations, the majority of mobile web users are mobile-only. For example, Egypt has 70%, India has 59 % and South Africa has 57% mobile-only users, who tend to be under 25.

Foresight scenario

In 2020, security management has become a risk-driven process whereby collaboration between international organizations is essential. This includes stakeholders from countries from all over the world, international and EU bodies, civil society organizations, research organizations and the private sector collaborate via e.g. security data compilation, crowd sourcing and information sharing. Since security problems and challenges cannot be solved by a single Member State or organization, user centricity and social aspects are increasingly important. Security mechanisms are desired to be designed adaptable to social change and evolving citizens' security needs, as well as resilient to negative effects of interdependencies in the world (e.g. economy). Public private partnerships are put in place for research & development, but there is also an increasing role for a common internet users' approach. The market also recognizes the high degree of interconnectivity and interdependency with third-country security situation and infrastructures and also seeks a legislative framework that supports international coordination. At the same time, it also seeks the adaptability to local and cultural situations, to user specific context and conditions, as well as societal dynamics including social factors changes, evolving security conditions and the gaps that emerge from these. A significant part of ICT Trust and Security research has developed into a social science discipline addressing the influence of societal factors on security strategies. The public perception of security technologies and their benefits, however, still varies across the globe. Varying levels of maturity of research in user-centric and user-driven security resulted in poor societal awareness in some countries that affect overall cyber security. The potential loss of public trust in institutions and agencies in some countries also affects global ICT trust and security.

Conclusions:

During the user centricity session at the BIC WGs workshop (Brussels, June 2012), it was concluded that designing user centric TPS solutions implies considering the: different kinds of users, different generations of users, different cultures and different societal values. The conclusion is also that we need strong collaboration between different actors and experts from different disciplines (psychologists, sociologists, economists, legal, government, education, ICT and security) to take into account the cultural heritage/history, societal & individual values, psychological characteristics, technology, laws and regulations, etc. For the next BIC workshops, we expect to move forward towards a more precise classification of user-centric research in the specific areas of e.g. identity and privacy, cybersecurity, trust management or mobile computing.

References

[1] BIC Workshop, Amsterdam, July 2012. Online: http://www.bic-trust.eu/events/bic-session-syssec-workshop/.

[2] Clarke, J., Wright, R., et al., INCO-Trust workshop 2010, Online: http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST

[3] GINI-SA project. Online: http://www.gini-sa.eu/

[4] STORK Project. Online: https://www.eid-stork.eu/

[5] BIC WGs Workshop, June 2012, Brussels. Online: http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

[6] BIC IAG Annual Forum 2011. Online: http://www.bic-trust.eu/events/1st-bic-annual-forum/

About the Authors

ALJOSA PASIC current position is Business Development Director in Atos Research & Innovation (ARI), based in Madrid, Spain. He graduated Information Technology at Electro technical Faculty of Technical University Eindhoven, The Netherlands, and has been working for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos) where he occupied different managerial positions. During this period he was participating in more than 50 international research, innovation or consulting projects, mainly related to the areas of information security or e-government. His current interests include Secure Software Engineering (as the chairman of NESSOS industry advisory group), electronic identity and privacy, GRC (governance, risk and compliance) as well as cybersecurity. He is member of EOS (European Organisation for Security) Board of Directors, and collaborates regularly with organisations such as ENISA, IFIP, IARIA, FI-PPP and others.

James Clarke has been working for the Waterford Institute of Technology (WIT) in the Telecommunications Software and Systems Group (TSSG), since February 2005. Prior to joining WIT-TSSG, Mr. Clarke worked at LAKE Communications in Ireland for eight years and Grumman Corporation in the United States for eight years. Since January 2011, Mr. Clarke has been the project coordinator of a European Framework Program 7 Co-ordination action entitled 'BIC ', which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. Previous to this, Mr. Clarke coordinated the successful FP7 INCO-Trust project. More information can be found at **http://www.tssg.org/about/people/james-clarke/.**