Nesnelerin İnterneti Uygulamalarında Kişisel Güvenin Özendirilmesi

Encouraging User-Trust to Internet-of-Things Implementations.

Atila Bostan
Computer Engineering Department
Atılım University
Ankara, Turkey
atila.bostan@atilim.edu.tr

Murat Karakaya
Computer Engineering Department
Atılım University
Ankara, Turkey
murat.karakaya@atilim.edu.tr

Erhan Gökçay
Software Engineering Department
Atılım University
Ankara, Turkey
erhan.gokcay@atilim.edu.tr

***Abstract*— In several scientific studies, it is stated that the foremost challenge in proliferation of internet-of-things (IoT) applications is the security. Trust is more notable than the other security dimensions in the acceptance and spread of IoT. In this study, with an emphasis on the security problem in IoT applications, the effective factors on establishing and flourishing user-trust in IoT applications are reported in a classification and the measures to consolidate trust and willingness-to-take-risk in IoT users are proposed.**

***Index Terms*— Trust in IoT, user-trust to IoT, factors in trust establishment, trust enhancement measures**

***Özet*— Bir çok bilimsel yayında güvenlik nesnelerin interneti'nin (IoT) yaygınlaşmasının önünde en önemli engel olarak belirtilmektedir. Güven ise IoT uygulamalarının yaygunlaşması ve kabüllenilmesi konusunda daha öne çıkan bir boyuttur. Bu çalışmada, IoT uygulamalarındaki güvenlik problemlerine dikkat çekilerek, IoT kullanıcılarında güven artıcı tedbirlerin neler olabileceği bir sınıflandıma ile önerilmektedir.**

***Anahtar Kelimeler*— Nesnelerin internetinde güven, IoT ve kullanıcı güveni, güven oluşmasındaki etmenler, güven artırıcı tedbirler**

I. INTRODUCTİON

The Internet of Things (IoT) is a novel paradigm which models the functional-autonomous interactions among sensors and actuators over a communication infrastructure [1-4]. In this sense of a definition, sensors and actuators attributed as the "things" and the communication infrastructure is generally referred as the "Internet". While the "things" are generally predicted to be small, standalone, typically mobile, intelligent and communicating objects, the communication infrastructure is commonly required to incorporate wireless medium [5-7]. In the scientific literature there is a great deal of publications discussing the future of IoT and the advantages which will be taken by the prospected applications in the field [8-10].

However there are considerable number of studies on the requirements and foundations that were proposed to accelerate the transformation from the internet of people/systems to IoT [8, 11, 12], they fall short to attract adequate scientific attention on the trust problem. Although few authors mentioned the trust problem in anticipated pervasion of IoT, they typically discussed the technical solutions to establish trust between things. They generally do not focus on the trust between human-user and systems/things. Nevertheless, user-to-systems/things-trust constitutes one of the important barriers in front of IoT dissemination. Certainly user trust is not fully a technical topic. It has psychological, social, economic and cultural dimensions as well [13].

By the nature of the IoT, user-to-things/systems trust seems to be the most important psychological barrier, since the lack of user control on interactions among systems [14]. Owner of an IoT capable-object would like to have control on the interactions with his/her object and on the information his/her device is sharing. People often have doubts about the posterior usage of the information s/he is sharing with a peer [15, 16]. Because the device that you are running may be serving for some other people or systems without your knowledge and control. That is to say, your credit card, financial, health, location, shopping information details may be intentionally or unintentionally shared with some third party systems/things by your interaction peer.

In this study we particularly focused on the challenge of trust in pervasion of IoT. In the following section we present the formal definition of trust and the effective factors in establishing a trust relationship with an exclusive view on user-to-things/systems trust. In the third section we emphasized the importance of judicial and supervision dimensions in user-trust establishment. Finally, we propose some measures in order to ease and foster user-trust to systems/things that will take part in materialization of IoT paradigm.

II. DEFİNİTİON AND CLASSıFıCATION OF TRUST

Elastic and pervasive usage of information technology has necessitated the change in security considerations [2, 17]. In information technology domain, security is generally classified in two fields, namely computer and network security and its constructs are determined with the classical security triad (CIA), confidentiality, integrity and availability [18]. Unfortunately, until recently, trust has been considered as a complimentary component in IT security. As the cloud computing and IoT paradigms are maturing and attracting more interest from the industry, the term trust comes into prominence and turns into an essential security foundation. At large, trust is often miss-referred as a term covering the security and privacy. In the dictionaries the term trust is defined as "belief that someone or something is reliable, good, honest, effective, etc." [19], "believing in another person or entity" [20]. In reality trust is a multifaceted fact. It has personal, cultural, economic, social and psychological constituents. Although it is made for social studies, the following definition is found to be more descriptive by the authors for the term trust.

"Trust is a mental state comprising; (1) expectancy, (2) belief, and (3) willingness to take risk"[21]

In this definition the components can be explained as [21];

(1) *expectancy*: the trustor expects some actions to be carried out or viable data/information to be sent/shared from/by the trustee. In example trustor expects a door control mechanism to open the door or a heat sensor to read and share accurate value.

(2) *belief*: the trustor believes that the trustee is capable to conduct the action that s/he declares. In other words, the trustee does not deceive the trustor.

(3) *Willingness to take risk*: with the insights of the belief (item 2 above) to trustee, the trustor is keen to take some amount of risk.

It is important to note, in the given definition of trust, expected behavior from the trustee is not under the trustors' control. However, the troustor strongly believe in that the trustee will perform the expected conduct. Undoubtedly, the experiences gained in the past interactions with the trustee have significant impact on the formation of trust in trustor. Moreover, the effect of range of behaviors that the trustee can take, measures or systems to control the trustee's behavior and compensation mechanisms that will indemnify the trustors' loss in case of a mishandling should not be underestimated.

By the above definition of trust, it is obvious that there is not a single factor effective on establishing and supporting the user-trust. While there are several dynamics that have influence on a user-trust emotion/relationship, user-trust types can be categorized under following classifications depending on the observed primary stimulus [21].

A. Trust by Reputation

Although trust and reputation are strongly related with each other, they are different concepts. Trust is a perception typically between to peers, but reputation is a communal assessment. If an entity has a high reputation rate in the community then it is anticipated that the majority of the people trust to it. A person who is to trust or distrust to an entity would definitely be affected by its reputation rate in the community.

Assessed trust-level has usually an important role in e-commerce and point-to-point file sharing applications as well. By all means, it would have impact on user decision on using an IoT enabled devices or systems.

B. Trust with SLA

Service Level Agreement (SLA) may assist in establishing a legal contract between user and IoT enabled device or system managers/producers. However there are several challenging dimensions in SLA usage. Users do not have the capability to verify whether the service provider properly fulfils the responsibilities in the agreement or not and frequently they do not have the tools and legal rights to test it. There are some proposals suggesting the employment of independent, objective third parties to test these aspects in the SLA and disseminate the results.

The surveys on the current SLA applications in the market have pointed out that the agreements are fully under the control of the service provider and do not have any nonrepudiation mechanisms. Furthermore, when the service provider updates or changes some topics in the SLA, habitually, users are not informed, never requested a new acceptance and in most of the cases they are assumed to have agreed with the new SLA specifications. With the observed state in the market, it is safe to say that SLAs are used just for the declaration of the service specifications by the service managers but falls short to be accepted as a legal agreement yet.

In any case, there are several studies pointing, the existence of an SLA and the specifications covered in help to increase user-preference on the services [22, 23].

C. Trust by Transparency

In this category of the trust, the aim is to inform the user about the inner structure and the ways that the functions are conducted. This is different than SLA. Hence, in SLA, service provider declares the service specifications but in transparency case the declaration or explanation is on how the system runs. It is left to users to assess whether the device/system is reliable, secure, dependable and trustable or not. In the current there is an alliance that practices this category of a user-trust establishment on cloud-services, namely Cloud Security Alliance, Security, Trust and Assurance Registry (CSA-STAR) [24]. In this registry cloud service providers are called to register their services by themselves and users are called to compare the cloud service parameters on this CSA-STAR service. On the other hand, the company named Computer Science Corporation (CSC) announced a request-response protocol called Cloud Trust Protocol (CTP) effective in querying the cloud-service details [25]. In summary, the essential weakness in these above mentioned two trust-by-transparency experiences, CSA-STAR and CSC-CTP, is that the information is presented by the service provider itself; any dishonest provider may deceive the user.

Although above explained two trust-by-transparency examples are in cloud services, they help in discovering the requirements for a trust-by-transparency application in IoT applications as well.

D. Trust by Certification

This category of the trust mechanism is similar to having a third party to verify the specifications of the service and to announce the compliance with a certificate. But the approach is different than the previous trust categories in that, the criteria which the service should conform to is been identified by the certification authority. This kind of certification mechanisms are generally criticized for suppressing the innovation, since the specifications are designated by the certification authority service providers would not focus on discovering novel ways to conduct functions. Other challenging aspect in trust by certification category is cascaded trust problem which can be explained with the question “does the user trust certification authority?”. The other problematic area in trust by certification, may be specific to information technology domain, is that the time need for testing and certification may, in most of the cases, be longer than product market life-time.

In the implementation field there are considerable number of certification examples. The most common certification is in the compliance to international or national standardization body specification where ISO, ISO, IEC, EN can be listed as the prevailing on international arena and TSE is in Turkey.

Trust by certification can assist the user trust building process in IoT implementations but by itself it would not be sufficient. Since the trust is a personal state of mind, whereas it is affected by public opinion. Hence no authority can issue a certificate for an individual assessment. However, with no doubt, certification will assist in verifying the device/systems specifications.

III. The Impact of Advertisement, Sanction Power, Supervision, Assurance and Insurance on User-Trust

In the definition of trust, given in the second section, expectation, belief and willingness to take risk are defined as the main components. Expectation is consequence of or strongly affected by the past experiences in individuals. While the belief is the state of mind in that the trustor is sure on that the trustee will fulfil his/her statement. Definitely, belief is the result of the past experiences as well. It is almost in possible to manipulate these two user-trust components with some external factors. Since the two components are strappingly related with earlier incidents. The measures taken at the present time would have effect on later decisions. One important point is that the expectation and belief assessments are made on the majority or average outcome of the observed influence. Thereby, in order to manipulate the user assessment novel experiences should have big enough effect to alter the mental evaluation. If the number of bad experiences outscores the good ones, it would not be possible to flip the user assessment with some limited number or range of good occurrences. In this regard, key point is that the users are usually not fully aware of the incidents practiced so far, therefore by restraining the propagation of bad incidents and exaggerating the good ones will help in having an impact on user assessment. In other words, it would be possible to alter the user evaluation by increasing the visibility of good experiences while obscuring the bad ones. The fact is that the users make their evaluations with the experiences that they have practiced or been informed of. In parallel with these, advertising the good-and-diverse positive incidents in IoT applications would, certainly, support developing affirmative trust to IoT devices/systems in users.

The third component in the trust is defined as willingness to take risk. However this component is closely related with the belief, it is more susceptible to external factors. Hence, there are several measures in today’s social and financial life to enhance user willingness to take risk. Consider practiced banking systems. Account holders lend their money or economically valued savings to another company or authority with a regulated evidence. Bank customers typically do not hesitate to take the risk or need to evaluate the risk they are taking with this transaction. Certainly, not only the past experiences are affective in this example, there are a number of factors that encourage account holders in taking this economic risk. It needs to note that there is an authority who has sanction power in possession and guaranties the legal rights will not be violated in this economical relation. Commonly, this authority role is played by the governments in practice. Governments announce the regulations and guaranties the rights will be protected in case the other party fails to follow them. By and large governments authorize themselves to inspect and control economic performance and records of the banks by the regulations. Normally, to be on the safe side, governments may cease economic transactions of a bank or take the management over, in case she detects enough number of risky evidences. Because, as being the guarantor, the money in the accounts will be paid back by the government to the account holders. On the other hand, the banks should generally transfer some percent of their current economic wealth under government control as a hypothec or deposit. This guarantee enhances the risk-and-sanction-power management. Thereby the relation between the bank and the government is extended into economic dimensions, is not limited with the law. In addition there are some insurance mechanisms used by banks and/or governments to minimize the economic risks.

The impact of measures, namely advertisements, sanction power, supervision, assurance and insurance mechanisms, on trust establishment and enhancement are undeniable. The question at this point is “is it possible to formulate a trust-enhancement-measures-set that will support the acceptance of IoT applications?”

Unfortunately, as the information technology is becoming popular and gaining wide usage, it is bringing out its own type of problems as well. Therefore, the measures that are successful in some other arena may not succeed in information technology. In the example above; discussed measures, sanction power, supervision, assurance and insurance are effective within the geographical boundaries of a government. But in today's applications it is not abnormal to use a service served in another country or sovereignty. That is to say, it is not that much easy for the trust enhancing measures in other domains to assist user-trust establishment in IoT applications. By the characteristics of information technology, users can not detect or control what is going on in a sensor, an information device or system. Who will be responsible for a mishandling or an undeclared harmful process? Moreover, how to compensate if a damage or loss is observed by means of a malicious component? How can a device or system depend on the information or service provided by other ones that are not under its control or under the control of some other sovereignty? These questions are specific to information systems and constitute the backbone of the trust challenges in upcoming IOT implementations.

IV. Implications and Conclusions

Among the challenges in proliferation of IoT, user-security risks and reservations are deemed as the prominent ones [26]. With the novel applications in the Internet and widespread usage of information systems it is necessary to extent the concept of information security to cover and handle the user-trust establishment as one of the security key components together with Confidentiality, Integrity and Availability triad. It is almost essential for an information system to incorporate and benefit from user-trust establishment and enhancement measures in order to reach certain amount of popularity. This user-trust challenge is obvious and the outstanding one in IoT applications.

User-trust is a complex and multidimensional concept. Although there is no single measure or mechanism, practiced so far, to establish user-trust relationship, there are several measures to stimulate and promote it in users. Observed and proven user-trust enhancement methods in social-life and economic domain should better be transferred into IoT dissemination and acceptance models as well. In that, these measures will help in developing and reinforcing the user-trust to IoT applications.

When the advertisement is excluded, since it is completely a commercial tool, the most essential factor in establishing and supporting user-trust is clearly the sanction power. Without an enforcement power it is almost impossible to have service providers or device producers to take or share some amount of risk. Consider the SLA implementations in the market today. Existence, content, how to publish, user acceptance procedures and evidences are generally not regulated by any power. Current SLA implementations can be considered no further than a goodwill declaration of service providers and device producers. Furthermore the update and renewal procedures for SLA's are still contentious. Assurance, insurance and supervision implementations all depend on an effective enforcement as well.

With the cross-border characteristics of IoT, it needs an international sanction power in action in order to enhance and support user-trust to IoT implementations. Although their focus and scope is different, there are several international regulatory bodies in practice. While these organizations typically lack in possessing complete sanction power, they employ limited enforcement power such as cancellation of a membership. It is possible to list significant number of international bodies in diverse scope and domains, such as political, economic, defense etc. On the other hand, some of political and economic organizations have attempted to regulate information transactions and trade over information systems or networks. There are published acts by United Nations (UN) [27, 28], European Union (EU) [29] and The Organization for Economic Co-operation and Development (OECD) [30, 31] on the regulations of electronic trade, information security and privacy. Definitely, international sanction power would assist user-trust establishment and enhancement in IoT implementations.

Driven by an international sanction power and acts, assurance, insurance and supervision would be more effective in the field of IoT on user-trust formation. Commonly in the information technology domain, data damages and losses are not restorable. But compensation measures may be utilized for recovery in order to encourage user to trust on IoT implementations.

References

[1] Yau, Stephen S. "Plenary Panel: Security of IoT." In Software Quality, Reliability and Security-Companion (QRS-C), 2015 IEEE International Conference on, pp. xxii-xxii. IEEE, 2015.

[2] Jones, Lauren K. The insecurity of things: How to manage the internet of things. Diss. UTICA COLLEGE, 2015.

[3] Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Vol. 3. IEEE, 2012.

[4] Li, Xiong, Zhou Xuan, and Liu Wen. "Research on the architecture of trusted security system based on the Internet of things." Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on. Vol. 2. IEEE, 2011.

[5] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29.7 (2013): 1645-1660.

[6] Kaukalias, Tasos, and Periklis Chatzimisios. "Internet of Things (IoT).", (2015).

[7] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[8] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29.7 (2013): 1645-1660.

[9] Ning, Huansheng, and Ziou Wang. "Future internet of things architecture: like mankind neural system or social organization framework?." IEEE Communications Letters 15.4 (2011): 461-463.

[10] Barnaghi, Payam, et al. "Semantics for the Internet of Things: early progress and back to the future." International Journal on Semantic Web and Information Systems (IJSWIS) 8.1 (2012): 1-21.

[11] Zhu, Qian, et al. "Iot gateway: Bridgingwireless sensor networks into internet of things." Embedded and Ubiquitous Computing

(EUC), 2010 IEEE/IFIP 8th International Conference on. IEEE, 2010.

[12] He, Wu, Gongjun Yan, and Li Da Xu. "Developing vehicular data cloud services in the IoT environment." IEEE Transactions on Industrial Informatics 10.2 (2014): 1587-1595.

[13] Gefen, David, and Detmar W. Straub. "Managing user trust in B2C e-services." E-service Journal 2.2 (2003): 7-24.

[14] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134.

[15] Sicari, Sabrina, et al. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.

[16] Hochleitner, Christina, et al. "Making devices trustworthy: security and trust feedback in the internet of things." Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK. 2012.

[17] Xu, Teng, James B. Wendt, and Miodrag Potkonjak. "Security of IoT systems: Design challenges and opportunities." Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design. IEEE Press, 2014.

[18] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed., Marcia Horton, Ed. New York, America: Prentice Hall, 2011.

[19] Definition of “Trust” in the dictionary of Merriam-Webster, , retrieved from http://www.merriam-webster.com/dictionary/trust on Aug. 03, 2016.

[20] Turkish Language Institution, Common Turkish Dictionary, retrieved from http://www.tdk.gov.tr/index.php?option=com_gts &view=gts on Aug. 03, 2016

[21] Huang, Jingwei, and David Nicol. "A formal-semantics-based calculus of trust." IEEE Internet Computing 14.5 (2010): 38-46.

[22] Chenkang, Wu, Zhu Yonghua, and S. Pan. "The SLA evaluation model for cloud computing." Proc. of the International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013). 2013.

[23] Kalepu, Sravanthi, Shonali Krishnaswamy, and Seng Wai Loke. , “Reputation= f (user ranking, compliance, verity)”, Web Services, 2004. Proceedings. IEEE International Conference on. IEEE, 2004.

[24] Cloud Security Alliance, Security, Trust & Assurance Registry, retrieved from https://cloudsecurityalliance.org/star/ on Aug. 04, 2016.

[25] Computer Science Corporation, Cloud Trust Protocol, retrieved from http://www.csc.com/cloud/insights/57785-cloudtrust_protocol_and_cloud_transparency on Aug. 04, 2016.

[26] Tankard, Colin. "The security issues of the Internet of Things." Computer Fraud & Security 2015.9 (2015): 11-14.

[27] International Telecommunication Union, International Telecommunication Regulations, Final Acts of The World Administrative Telegraph and Telephone Conference Melbourne, 1988, retrieved from www.itu.int/ITU-T/itr/files/ITR-e.doc on Aug. 04, 2016

[28] United Nations. General Assembly, Resolution 65/230, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, A/RES/65/230, New York: United Nations, 1 April 2011.

[29] European Union, Convention on Cybercrime, Budapest, November 23, 2001. Retrieved from http://www.coe.int/en/web/ conventions/full-list/-/conventions/ treaty/185 on Aug 04, 2016.

[30] Organisation for Economic Co-operation and Development. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD Publishing, 2002.

[31] The Organisation for Economic Co-operation and Development (OECD), OECD Policy Guidance on Online Identity Theft, retrieved from http://www.oecd.org/sti/consumer/40879136.pdf on Aug. 04, 2016.