A position paper for W3C Workshop on the Web of Things – Enablers and services for an open Web of Devices. 25–26 June 2014, Berlin, Germany

Trust-based Discovery for Web of Things Markets

Marko Vujasinovic, Alessio Gugliotta, Stefania Galizia
m.vujasinovic@innova-eu.net, a.gugliotta@innova-eu.net, s.galizia@innova-eu.net
INNOVA S.p.A.
Tecnopolo Tiburtina, Via G. Peroni, 386, 00132 Rome, Italy

Abstract. *The Web of Things marketplaces will be online markets for publishing and trading the Web of Things, Data, and Service APIs. On the Web of Things marketplaces, users will be searching for products that are trustworthy to them, in their specific application contexts, and especially in those contexts dealing with sensitive personal information or safety-critical operations. In this paper we briefly discuss our position regarding the trust management for the Web of Things marketplaces and stress out what is needed to enable the trust-based discovery of products and services on the Web of Things.*

Web of Things Marketplace and Trust

Internet of Things (IoT) opens up enormous potential for delivering value-added services in a various of application domains such as Smart Home, Smart Cities, Smart Retail, Smart Manufacturing or Smart Healthcare. It is predicted there will be over 20 billions of devices (i.e. objects) connected to the Internet by 2020 [1] . To unleash the potential and boost adoption, the IoT evolves into the Web of Things, which has foundation in the well-accepted and widespread Web technologies. The Web of Things is expected to open up a number of possibilities for developers and end-users.

No doubt, sooner or latter there will emerge online marketplaces for publishing, trading, and composing data and services of the Web of Things. For example, COMPOSE EU research project [2] is expected to provide an open marketplace for the Web of Things. Existing marketplaces for the IoT, such as Deutsche Telecom IoT Marketplace[1], may evolve into the Web of Things marketplaces.

Establishing the Web of Things marketplace is not a trivial effort. One of the challenges, as we see, is the management of trust and trust negotiation for the Web of Things marketplaces. Dealing with the trust is even more challenging in open marketplaces, where for example a central authority does not control the quality of the deployed products.

In a short, we define trust as an evaluated expectation a user[2] of a object (and associated service) has about the object/service behavior, before using the object/service in a specific context. To us, the trust and trust negotiation play a central role in the discovery of objects and services in the Web of Things marketplaces. The trust negotiation is a process of evaluating whether two participants, e.g. a service user and service provider, can engage into a trustworthy relationship, according to their respective trust policies and trust guarantees. In the Web of Things marketplaces, users will be searching (discovering) products that are trustworthy to them in user-specific application contexts. And especially in those contexts dealing with sensitive personal information or safety-critical operations. The users have specific trust policies (trust expectations) and look for products with trust guarantees

[1] https://marketplace.m2m.telekom.com

[2] The user may be an end-user, developer, a service, an object, or application, etc.

that satisfy the trust expectations.

How users will be, or should be, discovering trustworthy products in the Web of Things markets? Would it be sufficient enough, or not, to set up a reputation-based trust mechanism that traditional e-commerce marketplaces use? Can we reuse existing e-commerce and mobile apps marketplaces? Are there existing languages suitable for describing the Web of Things trust policies and trust guarantees?

Traditional marketplaces such as e-commerce marketplaces (e.g., Amazon or eBay) use reputation-based trust mechanisms that accumulate reviews and ratings about products and sellers, to help to the users to evaluate the trustworthiness of products and sellers. To us, the Web of Things marketplace differs from the traditional marketplaces, in the terms of trust management and trust negotiation. The reputation-based trust will be beneficial in the Web of Things marketplace, however, might not be not sufficient per se.

First of all, in the traditional marketplaces the trust relationship is unidirectional, in most cases. The unidirectional trust relationship means that users search for trustworthy products, not vice-versa (Products on the Amazon market do not care about the reputation of consumers). In the Web of Things marketplace, the trust relationship is bidirectional, in most cases. That is, objects and services may have trust expectation towards their users (not only end-users, but also other objects and services), and vice-versa. For example, a user trusts to a sensor that has a good reputation in the terms of the quality of data, while the sensor trusts only to users who authenticated using a security token and who have a good financial reputation e.g. paying services on time.

Then, the reputation seem to be the main trust indicator in the traditional marketplaces. On another side, in the Web of Things marketplace trust expectations could envelop additional indicators such as security and privacy guarantees, quality of a service or device, or quality of the data, and may be more detailed. The details may include expectations about specific security protocols (e.g. SSL or TSL for encryption), key exchange mechanisms (e.g. AES_128_GCM or AES_258_GCM), specific certificate provider (e.g. VeriSign or Go Daddy), and so on.

Our main statement is the trust is a subjective, multifaceted, and context-dependent concept. In the Web of Things scenarios, trust indicators and their level of details may be different to different users, may change in different contexts, or may be different in the same context for different users, given to users past experiences and skills. For an example, one might trust to the objects and services of a particular provider, regardless of accumulated users' ratings, while other might trust to the objects and services that have good ratings, regardless of who provider is. Or, one might trust if there are no known or unknown risks and threats associated, or trust only if a centralized authority has issued a trust certificate.

Therefore, our position is the Web of Things marketplace should adequately address the trust multifacetedness and context-dependency, to establish appropriate trust management and trust negotiation mechanisms to enable the evaluation of trustworthiness of the Web of Things products during their discovery and composition.

What is needed for the trust-based discovery? Where we are?

(1) Semantic vocabularies and semantic annotation. There should be formal means e.g. a formal semantic vocabularies, to semantically state (context)-specific trust expectations such as '*I trust to services having a good reputation and being popular*' or '*I trust to services having high reputation,* *ensuring data confidentiality using TSL/SSL protocol, but better if TSL protocol, and having authorization in means of tokens. Security is more relevant than reputation'.* The service providers should have the same formal means to semantically state the trust guarantees (trust characteristics) of their respective objects and services - e.g. '*Communication security and data confidentiality is ensured by encrypted TSL communication and OAuth2 authorization and authentication mechanisms'.* With a common language with formal semantics, the matching between the trust expectations and trust guarantees will likely have higher recall and precision.

Yet, there is no a semantic vocabulary suitable for annotating or describing trust expectations and guarantees in a common, standardized way, and with sufficient expressivity. However, there are certain semantic vocabularies and ontologies, in other domains, that can be reused. For example, W3C Semantic Sensor Network (SSN) Ontology [3] provides concepts such as Accuracy, Detection Limit, Drift, Frequency, Latency, Resolution, Response Time, and Sensitivity, that might be relevant in a perception of the trust towards the sensing devices. (E.g., *I trust to sensors that provide the data frequently and have a good sensitivity.*) USDL-Sec [4] vocabulary for describing service security aspects seems to be suitable for describing the security guarantees, such as authorization or confidentiality, in different levels of security details. Then, there are trust ontologies present in the literature (e.g. [5], [6]), however, those are conceptual models of the trust relationship. They capture notions such as trustor, trustee, trust relation, or trust typology (reputation-based, evidence-based, policy-based), but no details for stating trust expectations and guarantees. Quality of Service ontologies, such is WS-QoSOnto [7], previously built for annotating quality aspects of semantic web services can be reused to describe quality of service-based trust expectations and guarantees.

In a scope of the COMPOSE project, we develop a trust ontology (illustrated in Figure 1) and aim to integrated it with SSN, USDL-Sec, and other ontologies relevant for the trust considerations in the Web of Things. Among others, the ontology captures notions of TrustRelationship, TrustingParticipant, TrustorParticipant, TrustCriteria (trust expectations), TrustProfile (trust guarantees), TrustAttribute, Measurable TrustAttribute and NonMeasurable TrustAttribute.

(2) Semantic Matchers. Discovery of the trustworthy products is a semantic matching or semantic search task. The trust expectations of a user are semantically matched with the trust guarantees of a Web of Thing product. The trust expectations and guarantees may match exactly, almost (be subsumed), or be disjoint. If the trust guarantees match the trust expectations exactly or almost, the product classifies as trustworthy. If disjoint, the product classifies as distrusted. With the trust expectations and trust guarantees expressions commonalized and formalized using semantic vocabularies and machine-processable semantic annotations, the trust-based discovery engines will be capable to do better job, thanks to the semantics.

There are many existing semantic matchers and semantic search engines available. The existing ones can be reused to develop a special-purpose engine for matching the trust expectations with trust guarantees. In particular, we are developing a trust evaluation module on the top of a trust goal classification approach introduced in [8], which was designed for the trust-based discovery of semantic web services. In that approach, trust guarantees of the web services are matched against trust expectations by a classification technique to identify services that fit (classify) into the requirement. In addition to the classification, we now introduce the measure of similarity between the trust expectations and trust guarantees. The measure is a value between 0 and 1, and represents the trust level.

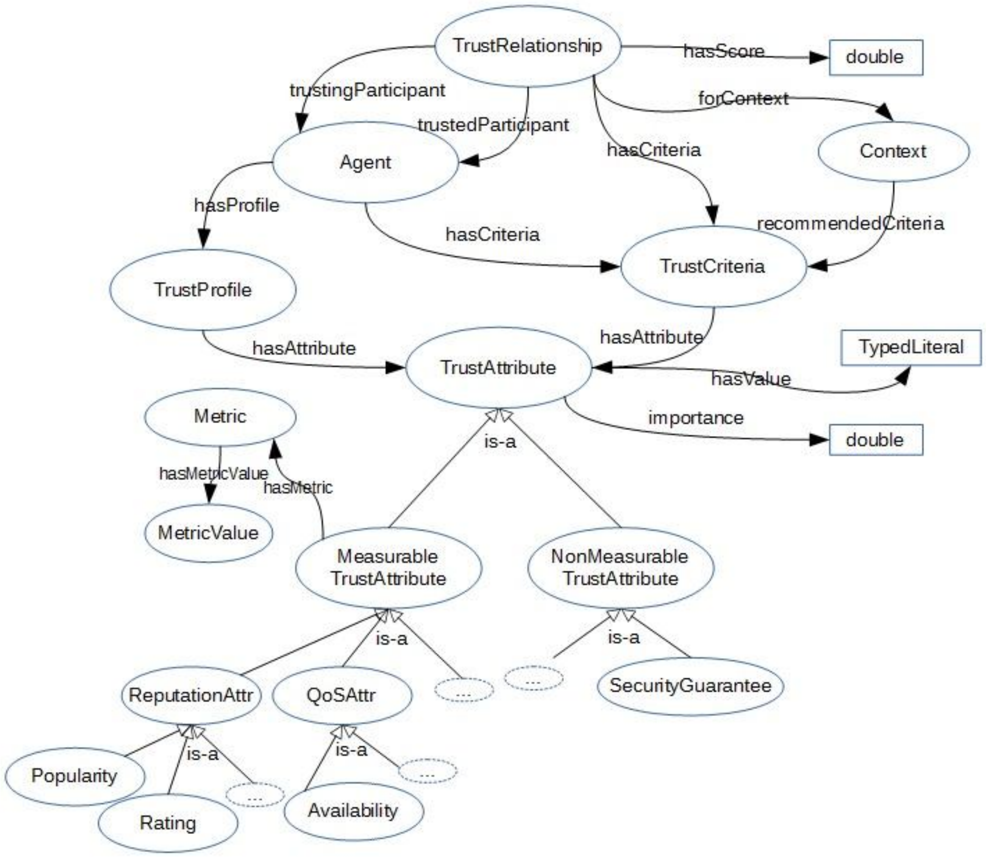

Figure 1 Trust ontology

(3) Monitors. Importantly, the trust guarantees should be constantly or periodically verified and monitored, by users and/or by established central authorities, in order to help to increase accuracy of the trust evaluation. The monitoring is collecting the evidence for the claimed trust guarantees. The monitoring of trust guarantees requires sophisticated mechanisms over the Internet with possible involvement of trusted third parties for detecting, isolating and limiting the negative behaviors. It is a challenge on its own.

The evidence of trust guarantees may be coming from different sources including users reviews and ratings, from various estimations such could be an estimation of popularity, then from third party services assessing the quality of services and data (e.g. detection of accuracy of a wind sensor by comparing the data with the data of other wind sensors in the same area) or performing static code analysis to detect possible negative effects of the execution, etc.

Conclusion

Marketplaces for the Web of Things should be approached differently than traditional marketplaces, because of the importance of the trust management and trust negotiation in the discovery and composition of the Web of Things objects, services, and applications. Trust is a contextual-dependent, multifaceted, and bidirectional concept. Marketplaces for the Web of Things need solutions that fully take into account such trust concept. Customers and providers on the Web of Things marketplace need a *standardized* formal vocabulary or language to formally annotate or state their trust expectations and guarantees as well as the trust expectations and guarantees of their products and services, in specific application context. In a scope of COMPOSE project, we are currently designing and prototyping a software tool/platform that leverages the formal descriptions to compute trust and includes a semantic matchmaker and (multiple and customizable) monitoring tools.

References

[1] Infographic: The Internet of Things By Jamie Cifuentes, May 5, 2013.

[2] Mandler, Benny, et al. "COMPOSE--A Journey from the Internet of Things to the Internet of Services." Advanced Information Networking and Applications Workshops, 27th International Conference on. IEEE, 2013.

[3] Compton, Michael, et al. "The SSN ontology of the W3C semantic sensor network incubator group." Web Semantics: Science, Services and Agents on the World Wide Web 17 (2012): 25-32.

[4] Unified Service Description Language - Security.
http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.USDL-SEC

[5] Anantharam, Pramod, et al. "Trust model for semantic sensor and social networks: A preliminary report." Aerospace and Electronics Conference (NAECON), Proceedings of the IEEE 2010 National. IEEE, 2010.

[6] Chang, Elizabeth, et al. "Trust ontologies for e-service environments." International Journal of Intelligent Systems 22.5 (2007): 519-545.

[7] Tran, Vuong Xuan. "WS-QoSOnto: a QoS ontology for web services." Service-Oriented System Engineering, 2008. SOSE'08. IEEE International Symposium on. IEEE, 2008.

[8] Galizia, Stefania, Gugliotta, Alession and J. Domingue. "A trust based methodology for web service selection". International Conference on Semantic Computing, IEEE, 2007.