Ideas for a Trust Indicator in the Internet of Things

Wolfgang Leister and Trenton Schulz
Norsk Regnesentral
Oslo, Norway
Email: wolfgang.leister@nr.no, trenton.schulz@nr.no

***Abstract*—The Internet of Things will connect many different devices. In order to realise this, users must be willing to trust the devices and communication that happens automatically. We explore the different meanings of trust and strategies that can be used to determine if something is trustworthy and propose a model for trust that takes into account people, devices, and their connections. The model uses à priori and à posteriori trust to give an indication of how much a user can trust or distrust the information provided by things. This trust indicator can inform users' decisions on whether or not to use a device or service.**

Keywords*—*Trust*; *trust model*; *Internet of Things.

I. Introduction

The *Internet of Things* (IoT) refers to uniquely identifiable objects (things) and their virtual representations in an Internet-like structure. This term was first used in 1999 by Ashton [1]. Other definitions of IoT have appeared as technology progresses. A *thing* is a real or virtual object, e.g., a device or a web service, offering one or more services. Since implementations of the IoT integrate many things belonging to different actors used for various purposes, we must question to what degree we can trust these things both as a individual entities and as a federation of entities.

Even when reading the value from one isolated thing we can identify challenges regarding trust. For instance, when looking at a watch we need to consider whether we can trust the time it displays: the watch might show the wrong time for some reason. We also might be observed looking at our watch, which might breach our privacy since observers might consider us impatient or bored. This is in line with Watzlawick's first axiom that suggests that it is impossible not to communicate [2]; as a consequence, humans always reveal some information about themselves. These problems are compounded when extending trust issues to the IoT where we are dealing with many different things. It would, therefore, be helpful to have a mechanism to measure how and when to trust things on the IoT and indicate this to the user; users could then take countermeasures if needed. These measures can be based on an applicable model and theory of trust. This would allow users of IoT services to consider their actions and reduce the costs of checking trustworthiness through other frameworks.

Our work is inspired by the use of the IoT in health care where monitoring systems using various sensors and devices form a communication internetwork. These devices also need to communicate with a health care infrastructure. In health care systems, the requirements for privacy, security, integrity and availability are especially high. We have previously analysed the security model in patient monitoring systems [3] and suggested a framework for implementing sensor networks in health care [4]. We intend to extend this work with a sustainable trust model.

We posit that trust in the IoT is not transparent enough for the user. Our contribution consists of ideas for a trust model and metrics for the IoT including both channels, things, humans, and services. In order to reduce threats regarding security, privacy, and functionality when using the IoT, we distinguish between dimensions of à priori and à posteriori trust, as well as computational, technical, and behavioural trust. The developed trust model and its metrics will be used to *a*) give indications at to which security mechanisms to employ in the implementations of systems; *b*) give indications to the users at any time of how much they can trust a system, allowing users the opportunity to consider using devices in the IoT, or to use different parameters or settings; and *c*) annotate data retrieved from a system with trust values derived from the trust model.

In this paper, we first define trust and trust models in Section II before presenting our model and metrics of trust in Section III. Finally, we provide an outlook in Section IV.

II. About Trust

For the purposes of this note, we define trust as the *degree of reliance a person or thing puts in a separate thing's behaviour in a specific context.* For the IoT, trust is defined as the expectation a thing will do what it claims without bringing harm to the user [5]. This includes the perception of being secure, e.g., resilient to attacks, and that the user *a*) knows who is being spoken to, *b*) knows what is going on, *c*) feels in control of what is going on, and *d*) understands the distributed services that are involved [6].

Trust also implies that users receive information that they believe to be true and of a certain quality and timeliness. The received information can be trustworthy (usable immediately), trustworthy with alteration (usable after alteration), or untrustworthy (worthless). In the absence of trust, the user needs to consider whether it might be beneficial to abstain from using certain services of the IoT.

A. Trust

Trust is defined in several disciplines, such as sociology, psychology, ethics, economics, management, and computer

 ISBN: 978-1-61208-225-7

science for different purposes and application areas. We distinguish between different types of trust, such as *a*) behavioural trust: expectations to the behaviour of a participant, often based on a game-theoretical approach; *b*) computational trust: the human notion of trust in the digital world, i.e., trust between agents that do not have their own agenda, such as nodes in a sensor network; and *c*) technical trust: establishing and evaluating a trust chain between devices in the IoT by means of information security technologies.

In the literature, we find a variety of definitions and categorisation of aspects of trust, such as in the review paper by Lamsal [7]. Most definitions that cover multiple disciplines define trust as the *willingness of a trustor to be vulnerable to actions of the trustee* [8] or refinements of this. See also the work by Rousseau et al. [9] and the first sections by Colquitt et al. [10]. Romano [11] defines trust as the *subjective assessment of another's influence in terms of the extent of one's perception about the quality and significance of another's impact over one's outcome in a given situation, such that one's expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation.*

Sabater and Sierra [12] review computational trust and reputation models. Gambetta [13] defines trust in terms of mathematics as *a particular level of the subjective probability with which an agent assesses that another agent . . . will perform a particular action. . . .* Here, trust can be quantified from *distrust*, via *no trust* to *blind trust*. Trust is only relevant if a possibility of distrust, betrayal, exit, or defection exists.

Literature using technical trust, as in the work by Fritsch et al. [6] identify the most important trust information for end users in the IoT as *a*) recognition or identification of the federation of things one connects to, *b*) ability to identify the owner, controller, or legally responsible entity behind a federation, and *c*) transparency concerning functionality, and security and privacy assurance information. We posit that this view only represents a part of the trust requirements in the IoT, and prefer the more multi-disciplinary definitions.

Cloud computing is another area where trust is a necessity. This includes security and privacy, availability, and conformance to laws from different areas (i.e., those using the cloud have strict rules about data access that the service provider must follow). Khan and Malluhi [14] detail these issues and point out that service-level agreements (SLA's) can help solve these problems. While this is true, we feel that the number of different things in the IoT will make it problematic to establish a SLA with each actor. An alternate method is necessary.

Marsh [15] formalises trust as a computational concept. He cites Deutsch [16] with the utility theory and 19 hypotheses about trust. The first hypothesis states that an individual makes a trusting choice when $Va^{+} \times S.P.^{+} > Va^{-} \times S.P.^{-} + K$, where Va^{+} and Va^{-} are positive and negative valence or utility, $S.P.^{+}$ and $S.P.^{-}$ are the corresponding subjective probabilities, and K is the security level for this individual.

Marsh presents an example heuristic formalism for trust where agents, knowledge, importance, and utility are used to define *basic trust* T_x, *general trust* $T_x(y)$, and *situational trust* $T_x(y, \alpha)$, all defined in the range $[-1, +1)$ [15, p. 59]. This notation can be used in a temporally-indexed notation. Further, Marsh [15, p. 68] outlines the cooperation threshold where the trust $T_x(y, \alpha)$ must be higher so that agent x cooperates with agent y in situation α. The cooperation threshold, in turn, is dependent on perceived risk, perceived competence, and importance; see also Coleman [17] and Gambetta [13].

B. Trust Strategies and Agent Dispositions

A trust indicator also needs to take into account the agent dispositions, such as optimism, pessimism, pragmatism, and realism [15, p. 65], in order to give suitable hints on the current trust situation. O'Hara et al. [18] lists five trust strategies in the semantic web that we can apply to things in the IoT: *1*) *optimistic strategy*: assume all agents are trustworthy unless proven otherwise, *2*) *pessimistic strategy*: assume all agents are untrustworthy unless proven otherwise, *3*) *centralised strategy*: trust information is managed by and obtained from centralised institutions, *4*) *investigative strategy*: check and evaluate agents to determine their trustworthiness, and *5*) *transitive strategy*: analyse networks of agents to determine their trustworthiness.

While all these strategies can be used in different situations in the IoT [6], the model and trust indicator that we describe here use the transitive strategy or the centralised strategy. We can trivially model the optimistic or pessimistic with any model. Our model requires other actors to properly model an investigative strategy.

C. Trust Models for the IoT

Gligor and Wing [19] present a theory of trust in networks of humans and computers that consists of elements of computational trust and behavioural trust. They present a simple communication model of entities and channels. The participants of this model can be human users, network hosts, or network applications; both honest users and machines, as well as intruders, are allowed. For human users, behavioural trust following a game-theoretical approach is used.

For computational trust, Gligor and Wing assume secure communication channels, so that they only need to consider whether a receiver (trustor) can trust the sender (trustee). In order to trust the received information, the value of information must be higher than the costs of trusting. Achieving trust can be done by verifying whether the sender can be trusted, e.g., by second opinions. However, such a second opinion might never arrive. Therefore, the receiver might be forced to use information without validation in some situations. Gligor and Wing use the concept of *isolation* that can be achieved by direct receiver verification, second opinion, etc. Trustworthiness, correctness, and the act of trusting are part of their framework.

While secure channels can be assumed for some applications, e.g., applications on the web, we cannot assume this for all networks in the IoT. Some types of sensor networks have restrictions with respect to resources, e.g., battery capacity

 ISBN: 978-1-61208-225-7

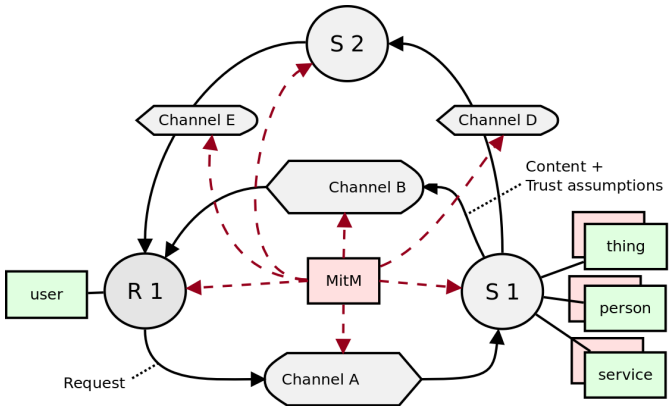

Fig. 1. Trust diagram of actors, the communication channels used, and a potential man in the middle for a scenario with one device, R_1, of the observer and two things, S_1 and S_2. S_2 offers a secondary channel from S_1 to R_1.

and power consumption, so that secure channels cannot be assumed. Therefore, we need to include the channels in our model of trust for the IoT.

III. Model and Metrics of Trust

In the IoT, we assume peers in a network that communicate with each other; peers can have roles as senders, receivers, or both. In this network, we have three types of actors: *a*) the things, devices, or services in the IoT; *b*) the persons with an intent or interest in the exchanged data; and *c*) the communication channels between things and between things and persons. Fig. 1 presents these actors and their relationships.

A. Characteristics of Actors in the IoT

Since we are interested in the specifics of the IoT, we disregard behavioural trust, and, instead, refer to the work by Gligor and Wing [19]. However, depending on who is controlling a thing, it can have its role dictated by its owner, such as being an honest node, a spy node, or otherwise compromised. Note also that things are trust-wise in a federation with the person controlling them.

To define the trust for things and channels we need to look at the possible threats that can arise from the use of the IoT. As outlined by Leister et al. [3], threats in health care applications include attacks on confidentiality, privacy, integrity, availability and non-repudiation. While these threats can be countered by technical measures, this is not always possible or practical.

For the channels, for direct communication and, indirectly, via other things, we can either *a*) use a secure channel, e.g, through cryptography and authentication, *b*) use channels with certain technical measures to counter some threats; or *c*) use unsecured channels. The threats imposed by a man-in-the-middle (MitM) attack include eavesdropping, modification of data (integrity), and lost data, e.g., through routing attacks. We can also model technical failures as a MitM attack with a random behaviour. All these are side-effects of using the IoT that users do not expect and thus breach trust.

Things need to have an identity in order to be assigned a trust value. Also services in the IoT need to be identifiable for this purpose. Consider services as a federation of things where the owner of a service needs to be identifiable; attacks on things can cause the same threats as for channels. Additionally, there might be deviations in data due to setup errors or for other technical reasons. For example, a clock that can experience a drift when not set regularly or a thermometer that is accurate but is affected by unwanted environmental influences. Another cause could be known biased actors, such as certain weather forecasts.

When presenting a too low trust value for a thing or channel to a user, the user can *a*) not send information, *b*) not request a value, *c*) employ technical measures to secure the value, *d*) discard a received value, *e*) delay usage or store a received value (and attached information) without using it until more evidence is collected, or *f*) adjust a received value by a suitable offset, e.g., from past experience.

B. A Trust Model for the IoT

As defined by Marsh [15], we use trust in the range $[-1, +1]$, the value 1 indicating complete (blind) trust[1], the value -1 indicating complete distrust, and the value 0 indicating indecision (i.e., more information is needed).

Let the observer be R_1. For the observer R_1, we define the *à priori trust* $-1 \leq \tau^{\triangleright}_{S_1} \leq 1$ as the trust before sending a message to an object; this trust consists of the trust of the Channel A and of the object (thing) T_1:

$$\tau^{\triangleright}_{S_1} = \tau^{\triangleright}_{A} \cdot \tau^{\triangleright}_{T_1}$$

The à priori trust can be used to decide whether to send the message, or not, with the help of a threshold value. Note that in most cases the trust value of both the onwards and the return path need to be considered since most requests will result in a sequence of responses from a node to the receiver.

For the observer R_1 we define the *à posteriori trust* $-1 \leq \tau^{\triangleleft}_{S_1} \leq 1$ as the trust after receiving a message from an object; this trust consists of the trust of the Channel B and of the object (thing) T_1:

$$\tau^{\triangleleft}_{S_1} = \tau^{\triangleleft}_{B} \cdot \tau^{\triangleleft}_{T_1}$$

The à posteriori trust is the trust value to decide whether a message can be used. The à posteriori trust comes with an adjustment function $a^{\triangleleft}_{S_1}$ that can be applied to the received message. The adjustment function contains components from Channel B and the object T_1. The à posteriori trust is the trust value *after* having applied the adjustment function to the value $v^{\triangleleft}_{S_1}$. In order to make a decision what to do with a value, R_1 receives and stores the tuple $(\tau^{\triangleleft}_{S_1}, a^{\triangleleft}_{S_1}, v^{\triangleleft}_{S_1})$.

When using these metrics to indicate trust, we need to look into *a*) the factor of time that temporally indexed notations need to be applied and *b*) the transitive behaviour. For the transitive behaviour, we need to study how a chain of nodes and channels behave as long as $\tau > 0$. Note that in the case of distrust, i.e., $\tau < 0$, we cannot set up a useful assumption

[1]The term *blind trust* poses philosophical problems; therefore, most authors set the trust range to $[-1, +1)$. For practical reasons, initially, we allow a trust value of exactly 1.

 ISBN: 978-1-61208-225-7

for the trust of the entire chain. Using technical measures to counter security and privacy threats we can obtain $\tau < 0$ while still the threat exists that a result will not arrive at the receiver due to some attack on the availability. Therefore, the trust estimates should be split up into separate values for security, privacy, availability, and so on.

IV. Outlook

We presented our ideas towards a formalism that tries to describe trust in the IoT. Issues regarding chains of nodes and channels and composition of nodes and channels to complex networks are challenges to such a framework. Another challenge could be perceived trust as a relation to the Quality of Experience (QoE) a user experiences from a service (e.g., distrusting a thing because the result arrived late or that the result is sometimes inaccurate). We envisage that trust values from measurements and user assessments can be established in a similar way as described by Leister et al. [20] for measured and perceived video quality (i.e., QoS vs. QoE).

On the practical side, another challenge to investigate are ways the trust indicator can best be presented to users in an understandable way. These could include a traffic light metaphor or a more elaborate dashboard where trust values and suggestions to the user are presented. There must be multiple ways to present this as some things may not have a display. We are confident that a formalism will help to create indicators that can guide users of services and data in the IoT, and that they can experience the benefits of the IoT rather than suffering from bogus services and unwanted information leaks.

Acknowledgements

This research is funded in part by the EU project FP7-258360 uTRUSTit: *Usable Trust in the Internet of Things*.

References

[1] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 22 July 2009, accessed March 9, 2012. [Online]. Available: http://www.rfidjournal.com/article/view/4986

[2] P. Watzlawick, J. H. Beavin, and M. D. D. Jackson, *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes*. W. W. Norton & Company, Mar. 1967.

[3] W. Leister, T. Fretland, and I. Balasingham, "Security and authentication architecture using MPEG-21 for wireless patient monitoring systems," *International Journal on Advances in Security*, vol. 2, no. 1, pp. 16–29, 2009.

[4] W. Leister, T. Schulz, A. Lie, K. Grythe, and I. Balasingham, "Quality of service, adaptation, and security provisioning in wireless patient monitoring systems," in *Biomedical Engineering, Trends in Electronics, Communications and Software*, A. N. Laskovski, Ed. Intech, 2011, ch. 36, pp. 711–736.

[5] I. N. Zoltán Hornak, D. Petró, J. Schrammel, P. Wolkerstorfer, L. Ellensohn, A. Geven, K. Kristjansdottir, L. Fritsch, T. Schulz, H. Abie, F. Pürzel, and V. Wittstock, "D.3.1 uTRUSTit Technology and Standard Report," uTRUSTit - Usable Trust in the Internet of Things, EU project deliverable D3.1, 2010.

[6] L. Fritsch, A.-K. Groven, and T. Schulz, "On the Internet of Things, Trust is Relative," in *Privacy, Trust and Interaction in the Internet of Things*, ser. Lectures in Computer Science, vol. 7040. Springer, 2011, pp. 263–269, in press.

[7] P. Lamsal, "Understanding trust and security," Online-Reference, October 2001, accessed March 9, 2012. [Online]. Available: http://www.cs.helsinki.fi/u/lamsal/asgn/trust/UnderstandingTrustAndSecurity.pdf

[8] R. C. Mayer, J. H. Davis, and F. Schoorman, "An Integrative Model of Organizational Trust," *Academy of Management Review*, vol. 20(3), pp. 709–734, 1995.

[9] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393–404, 1998.

[10] J. A. Colquitt, B. A. Scott, and J. A. LePine, "Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance." *J Appl Psychol*, vol. 92, no. 4, pp. 909–27, 2007.

[11] D. M. Romano, "The nature of trust: Conceptual and operational clarification," Ph.D. dissertation, Louisiana State University and Agricultural and Mechanical College, 2003.

[12] J. Sabater and C. Sierra, "Review on computational trust and reputation models," *Artif. Intell. Rev.*, vol. 24, pp. 33–60, September 2005.

[13] D. Gambetta, "Can We Trust Trust?" in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. University of Oxford, 2000, ch. 13, pp. 213–237.

[14] K. M. Khan and Q. M. Malluhi, "Establishing trust in cloud computing," *IT Professional*, vol. 12, no. 5, pp. 20–27, 2010.

[15] S. P. Marsh, "Formalising trust as a computational concept," Ph.D. dissertation, University of Stirling, April 1994.

[16] M. Deutsch, *The Resolution of Conflict*. New Haven and London: Yale University Press, 1973.

[17] J. S. Coleman, *The Foundations of Social Theory*. The Belknap Press of the University of Harvard, 1990.

[18] K. O'Hara, H. Alani, Y. Kalfoglou, and N. Shadbolt, "Trust strategies for the semantic web," in *ISWC 3rd International Workshop on Trust, Security, and Reputation on the Semantic Web*, 2004.

[19] V. Gligor and J. M. Wing, "Towards a theory of trust in networks of humans and computers," in *Proc. 19th International Workshop on Security Protocols*, ser. LNCS. Springer Verlag, March 28-30 2011.

[20] W. Leister, S. Boudko, and T. H. Røssvoll, "Adaptive video streaming through estimation of subjective video quality," *The International Journal on Advances in Systems and Measurements*, vol. 4, no. 1, pp. 109–121, 2011.

 ISBN: 978-1-61208-225-7