Security and trust challenges in the area of the Internet of Things

SUMMARY

DánielPetró, GyörgyVesztergombi

SEARCH-LAB Security Evaluation Analysis and Research Laboratory Ltd., Budafokiút 91., 1117 Budapest, Hungary

daniel.petro@search-lab.hu, gyorgy.vesztergombi@search-lab.hu

Abstract

The concept behind the Internet of Things (IoT) has shed light to new aspects of trust and security.Being a young trend, yet complex and manifold, the IoT poses a variety of trust and security issues – some of which are yet unseen – which are to be understood and effectively handled in order to establish its social acceptance in the future. In this paper, we present a framework that is generally applicable on present and future use cases of the IoT technologies accessible for various user types.

Keywords

Trust, Security, Internet of Things

Introduction

In the last two decades, technology has developed rapidly and is currently evolving towards interconnected systems. The *Internet of Things* is already becoming part of our life, while emerging new security and trust issues either remain unsolved or the solutions catch up with difficulty and delay. To effectively cope with these issues, it is essential to settle the basis of new approaches to human trust in the context of IoT, and its relation to the real security status of the user during everyday usage of the networked devices. The paper gives a short introduction of the examined IoT context, which is followed by the elaboration of the related security and trust issues that we identified. We then presenta possible way to face these challenges, which forms a part of the work ofthe uTRUSTit (Usable Trust in the Internet of Things) FP7 project. Finally we conclude with the outcomes of our investigation and provide the foreseen ways of further research work.

What is the IoT?

Being an unfolding technology, the definition of the Internet of Things is also forming. Today, this term mostly refers to physical objects (things) that are interconnected through their virtual representations in a (global) Internet-like structure, using such communication protocols as RFID or Bluetooth(see e.g.[1],[2]). This concept already gave birth to various use cases, among which *smart home* and *smart office*(see e.g. [3]) are probably the most commonly known scenarios.

Defining trust in the IoT

Trust, in its common understanding, is a human feeling affecting decision and behavior. Presence of trust provides the feeling of comfort, willingness to cooperate (or act as required), potential carelessness, while lack of trust leads to cautiousness, feeling insecurity, refusal to cooperate. Among the many different definitions and contexts of trust (see a compilation in [4]) we now narrow our focus to the human perception of trust with regards to the IoT. Our work in [4] assigned several terms to trust, e.g. a *subject* toward which trust is experienced, or *measures* through which the degree of trust can be assessed in a certain situation (such a measure can be money). [4]and[5] conclude that generally, trust is understood as an expectation of a subject's certain behavior or that a related event will (or will not) happen.

Defining security in the IoT

We also extended the concept of trust with the IoT user's experience of their security. In the definition of IoT security, we set off from the concept of a general system of interconnected devices.

Our overall approach has been to keep a balance between the real security status of the system and the user's perceived security (and therefore their trust)

when using the system. The objective of this approach is to prevent the user from overly trusting the system if it is insecure (which often leads to sensitive data falling in unauthorized hands), but building trust in the user if the system is secure. By keeping such a balance between trust and security, we expect a better social acceptance of the IoT and reduced business loss of IoT service providers in the long term.

Security and trust challenges inside the IoT

To reach the above goal, we created a generally applicable trust framework for the IoT. One pillar of this frameworkis structuring the IoT into so-called federations (see in later sections); another is providing personalized feedback to the user about the security status of IoT. The feedback enables the user to experience the valid amount of perceived trust towards a system/device/operation and thus make informed decisions on proceeding with or rejecting certain operations. In this paper, we concentrate on the first aspect.

Building the IoT security model

When analyzing the security and trust relationships inside the IoT (see [11]), one is dealing with federations of IoT devices. Federations, similar to private clouds described in [8], are formed by a group of linked devices, connected into a sub-network. Networks are delimited by a trust boundary, formed by sharing a circle of trust, or by linking to a chain of trust. Network formation may be based on a facility, on a person or by physical proximity of devices. Some of the resources inside the network may be shared among many users with loosely overlapping or distinctive trust roots.Trust boundaries are not hard and fixed barriers, but are subject to change as devices leave or enter the federation. Prime examples of federations are smart homes and smart offices. These federations correspond to a facility and organizations, or to a person owning most of the devices, as in the case of the smart home. Furthermore a device may be part of several independent federations.

Security and trust issues arise from two different perspectives, from the subject and object viewpoint. From the viewpoint of the federation, internal assets must be protected from outside threats. Common security objectives in this case are confidentiality, integrity and availability. The other viewpoint is that of a device that federates with an existing federation. Aside from protecting internal assets privacy considerations become a concern. A further worry is resource profiling, where the accommodating federation is in a position to profile the resource usage of the newly joined actor, thereby possibly violating privacy.

Another set of problems relates to delegation operations inside the IoT. Actors may invite other participants to join a federation, or access federation asset. For instance, if a homeowner association holds an e-voting event, participants have the option to delegate their voting rights to a trusted proxy. The necessity may arise if a homeowner is abroad and cannot attend the event. Another example is the management of a smart multimedia center. Family members enjoy a higher clearance level than guests. Nevertheless a guest may be granted a higher clearance level by a family member, in order to control playback and share music.

Analysis of the uTRUSTit working scenarios produced a set of common features that appeared in most scenarios. The scenarios worked out in the document [10] envision the possible applications of the IoT that may be of future. In order to analyze these systems, some architectural assumptions were made about them. We needed to use an architectural model that is general and non-restrictive enough for our investigations.

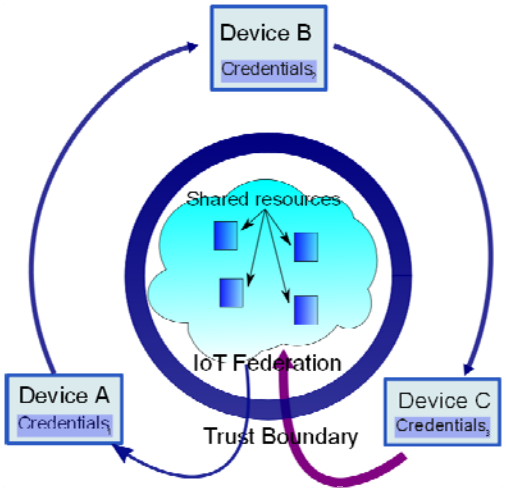

Figure 1 – Security model of IoT
(the inferior numbers show the way of delegated credentials)

Our primary concern was with security and trust, so the presented model only described the IoT from a security and trust perspective. We tried to make the security assumptions explicit that were implicit in the scenarios of [10].The basic actors and interactions were abstracted and formulated into one model.We further assumed that security mechanisms deployed in the IoT will follow and extend classic security design principles and best practices as described for example in [9] and [6].

Analysis and Countermeasures

In order to evaluate security risks following methodology was used:

The analysis was based on the IoT scenarios created in a previous work-phase. The scenarios were designed to feature rich interactions and exemplify typical and relevant IoT use cases. Building on this data the first phase consisted on a threat analysis. A detailed report of the threat analysis can be found in [11].

In the threat analysis phase we first identified and collected the assets (software, hardware and data) of the system using a systematic approach; assuring that security of the assets was the basis for further analysis.

Security objectives (requirements) were assigned to assets using the CIA (Confidentiality, Integrity, and Availability) model:

Confidentiality means that the asset (or information about the asset) must only be accessible by authorized parties.

Integrity means that the asset must not be modifiable; in case of software, it must not deviate from normal operation.

Availability means that the asset must be ready for use whenever it is needed.

Not all objectives are important for all assets. Where appropriate other security requirements – missing from the CIA model – were pointed out (e.g.: non-repudiation[1]).

We began the threat modeling process by defining misuse cases [7]– negative scenarios describing the ways the system should not work. We examined how the standard use cases defined in the [10]document could be subverted, endangering the system's assets. We then collected the threats discovered during the modeling process. From the threat descriptions we elaborated associated control objectives, focusing on those that required user interaction.

Insights gained from the analysis were built into the prototypes that were used to test user reactions under laboratory conditions.A virtual reality reconstruction of the scenarios was created to gauge user responses within smart home and smart office settings. The experiment was conducted with a number of participants and the results were used to improve the trust feedback aspect of the test system.

The security and trust feedback functionality was embodied by an IoT component which was named the Trust Feedback Toolkit (TFT). This is a central component inside the IoT federation that aggregates security and trust input from the federation components and provides feedback to the user. The TFT is aware of the global federation context and helps translate technical security feedback into intelligible messages tailored to specific users. A detailed description of the Trust Feedback Toolkit is presented in [12].

Conclusion and Future Work

In our investigations we tried to mitigate security risks and enhance the user's trust perceptions by constructing a dedicated Trust Feedback Toolkit component. The TFT consolidates signals, inputs and security metrics obtained by federation components. Based upon incoming data the TFT handles communication with the user. In this way security and trust information reaches the user from only one dedicated source, thereby providing a consistent,

[1]Non-repudiation refers to a state where the maker of a statement or document will not be able to deny the validity of it.

uniform interface. User evaluation tests point in the general direction that such an arrangement helps foster trust and increased user satisfaction.

Further results are to be expected from continuation of user tests. Previous tests were carried out in a virtual environment using immersive imaging and simulation technologies. In the next phase tests will be carried out using "real world scenarios", were the actual scenarios will berealized with physical devices.An actual TFT server will be deployed inside the scenario to test its functionality and evaluate its impact on the user experience.

Acknowledgements

This work was partially funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 258360 (uTRUSTit; see http://www.utrustit.eu/).

References

[1] Wikipedia – Internet of Things (http://en.wikipedia.org/wiki/Internet_of_Things)

[2] H. Sundmaeker, P. Guillemin, P Friess, S. Woelfflé–*Cerp-IoT: Vision and Challenges for Realising the Internet of Things*, 2010 (http://www.grifs-project.eu/data/File/CERP-IoT%20SRA_IoT_v11.pdf)

[3] Wikipedia – Smart Home (Home automation) (http://en.wikipedia.org/wiki/Smart_home)

[4] Z. Hornák, I. Nyilas, D. Petró, J. Schrammel, P. Wolkerstorfer, L. Ellensohn, A. Geven, K. Kristjansdottir, L. Fritsch, T. Schultz, H. Abie, F. Pürzel, V. Wittstock, –*Technology and Standard Report*(uTRUSTit project), 2010

[5] S. Döbelt, C. Hochleitner, M. Busch – *Defining, Understanding, Explaining TRUST within the uTRUSTitProject*, 2012

[6] Software Assurance Maturity Model, http://www.opensamm.org/downloads/SAMM-1.0-en_US.pdf,http://www.opensamm.org/downloads/SAMM-1.0-en_US.pdf

[7] G. Sindre, A. L. Opdahl – 'Capturing Security Requirements through Misuse Cases', NIK 2001, November 2001, http://www.nik.no/2001/21-sindre.pdf

[8] Rich Mogull, Ed. – *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,* Cloud Security Alliance, 2009 ,https://cloudsecurityalliance.org/csaguide.pdf

[9] Jerome H. Saltzer, and Michael D. Schroeder – *The Protection of Information in Computer Systems*, Proceedings of the IEEE 63, 9 pages 1278-1308, 1975

[10] T. Schulz, L. Fritsch, I.Solheim, I.Tjøstheim, D.Petró, H.Arfwedson, N. Back - *Definition of User Scenarios* (uTRUSTit Deliverable D2.2)

[11] D.Petró, Gy.Vesztergombi– *Threat Analysis* (uTRUSTit Deliverable D3.2)

[12] D.Petró, Gy. Vesztergombi – *Security Specification for the IoT* (uTRUSTit Deliverable D3.3)