Security versus Trust requirements: similarities and differences

Florian Gasteiger, Eve Hunter

Abstract If the goal of a system is to serve the users well both trust and security must be incorporated into the design process. The process for including security and trust comes in the form of requirements engineering. However understanding how to formulate the necessary requirements to ensure this, requires a review of topical literature. In this paper we present a comparison of security and trust requirements by examining previous scholarly work.

1 Introduction

When engineering a system, security has been nearly unquestionably deemed essential. Trust, also a vital part of the success and usability of a program, application, or system lacks a universal understanding of how to include it in burgeoning projects. Trust is defined by Merriam-Webster dictionary as the "assured reliance on the character, ability, strength, or truth of someone or something."[1] Given that people are (almost) always essential parts of any system, the effectiveness of said system must be trusted by users and employees alike. Security, defined as "the state of being protected or safe from harm," [2] is a key component of establishing trust within a system. Both security and trust are necessary for a system that wants to attract and maintain a loyal user base.
This paper gives an overview of security, trust, and the requirements for both of them in system engineering, then briefly compares and contrasts their properties in the process of implementation, otherwise known as requirement engineering.

2 Definitions and Background

2.1 Security and Trust

The following sections will examine security and trust outside of their role in requirements engineering in order to provide a sense of the intricacies of the development process. Evolving from common perceptions of security and trust to well-defined aspects of a system remains a difficult task even for experienced analysts.

2.1.1 Security

The Common Criteria, or ISO/IEC 15408 is a guide for the assessment of security in Information Technology. By providing a unified set of definitions Common Criteria provides a substantial base for security professionals to discuss security without any vocabulary mismatches. In the ISO/IEC 15408 there are six terms that include the word "security." The document defines a secure state as the "state in which the TSF [Target of Evaluation Security Functionality] data are consistent and the TSF continues correct enforcement of the SFRs [Security Functionality Requirements]."[3]

2.1.2 Trust

When establishing trust in a system, there is a plethora of considerations to take into account. On the one hand, trust is extremely context-driven. For example while a patient's trust in the medical system extents to the doctor as well as his or her subordinates, in a different situation the patient may be less willing to allow for the extension of their trust. This means that understanding the relationships between actors is a necessary prerequisite to understanding the system in which trust is needed.

Below is a definition of trust in the most general sense. It provides a basis from which to examine related aspects of the study of trust.

Definition:
Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X) [4]

Yew [5] extended the idea of trust to incorporate computational methods. This is a particularly challenging task due to the subjective nature of trust; the researcher must develop quantitative methods to assess qualitative criteria. Assessing trust concretely in systems will be addressed in the following section.

2.2 Security and Trust Requirements

During the software engineering process, a set of desires are communicated to a team who is from thenceforth tasked with designing the desired system. In order for the team to get the most complete picture of what the project manager is looking for, it is important to separate the things needed to obtain this vision. Common terminology is essential for any group of people looking to produce the best product possible. Requirements engineering as a whole is defined by van Lamsweerde as “concerned with the identification of goals to be achieved by the envisioned system.“[6] Yet requirements can be classified in a myriad of ways – from how the goals are stated to the types of goals necessary for the given system. The following sections summarize the ways of defining both security and trust requirements.

2.2.1 Security Requirements

Security requirements are often confused with two separate things: security goals and security controls. The two quotes below illustrate security requirements in relation to other aspects of the system.

> *“Security requirements capture security goals in more detail.”* [7]

The term “security goal” refers to whether or not an aspect of the system meets the standards of confidentiality, integrity, and availability (CIA). Security requirements take these assessments one step further and explain what exactly must be secured in order to maintain CIA security-levels.

> *“Security requirements are implemented into security controls.”* [8]

This quote highlights the dividing line between requirement and controls. Security controls come in the form of design or architectural features; they are very concrete, and implementable such as passwords, key swipe access, etc. Security requirements require a much more complex assessment of what the assets of the system are. Security requirements will address essential steps to protect business values or assets. Furthermore, security requirements can be a basis from which a company decides whether or not to utilize cutting edge technologies to meet their security requirements. As long as the business assets and values remain the same, the security requirements are timeless.[9]

2.2.2 Trust Requirements

Whereas security requirements have a discrete definition and role in the system engineering process, trust requirements are much less readily defined.
The consideration of trust as a requirement for a system has only recently been stud-

ied at length. Although Omer et al. clearly state that security is one dimension of trust [10, p.5], when deciding on the key factors for a system, the nebulousness of trust discourages project managers from considering it in depth. Currently there are only a few publications recommending methods for including trust management in modelling languages such as Tropos and Secure UML.
Giorgini et al. in particular propose an addition to Tropos (which by design indicates dependencies when present) to incorporate the idea of trust dependencies. In their words, “a functional dependency can lead to the delegation of tasks, whereas a trust dependency can lead to the delegation of permissions.“[11] This is important because when it comes to an issue such as access to personal data, the level of trust determines whether or not an actor can pass on their trust from the data owner as a form of delegation.[12] And unlike most forms of permission, trust is a social relationship that is difficult to regulate in the form of a digital credential and the like.
Managing trust requirements effectively means that it is essential to look at all aspects of an organization including relationships and management policies. This can be incredibly arduous for especially a large organization. Even trust requirements that come down to access control can be difficult to implement because a person may trust one individual but perhaps not their subordinate. [13]

2.3 Comparing Security and Trust Requirements

There is no one definition for either security or trust requirements. The following comparisons are based on the key description of security requirements. In this sense, trust requirements will be taken as steps (though not detailed, specific steps) to reach the ideal depth of trust relationships between entities of a system.
Below, security and trust requirements are compared and contrasted based on their ease of applicability.

2.3.1 Similarities

Designing a system for trust and designing a system for security have varying levels of complexities but they are both essential for tailoring effective relationships with the process or data owners.

1. *Both security and trust requirements should be implemented as soon as possible.*

   Due to lack of security training among system engineers, security is often added in as an afterthought. The same is true of trust. Considering (and implementing) both security and trust requirements from the beginning of the system analysis process creates a more reliable and secure system that can maintain users or clients without damaging its reputation, or worse, harming the users.

2. *Security and trust requirements influence each other.*

   Users are unlikely to use a system that they deem untrustworthy; to ensure that a user can trust the underlying processes or entities of a system, they must feel secure in doing so.

2.3.2 Differences

1. *Security requirements are more clearly defined than trust requirements.*

   The term “security requirement” is used to denote a very specific method of securing a system. [14] Trust, on the other hand, tends to be categorized in the broader category of ”trust management.“ Rather than trust requirements being easily identifiable, they are often couched in broader trust goals and complex inter- or intra-organizational relationships.

2. *Trust requirements require a much more complex analysis.*
   Because trust is based on a number of factors, it can be much trickier to determine the goals and situational picture of a system. Individual users in particular base their trust decisions on past history – this is a factor that cannot be standardized; even so, quantification of impressions would be an arduous and complex task.[12]

3 Conclusion

Trust and security are intertwined, some even see trust as a subset of security; because without trust there is no sense of security. This article has examined each requirement separately but they are best combined.

Despite discrepancies in general awareness of security and trust requirements, they are both vital parts of software development and even broader system planning. If, at the commencement of system planning, these two things are taken into consideration, systems as a whole will yield better results for managers, save future resources that may be used to implement them after initial development, and will serve the system’s clientéle much more reliably and effectively.

References

1. Merriam-Webster Dictionary: *Trust*, www.merriam-webster.com/dictionary/trust
2. Merriam-Webster Dictionary: *Security*, http://www.merriam-webster.com/dictionary/security
3. International Organization for Standardization: *ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security*, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341
4. Olmedilla D., Rana O.F., Matthews B., Nejdl W.: *Security and trust issues in semantic grids.* In: Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies, 2005
5. Chern Har Yew: *Architecture Supporting Computational Trust Formation* Western Ontario - Electronic Thesis and Dissertation Repository. Paper 86, 2011
6. Axel van Lamsweerde: *Requirements Engineering in the Year 00: A Research Perspective*, IEEE Computer Society Press, 2000
7. Fabian, Benjamin, et al.: *A Comparison Of Security Requirements Engineering Methods*, Requirements Engineering 15.1; 2010: pp.:7-40.
8. Altuhhov, O., Matulevičius, R., Naved, A.: *An Extension of Business Process Model and Notation for Security Risk Management*, IGI Global, 2015: pp.: 897-919
9. Donald G. Firesmith and Firesmith Consulting: *Engineering Security Requirements*, Journal of Object Technology, 2003: pp.: 53-68
10. Daniel Olmedilla, Omer F. Rana, Brian Matthews, Wolfgang Nejdl: *Security and Trust Issues in Semantic Grids*, Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany; 2006
11. Paolo Giorgini and Fabio Massacci and John Mylopoulos and Nicola Zannone: *Requirements Engineering Meets Trust Management - Model, Methodology, and Reasoning*, Springer Verlag, 2004: pp.: 176-190
12. Haley, C., Laney, R., Moffett, J., & Nuseibeh, B.: *Using trust assumptions with security requirements*, Requirements Engineering, 11(2); 2006: pp.:138-151.
13. Sara Jones, Marc Wilikens, Philip Morris, Marcelo Masera: *Trust Requirements in E-Business: A Conceptional Framework*, University of Hertfordshire; Oct. 1999
14. Massacci, F., Mylopoulos, J. & Zannone, N.: *Security Requirements Engineering: The SI* Modeling Language and the Secure Tropos Methodology*, Springer Berlin Heidelberg, 2010: pp.: 147-174