An Analysis of Software Quality Attributes and Their Contribution to Trustworthiness

Nazila Gol Mohammadi[1], Sachar Paulus[2], Mohamed Bishr[1], Andreas Metzger[1], Holger Koennecke[2], Sandro Hartenstein[2] and Klaus Pohl[1]

[1]*Paluno-The Ruhr Institute for Software Technology, Duisburg-Essen University, 45127 Essen, Essen, Germany*

[2]*Department of Economics, Brandenburg University of Applied Sciences, 14770 Brandenburg an der Havel, Germany*

Keywords: Trust, Trustworthiness, Trustworthiness Attributes (TA), Socio-Technical Systems (STS), Information and Communication Technologies (ICT).

Abstract: Whether a software, app, service or infrastructure is trustworthy represents a key success factor for its use and adoption by organizations and end-users. The notion of trustworthiness, though, is actually subject to individual interpretation, e.g. organizations require confidence about how their business critical data is handled whereas end-users may be more concerned about the usability. These concerns manifest as trustworthiness requirements towards modern apps and services. Understanding which Software Quality Attributes (SQA) foster trustworthiness thus becomes an increasingly important piece of knowledge for successful software development. To this end, this paper provides a first attempt to identify SQA, which contribute to trustworthiness. Based on a survey of the literature, we provide a structured overview on SQA and their contribution to trustworthiness. We also identify potential gaps with respect to attributes whose relationship to trustworthiness is understudied such as e.g. accessibility, level of service, etc. Further, we observe that most of the literature studies trustworthiness from a security perspective while there exist limited contributions in studying the social aspects of trustworthiness in computing. We expect this work to contribute to a better understanding of which attributes and characteristics of a software system should be considered to build trustworthy systems.

1 INTRODUCTION

Trust underlies almost every social and economic relation and is regarded as the glue that binds society together. Humans, processes and organisations, with different perceptions and goals, increasingly interact via the Internet. In such online settings, gaining and establishing trust relations within socio-economic systems becomes more difficult where interactions are mediated by technology rather than face-to-face communication and/or collaboration making it more difficult to infer trust through social clues. The question this paper deals with is about the software system attributes that can foster trustworthiness in and within Socio-Technical Systems (STS) mediated through online networks. STS are increasingly being part of our daily life in form of apps, Internet-based applications, services, etc. The people involved in online businesses, though, have generally limited information about each other and about the STS supporting their online and offline transactions. There are several reports indicating an increasing number of victims of cyber-crime leading to massive deterioration of trustworthiness in current STS. Therefore, individuals and organizations are more concerned about trusting and placing confidence on current STS and show interest in how to handle their business critical data. Consequently, trustworthiness of a software, app, service or infrastructure becomes a key factor for their wider use and adoption by organizations and end-users. Accordingly, as in any modern society, trust and trustworthiness in such systems play a larger role in reducing the complexity of transactions and result in positive impacts on the economy and social aspects of modern life.

ICT trends such as cloud computing, apps, services, smart devices and Future Internet facilitate the growing of STS and their integration in our daily life. They have enabled significant improvements in efficiency and cost reduction. However, the

Gol Mohammadi N., Paulus S., Bishr M., Metzger A., Koennecke H., Hartenstein S. and Pohl K..
An Analysis of Software Quality Attributes and Their Contribution to Trustworthiness .
DOI: 10.5220/0004502705420552
In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science* (CloudSecGov-2013), pages 542-552
ISBN: 978-989-8565-52-5

distributed nature and the use of the Internet as a medium for communication causes trustworthiness concerns. Because of the difficulty of preventing malicious attacks or the misuse of critical information, users might not trust these systems. Examples of STS are: healthcare systems/patient monitoring systems, market places and social networks. Users of these modern applications are concerned about their trustworthiness. Thus, STS need to be made trustworthy to mitigate the risks and trust concerns of their users. Understanding which Software Quality Attributes (SQA) and properties foster trustworthiness is thus increasingly important for successful trustworthy software and system development.

There are limited contributions that approach the trust and trustworthiness issues described from angles other than security. However, security is not the only aspect of trustworthiness. Most existing approaches have assumed that one-dimensional properties of services lead to trustworthiness of such services, and even to trust in it by users, such as a certification (e.g. Common Criteria), the presence of certain technologies (encryption), or the use of certain methodologies (SSE-CMM) (Pazos-Revilla and Siraj, 2008), (CMMISM, 2002), (Huang et al., 2008). In this work, we assume that such a one-dimensional approach will not work, and instead consider a multitude of attributes.

With a literature review, we attempt to identify and capture the attributes so far known as contributing to trustworthiness. These attributes have been classified to major quality categories. This paper provides a structured and comprehensive overview on SQA and their contribution to trustworthiness.

The reminder of this paper is structured as follows:
Section 2 provides a brief overview on the basics and background and Section 3 describes the classification of Trustworthiness Attributes (TA). The grouping of the attributes under a category is done according to the observed common underlying concepts. Section 4 discusses related work and gives recommendations, and Section 5 presents conclusions and future work.

2 FUNDAMENTALS AND BACKGROUND

This section introduces the trust from different perspectives and moves on to define the meaning of trustworthiness in this paper. We then identify the relation between trust and trustworthiness. Finally, we discuss how they relate to STS.

2.1 Trust and Trustworthiness: A Discussion

From a sociological perspective two converging branches of sociology characterize the field. The first focus is on the societal whole, its complex structures and social systems. The second focus is on societal members, individual actions and relations between them. This second strand brought to attention trust as an element emerging from individual interactions and based on individual actions (Sztompka, 1999). In this second branch, individuals rely on people engaged in representative activities (Dahrendorf, 2005), in other words, they rely on those who act on our behalf in matters of economy, politics, government and science. Such dependence implies high degrees of trust on part of the individual. Extending this view to Information Systems (IS), we also rely on systems to run daily activities across large swaths of our society. They can be referred to as STS which are comprised of networks of individuals and IS organized around certain tasks. The delegation of tasks to such STS by individuals or organizations entails establishing some level of trust in such systems by the individuals. Consequently, it can be said that the trustworthiness of such systems is an important quality that needs to be fostered and even engineered in the fabric of these systems to maintain high levels of trust within society.

One of the problems occurring when studying a notion like trust is that everyone experiences trust. Hence, a personal view of what trust actually is (Golembiewski and McConkie, 1975). This is the first intuitive explanation of why trust has multiple and varying definitions. A second explanation is the fact that there are multiple definitions of trust simply because there are that many types of trust (Deutsch, 1962), (Shapiro, 1987).

In (Sztompka, 1999) trust is defined as “a bet about the future contingent actions of others”. The components of this definition are belief and commitment. There is a belief that placing trust in a person or a system will lead to a good outcome and then a commitment to actually place trust and take an action to use this system based on this belief. E.g. when a user decides to use a system on the web, then he is confident that it will meet his expectations. In (Luhmann, 1979) a different outlook on trust is presented. Luhmann explains that “further increases

in complexity call for new mechanisms for the reduction of complexity" (Luhmann, 1979) and suggests that trust is a more effective mechanism for this purpose. Given this view we can assert that increasing trust in STS has the effect of reducing uncertainty and complexity both online and offline in our society and this in turn has positive social and economic impacts.

In this paper, we stick to the earlier mentioned definition of trust in (Sztompka, 1999) while extending it to include STS: "*a bet about the future contingent actions of others be they individuals or groups of individuals, or entire STS*".

Trustworthiness on the other hand has been used sometimes as a synonym for security and sometimes for dependability. Trustworthiness in general is a broad-spectrum term with notions including reliability, security, performance, and user experience as parts of trustworthiness (Mei et al., 2012).

However, given our chosen definition of trust we argue that while trust is an act carried out by a person, trustworthiness is a quality of the system that has the potential to influence the trust this person has in the system in a positive way. When studying attributes conducive to trustworthiness it is thus important to identify two types of attributes:

a. Trustworthiness attributes that have the potential to give the trustor a *perception* of the system's trustworthiness prior to consenting to use the system. We call these "Perceptive TA" (PTA)
b. Trustworthiness attributes that *ensure* the trusted individual or system will act according to well defined criteria as expected by the trustor. We call these "Operational TA" (OTA).

Trustworthiness can then be defined as the intersection of PTA and OTA so that a system always gives trustworthiness cues to the trustor and then reinforces these cues by honouring the placed trust. In this paper, we are not concerned with classifying the studied attributes according to the two categories above and will leave this to future work.

2.2 Socio-Technical Systems

STS are systems that include humans, organization and their IS. There are interactions between these autonomous participants, between human and organizations as a social and software system as technical interactions (Sommerville, 2011). These social and technical components strongly influence each other. Our focus is on distributed applications that enable connection and communication of people via the Internet. Therefore, here, STS are applications, services, and platforms where technology and human behaviour are mutually dependent (OPTET Consortium, 2012). Thus, in STS people or organizations may communicate or collaborate with other people and organizations that emanate from interactions mediated by technology rather than face-to-face communication or collaboration (Whitworth, 2009).

Internet-based applications are becoming an ever increasing part of our daily life. We use them every day for e-commerce, information access, and in our social life where we have inter-personal interactions. Humans, processes and organisations, as entities of these systems with different perceptions and goals, interact via the Internet. Section 1 explained our research focus and understanding of STS. The development and management of STS is challenging. Hence, it has been considered a complex system (Sommerville, 2011).

2.3 Trustworthiness in Socio-Technical Systems

As we discussed in the last section, STS are to be made trustworthy to merit the trust of their users. It has been defined as assurance that the system will perform as expected (Avizienis et al., 2004). Furthermore, trustworthiness of software has been defined as worthy of being trusted to fulfil requirements which may be needed for a particular software component, application, system (Li et al., 2009). Trustworthiness is a potentially central aspect of distributed STS. We argue it as a multi-dimensional construct combining specific attributes, properties and characteristics.

The relation between trust and trustworthiness concepts always depends on decision-making processes which have to be performed by users of the system explicitly or implicitly considering the risk and possible consequences. There could be an imbalance between the level of trust in and the trustworthiness of the system with the possibility of two extreme cases. Typical situations are e.g. when too conservative users miss potential benefits of the system or when too optimistic users take too much risk by using the system (data misuse, etc.). Hence, there are major concerns about the trustworthiness of STS as the underestimation of side-effects of untrustworthy systems and mismanaging the vital and critical trust requirements has led to cyber-crime, e-frauds, cyber-terrorism, and sabotage. Reports show an increased number of citizens that

have fallen victim to these crimes, e.g. data loss. All of these issues occur because of either lack of trustworthiness or the awareness thereof.

Therefore, trustworthiness has recently gained increasing attention in public discussion. Figure 1 illustrates the identified gap in research in building a well-accepted STS for supporting socio-economic systems in the real world. The supporting applications lack expected (demonstrated) characteristics of such kinds of systems in the real world. The first step in closing this gap thus is the identification of trustworthiness attributes that may contribute to trust of socio-economic entities. Then, STS should be made capable to present these properties and characteristics.

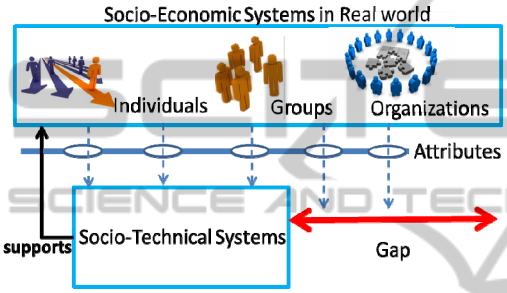

Figure 1: The Socio-Technical Gap inspired from (Whitworth, 2009).

There are, though, some inconsistencies between expected trust properties by the SC and promised trustworthiness from the SP in general. To mitigate these deficiencies and to bridge the gap resulting from the asymmetry between trust and trustworthiness, we will investigate which trustworthiness attributes a system can hold (with which mechanism and/or technologies), and whether these attributes are capable of contributing to trustworthiness addressing the trust concerns of user.

Trustworthiness in the literature has addressed the confidentiality of sensitive information, the integrity of valuable information, the prevention of unauthorized use of information, guaranteed QoS, the availability of critical data, reliability and integrity of infrastructure, the prevention of unauthorised use of infrastructure, etc. In order to prove being trustworthy, software applications could promise to cover a set of various quality attributes (Mei et al., 2012) depending on their domain and target users. Trustworthiness should promise a wide spectrum including reliability, security, performance, and user experience. But Trustworthiness is domain and application dependent and a relative attribute, i.e. if a system was trustworthy in respect to some QoS like performance, it would not necessarily be successful in being secure. Trustworthiness and trust should not be regarded as a single construct with a single effect, rather it is strongly context dependent.

Related to this observation is the fact that the demonstration of trustworthiness attributes like Common Criteria certifications (ISO 15408, 2009) or remote attestation procedures focus on security related attributes, whereas much more domains actually contribute to trustworthiness. E.g. a broad range of literature has argued and emphasized the relation between QoS and trustworthiness (San-Martín and Camarero, 2012), (Chen et al., 2009), (Harris and Goode, 2004), (Gomez et al., 2007), (Yolum and P. Singh, 2005), (Yan and Prehofer, 2007). Therefore, trustworthiness is influenced by a number of quality attributes than just security-related. Trustworthiness of entities and individuals has been investigated in open, distributed systems (e.g. online marketplaces, multi agent systems, and peer-to-peer systems).

Note that in this paper we strictly adhere to the perspective of a to-be-constructed system, and therefore will ignore potential trustworthiness (or trust) attributes like reputation or similar representing other users feedback, since they will only be available when the system is in use.

3 TRUSTWORTHINESS ATTRIBUTES

In this work, we investigate the properties and attributes of a software system that contribute to trustworthiness. To this end, we built on the software quality reference model defined by S-Cube (S-Cube, 2008). The S-Cube model is extensive and has considered several other models such as: (Boehm et al., 1976), (Adrion et al., 1982), (McCall et al., 1977), and (ISO 9126-1, 2001). In this paper we have excluded two types of the S-Cube SQA from our analysis. Firstly, some of the attributes contributing to trustworthiness are not identified in our literature review. Hence they were excluded. Secondly, some quality attributes, e.g. integrity, can be achieved, among other ways, through encryption. In this case we included the high level attribute (integrity) as a contributor to trustworthiness but did not include encryption on its own because it is encompassed by the higher level attribute. Both cases are further discussed in Section 4.

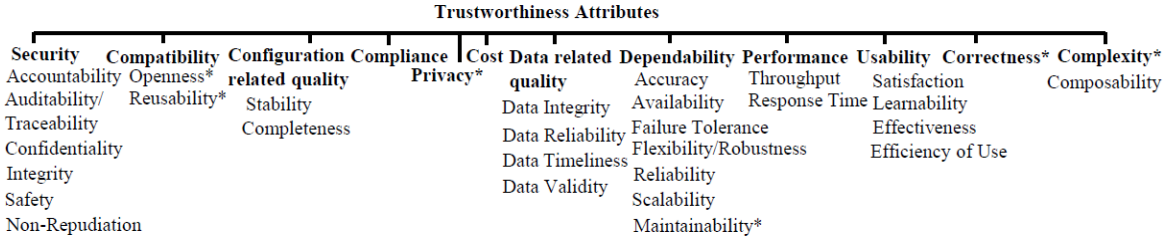

Figure 2: Trustworthiness attributes.

Additionally, we have included attributes that have been studied in the literature in term of trustworthiness. These attributes are marked with an asterisk (*). Attributes appeared in the literature as contributing characteristics of software systems to trustworthiness, are listed in Tables 1-11 with an indication of the respective papers. Because of space limitations, surveyed papers have been marked with index numbers and listed in Table 13. Figure 2 outlines the result of this work.

3.1 Security

Security covers the capability of a software system to protect entities against attacks and misuse despite certain vulnerabilities and to protect the access to resources. The sub-attributes of the security quality category are the following (listed in Table 1):

Table 1: Security category and its contributing attributes to trustworthiness.

Quality Category	Attribute	Citing
Security	1, 2, 3, 6, 8, 9, 11, 18, 19, 20, 24, 27, 30, 29, 31, 32, 33, 34, 35, 38, 39, 40, 41, 42, 43, 49, 52, 53, 55, 56, 57, 63, 64, 66, 22, 23, 67, 70, 71, 72	
	Accountability	43, 65
	Auditability/ Traceability	8, 20, 43
	Confidentiality	8, 9, 17, 38, 43, 53, 54, 58, 62, 63, 64
	Integrity	1, 8, 13, 20, 30, 34, 38, 41, 43, 46, 53, 54, 56, 58, 62, 63, 64, 61
	Safety	1, 6, 8, 20, 39, 48, 49, 53, 54, 57, 58, 62, 63, 64, 22, 23, 70
	Non-Repudiation	8, 43, 56

Accountability: The state of being accountable, liable to be called on to render an account, the obligation to bear the consequences for failure to perform as expected.

Auditability/Traceability: Capability of the service to be monitored and to generate in a reliable and secure way events producing an audit trail. Based on this audit a sequence of events can be reconstructed and examined. Security events could include authentication events, policy enforcement decisions, and others. The resulting audit trail may be used to detect attacks, confirm compliance with policy, deter abuse, or other purposes.

Confidentiality: The ability to limit access to the system and its data only to authorised agents. It is defined as the absence of unauthorized disclosure of information.

Integrity: The ability to ensure that the system and its data are not corrupted, improper system state alterations either accidental or malicious alternation or removal of information are prohibited.

Safety: The ability to operate without risk of injury or harm to users and the system's environment. It can be achieved by absence of consequences on the users and the environment.

Non-Repudiation: The ability to prove to the data sender that data have been delivered, and to prove the sender's identity to the recipient, so that neither the sender nor the recipient can deny operations of sending and receiving data.

3.2 Compatibility

Compatibility/Interoperability (Table 2) has been defined as the ability of diverse services to work constructively with each other. Actually, different services can coexist without side effects, without even knowing each other. Compatibility amounts to the necessity of two interacting parties to fulfil each other's constraints and, therefore, to correctly interact. The following sub-attributes belong to compatibility quality category:

Openness means the system is designed in such a way that it is transparent how it works and how to connect to the system. This relates to other attributes like interoperability, transparency and extensibility (McKnight and Kacmar, 2002) (Patil and Shyamansundar, 2005).

Reusability can be defined on two levels, namely, syntactic level and operational. The former relies on type definition and type compatibility rules. The later is about operation signatures.

Table 2: Compatibility or Interoperability.

Quality Category	Citing	
Compatibility/ Interoperability	22, 23, 67, 72	
	Openness*	8, 14, 20, 43, 72
	Reusability*	22, 23, 67, 72

3.3 Configuration-related Quality

This quality category contains quality attributes that influence the way a service is configured to function or characterize if the promised functional and quality level has been actually delivered during the service's lifetime period e.g. completeness, stability. The following sub-attributes belong to configuration-related quality category (listed in Table 3):

Table 3: Configuration related quality category and its contributing attributes to trustworthiness.

Quality Category	Attribute	Citing
Configuration-Related Quality	35, 72	
	Stability	1, 9, 57, 72
	Completeness	6, 64, 72

Change Cycle/Stability: Change related to the service in terms of its interface and/or implementation/recomposition.

Completeness: A measure of the difference between the specified set of features (e.g. functions) and the implemented set of features.

3.4 Compliance

The service should comply with standards (e.g. industry specific standards) and/or regulations. This can affect a number of other attributes, such as e.g. the security, portability and interoperability of the service (Table 4). Behaviour of a service should always comply with the user's expectation (specifications).

Table 4: Compliance attribute and its cite map.

Attribute	Citing
Compliance	6, 3, 60

3.5 Privacy

In internet connected systems, privacy (Table 5) from a system perspective is viewed as the system's ability and functionality that allows users to take control of the usage of their private information. From this system perspective privacy is a strong contributor to trustworthiness of the system. Systems that provide the users with the means to have visibility and control on how the users' private information is used will be more trustworthy systems. E.g. a system that guarantees a user that no third parties can access or use their private information is more trustworthy than a system that provides no such control or guarantees. Moreover, in most countries such as in the EU countries privacy is a human right and strict privacy laws must be respected. Consequently, when designing systems the designers must ensure through their design process that the way in which the system will handle private information is in compliance with the local and international laws in order to render these systems as trustworthy.

Table 5: Privacy attribute and its cite map.

Attribute	Citing
Privacy*	1, 13, 29, 31, 39, 43, 49, 58, 60, 61, 63, 64, 65

3.6 Cost

Cost (Table 6) is a (composite) quality attribute consisting of three (atomic) service attributes: cost model, fixed costs and variable costs. Actually, cost can be computed either from all atomic cost attributes or only from the fixed costs attribute.

Table 6: Cost attribute and its cite map.

Attribute	Citing
Cost	9, 26, 50

3.7 Data Related Quality

Data related quality (information and data quality) characterize input/output data by quality attributes that traditionally have been used in the information and data quality domains, e.g. accuracy and timeliness. The way that this information is provided (sensed or derived), the generated delivered time, and the level of detail affects the quality of context information. These attributes are an important factor that contributes to the trustworthiness in adaptive services. They should be designed and executed considering the quality of context that is delivered in the way that will be able to make rational and realistic decisions when and how to adapt. The following sub-attributes belong to data related quality category (listed in Table 7):

Data Integrity: It can be compromised by human errors, malicious attacks, intentional data modification, transmission errors, system/software bugs or viruses, or hardware malfunctions.

Data Reliability: Correctness of the data used by the system. It depends on the sub-systems used as well as on the provenance of the data.

Data Timeliness: The property of information being able to arrive early or at the right time.

Data Validity: The data values satisfy acceptance requirements of the validation criteria or fall within the respective domain of acceptable values. Validity criteria are often based on ”expert opinion” and are generally viewed as ”rules of thumb” although some validity criteria may be based on established theory or scientific fact.

Table 7: Data related quality category and its cite map.

Quality Category	Attribute	Citing
Data Related Quality	49, 14, 20, 57, 61	
	Data Integrity	14, 20, 56, 57
	Data Reliability	5, 14, 36, 68
	Data Timeliness	49, 67, 70
	Data Validity	56, 64, 68

3.8 Dependability

Dependability of a computing system is the property/ability that reliance can justifiably be placed on the service it delivers. It also has been defined as a correct and predictable execution and ensured that, when executed, it functions as intended. In (Avizienis, et al., 2004), dependability and trustworthiness are considered to have same goals while both suffering the same threats (faults, errors, and failures). The attributes belong to this quality category are as below (listed in Table 8):

Table 8: Dependability quality category and its cite map.

Quality Category	Attribute	Citing		
Dependability	8, 14, 54, 58, 59, 71			
	Accuracy	49		
	Availability	1, 8, 6, 9, 20, 22, 23, 39, 47, 49, 52, 53, 54, 58, 62, 64		
	Failure Tolerance	8, 20, 49, 6, 22, 23, 70		
	Flexibility/ Robustness	8, 20, 30		
		Adaptability/ Controllable	20, 31, 50, 53, 54, 55, 58, 62,1, 6, 22	
		Predictability*	9, 6, 14, 20, 50, 23	
		Reparability	6, 53, 54	
		Self-healability	49	
		Recoverability/ Survivability	8, 6, 9, 20, 22, 23, 24, 55, 62, 63, 64, 66, 67, 70	
			Recognition/ Observability / Diagnosability/ Monitorability	9, 20, 24, 31, 57, 6
	Reliability	1, 6, 8, 9, 14, 20, 22, 27, 36, 39, 45, 48, 49, 52, 53, 54, 58, 62, 63, 64, 67, 68, 70, 71		
	Scalability	49, 22, 72		
	Maintainability*	1, 8, 53, 54, 58, 62, 67		
		Testability	22, 23	

Accuracy: Definition of the error rate produced by the service calculated on the basis of the expected results.

Availability: The ability to deliver services whenever it is required.

Failure Tolerance: The ability of a service to provide its functionality to clients in case of failures. In general, it is the capability of a service to handle failures. The circumstances of service failures and how a service will react to failures are described. Compensation is its sub-attribute. It is the ability to undo the effects of a service invocation when using stateful services.

Flexibility/Robustness: It refers to the capability of the service to behave in an acceptable way in anomalous or unexpected situations or when the context changes. *Adaptability*, *reparability*, *self-healability*, *recoverability*, *predictability* and *survivability* are grouped under this attribute. Adaptability and controllability refer to the capability of the service to dynamically modify its state and behaviour according to the context, e.g. user preferences, device and network characteristics, available user peripherals, user location and status, natural environment characteristics, and service and content descriptions and can be expressed in parameters that are time and space dependent. *Reparability* is the ability of a system and its repair actions to cope with any unexpected situation. *Self-healability* is the property that enables a system to perceive that it is not operating correctly and, without human intervention, make the necessary adjustments to restore itself to normality. *Recoverability* and *survivability* allows the service to continue to fulfil its mission even if there are attacks, failures, or accidents and delivers essential services in hostile. Resistance, *monitorability* and recovery are grouped under survivability. Resistance is the ability of the service to repel attacks. *Recognition*, *observability*, *diagnosability*, and *monitorability* have been used interchangeably. It is the capability of a system and its monitors to exhibit different observables for different anticipated faulty situations. It is prerequisite of performing runtime checks on a system. Recovery is the ability of the service to restore essential services during attacks and to recover to full service after attack. *Predictability* is the expected behaviour of a non-deterministic system.

Reliability: The ability of a service to perform its required functions under stated conditions for a specified period of time (failure-free operation capability in specified circumstances and for a specified period of time).

Scalability: The capability of increasing the computing capacity of the SP’s computer system and the ability of the system to process more operations or transactions in a given period.

Maintainability is the ability of a system to undergo evolution with the corollary that the system should be designed so that evolution is not likely to introduce new faults into the system (Sommerville and Dewsbury, 2007). Maintainability has been defined as the process of making engineering changes to the system by involving the system designers and installers. Therefore, it is in contrast to adaptability, which is the process of changing a system to configure it for its environment of use. *Testability* is the possibility of validating software upon modification.

3.9 Performance

This quality category contains quality attributes that characterize how well a service performs. The following attributes belong to performance quality category (listed in Table 9):

Table 9: Performance quality category and its cite map.

Quality Category	Attribute	Citing
Performance	8, 9, 39, 47, 49, 22, 23, 72	
	Throughput	39
	Response Time	39, 47

Transaction Time: Time elapsed while a service is processing a transaction.

Throughput: It refers to the number of event responses handled during an interval. It can be further distinguished into input-data-throughput (arrival rate of user data in the input channel), communication throughput (user data output to a channel) and processing throughput (amount of data processed).

Response Time: The time that passes while the service is completing one complete transaction. *Latency* as sub-attribute of response time is the time passed from the arrival of the service request until the end of its execution/service. *Latency* itself has been constructed with *Execution time* and *delay time* in queue. The former is the time taken by a service to process its sequence of activities. The latter is the time it takes for a service request to actually be executed.

3.10 Usability

Usability/Representation collects all those quality attributes that can be measured subjectively according to user feedback. It refers to the ease with which a user can learn to operate, prepare input for, and interpret the output of the service. The attributes belong to usability quality category are described below (listed in Table 10):

Satisfaction: Freedom from discomfort and positive attitudes towards the use of the service. Attractiveness as a sub-attribute is the capability of the service to attract the user and their trust (e.g. having contact information and pictures of staff).

Learnability: Capability of the service to enable the user to learn how to apply/use it. *Comprehensibility* (sub-attribute) is the capability of the service to enable the user to understand whether its functionality is suitable, and how it can be used for particular tasks and under particular conditions of use. *Perceivable content* (sub-attribute) makes the service useable and understandable to users, unambiguous or difficult.

Effectiveness: Accuracy and completeness with which users achieve specified goals.

Efficiency of Use: Resources expended in relation to the accuracy and completeness with which users achieve their goals.

Table 10: Usability quality category and its cite map.

Quality Category	Attribute	Citing		
Usability	9, 10, 11, 12, 15, 16, 19, 30, 29, 67, 72			
	Satisfaction	1, 28, 45		
		Attractiveness	11, 12, 14, 15, 28, 69	
	Learnability	11, 13, 67, 72		
		Comprehensibility	11	
			Content Perceivability	11, 13
	Effectiveness	1, 20, 22		
	Efficiency of Use	29, 67		

3.11 Correctness

Correctness (Table 11) deals with the system behaviour conformed to the formal specification (accordance to expected behaviour and the absence of improper system states).

Table 11: Correctness and its cite map.

Attribute	Citing
Correctness*	1, 9, 6, 20, 24, 25, 37, 53, 63, 64, 68, 72

3.12 Complexity

Complexity (Table 12) deals with highly fragmented composite services which in most cases would be considered less trustworthy than a more atomic one.

Composability has been defined as the ability to create systems and applications with predictably satisfactory behaviour from components, subsystems, and other systems.

Table 12: Complexity and its cite map.

Attribute	Citing	
Complexity*	9, 67	
	Composability*	9

4 DISCUSSION

We discuss the domain, context and application dependence of trustworthiness by looking at a few example scenarios:

- Ambient Assisted Living (AAL) application and health care domain. For AAL systems, the set of attributes which have primarily been considered consists of: availability, confidentiality, integrity, maintainability, reliability and safety, but also performance and timeliness.
- For the area of critical infrastructures, the major trustworthiness attributes to be considered are: integrity, timeliness, correctness, failure tolerance, and availability.

Provability: The service performs provably as expected, resp. as defined. This is more a property of the engineering process rather than of the service delivered, but should be taken into account as well.

Predictability*:* In general, the service performs in such a way that the user can predict its behaviour, either according to past experience (= best practices), or just due to logic inference of activities.

Flexible continuity: In case the service does not perform as expected, or fails, then there is a process to not only fix the issue in adequate time, but also to inform the user, give them the chance to be involved, and to re-use the service as soon as possible. This relates to recoverability and flexibility, but specifically applies to situations with failure potential.

Level of Service is defined as the type of QoS commitment given to the application or user. It is often part of contractual agreements and therefore is often expressed in measurable terms. Although less well treated in literature related to trustworthiness, it constitutes an important trustworthiness component in most business applications. This attribute should be part of the "performance" group of attributes.

Accessibility defines whether the service is capable of serving requests, specifically to clients with limited capabilities. While many services are ready to use, they might not be accessible to specific clients. For instance, the connection between the service and the client is problematic or the service requests the clients to be able to read. This attribute should be part of the "usability" group of attributes.

Content Accessibility is ensuring that the content of the service can be navigated and read by everyone, regardless of location, experience, or the type of computer technology used. It is also part of the "usability" group of attributes.

Data Accuracy is defined as correctness of a data value or set of values as source in view of an expected level of exact computing. It should be part of the "data related qualities" set of attributes.

Data Completeness is defined as the availability of all required data. Completeness can refer to both the temporal and spatial aspect of data quality.

Data Consistency means that when a service fails and then restarts, or is evoked to different points in time, the data returned by the service should be still valid, respectively responding with the same result.

Resolution denotes the granularity of information treated, and although being of good value for decision making, it does not reflect an attribute of the system in general.

Operability is the capability of the service to enable the user to operate on it.

5 CONCLUSIONS AND FURTHER WORK

STS lie at the intersection of the social aspects of people, society and organizations with the technical aspects and IS used by and underlying such social structures. A premise of the STS theory is that optimization of the socio-elements or the technical-elements of a system independently of each other will increase the unpredictable relationships inside the system, particularly the relationships that may be harmful to the system.

Trust can be viewed as a mechanism to reduce complexity in society and trustworthiness can be viewed as a driver for building trusting relationships. Hence, determining the system attributes that foster trustworthiness contributes to building and optimizing STS such that higher trust can be achieved in such systems.

To identify the attributes that foster trustworthiness we explored an extensive literature survey guided by earlier work in the S-Cube project (S-Cube, 2008), which has been established based on (ISO 9126-1, 2001) to identify software attributes that affect trustworthiness. While passing through this survey, we also identified some software attributes that either have ambiguous definitions or their relationships to trust have not been well

studied. This study highlights several interesting issues about the subject of trustworthiness with respect to STS:

- The concept of trustworthiness needs rigorous specification and definition in the context of STS before we are able to build grounded trustworthiness measures.
- To be able to work operationally with trustworthiness attributes, metrics are necessary to set targets, measure progress, and identify the best possible investment by using ROI calculations. While this paper identifies software attributes that foster trustworthiness, it falls short of identifying software trustworthiness metrics that could be universally applied. Such metrics require further analysis and study.
- Much like trust, trustworthiness in the context of STS includes some subjective component, and always will to some extent. To limit the subjective nature of any trustworthiness metric, a restriction of the context in which the metric is used will be essential.

This is a work-in-progress paper. The main ideas and findings will be further investigated in the EU project OPTET. Our future research will focus on three important questions:

- It is important to understand how the attributes identified in this paper actually influence trust by the users of the system. Empirical research is necessary, and needs to be carried out. Just as for the identification of the attributes, existing literature will only look at individual aspects.
- We need to understand how to identify interdependencies between different attributes, and how consequently to define a "profile" (= set of trustworthiness attributes) for a certain application area.
- Substantial work is needed to investigate existing development methodologies, and to show how they can be enhanced to enable taking trustworthiness attributes into account, in a measurable and comparable way.
- Current certification and attestation programs need to be investigated how they could benefit from taking a wider range of attributes into account than just those related to security, as it is mostly the case today.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union's Seventh Framework Programme FP7/2007-2013 under grant agreement 317631 (OPTET).

REFERENCES

Adrion, W., Branstad, M. & Cherniavsky, J., 1982. Validation, Verification, and Testing of Computer Software. *ACM Computing Surveys*.

Avizienis, A., Laprie, J. C., Randell, B. & Landwehr, C., 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*.

Boehm, B. W., Brown, J. R. & Lipow, M., 1976. Quantitative Evaluation of Software Quality. *Proceedings of the 2nd ICSE*.

Chen, C. et al., 2009. A Novel Server-based Application Execution Architecture. *International Conference on Computational Science and Engineering*.

CMMISM, 2002. *Capability Maturity Model® Integration (CMMISM), Software Engineering Institute, Carnegie Mellon University Version 1.1*.

Dahrendorf, R., 2005. *Reflections on the Revolution in Europe*.Transaction Publishers.

Deutsch, M., 1962. Cooperation and trust: Some theoretical notes. *Lincoln: University of Nebraska Press*, pp. 275-319.

Golembiewski, R. & McConkie, M., 1975. The centrality of interpersonal trust in group processes. *Theories of group processes*, pp. 131-185.

Gomez, M., Carbo, J. & Benac-Earle, C., 2007. *An Anticipatory Trust Model for Open Distributed Systems, From Brains to Individual and Social Behavior*: Springer-Verlag.

Harris, L. C. & Goode, M. M., 2004. The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of Retailing*.

Huang, L., Bai, X. & Nair, S., 2008. Developing a SSE-CMM-based security risk assessment process for patient-centered healthcare systems, *30th ICSE* .

ISO 15408-1, Common Criteria, 2009. *Information technology -- Security techniques -- Evaluation criteria for IT security.* Geneva, Switzerland.

ISO 9126-1, 2001. *Software Engineering – Product quality–Part: Quality Model, International Organization of Standardization.* Geneva, Switzerland

Li, M., Li, J. & Song, H., 2009. Dengsheng Wu: Risk Management in the Trustworthy Software Process: A Novel Risk and Trustworthiness Measurement Model Framework. *5th International Joint Conference on INC, IMS and IDC*.

Luhmann, N., 1979. *Trust and Power*: JOHN WILEY AND SONS.

McCall, J. A., Richards, P. K. & Walters, G. F., 1977. *Factors in Software Quality*: US Department of Commerce, National Technical Information Service.

McKnight, D. H. C. V. & Kacmar, C., 2002. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*.

Mei, H., Huang, G. & Xie, T., 2012. Internetware: A software paradigm for internet computing. *IEEE computer Society*.

OPTET Consortium, 2012. *Project 317631 OPerational Trustworthiness Enabling Technologies, An. I DoW.*

Patil, V. & Shyamansundar, R. K., 2005 . Trust management for e-transactions.

Pazos-Revilla, M. & Siraj, A., 2008. Tools and techniques for SSE-CMM implementation. *The 12th World Multi-Conference on Systemics, Cybernetics and Informatics, Jointly with ISAS.*

San-Martín, S. & Camarero, C., 2012. A CROSS-NATIONAL STUDY ON ONLINE CONSUMER PERCEPTIONS, TRUST, AND LOYALTY. *Journal of Organizational Computing and Electronic Commerce*.

S-Cube, 2008. *Quality Reference Model for SBA*: S-Cube European Network of Excellence.

Shapiro, S. P., 1987. The Social Control of Impersonal Trust. *The American Journal of Sociology*, p. 623.

Sommerville, I., 2011. *Software engineering*: Perarson.

Sommerville, I. & Dewsbury, G., 2007. Dependable domestic systems design: A socio-technical approach. *Interacting with Computers*.

Sztompka, P., 1999. *Trust: A Sociological Theory*: Cambridge University Press.

Whitworth, B., 2009. A Brief Introduction to Sociotechnical Systems. *IGI Global*.

Yan, Z. & Prehofer, C., 2007. An adaptive trust control model for a trustworthy component software platform, Autonomic and Trusted Computing. *Lecture Notes in Computer Science* , pp. 226-238.

Yolum, P. & P. Singh, M., 2005. Engineering self-organizing referral networks for trustworthy service selection. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*.

APPENDIX

Table 13: The Paper indices

Nr.	Paper Reference	Nr.	Paper Reference
1	(Song & Wang, 2010)	37	(Aßmann, et al., 2006)
2	(Audun Jøsang, 2007)	38	(Aikebaier, et al., 2012)
3	(Tyrone Grandison, 2000)	39	(Hasselbring & Reussner, 2006)
4	(Mei, et al., 2012)	40	(Ying & Jiang, 2010)
5	(S-Cube, 2008)	41	(Qureshi, et al., 2011)
6	(Zuo-Wen, et al., 2010)	42	(Irvine & Levit, 2007)
7	(Homeland Security, 2009)	43	(Patil & Shyamansundar, 2005)
8	(ResiliNets, 2008)	44	(Verberne, et al., 2012)
9	(ANIKETOS, 2011)	45	(Harris & Goode, 2004)
10	(Corrittore, et al., 2003)	46	(Luarn & Lin, 2003)
11	(Wang & Emurian, 2005)	47	(Jing, et al., 2008)
12	(Scheffelmaier & Vinsonhaler, 2002)	48	(Shi, et al., 2012)
13	(Belanger, et al., 2002)	49	(Ding, et al., 2011)
14	(McKnight, et al., 2002)	50	(Gomez, et al., 2007)
15	(Lenzini, et al., 2010)	51	(Yolum & P. Singh, 2005)
16	(Chopra & Giorgini, 2011)	52	(Yan & Prehofer, 2007)
17	(Castelfranchi & Tan, 2002)	53	(Kuz, et al., 2012)
18	(Lipner, 2004)	54	(Avizienis, et al., 2004)
19	(Koufaris & Hampton-Sosa, 2004)	55	(Li-Ping, et al., 2009)
20	(Zheng, et al., 2009)	56	(Dai, et al., 2012)
21	(ISO/IEC 15408, 2009)	57	(Li, et al., 2009)
22	(Zhang & Zhang, 2005)	58	(Dewsbury, et al., 2003)
23	(DARPA, 2004)	59	(Paja, et al., 2013)
24	(Xiaoli, et al., 2007)	60	(Ba, 2001)
25	(Hussain, et al., 2006)	61	(Teler & Cristea, 2012)
26	(Limam & Boutaba, 2010)	62	(Sommerville & Dewsbury, 2007)
27	(Meng, et al., 2012)	63	(Schneider, 1999)
28	(Cassell & Timothy, 2000)	64	(Hall & McQuay, 2011)
29	(San-Martín & Camarero, 2012)	65	(Barber, 1998)
30	(Chen, et al., 2009)	66	(He, et al., 2009)
31	(Pavlidis, et al., 2009)	67	(Yang, 2011)
32	(Cofta, et al., 2011)	68	(Gefen, 2002)
33	(Reith, et al., 2007)	69	(Hussin, et al., 2007)
34	(Le-chang, et al., 2011)	70	(Yu, et al., 2010)
35	(Araújo Neto & Vieira, 2009)	71	(Ray & Chakraborty, 2004)
36	(Waluyo, et al., 2012)	72	(Yuan, et al., 2010)