Managing Risk in Secure System: Antecedents to Requirement Engineers' Trust-Assumption Decisions

Patrick I. Offor
Graduate School of Computer and Information Science
Nova Southeastern University
Fort Lauderdale, FL USA
po125@nova.edu

***Abstract*—Operating within a system context, security requirement engineers or analysts face enormous, diverse, and timely security requirement decisions today more than ever, primarily because of the complexities, rapidity, and evolving continuum of security threats that exist today, in part because of advances in technological capabilities and limited available resources. Although literature has shown that requirement engineers use trust assumption in limiting the scope of information systems security requirement analysis in their risk management strategy, examination of precursors to trust assumption decision is very limited. Therefore, the objective of this paper is to conceptualize, examine, and analyze the antecedents to requirement engineers trust assumption decisions. First, the study used problem frame approach to analyze the context and design decisions and to show the physical model of the system under investigation. Second, the paper used hypothesis testing to examine causality between the constructs and the phenomenon. Hence, this study argues that an analyst's trust assumption decisions of whether to include or exclude software, system, or subsystem from security requirement analysis is not made in a vacuity, but on the predisposition of the trustor and the characteristics of the trustee. The result indicates that the predisposition of the trustor and the characteristics of trustee are precursors to requirement engineers' trust assumption decisions.**

Keywords—risk management; information security; risk; information systems security; requirement engineers; trust assumption; characteristics of the trustee; predisposition of the trustor; security requirements; anti-requirement; trustor; trustee.

I. INTRODUCTION

Security requirements are major system (hardware and software) development requirements, especially for systems and subsystems designed or being designed to interface or connect to the Internet; or one, which has any form of network connectivity or has online interoperability capability. Security requirements are "restrictions or constraints placed on systems services" in order to achieve desired security objectives [1] and avoid anti-requirement. Anti-requirement is a successful realization of threat in an instant in time [2]. Haley et al. [1] assessed the vital use of trust assumptions in determining security requirement. Failure to identify and implement mitigation measures against security threats and vulnerabilities have exponential implications: it may introduce additional costs to the organization, may increase consumers' privacy concerns, and may broaden the gap between expected and actual stakeholders' expectations. It is no longer about assets, which are important just to the board of directors or employees of an organization, but includes assets or interests of the firms' partners and consumers across the world. Security requirement needs are intra- and inter-organization; perhaps intra- and inter-country needs as well. The point is that as more domains integrate with each other online and as technological advancement evolves, managing risk in a secure system becomes more difficult. This paper assesses antecedents to requirement engineers' decision-making process and substantiates [1] argument that the use of trust assumption is important because (1) it allows requirement engineers or analysts to limit the scope of security requirement analysis and (2) it limits analytical recursion. Organizations' need to limit the scope of any analysis in general and security requirement analysis in particular cannot be overemphasized. However, information about precursors and intricacies of such decision is scanty, especially in IS arena, in part because organizations are very reluctant and are guarded in revealing their IS threats and vulnerabilities in order to avoid unnecessary security exposure.

Despite the benefits of trust assumption conceptual framework expressed in [1] trusted base [2], and others, the unanswered question, perhaps the gap in literature is the absent of an empirical examination of precursors to requirement engineers' trust assumption decisions. This study is important because the goal is to identify the factors that influence trust assumption decisions, since cost of failure or inaccurate assumption could devastate a project, damage an organization financially, minimize its value, or impede on its reputation. Pragmatically, proper and accurate trust assumption decisions are crucial because undetected threats due to reduction in the scope of security requirement analysis based on trust assumptions could result in disruption of services, breach of privacy, loss of business intelligence, loss of revenue, and loss of productivity among other things. For example, over 60% of organizations discover or report major software errors at production [7], [12]. Kornecki and Liu [8] stated that about 70% of data defects are introduced at requirement and design phase. Therefore, this paper is aim at fulfilling the gap by examining the antecedents to requirement engineers' security

978-0-7695-5137-1/13 $26.00 © 2013 IEEE
DOI 10.1109/SocialCom.2013.74

requirements trust assumption decisions. In the study, we used problem frame to analyze the research problem in the context of everyday life physical domain. More importantly, the study examined the casual effect of the constructs of predisposition of the trustor (PoT) and the characteristics of the trustee (CoT) on trust assumption, using the underlying philosophical stance, which is "reality is objective and that objective truth can be found through systematic investigation and measurement" [3].

Operating in a system context, system engineers or analysts face diverse security requirements decisions today, more than ever, primarily because of the complexity of system requirements in general and security requirements in particular. Throughout system development life cycle, requirements engineers now deal with the "identification of the [security] goals to be achieved by the envisioned systems" [1], because security requirement has become part of system's key performance parameters (KPP) and key system attributes (KSA). Integration of security requirements to general system design is no longer an afterthought, but a required system development effort; from conception to retirement. Therefore, requirement engineers are obligated to consider both hardware and software security requirements in any system development planning, designing, implementation and sustainment. Requirement analysis effort increases in complexity as security threats evolve rapidly and as system development life cycle (SDLC) shifts toward a more rapid system development and deployment. Meanwhile, it is impractical for security requirement engineers to analyze all requirements during SDLC due to cost, scheduling, and performance constraints. Consequently, analysts prudently "define the context within which requirements analysis takes place by selecting the domains that are considered pertinent" [1] and potent.

Common to trust assumption, trusted base, and other similar concepts are the need for a reduction in the scope of security requirement analysis and the need to ensure confidentiality, integrity, availability (CIA) and communication. The presumption is that there are factors that influence requirement engineer's trust assumption decisions. Therefore, the postulation is that system's security characteristics construct, which we called the *characteristics of the trustee* and the requirement engineer's disposition construct, which we called the *predispositions of the trustor*, are the two major predictors of requirement engineers' trust assumption decisions. For example, an analyst may assume implicitly or explicitly that the MySQL, Microsoft SQL server, or Oracle database he or she needs for a system development has minimal residual risk. Residual risk is the level of risk that an organization is willing to accept or tolerate, knowing that it is impossible to avoid risk 100%. The assumption of minimal security risk could be because the analyst has placed some level of value on the software based on the product features, security features, network capability, or based on available regulations and partners' agreement of understandings and the analyst prior experiences, working with the software. Besides, the application of trust assumption goes beyond security requirement scope of analysis. In rapid or agile system development projects, especially one which involves enterprise resources planning (ERP), system functionalities, data availabilities, technical analyses, financial information, and human resources requirements are articulated, analyzed, developed, tested, and deployed. The system analysts in these areas use trust assumption of some sort in their scope of analysis, especially for the research development tests and evaluations (RDT&E) requirements. Therefore, understanding the premise upon which such decisions are made is important.

The rest of the paper is structured chronologically as follows: problem frame, security requirements, trustor-trustee conceptual framework, research method, data collection, data analysis, empirical validation of findings, limitations and future research, and conclusion.

II. PROBLEM FRAME

Using problem frame approach, we illustrated that the predisposition of the trustor and characteristics of the trustee have causal relationship on requirement engineers' trust assumption decisions. The use of problem frame here is "to analyze the problem in terms of the context and the design decisions the context represents" [1]. Central to problem frame approach is the practicality of interaction between domains, where the domains interface with each other through a common identifiable phenomenon, whose resulting behavior is indicative or observable [1]. According to [1], [4], problem frame has one special domain, the machine, which is the domain that transforms in order to fulfill a requirement. Satisfying security requirement depends largely on interaction between the domains and the machine capacity to satisfying or fulfilling the specification [4]. "A specification is an expression of the behavior of phenomena visible at the boundary of domains, whereas a requirement is a description of the problem to be solved" [1]. For example, in IS security-training context, a requirement might be to 'show IS awareness certification' as evidence of information system (IS) security awareness training. Here, the requirement did not specify the problem or the internal phenomena or behaviors. However, training is the problem and the training technique could be web-based, classroom instructions, or hands-on. Since these training delivery methods work differently (phenomenal deference at the boundaries), the specification must consider the differences, yet the requirement is unchanged. Context diagram and problem diagram are two fundamental diagrams for problem frame analysis [1]. A context diagram contains and depicts the domains (software, systems, or subsystems) under examination, i.e., it shows the interconnectedness of the domains, and the intermediate phenomena therein. Problem diagram, on the other hand, describes a problem in the system as articulated in the requirement. Review of literature revealed that most studies on trust assumptions had focused on software. To the best of our knowledge, examination of precursors to the security requirements trusts assumption decisions in the context of systems and subsystems is an unplowed academic area. Therefore, one of the contributions of this paper is an empirical examination of the security requirements of systems

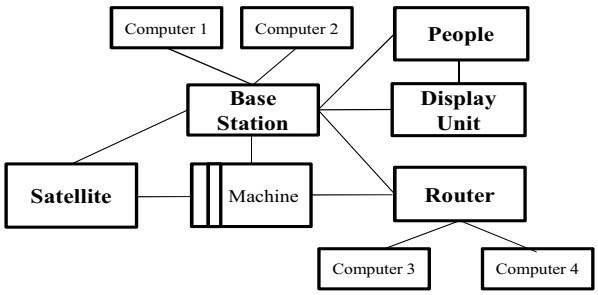

Fig. 1. VSAT context diagram.

and assessment of system components. Consequently, we used very small aperture terminal (VSAT) and video teleconferencing (VTC) configurations to illustrate that trust assumption is equally applicable to systems and subsystems configurations, and to show the casual influence of PoT and CoT on trust assumption.

A. Very Small Aperture Terminal

A VSAT system is a two-way satellite that transmits both narrow and broadband data to the satellites in orbit. Major VSAT domains shown in Fig. 1 are the satellite dish, the base station, the people, the display unit, and the router system. The VSAT is a system because a system is "a group of interacting, interrelated, or interdependent elements forming a complex whole" [10]. The VSAT domains expressed in this study are not exhaustive, but represent the five domains we used in explaining the concept. The domains interact with each other based on their network communication specifications in order to satisfy the security requirement. The network capability allows the hardwired computers (computer 1 and 2) and wireless computers (computer 3 and 4) to communicate on the Internet. We chose the VSAT because the system's security requirement needs could be transnational and it is anytime and anywhere deployment capable. However, this paper will limit its discussion of the problem domain on the router domain for the interest of precision, brevity, and clarity.

Fig. 2 is a router domain problem diagram. The requirement is for the requirement engineer to configure the router domain into the VSAT system. The analyst presumptive decision, using trust assumption, is to determine whether the router domain could be excluded from the security requirement analysis. The problem diagram indicates that the trustor (analyst) will use trust assumption to assess the trustee (router) based on the security characteristics of the domain and his or her predispositions in order to complete the 'configure router to the VSAT' security requirement analysis. The router domain

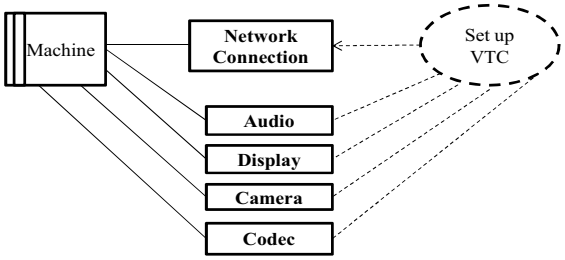

Fig. 3. Video teleconferencing context diagram.

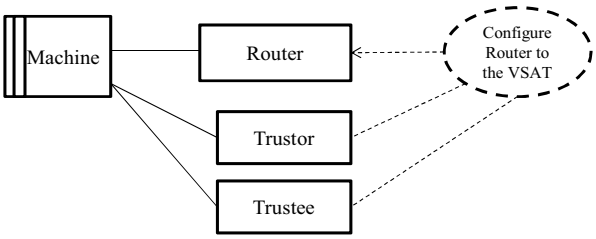

Fig 2. Router program diagram.

would be eliminated from analysis if the domain specifications meet the analyst's security requirement goals. Therefore, this study argues that limiting the scope of analysis based on trust assumption is predicated on the security characteristics of the domain and on the predisposition of the analyst.

B. Video Teleconferencing

The second illustration is the setting up of VTC between organizations and their headquarters or subordinate branch offices to minimize travel time and travel costs, or to reduce overhead. The task of setting up a VTC requires a requirement engineer to do the risk analysis for the project. Example of the minimum equipment requirement for a VTC are as follows: cameras, display devices (monitor or projector), audio equipment (microphone and speakers), network connections (secure network and bandwidth), and codec devices. Our interest here is to show the relationship between the precursors to trust assumption decisions and to show how they affect the scope of the VTC configuration security requirement analysis. Fig. 3 is a VTC context diagram, which depicts minimum domain or component requirement for the *set up VTC* requirement. Because the audio, display, and camera domains have limited security requirement, this illustration focused on the network connection domain in conjunction with the codec domain.

The use of the network domain for this illustration is necessary because the domain interacts with other organic devices in the network (computers) and interfaces with other domains external to the organization i.e., the Internet Service Provider (ISP). The codec domain receives video stream and audio signal from the cameras and microphones, compresses and transmits the video streams and signals over the network domain. Upon reaching the other end of the connection, another codec decompresses the video streams and audio signals for display on the display domain. Therefore, for an exclusion of the network domains from the security requirement analysis, the requirement engineer (trustor) would need to accept some residual risks using trust assumption.

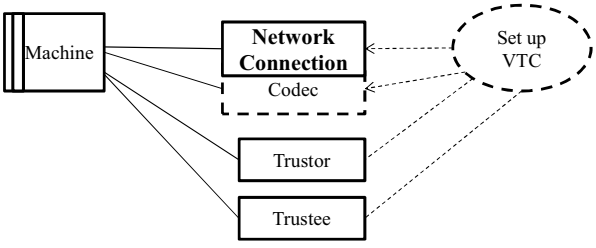

Fig. 4. Network connection problem diagram.

Hence, the paper argues as well that requirement engineers' trust assumption decision is based on the characteristics of the trustee and the analyst's predisposition as shown in Fig. 4.

III. SECURITY REQUIREMENTS

Kang and Jackson [4] described a requirement as "a problem to be solved to satisfy the customer." Security requirements, therefore, is described as an expression of constraints on behavior of a system to satisfy security goal [1]. In IS security, the aim is to ensure confidentiality (prevention of access to assets from unauthorized domains or users), integrity (prevention of modification of asset from unauthorized domains or users), availability (access to asset to authorized domains or users), and communication (mutual authentication among assets). In either the VSAT system or the VTC configuration example, the constraints depends on the type of equipment deployed, the processes instituted, and action taken to ensure CIA and authentication that limits undesired system or people. In Fig. 5, we used the router problem diagram to show the interaction between the constructs. Here, the trustor considers all possible security threats and develop security requirement. Whereas the security characteristics of the trustee are presented to the trustor in the form of system security characteristics, the presumption is that the trustor would assess the capabilities of the trustee's security characteristics in terms of their capacities to satisfy the established security requirement goals.

IV. TRUSTOR-TRUSTEE CONCEPTUAL FRAMEWORK

This trustor-trustee conceptual framework provides researchers and practitioners with the underlying predictive constructs that explain trust assumption decision underpinnings in security requirements scope of analysis. Conceptual framework or models are used to focus the interpretation of phenomenon [11]. Theoretical framework is the foundation for hypothetic-deductive research according to [13]; a representation of one's acceptance of how phenomena relate to each other and how their relationships are explained. While extensive researched on trust assumption phenomenon exits in literature, few studies to our knowledge, has examined antecedents to trust assumptions.

Fig. 6 is the path diagram or formative model of antecedents to requirement engineers' trust assumption decisions. For the formative model, "the indicators do not necessarily share the same theme and hence have no preconceived pattern of intercorrelation [*sic*]" [27]. The framework portrays two latent variables or common factors with their loadings: the predisposition of the trustor with two observed variables or indicators and the characteristics of the trustee with three indicators. Regulatory and organizational contractual agreements and prior experience indicators are shown to have inter-correlated to form the predisposition of the trustor. On the other hand, product features, security features, and network capabilities indicators are shown to have inter-correlated to form the characteristics of the trustee. In the model, squares represent observed variables, circles represent latent variables, and single-headed arrow shows the direction of expected causal influence [14]. The rest of this paper is an expatiation on the model and the provision of the predictive linkage among the variables.

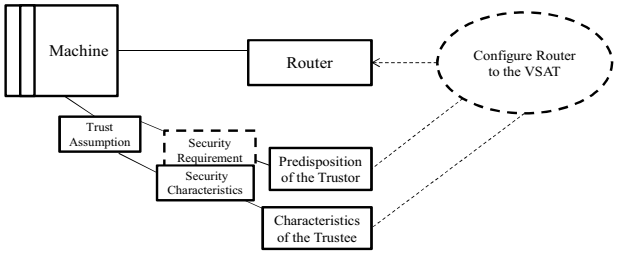

Fig. 5. Router problem diagram and trust assumption.

A. Predisposition of the Trustor

Since trust assumption is an "assumption by a requirements engineer that, in order to satisfy a security requirement, the membership or specification of a domain can depend on certain properties" [1], we suggest that predisposition of the trustor is of great importance to the phenomenon. Predisposition of trustor is described here as the requirement engineer or analyst's inclination to include or exclude a domain in the security requirement analysis. The view is that although the trustee may have reasonably anticipated all threats, it is inconceivable to think that the trustee had applied equal importance to all the threat considering the fact that changes to threat signatures is a continuum, as such; the probability of failure is constant. The second view is that the analyst will evaluate prudently, the cost of anti-requirement and the benefits of limiting the scope of security requirement analysis. The third is that the analyst may consider applicable regulatory or contractual protection available to the organization and will factor them into his or her decision thought process. The last, but by no means the least, is that the requirement engineer or analyst's prior experience with the domain of interest is paramount to his or her decisions. Although there is evidence of potential presence of first order and second order factors for the variable of interest, this study focused on regulations and contractual agreements, and prior experience as observed variables for the predisposition of the trustor. As a result, we posit the following hypothesis.

H_1: There is a causal relationship between the predisposition of the trustor and the requirement engineer or analyst's trust assumption decision.

1) Regulatory requirement and contractual agreements. Regulatory requirements are laws, restrictions, and licenses

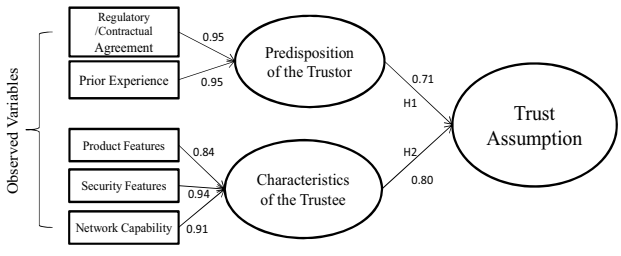

Fig. 6. Security requirement decision path diagram.

applicable to product, services, process, and business by local, state, or national government to protect individual, groups, organizations, and government agencies. The notion is that an analyst's trust in the component or software is partly because he or she believes that the manufacturer or supplier of the component or software would adhere to applicable laws or regulations. The analyst's belief in the domain capabilities could be because he or she expects the laws to translate into software code and systems' physical architecture that restrict behaviors [15]. Additionally, contractual agreements are individual-to-business, business-to-business, business-to-government, government-to-individual restrictions and parameters to achieve specified objectives. Using automakers as example, companies such as Ford, General Motor, Toyota, and other regularly sign agreements with their parts suppliers and dealers that ensure availability of the parts on demand and delivery of cars to dealerships on time. In system development context, requirement engineers for enterprise resourcce planning would have similar software agreements with the database, compiler, or application software and hardware providers. The assumption is that having and being aware that such agreements exist would help requirement engineers in their assessment; knowing that the company that supplies the router may be liable, financially or otherwise, if the router they supplied fails prematurely, despite meeting initial security requirement objective. Therefore, the presumption is that regulatory requirements and contractual agreement would influence requirement engineers' susceptibility in trust assumption determination.

2) Prior experience. Conventional wisdom is that people are wary about the unknown, as such they gravitate toward the things, people, systems, and the like that are familiar to them. In addition, individuals tend to engage in enhancing events and avoid threatening events, i.e., they respond positively to enhancing events—events consistent with individual self-identity and respond negatively to threatening events—events inconsistent with individual self-identity [16]. The supposition here is that requirement engineers, who have been on the job for a while, would have the capacity to make sense of the systems, subsystems, components, or software that regularly meet their organization security requirement. However, organization may routinely require requirement engineers to reanalyze proven system after an extended period. Hence, the presumption is that prior experience with a particular domain will influence an analyst's predisposition for inclusion or exclusion of the domain to requirement analysis.

TABLE 1. TRUSTEE (ROUTER) SECURITY FEATURES

Integrated Threat Control	**Trust and Identity**	**Network Foundation Protection**	**Secure Connectivity**
Internetwork Operating System (IOS) Firewall	PKI Client (x.509 Digital Certificates)	Auto-Secure and Unicast Reverse Path Forwarding (uRPF)	Virtual Tunnel Interface (VTI)
IOS Intrusion Prevention System (IPS)	Authentication, Authorization, and Accounting (AAA)	CPU and memory Threshold Notification	Easy VPN and Enhanced Easy VPN
IOS Filtering and NetFlow	IOS Certificate Server	Routing Protection, Access Control Lists (ACL)	IOS Secure Sockets Layer (SSL) VPN
Network-Based Application Recognition (NBAR)	Standard 802.1x-Based Identity Services	Secure Access Mode (silent mode) and Raw IP Traffic Export	Standard IP Security, Group Encrypted Transport VPN, and Dynamic Multipoint VPN
Flexible Packet Matching (FPM)		Source-Based Remote-Triggered Black Holing (RTBH) Filtering	Multi-VRF and Multiprotocol Label Switching (MPLS) Secure Contexts

B. *Characteristics of the Trustee*

In [1], one narrative was how constraints in an automated teller machine (ATM) ensured secure transaction, ensured that the ATM disburses right amount of money, and to the right person based on the customer's positive response to two security requirements: possession of an ATM card and provision of a correct personal identification number (PIN). Although there are many domains involved in the system configuration, IS security risk management rests on the system communication and authentication capabilities. Therefore, efforts aimed at ensuring CIA, must consider the ATM's service features, including operational mechanism, its security features, its secure communication capability, and its brand recognition value emanating from the component or software's performance history. Translating the ATM analogy in VSAT context, we argue that there is a causal relationship between the characteristics of the trustee: product features, security features, network capabilities, and the analyst trust assumption decisions.

H_2: There is a causal relationship between the characteristics of the trustee and the requirement engineer or analyst's trust assumption decision.

Product features. One of the main consideration in product features is the determination that ensures that the physical characteristics of the domain of interest meet the configuration objectives. In this case, the assessment is necessary because it helps the analyst to decide upfront whether to remove the router domain from the analysis prior to security requirement consideration. Evaluation of this features include, but not limited to the quality, size, weight, shape, bandwidth, durability, reliability, maintainability, and supportability of the router domain. Some of the analyst product feature considerations are whether the size and the weight of the router fit into the overall system configuration plan; whether the router has scalable bandwidth; would the router survive in diverse operating environment; and whether the router is low maintenance, portable, and supportable? Therefore, we argue that the greater the product features fit into the requirement engineer's requirement plan, the easier it is for the requirement engineer to exclude it from the analysis.

1) Security features. Table 1 depicts a listing of a network security features for an integrated services routers generation 2 platform [17], which is used as an example in the VSAT context. Although the list is not exhaustive, it encompasses some software and artifacts that controls, measures, and ensures confidentiality, integrity, availability, and communication. Since the focus is on the router domain and as a salient component of the trustee domain, the security characteristics of the router are perhaps the most critical factor

in the requirement engineer's or system analyst's consideration for internal security requirement distribution in fulfillment of the configure router to the VSAT requirement. Here, the analyst must make a decision whether router security characteristics meet the security requirement objective in order to remove it from the analysis. Therefore, we presume that a domain's security features is crucial and will have an impact in the analyst's thought process.

2) Network capability. The three core competencies of the router are protection of the all network threats, the provision of the borderless services, and the provision of the total cost ownership [17]. The network protection uses its security features to deliver secure high-quality voice and video communication services, secure wired and wireless network integration, as well as protection against eavesdropping, toll fraud, and denial of services (DoS). The borderless services allow system engineers to capitalize on either using existing network infrastructure to control potential threats or take advantage of the router's security features for maximization of security efforts. In addition, the system provides for secure cloud computing services and secures unified mobile architecture. Finally, the total cost ownership lowers capital expenditures (reduces the number of devices) and operating expenses (energy and maintenance cost) through a one-touch update feature, advance instrumentation panel, and hardened foundational security features. The real question here is whether these existing capability fits into the requirement plan. For example, if a need for a scalable network bandwidth exists, would the network domain meet such need?

V. RESEARCH METHOD

This study is a quantitative analysis aimed at testing the causal relationship between the preposition of the trustor and the characteristics of the trustee on requirement engineers or analysts' trust assumption decision in a field study. It is a hypothesis testing. The use of quantitative method in research studies is best "if the problem is identifying factors that influence an outcome, the utility of an intervention, or understanding the best predictors of outcomes" [29, pp. 21-22]. As in [13] hypothesis testing is "a means of testing if and if-then statements generated from the theoretical framework hold true when subjected to rigorous examination." The study used hypothesis testing because it is most suitable for testing the predictive or causal relationship expressed in the hypotheses. In addition, the reason for choosing hypothesis testing lies in the positivism philosophy, which is rooted in rational in naturalism (transfer of assumptions and methods of natural science to the study of social phenomenon or objects) and the essence of quantitative data [18], [21]. Research method or design is the structural and methodical path for data collection, analysis, and interpretation a researcher chooses for a study [19], [20]. In other words, research design is the archetype for conducting an investigation that deals with the question of what to study, why the study, the kind of data to collect, the relevancy of data, and the type of data analysis [22] to perform. Therefore, the use of hypothesis testing in this study is to examine, measure, quantify, analyze, and interprete the significant effect of the constucts.

VI. DATA COLLECTION

Managing risk in secure system requires specialized skill and expertise. In addition, identification and gaining access to suitable and appropriate research population and sample elements can be challenging, primarily, because of the sensitivity and secrecy associated with most organization's information security here in the United States and the critical nature of information security in general; as well as organization's information system security protective posture in the western world. Nonetheless, we solicited data for this study from seven expert participants, who are subject matter expert (SME) in information security or requirement analysts in a large organization with over 500 personnel in its information systems department and from the professional network, LinkedIn®. Four out of seven subjects responded to the email survey and two subjects responded from the embedded survey link. Although review of literature did not provide exact number of participants required for a study, [24] found that four or five subject accounted for 80% of proportion of usability problem identification; that means that first few subjects were enough for identifying major usability problem—additional subject is warranted only if revealing of new information is likely.

Descriptive statistics of the subjects' demographic data in Table 2 indicates that one out of the six participants is a female and the minimum and maximum age of the subjects were between 30-34 and 50-54 respectively. In addition, all the participants have master's degree or higher; and the subjects' current functional areas ranges from production and operation to data processing, information assurance and automation, and software requirement testing. Table 4 contains the survey instrument for this study. Initial survey items had eight questionnaires, four for each hypothesis, but three items were later deleted due to poor loading and poor inter-item correlation during factor analysis.

TABLE 2. DEMOGRAPHIC DESCRIPTIVE STATISTICS

Participants' Information		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	1. Male	5	83.3	83.3	83.3
	2. Female	1	16.7	16.7	100.0
	Total	6	100.0	100.0	
Age	4. 30 – 34	1	16.7	16.7	16.7
	6. 40 – 44	2	33.3	33.3	50.0
	7. 45 – 49	1	16.7	16.7	66.7
	8. 50 – 54	2	33.3	33.3	100.0
	Total	6	100.0	100.0	
Highest Level of Education	3. Master's degree	5	83.3	83.3	83.3
	4. Doctorate /Professional degree (Ph.D., MD, or JD)	1	16.7	16.7	100.0
	Total	6	100.0	100.0	
Functional Area	3. Production /Operation	1	16.7	16.7	16.7
	4. Data processing	1	16.7	16.7	33.3
	5. Information Assurance /Automation	3	50.0	50.0	83.3
	9. Software Requirements and Senior Functional Test Analyst	1	16.7	16.7	100.0
	Total	6	100.0	100.0	

VII. DATA ANALYSIS

A. Result of the Analysis

The study used 2-tailed test and one sample t-test to test for the statistical significance of the findings. The use of a 2-tailed test is indicative of non-consequential difference in the direction of the hypotheses or indicative of nondirectional hypotheses. Researchers use one sample t-test when the purpose is to use the sample drawn from a certain population to test whether the mean of the population is equal to the mean of comparison value or standard [13], [23]. In addition, fundamental to one-sample t-test statistical assumptions is the notion of independent observations, randomized sample, normal distribution of the observations and unknown population variance [23].

The result of the one sample t-test indicates a statistical significance for the hypotheses, which showed 2-tailed p-values of 0.00 for all indicators with alpha at 0.01. The summary item statistics in Table 3 depicts significant and strong inter-item correlation for the predisposition of the trustor construct at 0.798 and covariance at 0.70, and correlation of 0.713 and covariance of 0.289 for the characteristics of the trustee. The use of SPSS factor analysis showed the following strong factor loadings: PoT1 and PoT2 (0.95 and 0.95 respectively) and CoT1, CoT2, and CoT3 (0.84, 0.94, and 0.91 respectively). The *skew* is 2.45 and the *kurtosis* is 6.0; hence, based on the Skewness and Kurtosis respective normality distribution threshold of 3.0 and 10.0 respectively [28], the distribution showed normality. Skewness is a measure of the degree of asymmetric distribution among variables and "Kurtosis is an index of the peak or tails of the distribution" [28]. Based on this result, there is causal the relationships between H1 and H2, and trust assumption decisions; hence, all proposed hypotheses are supported and accepted as shown in Table 3.

B. Reliability (internal consistency)

Reliability or internal consistency is a "statement about measurement accuracy...the philosophical underpinnings of reliability suggests that the researcher is attempting to find proximal measures of the 'true scores' that perfectly describe the phenomenon" [9]. Reliability ensures that the measurement instrument is free from error [18]. It measures the extent to which the instrument will produce the same result when testing is conducted on repeat instances. It also measure the reliability that a construct is independent of other constructs in the study. Cronbach's alpha (α) is used to measure the reliability or internal consistency of items or indicators in a survey instrument. Reliability coefficient ranges from 0.0 to 1.0; it measures the "interconnectedness of the items and estimates the proportion of the variance in all the items that is accounted for by a common factor" [18]. Similarly, higher value of alpha means lower inter-item correlation. The Cronbach's alpha for this study is 0.66 (new scale) for latent variable of predisposition of the trustor (PoT1 and PoT2 indicators), and 0.88 for the characteristics of trustee (CoT1, CoT2, and CoT3 indicators). Although [18] stated that "reliabilities less than 0.60 are considered to be poor, those in the 0.70 range, acceptable, and those over 0.80 good." Cronbach's alpha equal or greater than 0.60 is acceptable for new scales [5], [6]. In addition, there is a negative relationship between sample size, number of items, and Cronbach's alpha [19], [31].

TABLE 3. SUMMARY OF ITEM STATISTICS

Hypothesis	Link	Inter-Item Correction	Inter-Item Covariance	# of Items	Supported/ Accepted
H1	PoT → Trust Assumption	0.798	0.700	2	Yes
H2	CoT → Trust Assumption	0.713	0.289	3	Yes

C. Construct Validity: Convergent and Discriminant

Construct validity is a measure between constructs in order to validate that research items for a given latent construct converge significantly and discriminate (little or no cross-loading) [9]. Sekaran and Bougie [13] described construct validity as one that "testifies to how well the results obtained from the use of the measure fit the theories around which the test was designed." In other words, construct validity test how well the chosen items in a study fits well together within the latent constructs and captures the essence of the constructs and how well a latent variable discriminates among other latent variables [9].

Convergent validity is a measure of how well a construct's indicators or observed variables measure the construct or latent variable. Assessment of convergent validity is conducted by calculating the latent variable's construct reliability (CR), the average variance extracted (AVE), and the squared factor loadings (communalities). The predisposition of the trustor has a CR of 0.95 and AVE of 0.90; communalities of 0.90 and 0.90 for the PoT1 and PoT2 respectively. The characteristic of the trustee has a CR of 0.93 and AVE of 0.81; communalities of 0.71, 0.89, and 0.84 for the CoT1, CoT2, and CoT3 respectively. The study's convergent validity measures exceed the following recommended thresholds: CR greater than 0.70, AVE greater than 0.50, standardized loading (communalities) value of 0.70 or greater, and CR greater than AVE [9].

Discriminant validity is a measure of how distinctive a construct is from one another. It establishes that the constructs are not correlated and the measurements are empirically founded [9]. The inter-construct correlation (IC) for the study is 0.133 and the squared inter-construct correlation (SIC) is 0.018. Discriminant validity exists if the AVE is greater than the SIC. The study's average variance extracted for the constructs are greater than the squared inter-construct correlations. Therefore, the indicators have more in common with their related latent variables than in other latent variables.

VIII. LIMITATIONS AND FUTURE RESEARCH

The study's inability to acquire more respondents or subjects is a limitation; hence, future studies would need to expand the sample pool. Another limitation is the reluctance among experts in the field to participate more in IS security studies because of their concerns; fear of exposing their

organizations' vulnerabilities. Although, this study is on risk management in a secure system, future work should examine other factors such as software or hardware failure rates, analyst's cost-benefit analysis, or brand name recognitions as contributing factors or influencers to requirement engineers' trust assumption decisions.

IX. CONCLUSION

Predisposition of the trustor and characteristics of the trustee have causal relationship on trust assumption decisions. The study used problem frame approach to show that trust assumption is a product of the trustee's characteristics and trustor's predisposition. This study revealed that the context is not limited to software development, but that it is applicable also to systems and subsystems configuration. Empirically, the study used hypothesis testing to illustrate that requirement engineers or analysts' trust assumption decisions are not made in vacuity, but significantly on the predisposition of the trustor and on the characteristics of the trustee.

TABLE 5. SURVEY INSTRUMENT

Latent Variable	Indicator Code	Items	Item Loading	Dependent variable
Predisposition of the Trustor	PoT1	As a requirement engineer or analyst, I trust that our external partners will honor regulation and inter organization contractual agreements relating to software or hardware of systems or sub-systems whenever I am analyzing the scope of security requirements.	0.95	Trust Assumption
	PoT2	As a requirement engineer or analyst, I rely on my experiences whenever I am analyzing the scope of the security requirements of software or hardware of systems or sub-systems.	0.95	
Characteristics of the Trustee	CoT1	As a requirement engineer or analyst, I consider the product features of software or hardware of a system or sub-systems whenever I am analyzing the scope of the security requirements.	0.84	Trust Assumption
	CoT2	As a requirement engineer or analyst, I trust the security features or specifications of the hardware or software product will work as prescribed whenever I am analyzing the scope of security requirements.	0.94	
	CoT3	As a requirement engineer or analyst, I trust that the network capabilities of the hardware or software a product will work as prescribed whenever I am analyzing the scope of security requirements.	0.91	

REFERENCES

[1] B. Haley, C. Laney, D. Moffett, and B. Nuseibeh, "Using trust assumptions with security requirements," *Requirements Engineering,* vol. 11, pp. 138-151, 2006.

[2] L.-C. Lin, B. Nuseibeh, D. Ince, M. Jackson, and J. Moffett, "Analysing security threats and vulnerabilities using abuse frames," *ETAPS-04*, 2003.

[3] L. M. Gallant, "Experience design methodology: The four questions," *Academic Exchange*, pp. 82-87.

[4] E. Kang and D. Jackson, "Dependability arguments with trusted bases," in *Requirements Engineering Conference (RE), 2010 18th IEEE International*, 2010, pp. 262-271.

[5] K. K. Boyer, G. K. Leong, P. T. Ward, and L. J. Krajewski, "Unlocking the potential of advanced manufacturing technologies," *Journal of Operations Management,* vol. 15, pp. 331-347, 1997.

[6] S. C. Dunn, R. F. Seaker, and M. A. Waller, "Latent variables in business logistics research: scale development and validation," *Journal of Business Logistics,* vol. 15, pp. 145-145, 1994.

[7] G. Tassey, "The economic impacts of inadequate infrastructure for software testing," *National Institute of Standards and Technology,* pp. 02-3, 2002.

[8] A. J. Kornecki and M. Liu, "Fault tree analysis for safety/security verification in aviation software," *Electronics,* vol. 2, pp. 41-56, 2013.

[9] D. Straub, M.-C. Boudreau, and D. Gefen, "Validation guidelines for IS positivist research," *Communications of the Association for Information Systems,* vol. 13, pp. 380-427, 2004.

[10] M. M. Durland and K. A. Fredericks, "An introduction to social network analysis," *New Directions for Evaluation,* vol. 2005, pp. 5-13, 2005.

[11] M. E. Botha, "Theory development in perspective: The role of conceptual frameworks and models in theory development," *Journal of Advanced Nursing,* vol. 14, pp. 49-55, 1989.

[12] S. Cleveland and T.J. Ellis, "Toward a model for customer-driven release management" presented at the *Americas Conference on Information Systems*, Chicago, IL, 2013.

[13] U. Sekaran, and R. Bougie, *Research methods for business: A skill building approach*, 5th ed. Great Britain: John Wiley, 2009.

[14] J. J. Albright and H. M. Park, "Confirmatory factor analysis using Amos, LISREL, Mplus, and SAS/STAT CALIS," *The Trustees of Indiana University,* vol. 1, pp. 1-85, 2009.

[15] J. Grimmelmann, "Regulation by software," *Yale Law Journal,* vol. 114, pp. 1719-1758, 2005.

[16] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," *Journal of Management Information Systems,* vol. 28, pp. 203-236, 2011.

[17] Cisco Website, "Network eecurity features for Cisco integrated services routers generation 2 platform," retrieved from *http://www.cisco.com/en /US/prod/collateral/routers/ps10538/data_sheet_c78-556151_ps10537_ Products_Data_Sheet*, 2013.

[18] W. P. Vogt, *Dictionary of statistics & methodology: A nontechnical guide for the social sciences,* 3rd ed. Thousand Oaks, California: SAGE Publications, 2005.

[19] N. J. Salkind, *Exploring research*, 8th ed. Boston: Prentice Hall, 2012.

[20] C. Nachmias, D. Nachmias, *Research methods in the social sciences*, 4th ed. London: Melbourne, 1992.

[21] D. Straub, D. Gefen, M. C. Boudreau, *The ISWorld quantitative, positivist research methods.* Retrieved from http://dstraub.cis.gsu.edu:88 /quant, 2004.

[22] S. G. Phillber, M. R. Schwab, and G. S. Sloss, *Social research*, Peacock Pblishers, 1980.

[23] B. J. Dretzke, *Statistics with Microsoft excel*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2005.

[24] R. A. Virzi, "Refining the test phase of usability evaluation: How many subjects is enough?," *Human Factors: The Journal of the Human Factors and Ergonomics Society,* vol. 34, pp. 457-468, 1992.

[25] W. Li-Ping, "Comparative advantage theory and its revelation to China's foreign trade," in *Management and Service Science, 2009. MASS '09. International Conference on*, 2009, pp. 1-4.

[26] Z. YeFei, "Building the relationships model of firm resources and competitive advantage," in *Robotics and Applications (ISRA), 2012 IEEE Symposium on*, 2012, pp. 413-415.

[27] T. Coltman, T. M. Devinney, D. F. Midgley, and S. Venaik, "Formative versus reflective measurement models: Two applications of formative measurement," *Journal of Business Research,* vol. 61, pp. 1250-1262, 2008.

[28] R. Weston and P. A. Gore, "A brief guide to structural equation modeling," *The Counseling Psychologist,* vol. 34, pp. 719-751, 2006.

[29] J. W. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*, 2nd ed. Thosand Oaks, CA: Sage Publications, 2005.

[30] R. Reh, M. L. Mursidi, and N. A. A. Husin, "Reliability analysis for pilot survey in integrated survey management system," in *Software Engineering (MySEC), 2011 5th Malaysian Conference in*, 2011, pp. 220-222.

[31] P. K. Kopalle and D. R. Lehmann, "Alpha inflation? The impact of eliminating scale items on Cronbach's Alpha," *Organizational Behavior and Human Decision Processes,* vol. 70, pp. 189-197, 1997.