CSEC 559 Seminar in Computing Security
Project Report

A SYSTEMIC REVIEW OF USER TRUST IN SECURITY SYSTEMS

May 19, 2020

John Lawrence, Stacey Watson
Department of Computing Security
College of Computing and Information Sciences
Rochester Institute of Technology
jbl4908@rit.edu, slwics@rit.edu

1 Abstract

This paper analyzes the factors involved in the establishment of trust between a user and a system. To do this, a variety of papers are analyzed with topics pertaining to user trust in technological systems. These papers range in industry and application, which is used to generate a more general and encompassing finding through data extraction and synthesis. The findings of the paper display 5 variables at different levels of importance. These variables are then translated from qualitative values to quantitative values in the form a calculated user trust coefficient. This user trust coefficient provides a metric for determining an organizations current capabilities in generating user trust. In future, the metric will require supplementary procedures to accompany it for more in depth user trust analysis.

2 Background

The concept of trust and the analysis of it is an old field in psychology. The means by which a person believes another person will do what is expected despite pressures to do otherwise is indeed a fascinating subject that spans all generations. We have seen how this study can be used for both constructive and destructive purposes. For this paper we will be looking into how trust correlates with a security system and what technical elements we can control to influence how this trust is acquired.

One thing to note about previous literature on this topic is that it tends to be focused on a specific discipline or industry in the tech space. A good starting example would be the work done by Gefen et al. analyzing the steps necessary to create a system by which users can establish with [1]. The industry in this study was focused on e-Commerce sites and the trust in the storefront. A major finding of this study was the need for communication between the developer and consumer to be possible in some form for the trust process to occur most efficiently. An example could be a direct chat or call system, though a simple FAQ was also found to produce benefits. Based on this it is safe to say any site selling a product or service would need this in order to begin the establishment of trust.

For establishing trust within a service and/or system however the factors at play are tied more with the technology. According to A. Rashidi in the Journal on Cloud Computing, the factors that most influence trust in a cloud system are (in order of importance): Recovery, Availability, Privileged User Access, Compliance, Viability, Location [2]. These findings can be translated to the CIA triad by combining Recovery with Availability. Leaving the others to be partially confidentiality and integrity. Based on the findings of Zhou in his paper on trust in mobile banking, we can state that integrity most likely takes the edge over confidentiality when it comes to online trust [3].

For systems that rely on user-to-user or peer-to-peer, trust was found to be much harder to achieve. According to Cardoso et al. "the user tends to refrain from interacting with the unknown user when a relevant/important asset or goal is at stake" [4]. Their testing attempted to visualize this through video games, and their analysis indicated a much more exclusive and controlled distribution of trust in these sort of systems.

This leads us to how systems can lose trust from users. The paper by K. L. Vu et al. analyzed the affect infringing upon their computer policy had on the level of trust a user had in the website. Their findings show that sites that broke their policy did have a trust loss and websites that did not gained some trust [5]. Interestingly sites that are similar to other sites a user uses, regardless of familiarity, were resistant to negative changes in trust compared to those without similarity. Another notable cause of a reduction in trust was found by Zhang during his analysis of trust in digital right management systems [6]. There he discovered how since the system will assume guilt until proven innocence it displays a lack of trust from the system in the user. In turn, the user responds by lowering their trust in the system. Because of this it is clear that if a system has to establish trust in a user it is done as invisible and quickly as possible. This is most likely because the user knows they

are legitimate and thus the initial lack of trust may be seen as misjudgement by the system instead of a security check.

The further qualitative analysis of these technical, user, and task elements was undertaken by J. Xu et al. in their paper on how different users establish trust differently [7]. Their findings displayed that "mean average trust in technology ratings was significantly lower in the low reliability condition than that in the normal condition" reinforcing the finding that availability and integrity take a higher role in trust than confidentiality. Furthermore, while user and task influence the way trust is created the technology being used has the most control in the trust process. Because of this, we can say that not only can developers influence trust but they are also one of the primary agents to do so.

To finalize our research we looked more into the psychology at work with these technical systems. B. J. Dievorst and U. Simonsohn of the Journal of Expiremental Psychology tested their hypothesis that people do disregard "to-be-ignored information" and came up with a negative result [8]. This 'to-be-ignored' information includes hindsight bias and the curse of knowledge bias, which are cognitive biases involved in the decision making of trust. Based on their findings these biases are also more prevalent towards technological systems due to what they call "algorithm aversion". This is to say that a human has much lower tolerance for a algorithm error than a human error.

The human element here was then needed to be tested. According to a paper by B Yuksel et al. an attractive digital agent is more resistant to a loss in trust when having low reliability compared to a less attractive agent [9]. This was a negative result to their hypothesis that reliability is more important than appearance. It is possible then that this "algorithm aversion" can be overcome by having an attractive human presence as the presenter of the system.

3 Review Questions

During the paper survey questions were developed to help hone the data extraction process. These questions are intended to guide the review method and data analysis portion of the paper. In doing so, they ensure the hypothesis and queries are maintained throughout the paper.

Primary	What are the elements that factor into trust calculation by users?
Primary	Which factors are restricted the to the specific system being analyzed?
Primary	Why do these elements influence trust?
Secondary	What are the elements that factor into trust calculation by users?
Primary	Who and/or what does the user interact with in this system?
Primary	Does the type of entity the user interacts with affect trust values?
Primary	What cognitive biases affect the users ability to create trust in this case?
Secondary	Does the type of entity the user interacts with affect trust values?

4 Review Methods

Data sources and search strategy As a search strategy, we made a primary effort to balance out negative journals with positive. Seeking at least 33% of sources to be negative findings. To do this, we searched for studies with a hypothesis that either had to be modified or was presented as false based on the data presented. We managed to achieve a 33% of our sources being negative findings based on this criteria. In doing so, the paper should be better suited to avoid confirmation biases.

4.1 Study Selection

The key topics of our research was in both the psychological and technological elements of trust in UI and Security systems. In the papers gathered we wanted at least 2 of these 4 elements to be present to have papers focused on this specific area. Our sources in the review all met this criteria. By achieving this filter in its entirety we ensure that the sources used for our analysis are tailor fitted for the our review questions.

4.2 Study Quality assessment

To verify the quality of the papers, they had to have been published by those with either the backing of a publisher or journal body that specializes in the area or the author must have a degree of Master or higher in the discipline being published on. Furthermore, the sources of these papers were analyzed for authenticity and relevance. Papers that had sources of more than 60% not relevant to one of the 4 elements of our paper were not to be included.

4.3 Data extraction

Extraction of data focused on the two types of data, qualitative and quantitative. Many papers focused on a single one of these types, though some provided ample amounts of both. Extracted data had to have been proved in the paper by their own primary research. This is done to prevent secondary sources from being used under the wrong name and to prevent them from taking up a majority of our study.

4.4 Data Synthesis

These two data types were then organized together so qualitative was analyzed against qualitative and likewise with quantitative. This makes it easier to develop initial models and patterns from the extracted data later. Once this was complete the analysis of both types of data can occur and produce the final results of our research.

5 Included and Excluded Studies

Study Name	Excluded/Included	Reasoning
Data Trustworthiness Evaluation in Mobile Crowd Sensing Systems with Users Trust Dispositions Consideration	Excluded	The trust in this system is entirely created and modified by devices with no input from users.
Managing User Trust in B2C e-Services	Included	Provides test results and discussion on how users develop trust in a digital storefront environment.
How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology	Included	Defines 3 factors in the establishment of trust. Provides evidence as to why technology precedes user and task.
Robo-Taxi service fleet sizing: assessing the impact of user trust and willingness-to-use	Excluded	The basis of establishing trust in this system is too physically oriented. Making it not applicable to most other systems.
A Model for User Trust in Cloud Computing	Included	Produces a straightforward and well cited group of cloud trust factors.
Understanding users initial trust in mobile banking: An elaboration likelihood perspective	Included	Provides trust analysis from the financial service perspective. Introduces user efficacy as a factor.
A User Trust System for Online Games Part I: An Activity Theory Approach for Trust Representation	Included	Provides analysis of user-to-user oriented communication and trust. Good juxtaposition to user-to-system
Security, trust and risk in digital rights management ecosystem	Included	Paper analyzes trust from digital rights perspective. Provides info on how establishing trust can incidentally reduce user trust.
Influence of the Privacy Bird user agent on user trust of different web sites.	Included	Provides evidence on how familiarity and design customs influence trust values.
Intentionally biased: People purposely use to-be-ignored information, can be persuaded not	Included	Introduces psychological biases as factors. Also suggests "algorithm aversion".
Brains or Beauty: How to Engender Trust in User-Agent Interactions	Included	Analyzes how physical attractive properties can correlate from human to systems and the impact.

6 Results

The findings from this systemic review indicate that there is a possible function to be developed based on using the variables most important for developing trust with the output being a 'trust' co-efficient. Taking a look through my studies I can say that the importance of these variables falls close to this order:

1. Familiarity - This is key, a system that falls in line with a user mental image of how it should look gains trust faster and loses it slower.

2. System Type - While unavoidable the service being offered greatly impacts how trust is given and lost. Digital Rights Management (DRM) has a much harder time with trust than Video Games.

3. Technology - The speed and efficiency of the system is key for trust. In studies it was found to take precedent over the type of user and the specific task being performed.

4. People Based - Several of my studies indicated how having a human interaction option was key to trust. The key term for this is "algorithm aversion". Means of gaining this is direct chat with developers, patch/update postings, forums, and FAQs.

5. Finally we come to the CIA triad, which seems to be reversed in order of importance (AIC) in most cases for trust strangely. The likelihood for this reversal and lack of importance is how most users do not consider these elements or come in contact with them as blatantly as the higher ranked elements on this list according to my papers.

Based on the synthesis of these variables and rankings, we are able to translate their values into an algorithm to calculate a Trust Coefficient.

$$(f + s + t + p + a)/7.0 = t_e \tag{1}$$

With t_e being the Trust Coefficient. Using this example for a mock new site we can display the effectiveness of this coefficient, as shown in Figure 2.

Element	Range of Points	Calculated by	Variable
Familiarity	0-2	User testing, Model Analysis	f
System Type	0-1.5	Entertainment, Public Forum: Full 1.5 News, Banking: ~1.0 Rights Management: ~0.7	s
Technology	0-1.3	Ranking the speed and efficiency against competitor software	t
People Based	0-1.3	User testing, without user testing direct developer chat would provide full 1.3 with all values being respective to that level of communication.	p
AIC Triad	0-0.9	Choose your model for determining your CIA (in this case AIC) stance. Examples: NIST, ISO, PCI, etc.	a

Figure 1: Coefficient Table

Familiarity Testing results in: 1.7 System Type puts it at around: 1.0 Technology is updated but not cutting edge: 1.1 People Based is a bit lacking with only a support ticket: 0.8 AIC Triad model based on NIST RMF puts it at: 0.8
Sum: 1.7 + 1.0 + 1.1 + 0.8 + 0.8 = 5.4
Coefficient: (5.4 / 7.0) = 0.77 Ranking of C+ on Trust Scale

Figure 2: Example of Coefficient Use Case

7 Discussion

This trust coefficient should provide an easy means of determining a companies current trust capabilities with its users. This format was chosen based upon the desire for security and software development employees alike for "quick and easy" metrics. We see this with the wide usage of CVSS in security reports and presentations.

The issue with the usage of coefficients is that they have to simplify an issue to a single number, and it can be hard to determine specific issues present. For example, if they see they have a B from their user trust coefficient it may hide a notable weakness that is compensated by everything else.

For this reason security coefficients and like-minded metrics must be used in conjunction with further breakdowns and analysis. By following the same path performed in this review to develop the algorithm a breakdown may be able to be performed. As such it seems evident that with this new user trust standard there must also come user trust analysis procedures.

8 Conclusions

In this review we developed a user trust coefficient which serves as a new and unique metric for a previously ignored area of user security design, user trust capabilities. The coefficient can be calculated quickly and easily to ensure both security professionals and the average user can understand and gain from its use.

The coefficient was developed based upon 5 common variables of trust and their importance from the review. By reducing the complexity to a single number however, we had a discussion on the future of user trust management. The discussion found that new procedures for analyzing user trust to work alongside the coefficient would help to compensate for the lack of complexity and depth a single metric can provide.

9 Acknowledgment

I thank my project advisors Professor Stacey Watson and the CSEC 599 Class for their support and guidance during the production of this paper. I would like to thank the Rochester Institute of Technology Libraries for their assistance in the Literature Review and Background portion of this paper. Finally I would like to thank my family for their continued support in my academic endeavors.

10 Conflict Of Interest

The author of this review is a member of the information security community and as such has an interest in producing positive results from a security study.

References

[1] Gefen and Straub, "Managing user trust in b2c e-services," *e-Service Journal*, vol. 2, no. 2, p. 7, 2003.

[2] A. Rashidi, "A model for user trust in cloud computing," *International Journal on Cloud Computing: Services and Architecture*, vol. 2, no. 2, p. 1â8, 2012.

[3] T. Zhou, "Understanding usersâ initial trust in mobile banking: An elaboration likelihood perspective," *Computers in Human Behavior*, vol. 28, no. 4, p. 1518â1525, 2012.

[4] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire, "A user trust system for online gamesâpart i: An activity theory approach for trust representation," *IEEE Transactions on Computational Intelligence and AI in Games*, vol. 9, no. 3, p. 305â320, 2017.

[5] K.-P. L. Vu, V. Chambers, B. Creekmur, D. Cho, and R. W. Proctor, "Influence of the privacy birdÂ® user agent on user trust of different web sites," *Computers in Industry*, vol. 61, no. 4, p. 311â317, 2010.

[6] Z. Zhang, "Security, trust and risk in digital rights management ecosystem," *2010 International Conference on High Performance Computing Simulation*, 2010.

[7] J. Xu, K. Le, A. Deitermann, and E. Montague, "How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology," *Applied Ergonomics*, vol. 45, no. 6, p. 1495â1503, 2014.

[8] B. Dietvorst and U. Simonsohn, "Supplemental material for intentionally âbiasedâ: People purposely use to-be-ignored information, but can be persuaded not to," *Journal of Experimental Psychology: General*, 2018.

[9] B. F. Yuksel, P. Collisson, and M. Czerwinski, "Brains or beauty," *ACM Transactions on Internet Technology*, vol. 17, no. 1, p. 1â20, Apr 2017.