Transactions on Replication Research

Conceptual Replication ISSN 2473-3458

Evaluating the Role of Trust in Adoption: A Conceptual Replication in the Context of Open Source Systems

Mario Silic
Institute of Information Management
University of St. Gallen, Switzerland
mario.silic@unisg.ch

Jordan B. Barlow
Information Systems & Decision Sciences
California State University, Fullerton, USA
jobarlow@fullerton.edu

Andrea Back
Institute of Information Management
University of St. Gallen, Switzerland
andrea.back@unisg.ch

Abstract:

This study is a conceptual replication of the Chandra, Srivastava, & Theng (2010) study on the role of trust in adopting a unique type of technology. Whereas Chandra et al. focused on mobile payment systems, we apply their theoretical model to the context of adopting open source software (OSS). Results are largely consistent and comparable with those of the original model; we also found that user trust plays a vital role in OSS adoption intention. However, two of the hypotheses had significantly different results in our model when compared to the original—specifically, perceived reputation did not have a significant impact on trust in the technology, and trust had a more powerful effect on the perceived usefulness of the technology. We argue that users' expectations regarding trust are different depending on the type of technology that a user intends to adopt.

Keywords: Open source software, trust, adoption, TAM

The manuscript was received 10/14/2016 and was with the authors 7 months for 2 revisions.

1 Introduction

The open source software (OSS) movement has resulted in the introduction of several tech industry icons, such as the Apache web server, Linux, and Firefox. A majority of iOS and Android apps are now based on OSS frameworks or libraries, such as jQuery, Ionic, or ImpactJS. On Github, over 14 million people have created over 35 million projects (Github, 2016), with over 80% of developers having used OSS tools as part of their projects.[1]

Two prominent examples are Google and Facebook, which are widely using the open source philosophy not only to enhance their infrastructure, but also to further promote OSS (Arrington, 2006; Developer, 2010). Organizational use of OSS is rising in many areas such as cloud/virtualization, content management, and mobile (Black Duck, 2014). OSS server products and technology account for over 54% (Netcraft, 2014) of all worldwide servers.

Organizations implementing open source software often rely on the contributions of anonymous individuals, or at least individuals from outside their own organization or control, which raises the issue of trust (De Laat, 2010). Consequently, a potential OSS user (in organizational settings, the IT decision maker) has to make an OSS adoption decision based on arguments from both OSS proponents and opponents. However, the OSS evaluation process can be time-consuming and labor-intensive (Tiangco, Stockwell, Sapsford, Rainer,

[1] http://www.zdnet.com/five-out-of-six-developers-now-using-or-deploying-open-source-7000008499/

& Swanton, 2005); thus, many enterprises are not doing thorough cost-benefit analyses (Ven, Verelst, & Mannaert, 2008). OSS has numerous advantages for enterprises, such as lowering expenditure through reduced scaling costs, license fees, hardware needs, etc. (Fitzgerald & Kenny, 2004; Schweik & English, 2012). At the same time, security, reliability, and performance are top technological risks that IT decision makers take into account when considering OSS adoption (Silic & Back, 2015a; Silic & Back, 2015b; Silic & Back, 2017; Silic, Back, & Silic, 2015) where trust can play an important role (Silic & Back, 2013).

For many large OSS projects (e.g., Apache, MySQL, Firefox), there is more visibility when it comes to measuring and tracking these technological risk factors; for many small to medium size OSS projects (e.g., FileZilla, VLC media player, phpMyAdmin), the same cannot be confirmed. For example, in 2012, a security incident affected piwik (a popular open source web analytics application), and malicious code was embedded that affected over 480,000 websites. In 2014, the Heartbleed security bug found in the open-source OpenSSL product affected all major websites, including Google, Facebook, and Yahoo. These incidents led to high media coverage, where OSS products are usually marked as being vulnerable, insecure, and potentially dangerous for enterprises (PC World, 2014; The Register, 2013). Consequently, many enterprises are reluctant to adopt an OSS product because organizational or individual IT decision makers (whom we refer to as potential OSS users in this paper) are unsure if, and to what extent, they can trust OSS.

Past research on OSS adoption has found social identification (Gwebu & Wang, 2011) and organizational-level openness (Marsan, Paré, & Beaudry, 2012) to be important drivers of OSS adoption. Further, Hauge, Sørensen, & Conradi (2008) found that OSS is becoming more integrated in vertical software solutions, which suggests OSS adoption may continue in other sectors.

The objective of this study is to conceptually replicate a study by Chandra et al. (2010) to understand how user trust is affecting the adoption intention of open source software, and what factors influence such trust in OSS. We found the Chandra et al. (2010) model to be particularly interesting and suitable for the OSS context because its core concepts can be easily applied and replicable to the OSS realm. Consequently, the reason for replicating the Chandra et al. (2010) study in the OSS realm is that OSS foundations are similar to m-commerce foundations in that both contexts are dependent on consumer trust to drive the technology adoption. In other words, our goal was to examine the effects of the technology on trust, and the role of trust on adoption, and the model already developed by Chandra et al. (2010) fit well with this goal. Chandra et al. (2010) have developed a clear model of trust and adoption, with strong ties and reference to the trust and adoption literature. Due to these conceptual and foundational similarities, and the strong model already proposed by Chandra et al., we believe that the OSS realm is a good replication candidate of the original Chandra et al. (2010) study, and that a replication of this study would be preferable to “reinventing the wheel” by developing a different model and literature review of trust and adoption.

Before discussing prior research on trust issues with OSS, we note that Chandra et al. (2010) incorporate the technology acceptance model, TAM (Davis, Bagozzi, & Warshaw, 1989) into their research model. Thus, our study not only replicates Chandra et al. (2010), but also provides additional replication value to the original TAM model. Through a number of empirical studies, TAM has been shown to be a parsimonious and robust model of technology acceptance in various international contexts, with a reliable instrument (e.g. Miller & Khera, 2010; Straub, Keil, & Brenner, 1997). Many technology acceptance models are based on TAM, using its basic constructs and adding new ones. For the purposes of parsimony, and to be consistent with other research integrating trust with acceptance constructs (Chandra et al., 2010; Pavlou, 2003) we chose to base our model on TAM and not on other, more complex models.

Among the studies that have considered trust and security issues with OSS, scholars have mostly focused on the IT security-related risks of one single OSS product or just a few OSS products only (Alhazmi, Malaiya, & Ray, 2007; Browne, Arbaugh, McHugh, & Fithen, 2001; Frei, May, Fiedler, & Plattner, 2006; Neuhaus, Zimmermann, Holler, & Zeller, 2007). Most of these studies face generalizability challenges since either they were focusing on a single (specific) OSS product in a particular organization/country (Goode, 2005) or their research setting was public administration (Federspiel & Brincker, 2010) and software companies (Hauge, Ayala, & Conradi, 2010). Interestingly, the majority of past studies focused on trust between OSS team members (De Laat, 2010; Von Krogh, Spaeth, & Lakhani, 2003) or investigated OSS trustworthiness (Del Bianco, Lavazza, Morasca, & Taibi, 2011). However, understanding the relationship between trust in the software itself and OSS adoption intention, particularly from the IT decision maker perspective, has received little attention.

We believe that trust in open source software has not received adequate research focus thus far. To fill this research gap, our study aims to investigate factors that influence user trust and the way trust is related to the adoption intention in the context of OSS.

Chandra et al. (2010) identified two broad dimensions of trust facilitators for mobile payment adoption: technology characteristics and provider characteristics. Specifically, they focused on perceived reputation, perceived opportunism, perceived environmental risk, and perceived structural assurance. As shown in Figure 1, they hypothesized that such factors would affect the way that users put their trust into m-payment systems. They also theorized how such trust in an m-payment system would affect the users' perceptions of usefulness, ease of use, and ultimately intention to adopt such software.

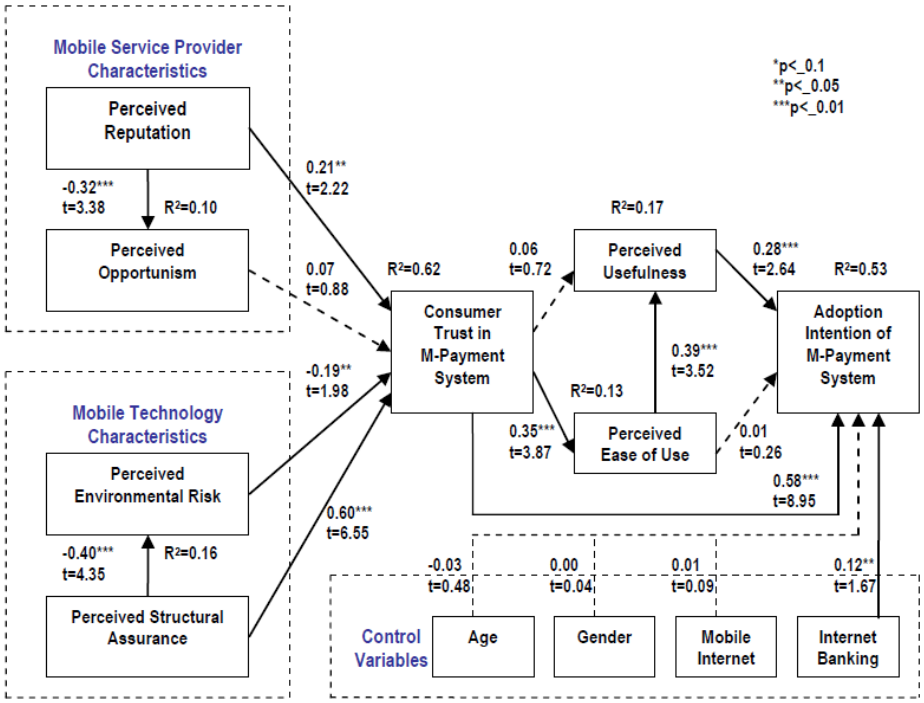

Figure 1. Results from Chandra et al. (2010)

Based on the original study, we apply their theoretical model to the open source software (OSS) context and propose the following hypotheses:

Hypothesis 1: Perceived reputation of OSS will have a positive impact on user trust in OSS.

Hypothesis 2: Perceived opportunism of OSS will have a negative impact on user trust in OSS.

Hypothesis 3: Perceived reputation of OSS is negatively associated with perceived opportunism.

Hypothesis 4: Perceived environmental risk will have a negative impact on user trust in OSS.

Hypothesis 5: Perceived structural assurance will have a positive impact on user trust in OSS.

Hypothesis 6: Perceived structural assurance will have a negative impact on perceived environmental risk in OSS.

Hypothesis 7a: User trust in OSS will have a positive impact on the perceived usefulness of the OSS.

Hypothesis 7b: User trust in OSS will have a positive impact on perceived ease of use of OSS.

Hypothesis 7c: User trust in OSS will have a positive impact on the adoption intention of OSS.

Hypothesis 8a: Perceived ease of use of the OSS will have a positive impact on the perceived usefulness of OSS.

Hypothesis 8b: Perceived ease of use of the OSS will have a positive impact on adoption intention for the OSS.

Hypothesis 8c: Perceived usefulness of the OSS is positively associated with the adoption intention for the OSS.

The replicated research model is shown in Figure 2.

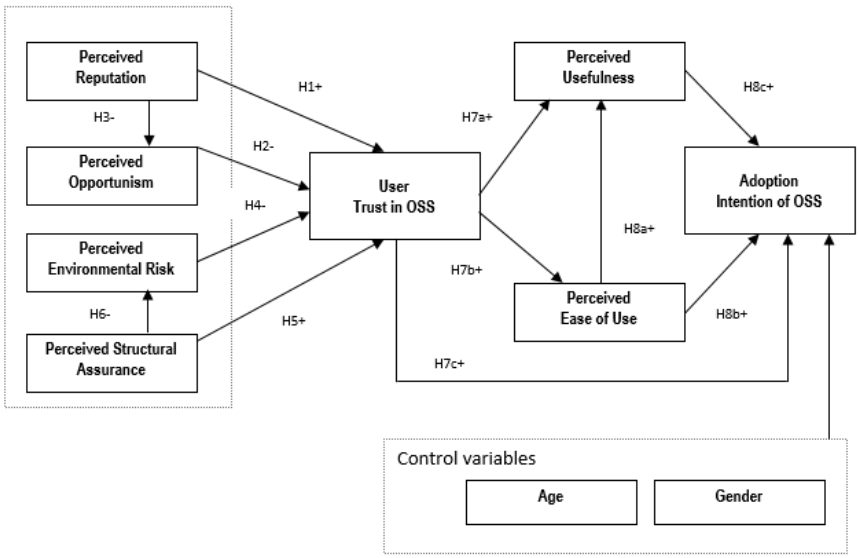

Figure 2. OSS Trust and Adoption Research Model

2 Research Method

2.1 Participants

Like Chandra et al. (2010), we conducted a survey methodology to test our hypotheses. We contacted 450 IT professionals via e-mail with a request to participate in an online survey.[2] Participants were recruited from two main sources: (1) LinkedIn, an online social media site for professional networking, and (2) a database of contacts created from participants of a previous study on OSS who provided their consent to be part of other OSS studies. All contacted participants received an explanation about the study aims explaining that the study is about OSS. We asked them to participate only if they have experience on OSS product implementation. To ensure participants clearly understood, we also provided a short example in the email but also on the survey start page about OSS implementations in organizations.

We received 162 responses from 34 different countries. Of the 162 responses, 10 were removed for validity issues (specifically, the recorded time to complete the survey was less than 5 minutes). We ended with 152 responses as the final sample size, a response rate of 34%. Of the 152 participants, 144 were men (94.8%) and 8 were women (5.2%); the average participant age was 41.5. Interestingly, compared to the original study, we had a much higher proportion of men, which could have some influence on the results. We did not specifically target Chief Information Officers (CIOs) because (1) many of the contacted organizations did not have the CIO function, and (2) we wanted to involve different organizational functions that had to deal with the OSS adoption decision-making process (see Appendix B for full demographics details).

2.2 Measures

To build the survey instrument, we adapted previously validated survey measures from Chandra et al. (2010). Two control variables were also included in our model (gender and age). These controls were also used in the Chandra et al. (2010) study. They used two other controls in their final analysis (experience with Internet banking and mobile Internet usage) which were not relevant to the context of open source systems; thus, we did not include these control variables in our model. Chandra et al. (2010) also collected education levels, but dropped this measure in their final analysis; thus, we chose not to include it in ours. To ensure

[2] The original study used data from 109 Singapore residents who also completed a survey. It is unclear how the participants were specifically recruited.

quality and avoid any misunderstandings of the survey measures, we conducted a pilot study with five information professionals. Based on their input, we made minor adjustments (specifically, we slightly modified perceived reputation to make it more understandable for participants).

2.3 Procedures

All contacted information professionals held IT-related positions (chief information security officers, programmers, security engineers, etc.) and consequently, should have had good foundational knowledge to understand challenges related to trust and open source technology. By surveying a variety of respondents from different positions, organizations, and countries, we aimed to collect a wide variety of views from information professionals that are responsible for various tasks in the entire OSS adoption procedure. We did not focus on a single OSS product or project; rather, we instructed participants to think of different OSS that they implemented within their organization and to answer the survey items (Appendix A) based on their experience with that OSS.

3 Analysis and Results

3.1 PLS Analysis

We employed variance-based structural equation modeling (SEM) techniques (Chin, 1998; Chin, Marcolin, & Newsted, 2003) to analyze the survey data. WarpPLS 3.0 (Kock, 2012) is a powerful PLS-based structural equation modeling (SEM) software, having the capability to test both linear and non-linear relationships. Furthermore, co-variance-based SEM requires a larger sample size, whereas PLS can produce stable path coefficients and significant p-values with lower sample sizes (Kock, 2012). PLS was also used to test the model in the Chandra et al. (2010) study.

3.2 Measurement Model and Construct Validity

P-values for both the average path coefficient (APC) and the average r-squared (ARS) should be lower than 0.05 (Kock, 2012). In our model, APC = 0.312 ($p < 0.001$) and ARS = 0.460 ($p < 0.001$). Additionally, the average variance inflation factor (AVIF) should be lower than 5 (Kock, 2012). In our model, AVIF = 1.793. Thus, we have reason to assume that our model has acceptable predictive and explanatory quality.

The composite reliabilities (Appendix C, Table C.1) of the different measures range from 0.84 to 0.97 (values ranged from 0.946 to 0.995 in the original study), which exceed the recommended threshold value of 0.70 (Chin, 1998). Also, following the recommendation of Fornell and Larcker (1981), the average variance extracted (AVE) (Appendix C, Table C.1) for each variable construct exceeds 0.50.

Next, the AVE of each latent construct should be higher than the construct's highest squared correlation with any other latent construct (Fornell & Larcker, 1981). Based on the discriminant validity test, where the square root of the constructs' AVE is on the diagonal and the correlations between the constructs are in the lower left triangle (Appendix C, Table C.2), we conclude that the model's constructs display appropriate levels of discriminant validity.

Using WarpPLS, we checked loadings and cross loadings for each indicator and construct (Appendix C, Table C.4). The results of this test indicate that all items are more highly loaded on their respective construct than on any other. All but two (PER1 and PER2) of the items' loadings were greater than 0.70 (all significant, $p<0.001$). Thus, these items were not retained and were deleted from the model.

3.3 Common Method Bias

We used two procedures to check for common method variance: Harman's single-factor test (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Podsakoff & Organ, 1986) and the statistical approach developed by Liang, Saraf, Hu, & Xue (2007). The first test showed that the largest factor accounted for 34 percent of the variance indicating that common method bias is most likely not an issue. In the second test, we checked for variances of each observed indicator explained by its substantive construct and the method factor. The average substantively explained variance of the indicators was 0.896, and method factor variance is 0.005, which represents a 179:1 ratio. Also, a large majority of the method factor loadings are not significant, which confirms that common method is not an issue for the study. Both procedures confirmed that common method bias was not a problem. Several additional recommendations from Podsakoff et al. (2003) were followed. Specifically, to reduce the potential for social desirability bias, full anonymity was assured to all

participants, and we included a statement reminding participants that there are no “good” or “bad” answers to the survey. Further, we randomized questions to avoid automatic answering and to minimize pattern detection.

3.4 Structural Model

To assess our hypotheses, we examined the parameters provided by the PLS structural model. We applied the bootstrapping resampling procedure (500 samples) to estimate the significance of paths in our structural model. R^2 values of the dependent variables represent the predictability of the theoretical model and standardized path coefficients indicate the strength of the relationship between the independent and dependent variable (Chin, 1998). To assess our hypotheses, we examined the parameters provided by the PLS structural model.

Results indicate an R^2 value of 0.74, which means that the theoretical model explained a substantial amount of variance in adoption intention. The model also accounts for 66% of the variance for user trust in OSS. Thus, our theoretical model shows substantial explanatory power.

Our structural model results indicate that all of our hypotheses are supported except H1 (perceived reputation did not directly influence user trust; B = 0.15, NS). We do note that several of our hypotheses also have a significance level between 0.05 and 0.1; readers may use caution in interpreting the significance of these findings. Perceived opportunism (B = -0.11, p < 0.1), perceived environmental risk (B = -0.15, p < 0.01) and perceived structural assurance (B = 0.49, p < 0.01) had significant effects on user trust, thereby supporting hypotheses 2, 4 and 5. Perceived reputation had a significant effect on perceived opportunism (B = -0.42, p < 0.1), and perceived structural assurance had a significant effect on perceived environmental risk (B = -0.50, p < 0.1), supporting hypotheses 3 and 6.

In addition, user trust (B = 0.41, p < 0.01), perceived ease of use (B = 0.11, p < 0.1) and perceived usefulness (B = 0.40, p < 0.01) had significant effects on adoption intention. User trust had a significant effect on perceived ease of use (B = 0.51, p < 0.01) and perceived usefulness (B = 0.50, p < 0.01). Perceived ease of use also significantly affected perceived usefulness (B = 0.37, p < 0.01). Thus, hypotheses 7 and 8 were fully supported. The influence of age and gender, the control variables, was not significant. Results are summarized below in Figure 3 and Table 1.

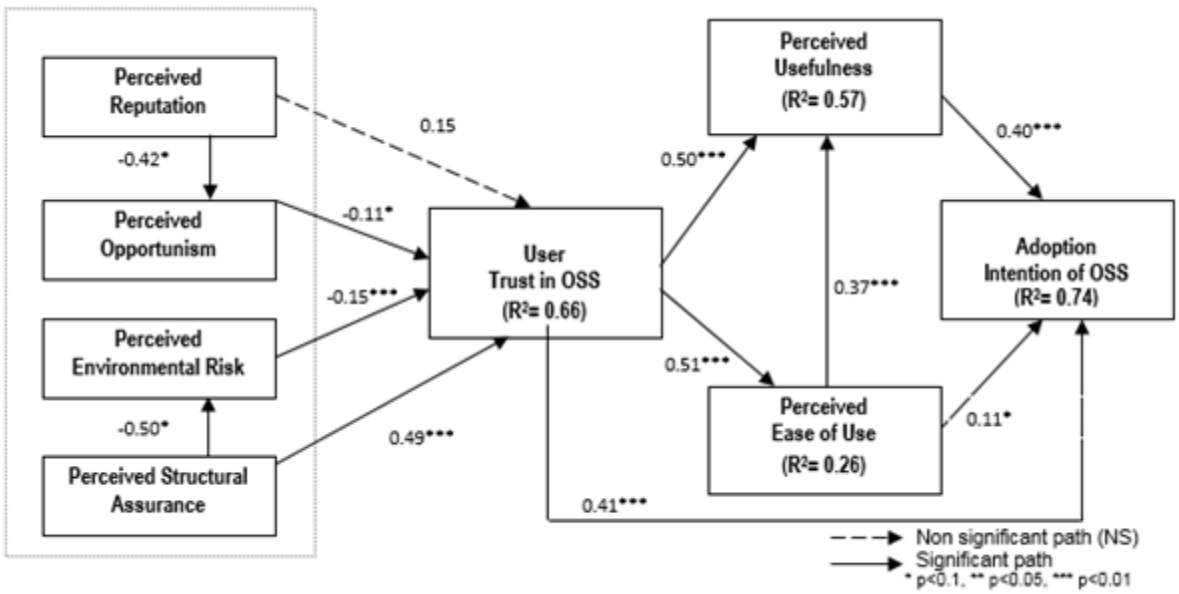

Figure 3. Results

Table 1. Comparison of findings to Chandra et al. (2010)		
Hypothesis	**Supported in Chandra et al.?**	**Supported in current study?**
H1: Perceived reputation → trust	Yes (p<0.05)	No
H2: Perceived opportunism → trust	No	Yes, though weak (p<0.1)
H3: Perceived reputation → perceived opportunism	Yes (p<0.01)	Yes, though weak (p<0.1)
H4: Perceived environmental risk → trust	Yes (p<0.05)	Yes (p<0.01)
H5: Perceived structural assurance → trust	Yes (p<0.01)	Yes (p<0.01)
H6: Perceived structural assurance → perceived env. risk	Yes (p<0.01)	Yes, though weak (p<0.1)
H7a: Trust → perceived usefulness	No	Yes (p<0.01)
H7b: Trust → perceived ease of use	Yes (p<0.01)	Yes (p<0.01)
H7c: Trust → adoption intention	Yes (p<0.01)	Yes (p<0.01)
H8a: Perceived ease of use → perceived usefulness	Yes (p<0.01)	Yes (p<0.01)
H8b: Perceived ease of use → adoption intention	No	Yes, though weak (p<0.1)
H8c: Perceived usefulness → adoption intention	Yes (p<0.01)	Yes (p<0.01)

4 Discussion

4.1 Interpretation of Results

In this study, we conceptually replicated the study of Chandra et al. (2010) that was empirically validated in an m-payment context. Similar to the original model, we found that perceived usefulness has a positive and significant influence on the intention to adopt OSS, but that perceived ease of use was a weak predictor of adoption (in the Chandra et al. study, the relationship was non-significant; in our study, it was significant only at the p<0.1 level). Both studies also show that user trust is an important antecedent to OSS adoption intention. Moreover, trust explains a higher portion of the variance of adoption than it explains of PEU or PU.

Interestingly, the relationship between trust and perceived usefulness was not significant in the Chandra et al. model, but was a significant predictor in our model. This could be explained by the fact that users' expectations are different in the OSS context. As OSS products are generally free of charge, users expect that if they are developed in a trustworthy way by eager volunteers, the software should be useful for the purpose it was designed for. If users do not trust open source software, they may believe that its developers would not successfully create a useful product. For technology in the commercial context, trust in the product does not necessarily change their opinion on how useful the technology will be for them.

Beyond predicting adoption intention, our model also tested several predictors of user trust in OSS. As indicated in past literature (e.g. Pavlou, Huigang, & Yajiong, 2007), our results confirm that perceived structural assurance and perceived environmental risk are important factors negatively influencing user trust when adopting OSS, confirming the same results found in the Chandra et al. (2010) study. The risk behind the use of OSS and the fact that by its nature, OSS source code can be accessed and modified by unknown individuals, decreases user trust, consistent with previous findings on the relationship between risk and trust (Grazioli & Jarvenpaa, 2000; Malhotra, Kim, & Agarwal, 2004; Pavlou, 2003). In addition, structural assurance is negatively associated with environmental risk. In other words, to reduce perceived risk when adopting OSS, it is necessary to implement an adequate structural assurance. This relates to leveraging trust on the institutional level. In the OSS context, it can mean involvement of a well-known organization or institution that would act as a guarantor of trust. Despite the obvious advantages of having a well-known organization acting as trustworthy agent, this can be more difficult to achieve in the OSS context, because OSS is by its definition open and therefore available for modifications by anyone.

Perceived opportunism was not a significant predictor of trust in the m-payment context (Chandra et al., 2010). In our model, there was a weak relationship (significant only at the p<0.1 level). The small difference in the models may be due to a perception that in commercial systems, opportunism will not ultimately affect the product, because those acting opportunistically will be held accountable by the market – that is, if the opportunistic behavior were to affect system functionality, the developers would have more to lose

financially. In the open source context, potential users may be more likely to feel that opportunistic behavior in open source development may affect the product's functionality or security, because developers have nothing to lose, at least financially.

Unlike the above three predictors of trust in OSS, we found that the perceived reputation of OSS is not directly related to users' trust in OSS. This contradicts the findings in the m-payment context (Chandra et al., 2010). The role of "reputation of mobile service provider" was identified as an important antecedent to trust in mobile payment systems, and the reputation of the vendor in the online shopping context was found to be an important factor in initial trust for potential consumers (Jarvenpaa, Tractinsky, & Saarinen, 1999; McKnight, Choudhury, & Kacmar, 2002). Conversely, our results suggest that good reputation does not seem to influence user trust in an open source software context. Past studies have largely confirmed the positive relationship between trust and reputation (e.g., Jarvenpaa, Tractinsky, & Saarinen, 1999; McKnight et al., 2002). However, several other studies have found that reputation does not influence people to have higher trust in a mobile banking system. (Johnson & Grayson, 2005; Kim, Shin, & Lee, 2009). These studies provide an explanation for their contradictory finding by suggesting that once the reputation of the mobile banking firm has reached a certain level, it no longer positively influences trust in the service that is provided. Similarly, we believe that in the OSS context, if the reputation is already achieved and has reached a certain level (e.g., through the OSS community feedback), then reputation will likely have less influence on trust.

Another possible explanation for our result could be that potential users of open source software base their trust decisions on their pre-existing opinions of open source philosophy rather than on reputations of individual developers. That is, potential users may decide to trust (or not trust) in open source software based on the underlying principles of open source development regardless of who the specific software developer is. In other words, users' trust in OSS is based on the industry as a whole rather than on individual developers. A third possible explanation could be that OSS is so widespread in the user's daily software use[3] that reputation is no longer a deciding factor. Past research showed that users with some experience with mobile service providers did not find reputation to be an important factor for initial consumer trust (Chandra et al., 2010). Finally, this finding may also result from the fact that we considered OSS in general, while the original study focused on a single mobile vendor.

4.2 Theoretical Contributions

Our study makes several contributions to the information systems literature. First, in the existing literature, the relationships between adoption intention and user trust and its antecedents have not been adequately addressed in the unique open source context. Because the number of IT projects being developed using the open source model is continually increasing, it is critical to understand the effect of trust in how organizations can implement these technologies. Our research aimed to fill this gap by providing insights on user trust antecedents: perceived reputation, perceived opportunism, perceived environmental risk and perceived structural assurance. These new theoretical insights will help researchers to better understand user trust-related antecedents and their influence on technology adoption in this important context. Our study also confirmed that trust has a stronger influence on adoption of open source software than perceived usefulness or ease of use.

Next, this study provides a valuable conceptual replication of the Chandra et al. (2010) model. The relationships in the original model were further validated empirically, with few exceptions. Trust in OSS was a significant predictor of perceived usefulness of OSS, while trust in m-payment systems was not a significant predictor of perceived usefulness of that type of system. We believe these different results are due to the fact that users often believe software developed by volunteers with no pay are more likely to be useful as long as they were built in a trustworthy way, while trust in commercial software does not guarantee that the software will be useful, since it was primarily created for financial gain. Perceived reputation was not as important in the OSS context as it was in the m-payment context.

Finally, although the technology acceptance model has been studied in hundreds of research studies, the integration of trust into adoption models is relatively less studied. However, past research has demonstrated a strong relationship between trust, perceived usefulness (PU), and perceived ease of use (PEOU) in areas such as e-government services (e.g. Horst, Kuttschreuter, & Gutteling 2007) and e-commerce (Kim, Ferrin, & Rao 2008). In particular, the right side of the model used by Chandra et al. and replicated in this study

[3] E.g., in late 2015, Mozilla Firefox and Google Chrome represented over 60% of all desktop internet users (http://en.wikipedia.org/wiki/Usage_share_of_web_browsers, retrieved September 10, 2015).

(i.e., the relationships between trust, PEOU, PU, and adoption) provides an important addition to the body of replication research validating these relationships in various contexts (Moqbel & Bartelt, 2015; Pavlou, 2003).

Overall, we believe that our study findings are important as we uniquely applied the Chandra et al. model in the specific OSS context and revealed new and different insights on the relationships between antecedents of the initial trust formation and the OSS adoption intentions.

4.3 Practical Implications

Our study has important implications for practitioners. Trust seems to be the key driver facilitating the adoption decision-making process, and should be carefully considered when adopting a new technology, regardless of whether it is open or closed source. The overall acceptability of the OSS technology may rely on trust-related antecedents, and, as such, requires more attention by decision makers.

Further, practitioners should provide thorough testing of the applications and software that are introduced into the organization in an effort to ensure that potential users will find the software trustworthy. Such testing, along with other change management techniques focused on demonstrating low opportunism, low risk, and high structural assurance, should improve the trust users put towards OSS systems.

4.4 Limitations and Future Research

One limitation of this research is that some of the relationships in the model may be bi-directional, and it is hard to test the direction using the survey methodology. For example, we hypothesized and tested that perceived reputation could affect the perceptions of opportunism of OSS. However, the opposite could be argued as well – the perceptions of opportunism will affect the perceived reputation of OSS.

Another limitation to this study is that we do not distinguish between incremental innovation and radical innovation. That is, OSS can be adopted for various reasons, and there may be a difference in adoption intentions between these types of potential adoption. Instead, we only captured high-level perceptions of adopting OSS in any form. Future research should more specifically test the effects of trust on adopting OSS for various types of projects. Finally, in this study we did not control for experience level with OSS; a participant's prior experience with OSS software could potentially influence their responses to the survey.

In addition to future research to address limitations of the current study, there are several other avenues for future research. For example, cultural aspects could be studied by introducing cultural dimension antecedents, as it could be interesting to understand how cultural context influences trust in OSS, and ultimately OSS adoption.

4.5 Conclusion

In summary, our replication of the Chandra et al. (2010) model of trust in adoption decisions provides further validation of their model. We also conclude that trust is a particularly important part of the decision-making process in the unique context of open source software systems.

References

Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers & Security,* 26(3), 219-228.

Arrington. (2006, October 10). *Google "Docs & Spreadsheets" Launches*. Retrieved from http://techcrunch.com/2006/10/10/google-docs-spreadsheets-launches/

Bhimani, A. (1996). Securing the commercial Internet. *Communications of the ACM,* 39(6), 29-35.

Black Duck. (2014). *The Eighth Annual Future of Open Source Survey*. Retrieved from http://www.blackducksoftware.com/future-of-open-source,

Browne, H. K., Arbaugh, W. A., McHugh, J., & Fithen, W. L. (2001). A trend analysis of exploitations. *Proceedings of the IEEE Symposium on Security and Privacy* (2001), 214-229.

Chandra, S., Srivastava, S. C., & Theng, Y.-L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems,* 27, Article 29, 561-588.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research,* 295(2), 295-336.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research,* 14(2), 189-217.

Cockburn, C. & Wilson, T. D. (1996). Business use of the world-wide web. *International Journal of Information Management,* 16(2), 83-102.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science,* 35(8), 982-1003.

De Laat, P. B. (2010). How can contributors to open-source communities be trusted? On the assumption, inference, and substitution of trust. *Ethics and Information Technology,* 12(4), 327-341.

Del Bianco, V., Lavazza, L., Morasca, S., & Taibi, D. (2011). A survey on open source software trustworthiness. *IEEE Software,* 28(5), 67-75.

Developer (2010). *Inside Facebook's Open Source Infrastructure*. Retrieved from http://www.developer.com/open/article.php/3894566/Inside-Facebooks-Open-Source-Infrastructure.htm

Doney, P. M. & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, 61(2), 35-51.

Federspiel, S. B. & Brincker, B. (2010). Software as risk: Introduction of open standards in the danish public sector. *Information Society,* 26(1), 38-47.

Fitzgerald, B. & Kenny, T. (2004). Developing an information systems infrastructure with open source software. *IEEE Software,* 21(1), 50-55.

Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18(1), 39.

Frei, S., May, M., Fiedler, U., & Plattner, B. (2006). Large-scale vulnerability analysis. *Proceedings of the 2006 SIGCOMM Workshop on Large-scale Attack Defense*, 131-138.

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega,* 28(6), 725-737.

Github. (2016). *About Github*. Retrieved April 2016 from https://github.com/about

Goode, S. (2005). Something for nothing: Management rejection of open source software in Australia's top firms. *Information & Management,* 42(5), 669-681.

Grazioli, S. & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man and Cybernetics,* 30(4), 395-410.

Gwebu, K. L. & Wang, J. (2011). Adoption of Open Source Software: The role of social identification. *Decision Support Systems,* 51(1), 220-229.

Hauge, Ø., Ayala, C., & Conradi, R. (2010). Adoption of open source software in software-intensive organizations–A systematic literature review. *Information and Software Technology,* 52(11), 1133-1154.

Hauge, Ø., Sørensen, C.-F., & Conradi, R. (2008). Adoption of open source in the software industry. *Proceedings of the IFIP International Conference on Open Source Systems*, 211-221.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999a). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication,* 5(2), 1-35.

John, G. (1984). An empirical investigation of some antecedents of opportunism in a marketing channel. *Journal of Marketing Research*, 21(3), 278-289.

Johnson, D. & Grayson, K. (2005). Cognitive and affective trust in service relationships. *Journal of Business Research,* 58(4), 500-507.

Kim, G., Shin, B., & Lee, H. G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal,* 19(3), 283-311.

Kock, N. (2012). PLS 3.0 user manual. *Script Warp Systems, Laredo, Texas, USA*, 29-33.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly,* 31(1), 59-87.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research,* 15(4), 336-355.

Marsan, J., Paré, G., & Beaudry, A. (2012). Adoption of open source software in organizations: A socio-cognitive perspective. *The Journal of Strategic Information Systems,* 21(4), 257-273.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2000). Trust in e-commerce vendors: A two-stage model. *Proceedings of the Twenty First International Conference on Information Systems*, 532-536.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research,* 13(3), 334-359.

Miller, J. & Khera, O. (2010). Digital library adoption and the technology acceptance model: A cross-country analysis. *The Electronic Journal of Information Systems in Developing Countries,* 40(6), 1-19.

Moqbel, M. & Bartelt, V. L. (2015). Consumer acceptance of personal cloud: Integrating trust and risk with the technology acceptance model. *AIS Transactions on Replication Research,* 1, Article 5.

Netcraft. (2014). Web server survey. Retrieved January 2015, from http://news.netcraft.com/archives/2013/08/09/august-2013-web-server-survey.html

Neuhaus, S., Zimmermann, T., Holler, C., & Zeller, A. (2007). Predicting vulnerable software components. *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 529-540.

Pavlou. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce,* 7(3), 101-134.

Pavlou, Huigang, & Yajiong. (2007). Understanding and mitigating uncertainty in online environments: A principal-agent perspective. *MIS Quarterly,* 31(1), 105-136.

PC World. (2014). Is open source to blame for the Heartbleed bug? Retrieved from http://www.pcworld.com/article/2141740/is-open-source-to-blame-for-the-heartbleed-bug.html

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology,* 88(5), 879-903.

Podsakoff, P. M. & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management,* 12(4), 531-544.

Schweik, C. M. & English, R. C. (2012). *Internet Success: A Study of Open-source Software Commons*: MIT Press.

Silic, M. & Back, A. (2013). Information security and open source dual use security software: Trust paradox. Paper presented at the IFIP International Conference on Open Source Systems, 194-206.

Silic, M. & Back, A. (2015a). Identification and importance of the technological risks of open source software in the enterprise adoption context. Paper presented at the 12th International Conference on Wirtschaftsinformatik, Osnabrück, Germany, 1163-1176.

Silic, M. & Back, A. (2015b). The Influence of risk factors in decision-making process for open source software adoption. *International Journal of Information Technology & Decision Making*, 15(1), 151-185.

Silic, M. & Back, A. (2017). Open source software adoption: Lessons from Linux in Munich. *IT Professional,* 19(1), 42-47.

Silic, M., Back, A., & Silic, D. (2015). Taxonomy of technological risks of open source software in the enterprise adoption context. *Information and Computer Security,* 23(5), 570-583.

Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management,* 33(1), 1-11.

Sweeney, J. C., Soutar, G. N., & Johnson, L. W. (1999). The role of perceived risk in the quality-value relationship: A study in a retail environment. *Journal of Retailing,* 75(1), 77-105.

The Register. (2013, January 10). Ruby off the rails: Enormo security hole puts 240k sites at risk. Retrieved from http://www.theregister.co.uk/2013/01/10/ruby_on_rails_security_vuln/

Tiangco, F., Stockwell, A., Sapsford, J., Rainer, A., & Swanton, E. (2005). Open-source software in an occupational health application: The case of Heales Medical Ltd*. Proceedings of the First International Conference on Open Source Systems*, 130-134.

Ven, K., Verelst, J., & Mannaert, H. (2008). Should you adopt open source software? *IEEE Software,* 25(3), 54-59.

Venkatesh, V. & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science,* 46(2), 186-204.

Von Krogh, G., Spaeth, S., & Lakhani, K. R. (2003). Community, joining, and specialization in open source software innovation: A case study. *Research Policy,* 32(7), 1217-1241.

Appendix A: Survey Items

Table A1. Survey Items

Construct	Items	Source
Perceived Reputation	I believe Open Source Software has a good reputation. I believe Open Source Software has a reputation for being fair. I believe Open Source Software has a reputation for being honest (in its intentions).	(Doney & Cannon, 1997; Jarvenpaa, Tractinsky, & Saarinen, 1999)
Perceived Opportunism	I believe that Open Source Software may use customer information without permission. I believe that Open Source Software might alter information in its own self interest. I believe that Open Source Software may promise things without actually doing them.	(John, 1984)
Perceived Environmental Risk	Information about my Open Source Software activities would be known to others. I believe Open Source Software source code may be modified or deleted by others. I believe there is a high probability of losing a great deal in using Open Source Software. I would label adopting Open Source Software as a potential loss. I believe that overall riskiness of Open Source Software is high.	(Bhimani, 1996; Cockburn & Wilson, 1996; Sweeney, Soutar, & Johnson, 1999)
Perceived Structural Assurance	I believe Open Source Software has enough safeguards to make me feel comfortable using it for penetration testing activities. I feel assured that legal and technological structures adequately protect me from problems on the Open Source Software. I feel confident that encryption and other technological safeguards make it safe for me to use Open Source Software. In general, Open Source Software provides robust and safe environment to perform Security Testing.	(McKnight, Choudhury, & Kacmar, 2000)
Trust	I trust Open Source Software to be reliable. I trust Open Source Software to be secure. I believe Open Source Software is trustworthy. I trust Open Source Software. Even if Open Source Software is not monitored, I'd trust it to do the job correctly.	(Gefen, 2000; Jarvenpaa et al., 1999)
Perceived Usefulness	Using Open Source Software would enable me to accomplish tasks quickly. Using Open Source Software would improve my performance in performing tasks. Using Open Source Software would enhance my effectiveness in performing tasks. Using Open Source Software would make it easier for me to manage and perform tasks. Overall, I find that Open Source Software is useful for performing tasks.	(Davis, 1989)
Perceived Ease of Use	Learning to use Open Source Software would be easy for me. It would be easy to get Open Source Software to do what I want it to do. My interaction with Open Source Software would be clear and understandable. It would be easy for me to become skillful at using Open Source Software. Overall, I would find Open Source Software to be easy to use.	(Davis, 1989)
Adoption Intention	Given a chance, I intend to adopt Open Source Software in the future. Given a chance, I predict that I will frequently use Open Source Software in the future. I will strongly recommend others to use Open Source Software.	(Davis, 1989; Davis, Bagozzi, & Warshaw, 1989; Venkatesh & Davis, 2000)

Appendix B: Demographics

Table B1. Summary of Respondents by Country

Country	n	Country	n	Country	n	Country	n	Country	n
Australia	3	Finland	2	Italy	4	Portugal	1	Switzerland	2
Belgium	3	France	7	Jordan	1	Romania	1	Taiwan	1
Brazil	8	Germany	1	Mexico	1	Russian Federation	2	Turkey	1
Canada	10	Greece	3	Netherlands	5	Singapore	2	Ukraine	3
Chile	2	India	6	Norway	1	South Africa	3	United Kingdom	8
Croatia	3	Indonesia	1	Pakistan	2	Spain	4	United States	52
Denmark	2	Israel	2	Poland	3	Sweden	2		

Table B2. Summary of Respondents by Age and Gender

Age	n	%		Gender	n	%
< 30	10	6.58%		Male	144	94.8%
30-40	66	43.42%		Female	8	5.2%
41-50	50	32.89%				
> 50	26	17.11%				

Table B3. Summary of Respondents by Industry

Industry	n	%	Industry	n	%
Consulting	43	28.29%	Military and Protective	3	1.97%
Engineering	10	6.58%	IT Support (Call Center)	3	1.97%
Entrepreneurship	4	2.63%	Other*	28	18.42%
Information Technology	61	40.13%	*17 different industries represented		

Table B4. Summary of Respondents by Organizational Position

Industry	n	%	Industry	n	%
CxO	23	15.13%	Security Professional	73	48.03%
Director	13	8.55%	Senior Manager	5	3.29%
Information Security Manager	18	11.84%	Other*	17	11.18%
Project Manager	3	1.97%	*16 different positions represented		

Table B5. Summary of Respondents by Work Experience and Organization Size

Years of experience	n	%		Organization size	n	%
< 1 year	23	14.94%		Large: over 250 employees	83	53.90%
1-3 years	45	29.22%		Medium: 50-250 employees	24	15.58%
3-8 years	27	17.53%		Small: less than 50 employees	47	30.52%
> 8 years	59	38.31%				

Appendix C: Model and Construct Validity Results

Table C1. Assessment of the Measurement Model		
Variable constructs	**AVE**	**Composite Reliability**
Perceived Reputation (PR)	0.836	0.939
Perceived Opportunism (PO)	0.754	0.902
Perceived Environmental Risk (PER)	0.756	0.902
Perceived Structural Assurance (PSA)	0.762	0.928
Trust (TR)	0.796	0.951
Perceived Usefulness (PU)	0.832	0.961
Perceived Ease of Use (PEU)	0.844	0.964
Adoption Intention (AI)	0.900	0.964

Table C2. Discriminant Validity (Intercorrelations) of Constructs								
	PR	**PO**	**PER**	**PSA**	**TR**	**PU**	**PEU**	**AI**
PR	**0.914**							
PO	-0.356	**0.868**						
PER	-0.520	0.589	**0.869**					
PSA	0.622	-0.471	-0.470	**0.873**				
TR	0.593	-0.561	-0.616	0.744	**0.892**			
PU	0.575	-0.425	-0.570	0.549	0.705	**0.912**		
PEU	0.448	-0.384	-0.460	0.453	0.546	0.640	**0.919**	
AI	0.630	-0.510	-0.605	0.639	0.776	0.805	0.633	**0.949**

Table C3. Full Collinearity VIFs							
PR	**PO**	**PER**	**PSA**	**TR**	**PU**	**PEU**	**AI**
2.037	1.766	2.147	2.603	3.889	3.304	1.837	4.288

Table C4. Factor Loadings and Cross Loadings								
PR1	**0.905**	0.058	0	-0.047	0.021	0.035	0.02	0.119
PR2	**0.904**	-0.056	0.11	-0.009	0.072	-0.03	-0.003	-0.103
PR3	**0.934**	-0.001	-0.107	0.054	-0.09	-0.005	-0.017	-0.016
PO1	0.091	**0.885**	-0.037	-0.115	0.295	-0.161	0.103	-0.066
PO2	-0.035	**0.898**	0.074	-0.095	0.068	0.048	0.082	-0.01
PO3	-0.06	**0.82**	-0.042	0.229	-0.393	0.122	-0.201	0.082
PER3	0.016	-0.199	**0.821**	0.01	-0.055	-0.203	0.13	0.146
PER4	-0.017	0.076	**0.905**	-0.066	0.06	0.141	-0.061	-0.095
PER5	0.003	0.108	**0.88**	0.059	-0.01	0.045	-0.059	-0.039
PSA1	0.038	0.114	-0.114	**0.883**	-0.074	-0.003	-0.067	0.017
PSA2	-0.059	-0.069	0.216	**0.852**	0.157	0.004	0.204	-0.189
PSA3	-0.124	0.039	-0.029	**0.887**	0.036	-0.108	-0.09	0.167
PSA4	0.145	-0.088	-0.067	**0.869**	-0.115	0.11	-0.041	-0.003

Table C4. Factor Loadings and Cross Loadings								
TR1	0.038	0.115	-0.044	0.05	**0.933**	0.053	0.084	-0.009
TR2	-0.107	-0.089	0.052	0.21	**0.915**	-0.046	-0.02	-0.056
TR3	-0.028	0.03	-0.128	0.031	**0.953**	-0.021	0.011	-0.003
TR4	-0.003	-0.054	-0.005	0.056	**0.916**	-0.018	0.038	-0.002
TR5	0.126	-0.007	0.165	-0.441	**0.725**	0.039	-0.145	0.088
PU1	-0.051	0.002	-0.066	0.049	-0.051	**0.874**	0.039	0.116
PU2	0.036	0.007	0.067	-0.018	-0.01	**0.955**	-0.005	-0.028
PU3	-0.022	-0.011	-0.009	-0.029	-0.088	**0.892**	-0.063	0.002
PU4	0.05	-0.03	0.065	-0.117	0.031	**0.939**	0.005	-0.116
PU5	-0.019	0.032	-0.065	0.122	0.116	**0.898**	0.024	0.036
PEU1	0.074	-0.035	0.053	0.059	-0.114	0.111	**0.903**	-0.115
PEU2	0.016	-0.165	0.089	0.147	-0.136	0.167	**0.907**	-0.222
PEU3	-0.083	0.022	-0.13	-0.032	0.097	-0.03	**0.911**	0.065
PEU4	0.009	0.043	-0.003	-0.063	0.007	-0.132	**0.941**	0.085
PEU5	-0.015	0.13	-0.008	-0.106	0.141	-0.107	**0.932**	0.178
AI1	-0.059	0.035	-0.026	0.044	-0.083	0.015	-0.018	**0.926**
AI2	0.014	-0.032	0.038	-0.012	0.017	0.073	0.022	**0.968**
AI3	0.043	-0.001	-0.013	-0.031	0.063	-0.089	-0.005	**0.951**

About the Authors

Mario Silic is a post-doctoral researcher at the Institute of Information Management, University of St. Gallen, Switzerland. He holds a Ph.D. from University of St Gallen, Switzerland. His research motivation focuses on the fields of information security, open source software, human-computer interaction and mobile. He has published research in *Information & Management, Computers & Security, Information Management & Computer Security, International Journal of Information Technology & Decision Making, Records Management Journal, Journal of Global Information Management,* and others.

Jordan B. Barlow is an assistant professor in the department of Information Systems & Decision Sciences at California State University, Fullerton. His research centers on issues of virtual collaboration, communication, collective intelligence, and information security. His research has appeared in *MIS Quarterly, Journal of Management Information Systems, Journal of the Association for Information Systems*, *Information & Management*, *Communications of the Association for Information Systems*, and others.

Andrea Back is full professor at the Institute of Information Management, University of St. Gallen, Switzerland. As academic director she leads the research centers Learning Center, CC Mobile Business, and Competence Network Business 2.0 Her scientific work in academia and practice covers IT-innovation driven issues in the fields of Corporate Learning, Enterprise 2.0 & Knowledge Management, and Mobile Business. She teaches courses in Business Innovation, in Bachelor, Masters, and Ph.D. programs. She has published numerous research articles, and is author, co-author, and editor of more than 10 books.