Identifying prototypical trust signals in open-source software libraries: A think aloud study

Rob Huw Peace
rhp34@bath.ac.uk

Dr. Laura G.E. Smith
L.G.E.Smith@bath.ac.uk

Prof. Adam Joinson
A.Joinson@bath.ac.uk

UNIVERSITY OF BATH

Introduction

Open-source software (OSS) libraries are websites or platforms where users can openly reuse, modify and publish code and software packages (Wu & Lin, 2001).

However, the open nature of the libraries leave them vulnerable to malignant actors through the uploading of malicious code or packages (Millar, 2017).

This highlights the risk that users face when choosing whether to trust whether or not to download or reuse OSS code/packages.

Therefore, identifying users' perceptions of trust signals within OSS libraries may potentially help to mitigate the aforementioned risk through informing users, websites or policy of the types of signals users perceive to be trustworthy.

Objective

Identify the users' perceptions of trust signals in open-source software libraries

Methodology

A think aloud methodology (Zhang & Zhang, 2019) was employed to identify users' perceptions of trust signals within OSS libraries that users perceive to be trustworthy.

10 participants with experience of using R were recruited through a mixture of opportunity and volunteer sampling.

20 minute interviews were held whilst participants interacted with the Comprehensive R archive network (CRAN) (Hornik, 2012).

A thematic analysis was then applied to the collected data to interpret themes of trust signals (Braun & Clarke, 2012).

Results: Themes interpreted from the data

"Everything in one place links that are clear and lead you on to other sources and sort of gives me an overall trust in in a package that I could use it that I can trust" **Participant 10**

Processing fluency (Landwehr & Eckmann, 2020) is a cognitive process that may influence an individual's evaluation of information depending on how easy the information is to process.

"This looks quite good (the README file). There is plenty of information and it's quite clear you're more likely to trust it then" **Participant 1**

This was reflected in the interviews through increased perceptions of trust for easier to process information. For instance, complexity of README files, the way the package details are formatted and the website layout all appeared to effect participants' perceptions of trust with less complex information signalling greater trust.

"So anything (GitHub account) with a minimum of five followers will make me trust it more" **Participant 8**

"There's so many great forums where people will say use this package for that and here's how they work and stuff. I tend to find their better than going into the documentation on here" **Participant 6**

Social proof (Roethke, Klumpe, Adam, & Benlian, 2020) Suggests that individuals may be influenced to assume the actions of others in an attempt to identify the correct Behaviour.

"This doesn't have any weird dependencies in there which makes me trust it more" **Participant 5**

Examples of participants' perceptions of social proof trust Indicators included the amount of followers on GitHub, comments on forums about packages and ratings systems for code. These examples highlight how other users' behaviour influenced the participants' perceptions of trustworthiness about OSS packages.

"So I guess this email address. It's coming from an American university, so I guess that's a little bit more credible" **Participant 9**

Institutional trust (Maduku, 2016) is a relationship between a trustor and an organisation in which the trustor's belief about the assurances of an organisation mitigate the vulnerability of the perceived risk.

"But you feel like it would be trustworthy given that it is from an actual university, so they wouldn't post something dodgy out there" **Participant 4**

Examples of participants' perceived institutional trust identifiers within the data include university email addresses, academic papers, and Orcid symbols. These trust signals appear to increase participants' trust in academia as an institution.

Expectancy violation theory (Bevan, Ang, & Fearns, 2014) is a theory that explains how users perceive and understand violations to social norms and expectations.

"I'd click on the link cause it's kind of fitting with my perception of how it should look" **Participant 9**

Several instances highlighted how participants' expectations within CRAN affected their perceptions of trustworthiness. For example, logical dependencies within packages, previous experience in OSS libraries, and descriptive names for packages signalled how a participant's expectancies may signify perceptions of trustworthiness if the expectancies are not violated.

Discussion

Processing fluency signals emphasised a lesser amount of complexity increasing the perceptions of trust. However, this may be because of the perceived increase in website design to help accessibility and understanding.

Institutional trust was highlighted through university trust identifiers. However, as the participants were PhD students social identity theory may have also contributed to the trusting of academia through ingroup bias.

Social proof highlights an important social factor to perceptions of trust in OSS libraries.

Expectancy violation theory stresses how a user's expectations may positively or negatively affect perceptions of trust.

Security ramifications for users, platforms and policy.

Further research

The role of distrust in OSS libraries

Understanding the complexity of digital trust

References

Bevan, J. L., Ang, P.-C., & Fearns, J. B. (2014). Being unfriended on Facebook: An application of expectancy violation theory. *Computers in Human Behavior, 33*, 171-178.

Hornik, K. (2012). The comprehensive R archive network. *Wiley interdisciplinary reviews: Computational statistics, 4*(4), 394-398.

Maduku, D. K. (2016). The effect of institutional trust on internet banking acceptance: Perspectives of South African banking retail customers. *South African Journal of Economic and Management Sciences, 19*(4), 533-548.

Millar, S. (2017). Vulnerability Detection in Open Source Software: The Cure and the Cause. Roethke, K., Klumpe, J., Adam, M., & Benlian, A. (2020). Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations. *Decision Support Systems, 131*, 113268.

Wu, M.-W., & Lin, Y.-D. (2001). Open source software development: an overview. *Computer, 34*(6), 33-38.

Braun, V., & Clarke, V. (2012). Thematic analysis.

Landwehr, J. R., & Eckmann, L. (2020). The nature of processing fluency: Amplification versus hedonic marking. *Journal of Experimental Social Psychology, 90*, 103997.

Zhang, L. J., & Zhang, D. (2019). Think-aloud protocols. In *The Routledge handbook of research methods in applied linguistics* (pp. 302-311): Routledge.